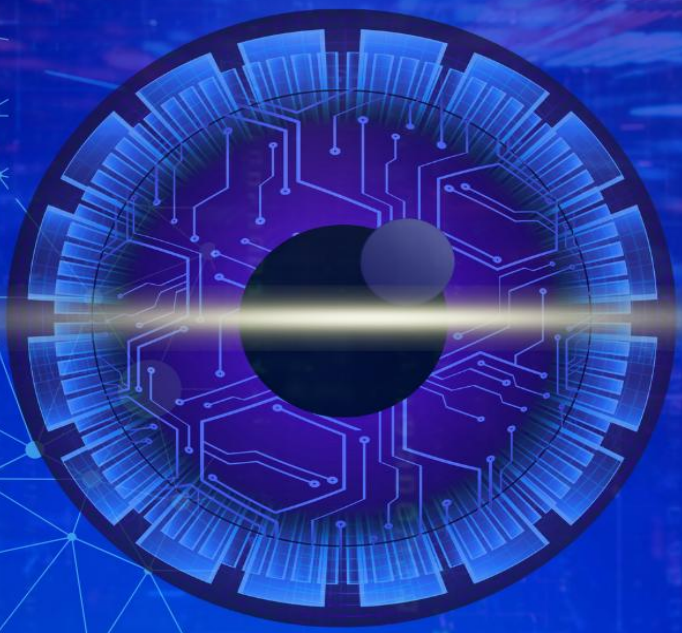
แนวปฏิบัติการใช้ซีโร่ทรัสต์
Zero Trust Guidelines



สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

คำนำ

การพัฒนา การเปลี่ยนแปลงของระบบเทคโนโลยีสารสนเทศ การเข้าถึงทรัพยากร และภัยคุกคามทางไซเบอร์ในปัจจุบันเป็นไปอย่างรวดเร็วและมีความแตกต่างจากอดีตเป็นอย่างมาก การรักษาความมั่นคงปลอดภัยสารสนเทศแบบดั้งเดิมที่เน้นการป้องกันที่ขอบเขตเครือข่าย (Perimeter-based Security) อาจไม่สามารถปกป้องทรัพยากรขององค์กรได้อย่างมีประสิทธิภาพโดยเฉพาะในระบบเครือข่ายที่มีความซับซ้อน เช่น ระบบเครือข่ายขององค์กรที่มีสาขากระจายทั่วโลก หรือองค์กรที่มีการใช้คลาวด์แบบผสม สมมติฐานที่ว่าผู้ที่อยู่ภายในเครือข่ายมีความน่าเชื่อถือมากกว่าผู้ที่อยู่ภายนอกไม่สามารถใช้ได้อีกต่อไปเนื่องจากพนักงานขององค์กรอาจทำงานจากระยะไกล ใช้อุปกรณ์ส่วนตัว เชื่อมต่อผ่านระบบเครือข่ายสาธารณะ หรืออาจมีผู้ไม่ประสงค์ดีฝังตัวเข้าถึงทรัพยากรขององค์กรจากภายในเครือข่ายขององค์กรเอง

เพื่อรับมือกับความท้าทายดังกล่าวสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) โดยศูนย์วิจัยความมั่นคงปลอดภัยไซเบอร์จึงได้จัดทำแนวปฏิบัติการใช้ซีโร่ทรัสต์ (Zero Trust Guidelines) โดยได้ศึกษา รวบรวมและวิเคราะห์ข้อมูลจากเอกสารมาตรฐานและรายงานเชิงเทคนิคที่เป็นที่ยอมรับและได้รับความเชื่อถือในระดับสากล เช่น NIST Special Publication 800-207 "Zero Trust Architecture" และ ISO/IEC 27000 Series รวมถึงกฎระเบียบและแนวปฏิบัติภายในประเทศ เพื่อให้ผู้อ่านในกลุ่มต่าง ๆ ตั้งแต่ผู้บริหาร ผู้กำหนดนโยบาย กลุ่มผู้ปฏิบัติงานด้านเทคนิค ผู้ดูแลระบบ วิศวกรความมั่นคงปลอดภัย จนถึงผู้ที่สนใจที่อาจยังไม่มีความรู้เกี่ยวกับ Zero Trust มาก่อนได้ทราบถึงที่มาและความสำคัญ หลักการสำคัญของ Zero Trust และการนำ Zero Trust ไปประยุกต์ใช้ โดยเฉพาะองค์กรที่ควรปรับเปลี่ยนกระบวนทัศน์สู่สถาปัตยกรรม Zero Trust ภายใต้หลักการสำคัญคือ "อย่าเชื่อทันที จงตรวจสอบเสมอ" (Never Trust, Always Verify) ที่มุ่งเน้นการตรวจสอบทั้งตัวตน สถานะอุปกรณ์ และบริบทแวดล้อมอย่างเข้มงวดในทุกคำขอเข้าถึงทรัพยากรแบบรายเซสชัน เพื่อลดความเสี่ยงจากการถูกโจมตีและสร้างความยืดหยุ่นทางไซเบอร์ ช่วยยกระดับการรักษาความมั่นคงปลอดภัยขององค์กรและประเทศ นำไปสู่การขับเคลื่อนประเทศสู่อนาคตดิจิทัลที่มั่นคงปลอดภัยและยั่งยืนต่อไป

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

กิตติกรรมประกาศ

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติขอขอบคุณผู้ทรงคุณวุฒิจากหลายภาคส่วน ทั้งผู้ทรงคุณวุฒิจากภาครัฐ ภาคเอกชน ภาควิชาการ ภาคประชาสังคม ทั้งที่เอ่ยนามและมิได้เอ่ยนามในที่นี้ ที่ได้สละเวลา ความรู้ และความสามารถ รวมทั้งอนุเคราะห์ข้อมูลและข้อเสนอแนะที่เป็นประโยชน์ต่อการจัดทำ “แนวปฏิบัติการใช้ซีโร่ทรัสต์ (Zero Trust Guidelines)” ฉบับนี้จนสำเร็จ

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติขอขอบคุณคณะทำงานจัดทำแนวปฏิบัติการใช้ซีโร่ทรัสต์ ดังต่อไปนี้

ดร.ชาลี วรกุลพิพัฒน์	คณะทำงาน
ผู้ช่วยศาสตราจารย์ ดร.ทรงพล ตีระกนก	คณะทำงาน
นางสาวพิกุลทอง แก้วดวงตา	คณะทำงาน
ดร.เมฆินทร์ วรศาสตร์	คณะทำงาน
ดร.รัฐิติ์พงษ์ พุทธเจริญ	คณะทำงาน
ผู้ช่วยศาสตราจารย์ ดร.ศุภกร กังพิศดาร	คณะทำงาน
นายสุทธินันท์ แท่นนิล	คณะทำงาน
รองศาสตราจารย์ ดร.สุรทศ ไตรติลานันท์	คณะทำงาน

ทุกท่านได้ใช้ความรู้ ความสามารถ และประสบการณ์ ในการให้ข้อมูลและข้อเสนอแนะอันเป็นประโยชน์และอันทรงคุณค่า ทั้งในที่ประชุมและผ่านช่องทางออนไลน์ซึ่งเป็นส่วนสำคัญอย่างยิ่งในการพัฒนาแนวปฏิบัติฉบับนี้ให้สำเร็จลุล่วง

สุดท้ายนี้ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติขอขอบคุณหน่วยงานที่ร่วมสนับสนุนการจัดทำแนวปฏิบัติฉบับนี้ โดยได้เสียสละทรัพยากร โดยเฉพาะบุคลากรผู้มีความเชี่ยวชาญมาร่วมจัดทำ ให้ข้อเสนอแนะและปรับปรุงแนวปฏิบัติฉบับนี้ให้มีความครบถ้วน เป็นประโยชน์ และสามารถนำไปใช้งานได้กับองค์กรทั้งภาครัฐและเอกชน เหมาะสมกับบริบทของประเทศไทย

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

หน่วยงานที่ร่วมสนับสนุนการจัดทำแนวปฏิบัติฉบับนี้

รายการบันทึกการปรับปรุงฉบับเอกสาร

ลำดับ	เวอร์ชัน	วันที่	รายละเอียดการแก้ไข	ผู้แก้ไข
๑	v1.0	๓ ก.พ. ๖๙	ฉบับเผยแพร่ร่างแรก	คณะทำงาน

แนะนำเนื้อหาที่ควรอ่านสำหรับแต่ละกลุ่มผู้อ่าน

ระบบรักษาความมั่นคงปลอดภัยแบบ Zero Trust

แนวปฏิบัตินี้จัดทำขึ้นเพื่อรองรับผู้อ่านที่มีระดับความรู้และความต้องการที่แตกต่างกัน โดยแบ่งเป็น ๒ กลุ่มหลัก ดังนี้

๑. ผู้ที่ไม่มีพื้นฐานความรู้หรือต้องการทำความเข้าใจ Zero Trust เบื้องต้น

หากท่านเป็นผู้บริหาร ผู้กำหนดนโยบาย หรือบุคคลที่ต้องการทำความเข้าใจแนวคิด Zero Trust เป็นครั้งแรก แนะนำให้ศึกษาเนื้อหาในลำดับดังต่อไปนี้

บทที่ ๑ บทนำ เพื่อทำความเข้าใจความเป็นมาและความสำคัญ พร้อมทั้งแนะนำวัตถุประสงค์ กลุ่มเป้าหมายและการนำไปใช้ และขอบเขตของเอกสารฉบับนี้

บทที่ ๒ ภาพรวมภัยคุกคาม หลักการพื้นฐาน และกรอบการกำกับดูแล Zero Trust เพื่อทำความเข้าใจ ภัยคุกคามในปัจจุบัน หลักการพื้นฐานและแนวคิด องค์ประกอบพื้นฐาน มาตรฐานและกฎหมายที่เกี่ยวข้อง และการกำกับดูแล Zero Trust

บทที่ ๓ แนวทางการเปลี่ยนผ่าน (Migration) สู่ Zero Trust และการดำเนินงานระบบ Zero Trust เพื่อทราบถึงแนวทางการเปลี่ยนผ่านไปสู่ Zero Trust การวิเคราะห์ช่องว่าง (Gap Analysis) รวมถึงแนวปฏิบัติในการดำเนินงานอย่างเป็นระบบ

บทที่ ๔ สถาปัตยกรรมของ Zero Trust และรูปแบบการใช้งาน เพื่อเข้าใจองค์ประกอบสถาปัตยกรรม แนวทางพัฒนา Zero Trust และทางเลือกในการนำ Zero Trust ไปใช้งาน

๒. กลุ่มผู้ปฏิบัติงานด้านเทคนิค หรือผู้ที่ต้องการนำ Zero Trust ไปใช้งานจริงหากท่านเป็นผู้ดูแลระบบวิศวกรความมั่นคงปลอดภัย หรือผู้รับผิดชอบการนำ Zero Trust ไปปฏิบัติ

แนะนำให้ศึกษาเนื้อหาทั้งหมด โดยเฉพาะบทต่อไปนี้

บทที่ ๕ แนวทางปฏิบัติในการติดตั้งและนำไปใช้งาน (Implementation and Deployment) ระบบ Zero Trust เพื่อเข้าใจขั้นตอนในการติดตั้ง Zero Trust Network Access (ZTNA) และแนวทางปฏิบัติในการติดตั้ง ZTNA ทั้งในรูปแบบภายในองค์กร รูปแบบคลาวด์ และแบบไฮบริด รวมถึงการนำ Zero Trust ไปใช้งานในสภาวะแวดล้อมที่แตกต่างกัน

ภาคผนวก รายการตรวจสอบ แนวทางในการกำหนดขอบเขตของงาน (Terms of Reference) แนวทางปฏิบัติตาม Zero Trust Maturity Model (ZTMM) และอภิธานศัพท์

สารบัญ

บทที่ ๑
บทนำ

๑.๑ ความเป็นมาและความสำคัญของ Zero Trust

ปัญหาของการรักษาความมั่นคงปลอดภัยแบบมีขอบเขต (Perimeter-based Security)

ปัจจุบันการรักษาความมั่นคงปลอดภัยของสินทรัพย์หรือข้อมูลมักอาศัยรูปแบบ "ปราสาทและคูเมือง" (Castle and Moat Model) โดยเปรียบทรัพย์สินมีค่าเป็นปราสาท มีกำแพงและคูเมืองป้องกันการเข้าถึงจากผู้ไม่ประสงค์ดี องค์กรจะสร้างทางเข้าออก เช่น เกตเวย์ พร้อมวางอุปกรณ์เฝ้าระวัง และบังคับทิศทางการสื่อสารให้ผ่านจุดตรวจสอบเหล่านี้เท่านั้น รูปแบบนี้ตั้งอยู่บนความเชื่อว่าเครือข่ายภายในองค์กรปลอดภัยกว่าภายนอก ส่งผลให้การตรวจสอบภายในหละหลวม ซึ่งวิธีนี้มีจุดอ่อนสำคัญหลายประการ

การเคลื่อนตัวในเครือข่ายอย่างไร้อุปสรรค (Unhindered Lateral Movement)

ในเอกสาร NIST SP 800-207 ได้ชี้ให้เห็นถึงช่องโหว่สำคัญของการรักษาความมั่นคงปลอดภัยแบบมีขอบเขต นั่นคือเมื่อผู้ไม่ประสงค์ดีสามารถหลบเลี่ยงการตรวจจับที่ขอบเขตขององค์กรได้แล้ว พวกเขาจะสามารถเคลื่อนย้ายจากอุปกรณ์หนึ่งไปสู่อีกอุปกรณ์หนึ่งได้อย่างอิสระและ "ไร้อุปสรรค" เนื่องจากเครือข่ายภายในไม่มีมาตรการตรวจสอบที่เข้มงวดเพียงพอ ส่งผลให้ผู้โจมตีที่เล็ดลอดเข้าไปจะสามารถโจมตีระบบและอุปกรณ์ได้อย่างอิสระเกินกว่าที่ควรจะเป็น

กรณีศึกษา Colonial Pipeline และช่องโหว่ของระบบเครือข่ายส่วนตัวเสมือน (VPN)

ตัวอย่างที่ชัดเจน คือ กรณี Colonial Pipeline ในปี ๒๐๒๑ ที่ผู้โจมตีสามารถเข้าถึงระบบได้ผ่านระบบเครือข่ายส่วนตัวเสมือน โดยใช้ข้อมูลการยืนยันตัวตน (Credentials) ที่รั่วไหล เมื่อเข้าสู่ระบบได้แล้ว ผู้โจมตีสามารถทำการโจมตีแบบการเคลื่อนตัวในเครือข่าย (Lateral Movement) และเข้าถึงทรัพยากรสำคัญต่าง ๆ ได้โดยไม่มีการตรวจสอบเพิ่มเติม เนื่องจากระบบถือว่าทุกอย่างภายในเครือข่าย "เชื่อถือได้" หาก Colonial Pipeline มีสถาปัตยกรรม Zero Trust การโจมตีครั้งนี้จะยากขึ้นมาก เพราะแม้ผู้โจมตีจะผ่านระบบเครือข่ายส่วนตัวเสมือนได้ พวกเขาจะต้องผ่านการยืนยันตัวตนและการตรวจสอบสิทธิ (Authorization) ในทุกครั้งที่พยายามเข้าถึงทรัพยากรแต่ละส่วน ซึ่งจะจำกัดขอบเขตความเสียหายและช่วยตรวจจับพฤติกรรมผิดปกติได้เร็วขึ้น กรณีนี้แสดงให้เห็นว่าการพึ่งพาระบบเครือข่ายส่วนตัวเสมือน และการรักษาความมั่นคงปลอดภัยแบบมีขอบเขตเพียงอย่างเดียว โดยไม่มีการตรวจสอบภายในที่เข้มงวดนั้นไม่เพียงพอต่อภัยคุกคามสมัยใหม่

ความท้าทายในการกำหนดขอบเขตความมั่นคงปลอดภัยในปัจจุบัน

ในปัจจุบันเครือข่ายและโครงสร้างพื้นฐานทางสารสนเทศขององค์กรซับซ้อนมากขึ้น ระบบประกอบไปด้วยทั้งเครือข่ายภายใน สาขา อุปกรณ์เคลื่อนที่ และบริการคลาวด์ (Cloud-based Software & Storage) การจำกัดการเข้าถึงให้มีเพียงไม่กี่ช่องทางและการสร้างขอบเขตที่ชัดเจนจึงกลายเป็นความท้าทายที่ยากขึ้น

นอกจากนี้เมื่อพิจารณารูปแบบการทำงานที่เปลี่ยนแปลงไป เช่น การทำงานจากที่บ้าน หรือการทำงานจากทุกที่ คำถามสำคัญ คือ เราจะกำหนดขอบเขต (Perimeter) ไว้ที่ใด หากไม่สามารถกำหนดขอบเขตที่ชัดเจนได้ การรักษาความมั่นคงปลอดภัยให้แก่สินทรัพย์ก็เป็นไปไม่ได้ สิ่งนี้เป็นตัวบ่งชี้ว่าวิธีการรักษาความมั่นคงปลอดภัยแบบมีขอบเขตอาจไม่เหมาะสมสำหรับยุคปัจจุบัน

เมื่อวิธีการโจมตีเปลี่ยน วิธีการรับมือย่อมต้องเปลี่ยนตาม

ภัยทางไซเบอร์ในปัจจุบันเปลี่ยนแปลงอย่างรวดเร็ว ผู้โจมตีพัฒนาวิธีการใหม่ ช่องทางการโจมตี และรูปแบบการโจมตี ที่ซับซ้อนมากขึ้น ตัวอย่างเช่น การโจมตีรูปแบบใหม่ (Zero Day Attacks) การโจมตีห่วงโซ่อุปทาน (Supply Chain Attacks) หรือแม้แต่การจ้างวานให้ผู้อื่นทำการโจมตีแทนตน (Attack-as-a-Service) สิ่งที่น่าสนใจ คือ แม้ภัยคุกคามจะซับซ้อนขึ้น แต่หนึ่งในปัจจัยสำคัญที่ทำให้การโจมตีประสบความสำเร็จได้ง่ายกลับเป็นเรื่องพื้นฐาน นั่นคือการละเลยมาตรการรักษาความมั่นคงปลอดภัยพื้นฐาน เช่น การยืนยันตัวตน (Authentication) ที่เข้มแข็งผ่านการยืนยันตัวตนแบบหลายปัจจัย (Multi-Factor Authentication: MFA) หรือการรักษาความมั่นคงปลอดภัยในระดับอุปกรณ์ (Device Security) สถานการณ์เหล่านี้ชี้ให้เห็นว่า องค์กรจำเป็นต้องปรับเปลี่ยนกระบวนการด้านความมั่นคงปลอดภัยให้เท่าทันภัยคุกคามที่มีวิวัฒนาการอย่างต่อเนื่อง

แนะนำแนวคิด Zero Trust “อย่าเชื่อทันที จงตรวจสอบเสมอ (Never Trust, Always Verify)”

จากข้อมูลทั้งหมดข้างต้นจึงเป็นที่มาของหลักการ Zero Trust ซึ่งเป็นกระบวนการใหม่ด้านความมั่นคงปลอดภัยที่เน้นว่า "อย่าเชื่อทันที จงตรวจสอบเสมอ" หลักการนี้หมายความว่า ไม่ว่าผู้ใช้หรืออุปกรณ์จะอยู่ภายในหรือภายนอกเครือข่ายองค์กรทุกคำขอเข้าถึงทรัพยากรต้องผ่านการตรวจสอบและยืนยันตัวตนอย่างเข้มงวดทุกครั้ง เพื่อสร้างความมั่นใจว่าทุกการเข้าถึงมีขอบเขตที่จำกัดและมีความมั่นคงปลอดภัย ซึ่งจะช่วยลดความเสี่ยงจากการโจมตีแบบการเคลื่อนตัวในเครือข่าย ข้อสำคัญคือ Zero Trust ไม่ใช่ผลิตภัณฑ์เดียว แต่เป็นสถาปัตยกรรม และกรอบการทำงาน ที่ประกอบด้วยหลักการ กระบวนการ และเทคโนโลยีต่าง ๆ ที่ทำงานร่วมกัน

๑.๒ วัตถุประสงค์ของแนวปฏิบัติ

แนวปฏิบัตินี้จัดทำขึ้นเพื่อช่วยให้องค์กรต่าง ๆ สามารถเข้าใจและนำสถาปัตยกรรม Zero Trust (Zero Trust Architecture: ZTA) ไปประยุกต์ใช้ได้อย่างมีประสิทธิภาพ โดยมีวัตถุประสงค์หลักดังนี้

๑) เพื่อเป็นแนวทางเบื้องต้นสำหรับองค์กรในการเริ่มต้นนำ Zero Trust มาใช้งานแม้ไม่มีความรู้เชิงลึกมาก่อน

๒) เพื่อสร้างความเข้าใจพื้นฐานเกี่ยวกับหลักการ แนวคิด และองค์ประกอบสำคัญของ Zero Trust ที่สามารถนำไปปรับใช้ได้จริง

๓) เพื่อช่วยให้องค์กรสามารถประเมินสถานะความพร้อมปัจจุบัน วางแผน และกำหนดทิศทางในการพัฒนาระบบรักษาความมั่นคงปลอดภัยไปสู่ Zero Trust อย่างเป็นขั้นตอน

๔) เพื่อให้องค์กรสามารถนำแนวทางไปปรับใช้ตามบริบท ขนาด และความพร้อมของตนเอง โดยไม่จำเป็นต้องดำเนินการทั้งหมดพร้อมกัน

๕) เพื่อเป็นแนวทางในการจัดทำข้อกำหนดและเอกสารประกวดราคา ที่มีการระบุความต้องการด้าน Zero Trust อย่างชัดเจน เพื่อให้การจัดซื้อจัดจ้างสอดคล้องกับหลักการ Zero Trust

๑.๓ กลุ่มเป้าหมายและการนำไปใช้

แนวปฏิบัตินี้เหมาะสำหรับบุคคลและองค์กรที่หลากหลาย ได้แก่

๑) องค์กรในทุกภาคส่วน ทั้งภาครัฐและเอกชน โดยเฉพาะองค์กรที่มีข้อมูลสำคัญและต้องการเสริมสร้างความมั่นคงปลอดภัยไซเบอร์

๒) ผู้บริหารระดับสูง (C-Level Executives) และผู้กำหนดนโยบายด้านความมั่นคงปลอดภัยสารสนเทศ ที่ต้องการทำความเข้าใจภาพรวมและประโยชน์ของ Zero Trust

๓) ผู้จัดการและหัวหน้าทีมไอทีหรือทีมรักษาความมั่นคงปลอดภัย ที่รับผิดชอบการวางแผนและกำกับดูแลการนำ Zero Trust ไปใช้

๔) ผู้ปฏิบัติงานด้านเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยไซเบอร์ ที่ต้องการความรู้เชิงปฏิบัติในการออกแบบและติดตั้งระบบ

๕) องค์กรที่ต้องการปรับปรุงระบบรักษาความมั่นคงปลอดภัยให้ทันสมัย รองรับรูปแบบการทำงานที่เปลี่ยนไปและมีประสิทธิภาพมากขึ้น

๖) องค์กรที่กำลังเผชิญกับข้อจำกัดของระบบรักษาความมั่นคงปลอดภัยแบบเดิม เช่น การใช้ระบบเครือข่ายส่วนตัวเสมือนหรือการรักษาความมั่นคงปลอดภัยแบบมีขอบเขตที่ไม่เพียงพอต่อภัยคุกคามสมัยใหม่

๑.๔ ขอบเขตของแนวปฏิบัติ

เพื่อให้แนวปฏิบัตินี้มีความยืดหยุ่นและสามารถนำไปปรับใช้ได้กว้างขวาง จึงกำหนดขอบเขตดังนี้

๑) การไม่ยึดติดกับผู้ผลิตรายใดรายหนึ่ง (Vendor Neutral) ไม่เจาะจงผลิตภัณฑ์ โซลูชัน หรือเทคโนโลยีของผู้ผลิตใดเป็นการเฉพาะ เพื่อให้องค์กรสามารถเลือกใช้เครื่องมือที่เหมาะสมกับความต้องการและงบประมาณของตนเอง

๒) เป็นแนวทางทั่วไป มุ่งเน้นหลักการและแนวคิดพื้นฐาน ไม่ใช่คู่มือการติดตั้ง การกำหนดค่าหรือการใช้งานเฉพาะเจาะจง

๓) ไม่กำหนดข้อบังคับที่เข้มงวด ไม่กำหนดกฎเกณฑ์หรือข้อกำหนดที่เฉพาะเจาะจงว่าองค์กรต้องนำเทคโนโลยีหรือมาตรการใดไปใช้ เนื่องจากแต่ละองค์กรมีภารกิจ ขนาด บริบท และความต้องการที่แตกต่างกัน

๔) เน้นการให้ความรู้และสร้างความเข้าใจ มุ่งเน้นการให้ความรู้ หลักการ และแนวทางที่องค์กรสามารถนำไปศึกษา วิเคราะห์ และปรับใช้ตามบริบท ความพร้อมและกำหนดลำดับความสำคัญ

๕) รองรับการนำไปใช้แบบค่อยเป็นค่อยไป (Gradual Implementation) องค์กรสามารถเริ่มต้นจากส่วนที่มีความพร้อมมากที่สุดและขยายผลไปยังส่วนอื่น ๆ ตามลำดับ

บทที่ ๒

ภาพรวมภัยคุกคาม หลักการพื้นฐาน และกรอบการกำกับดูแล Zero Trust

๒.๑ ภาพรวมภัยคุกคามและผลกระทบที่เกี่ยวข้องกับ Zero Trust

สถาปัตยกรรม Zero Trust ถูกพัฒนาขึ้นเพื่อตอบสนองต่อสภาพแวดล้อมที่การกำหนดขอบเขตความมั่นคงปลอดภัย (Perimeter) ทำได้ยากหรือไม่สามารถทำได้อย่างชัดเจนเนื่องจากการเปลี่ยนแปลงทางธุรกิจและเทคโนโลยีที่สร้างความเสี่ยงสูงขึ้นอย่างหลีกเลี่ยงไม่ได้

๒.๑.๑ ภัยคุกคามที่เกิดจากสภาพแวดล้อมความเสี่ยงสูงยุคใหม่

ภัยคุกคามเหล่านี้เกิดขึ้นจากการที่ความมั่นคงปลอดภัยแบบมีขอบเขตมีช่องว่างที่เกิดจาก “ความเชื่อถือโดยปริยาย” (Implicit Trust) ที่มีอยู่ในเครือข่ายภายใน ซึ่งมีตัวอย่างแสดงในตารางที่ ๑

ตารางที่ ๑ แสดงปัจจัยความเสี่ยงภัยคุกคามยุคใหม่

ปัจจัยความเสี่ยงยุคใหม่	ภัยคุกคามหลัก	กลไก Zero Trust ที่เข้ามาแก้ไข
การทำงานจากทุกที่ และ อุปกรณ์หลากหลาย	การทำงานแบบไฮบริดความเสี่ยงด้านการเข้าถึงจากระยะไกล (Remote Access Risk) การเข้าถึงจากอุปกรณ์ส่วนตัวหรือเครือข่ายสาธารณะที่ไม่น่าเชื่อถือ	นำโมเดลที่เน้นตัวตนเป็นศูนย์กลาง (Identity-Centric Model) และกรอบแนวคิด Secure Access Service Edge and Security Service Edge (SASE/SSE)[๒] บังคับใช้การยืนยันตัวตนแบบหลายปัจจัยและตรวจสอบสถานะของอุปกรณ์ โดยไม่ขึ้นกับสถานที่
ภัยคุกคามจากทั้งโลกตลอดเวลา (Global Persistent Threats)	การโจมตีแบบการเคลื่อนตัวในเครือข่าย (Lateral Movement) และบัญชีผู้ใช้ถูกขโมย (Compromised Credentials) การที่ผู้โจมตีเจาะระบบสำเร็จแล้วแพร่กระจายภายในเครือข่าย	การแบ่งส่วนเครือข่ายแบบย่อย (Micro-segmentation) และการตรวจสอบอย่างต่อเนื่อง (Continuous Verification) จำแนก และจำกัดการเข้าถึงทรัพยากรทุกชิ้น โดยมีการตรวจสอบสิทธิและระดับความมั่นคงปลอดภัยระหว่างการเข้าถึงอย่างต่อเนื่อง
ความเสี่ยงของห่วงโซ่อุปทาน (Supply Chain Risk)	การที่ผู้โจมตีใช้ช่องโหว่ของผู้ให้บริการภายนอก (Third-party Compromise) หรือพันธมิตรเพื่อเข้าถึงระบบขององค์กรผ่านการเชื่อมต่อที่เชื่อถือได้	การกำหนดสิทธิเท่าที่จำเป็น (Least Privilege Access) ให้บริการภายนอกสามารถเข้าถึงเฉพาะทรัพยากรที่จำเป็น (Resource-Specific Access) อย่างเคร่งครัด

๒.๑.๒ ภัยคุกคามที่ Zero Trust มุ่งเป้าหมายในการแก้ไข

Zero Trust มุ่งเน้นการแก้ไขช่องโหว่ที่อยู่ภายในขอบเขตเครือข่ายที่เชื่อถือได้ (Trusted Perimeter) ซึ่งเป็นหลักการของความมั่นคงปลอดภัยแบบเดิม ดังตัวอย่างแสดงในตารางที่ ๒

ตารางที่ ๒ แสดงภัยคุกคามหลักที่ Zero Trust มุ่งเป้าหมายในการแก้ไข

ภัยคุกคาม	คำอธิบายโดยละเอียด	ทำไม Zero Trust ถึงแก้ไขได้
การโจมตีแบบการเคลื่อนตัวในเครือข่าย	การที่ผู้โจมตีหรือมัลแวร์เรียกค่าไถ่ (Ransomware) สามารถเคลื่อนที่จากเครื่องคอมพิวเตอร์ที่ถูกยึดครองเป็นด่านแรก (Initial Foothold) ไปยังทรัพยากรที่มีความสำคัญอื่น ๆ (เช่น ศูนย์ข้อมูลกลางหรือเครื่องแม่ข่ายสำหรับสำรองข้อมูล) ภายในเครือข่าย โดยอาศัยความเชื่อถือโดยปริยายที่ระบบมีต่อผู้ใช้หรืออุปกรณ์ภายใน	การแบ่งส่วนเครือข่ายแบบย่อยและการกำหนดสิทธิเท่าที่จำเป็นจะจำกัดการเชื่อมต่อระหว่างเวิร์กโหลด และทรัพยากรทำให้มีเฉพาะสิ่งที่จำเป็นตามนโยบายเท่านั้นที่สามารถเชื่อมต่อระหว่างกันได้ ส่งผลให้การแพร่กระจายถูกหยุดยั้ง
ภัยคุกคามจากคนภายใน (Insider Threat)	ภัยคุกคามจากบุคลากรภายในที่มีสิทธิเข้าถึงพิเศษ (Privileged Users) ที่ใช้สิทธิโดยมิชอบ หรือจากความผิดพลาดของบุคลากรเอง	การตรวจสอบอย่างต่อเนื่องและโมเดลที่เน้นตัวตนเป็นศูนย์กลางทำให้การเข้าถึงถูกจำกัดและการตรวจสอบตลอดเวลา ลดความเสี่ยงในการทุจริตหรือความผิดพลาด
บัญชีผู้ใช้ถูกขโมย	บัญชีผู้ใช้ที่ถูกขโมย เช่น โดยฟิชชิง (Phishing) และนำมาใช้เพื่อปลอมตัวเป็นผู้ใช้ที่ถูกต้อง ซึ่งสามารถเข้าถึงระบบภายในได้อย่างอิสระเมื่อผ่านด่านแรกไปได้	การยืนยันตัวตนแบบหลายปัจจัยและการประเมินสถานะของอุปกรณ์ถูกบังคับใช้โดยส่วนขับเคลื่อนนโยบาย (Policy Engine: PE) ก่อนอนุญาตการเข้าถึงทุกครั้ง
การทำงานแบบไฮบริดและความเสี่ยงด้านการเข้าถึงจากระยะไกล	ความเสี่ยงจากการเข้าถึงทรัพยากรองค์กรจากอุปกรณ์ส่วนตัวหรือเครือข่ายสาธารณะที่ขาดการควบคุมความมั่นคงปลอดภัย	กรอบแนวคิด SASE/SSE ซึ่งรวมคุณสมบัติของ Zero Trust ทำให้การควบคุมการเข้าถึงถูกนำไปบังคับใช้บนเกตเวย์คลาวด์ โดยไม่ขึ้นอยู่กับสถานที่ตั้งทางกายภาพ

๒.๑.๓ ผลกระทบเชิงกลยุทธ์ต่อองค์กรและประเทศ

การนำ Zero Trust มาใช้ถือเป็นความจำเป็นเร่งด่วน เนื่องจากผลกระทบของภัยคุกคามสมัยใหม่ต่อเสถียรภาพทางเศรษฐกิจและความมั่นคงของชาติมีสูงมาก ซึ่งมีตัวอย่างแสดงในตารางที่ ๓

ตารางที่ ๓ แสดงระดับผลกระทบเชิงกลยุทธ์ต่อองค์กรและประเทศ

ระดับผลกระทบ	ผลกระทบหลักจากภัยคุกคาม	ความจำเป็นและผลประโยชน์ของ Zero Trust
ระดับองค์กร	**ความเสียหายทางธุรกิจ** การหยุดชะงักของบริการ การสูญเสียรายได้ และความเสียหายต่อชื่อเสียง **ความเสี่ยงด้านกฎหมาย** การไม่ปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล[๕] (การรั่วไหลของข้อมูลส่วนบุคคล (Personally Identifiable Information: PII)) และการละเมิด พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์	**ลดความเสี่ยง** Zero Trust ลดความเสี่ยงจากการถูกเจาะระบบและการแพร่กระจายความเสียหาย **การกำกับดูแล** Zero Trust ช่วยให้องค์กรปฏิบัติตามมาตรการจัดการความมั่นคงปลอดภัยสารสนเทศตาม ISO/IEC 27001/27002[๔] ได้อย่างมีประสิทธิภาพ
ระดับประเทศ	**ความไม่มั่นคงของโครงสร้างพื้นฐานสำคัญทางสารสนเทศ** (Critical Information Infrastructure: CII) การโจมตีต่อ CII ส่งผลกระทบต่อความมั่นคงของชาติ **ความน่าเชื่อถือทางเศรษฐกิจ** การที่ข้อมูลรั่วไหลหรือถูกเรียกค่าไถ่ในวงกว้างลดความน่าเชื่อถือในการทำธุรกรรมระหว่างประเทศ	**ยกระดับการป้องกัน CII** Zero Trust เสริมความสามารถในการป้องกัน CII **การเป็นมาตรฐานสากล** การนำ Zero Trust มาเป็นแนวทางในการปรับตัวเข้าสู่เกณฑ์มาตรฐานอุตสาหกรรมระดับโลก (Global Industry Benchmark, NIST, 2020) และส่งเสริมอธิปไตยข้อมูล (Data Sovereignty)

การพิจารณาผลกระทบจากภัยคุกคามดังกล่าวแสดงให้เห็นว่า Zero Trust เป็นกลยุทธ์พื้นฐานที่จำเป็นในการรับมือกับภัยคุกคามยุคใหม่ เพื่อให้องค์กรและประเทศสามารถดำเนินงานได้อย่างต่อเนื่อง และมั่นคงปลอดภัยในยุคที่ไม่มีขอบเขตความมั่นคงปลอดภัยที่ชัดเจนอีกต่อไป

๒.๑.๔ การเปลี่ยนสมมติฐานหลักด้านความมั่นคงปลอดภัย

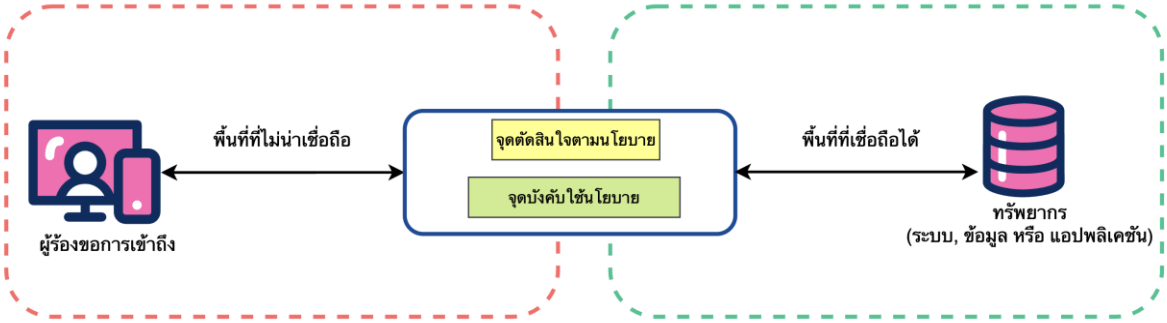
Zero Trust ได้เปลี่ยนสมมติฐานด้านความมั่นคงปลอดภัยขององค์กรอย่างสิ้นเชิง โดยรายละเอียดได้แสดงไว้ในตารางที่ ๔ ดังนี้

ตารางที่ ๔ แสดงการเปลี่ยนสมมติฐานหลักด้านความมั่นคงปลอดภัย

ลักษณะ	สมมติฐานแบบดั้งเดิม	สมมติฐาน Zero Trust
ความเชื่อถือ	หากผู้ใช้ผ่านขอบเขตเครือข่ายเข้ามาภายในได้ผู้ใช้นั้นน่าเชื่อถือ	เครือข่ายใดๆ (ทั้งภายในและภายนอก) ถือเป็นพื้นที่ที่ไม่น่าเชื่อถือ
จุดควบคุม	เน้นการป้องกันขอบเขตนอกสุดด้วยไฟร์วอลล์	เน้นการควบคุมที่ทรัพยากร และตัวตน (Identity)

๒.๒ Zero Trust คืออะไร

Zero Trust คือ กรอบการทำงานเชิงกลยุทธ์ ที่ถูกออกแบบมาเพื่อปรับเปลี่ยนกระบวนทัศน์ด้านความมั่นคงปลอดภัยไซเบอร์ขององค์กร โดยมีหลักการพื้นฐานคือ “อย่าเชื่อทันที จงตรวจสอบเสมอ”[๑]



รูปที่ ๑ การเข้าถึงแบบ Zero Trust

รูปที่ ๑ แนวคิดหลักของการเข้าถึงแบบ Zero Trust ในระดับปรัชญา โดยเปลี่ยนจากสมมติฐานแบบดั้งเดิมที่เชื่อถือเครือข่ายภายใน ไปสู่การกำหนดให้การเข้าถึงทั้งหมดเริ่มต้นจากเขตพื้นที่ที่ไม่น่าเชื่อถือ

ผู้ร้องขอการเข้าถึงและอุปกรณ์ที่ต้องการเข้าถึงทรัพยากร จะต้องผ่านจุดตัดสินใจตามนโยบาย (Policy Decision Point: PDP) และจุดบังคับใช้นโยบาย (Policy Enforcement Point: PEP) ก่อนเสมอโดยจะทำหน้าที่ตรวจสอบอย่างต่อเนื่องโดยพิจารณาบริบททั้งหมด เช่น

ตัวตนของผู้ใช้

สถานะของอุปกรณ์

บริบทอื่น ๆ (เช่น เวลา สถานที่ หรือความอ่อนไหวของข้อมูล)

ก่อนจะตัดสินใจให้สิทธิการเข้าถึงทรัพยากร

การอนุญาตให้เข้าถึงทรัพยากรนั้นจะอยู่ภายใต้การกำหนดสิทธิเท่าที่จำเป็นและอนุญาตแบบต่อเซสชัน (Per-session) เท่านั้น โดยทรัพยากรนั้นจะตั้งอยู่ในพื้นที่ที่น่าเชื่อถือโดยปริยาย (Implicit Trust Zone) ซึ่งหมายถึงทรัพยากรเหล่านี้ถูกปกป้องจากภายนอก แต่ก็ไม่ได้ “เชื่อถือ” การเข้าถึงจากภายในโดยอัตโนมัติเช่นกัน อย่างไรก็ดีสิ่งที่องค์กรจำเป็นต้องคำนึงและระวัง คือ การมีพื้นที่ที่น่าเชื่อถือโดยปริยายที่มีจำนวนมากเกินไปหรือใหญ่เกินไป เช่น มีหลายระบบที่ไม่เกี่ยวข้องกัน อยู่ในพื้นที่เดียวกัน ย่อมไม่ใช่เรื่องดีแบ่งทรัพยากร เช่น ระบบต่าง ๆ ออกเป็นเขตป้องกันแบบไมโครเพอริมิเตอร์ ที่มีขนาดเล็กและง่ายต่อการป้องกัน ย่อมเป็นผลดีต่อองค์กร ทั้งในด้านการรักษาความมั่นคงปลอดภัย ตอบสนองต่อภัยคุกคามและการเฝ้าระวัง

โดยในสถาปัตยกรรม Zero Trust องค์กรจะสร้างจุดตัดสินใจตามนโยบายและจุดบังคับใช้นโยบาย (ดังแสดงในรูปที่ ๑) เพื่อเป็นจุดตรวจสอบความมั่นคงปลอดภัยที่อยู่ใกล้กับทรัพยากรที่สุด ทำหน้าที่เสมือนเป็นประตูเปิดหรือปิด เข้าไปยังแต่ละพื้นที่ปลอดภัย ทั้งนี้จุดตัดสินใจตามนโยบายและจุดบังคับใช้นโยบายจะทำการตรวจสอบตัวตน สิทธิของผู้ขอการเข้าถึง ซึ่งเมื่อได้รับการอนุญาตแล้วผู้ขอการเข้าถึงนั้นจะได้รับความเชื่อถือตามบริบท เป็นการชั่วคราวเพื่อใช้ในการเข้าถึงทรัพยากรที่ร้องขอเฉพาะในเซสชันนั้น ๆ

แนวคิดนี้เป็นการยืนยันหลักการ "อย่าเชื่อทันที จงตรวจสอบเสมอ" และ "เครือข่ายใด ๆ ถือเป็นพื้นที่ที่ไม่น่าเชื่อถือ" ซึ่งเป็นหัวใจของสถาปัตยกรรม Zero Trust

๒.๒.๑ สรุปปรัชญาและแนวคิดหลักของ Zero Trust

Zero Trust ปฏิเสธสมมติฐานหลักของสถาปัตยกรรมความมั่นคงปลอดภัยแบบดั้งเดิมที่ให้ "การเชื่อถือโดยปริยาย" แก่ผู้ใช้หรืออุปกรณ์ที่อยู่ภายในเครือข่าย หลักการของ Zero Trust กำหนดให้เครือข่ายใด ๆ ถือเป็นพื้นที่ที่ไม่น่าเชื่อถือการรักษาความมั่นคงปลอดภัย ย้ายจากการป้องกันที่ขอบเขตนอกสุดไปสู่การควบคุมที่ทรัพยากร และตัวตนของผู้ใช้หรืออุปกรณ์ Zero Trust จึงเป็นการควบคุมการเข้าถึงในระดับที่ละเอียดยิ่งขึ้น โดยการอนุญาตสิทธิจะถูกกำหนดแบบต่อเซสชัน และเป็นไปตามหลักการกำหนดสิทธิเท่าที่จำเป็น

๒.๒.๒ ความแตกต่างระหว่างความมั่นคงปลอดภัยแบบดั้งเดิมและ Zero Trust

เพื่อให้เกิดความเข้าใจที่ชัดเจน Zero Trust แตกต่างจากความมั่นคงปลอดภัยแบบดั้งเดิมในประเด็นหลัก ดังที่แสดงตารางที่ ๕ ต่อไปนี้

ตารางที่ ๕ เปรียบเทียบความแตกต่างระหว่างความมั่นคงปลอดภัยแบบดั้งเดิมและ Zero Trust

ลักษณะ	ความมั่นคงปลอดภัยแบบเดิม	Zero Trust
ปรัชญาหลัก	สร้างป้อมปราการ (Hard Shell) เน้นการป้องกันขอบเขต	ไม่มีขอบเขตเครือข่าย เน้นการตรวจสอบทุกจุดอย่างต่อเนื่อง
จุดเน้นความมั่นคงปลอดภัย	ขอบเขตเครือข่าย	ตัวตนและทรัพยากร
หลักการเข้าถึง	สิทธิการเชื่อถือโดยปริยาย	สิทธิเข้าถึงแบบจำกัดเท่าที่จำเป็นต่อเซสชัน

๒.๓ หลักการพื้นฐานของ Zero Trust

หลักการพื้นฐานของ Zero Trust ที่เป็นที่ยอมรับในระดับสากล คือ ๗ หลักการ (Tenets) ซึ่งกำหนดโดย NIST Special Publication 800-207 "Zero Trust Architecture" (NIST, 2020) หลักการเหล่านี้เป็นแนวคิดที่เป็นแกนหลักที่ต้องนำไปปฏิบัติในการออกแบบสถาปัตยกรรม Zero Trust ตามรูปที่ ๒

รูปที่ ๒ หลักการพื้นฐานของ Zero Trust

๒.๓.๑ หลักการพื้นฐาน ๗ ประการของ Zero Trust

หลักการเหล่านี้กำหนดแนวทางสำหรับการตัดสินใจให้สิทธิการเข้าถึงทรัพยากรทั้งหมดในองค์กร

๑) ทรัพยากรทั้งหมดถือเป็นทรัพยากรที่ต้องได้รับการปกป้อง

ระบบจะต้องถือว่าทรัพยากรทั้งหมด ไม่ว่าจะเป็นข้อมูล แอปพลิเคชัน หรือบริการ เป็นสินทรัพย์ที่ต้องได้รับการปกป้องเป็นรายบุคคล การกำหนดนโยบายต้องเริ่มต้นจากการระบุว่าทรัพยากรใดที่ผู้ใช้ต้องการเข้าถึง

๒) การสื่อสารทั้งหมดได้รับการรักษาความมั่นคงปลอดภัย

การสื่อสารทั้งหมดต้องได้รับการเข้ารหัสและตรวจสอบความสมบูรณ์ (Integrity Check) เพื่อป้องกันการดักฟังหรือการแก้ไขข้อมูล ไม่ว่าการสื่อสารนั้นจะเกิดขึ้นภายในเครือข่าย หรือภายนอกเครือข่าย โดยไม่มีการยกเว้น

๓) การเข้าถึงจะได้รับอนุญาตเป็นรายเซสชัน

๓.๑) การเข้าถึงจะถูกให้สิทธิแบบต่อเซสชันและกำหนดสิทธิการเข้าถึงเท่าที่จำเป็น

๓.๒) สิทธิการเข้าถึงต้องถูกยกเลิกเมื่อเซสชันสิ้นสุดลงและต้องมีการตรวจสอบซ้ำทุกครั้งที่ผู้ใช้มีการร้องขอการเข้าถึงใหม่

๔) การเข้าถึงที่ปรับเปลี่ยนได้ และบังคับใช้อย่างเคร่งครัด

๔.๑) ก่อนให้สิทธิการเข้าถึงส่วนขับเคลื่อนนโยบายจะต้องตรวจสอบสถานะของอุปกรณ์และตัวตนของผู้ใช้อย่างเข้มงวด

๔.๒) การตรวจสอบรวมถึงการตรวจสอบสถานะแพตช์ การทำงานของซอฟต์แวร์ป้องกันไวรัส และสถานะการตั้งค่าที่ถูกต้อง

๕) การรับรองและการอนุญาตแบบไดนามิก (Dynamic)

๕.๑) นโยบายการเข้าถึงจะต้องเป็นแบบไดนามิก โดยพิจารณาจากปัจจัยด้านบริบทในขณะนั้น เช่น สถานที่ เวลา ประเภทของข้อมูลที่เข้าถึง และความเสี่ยงที่ประเมินจากข้อมูลข่าวกรองด้านภัยคุกคาม

๕.๒) ตัวอย่าง เช่น อุปกรณ์หรือผู้ใช้ที่ขอเข้าถึงทรัพยากร ที่ไม่มีการติดตั้งซอฟต์แวร์ป้องกันมัลแวร์ในช่วงนอกเวลาทำการไม่ควรได้รับสิทธิการเข้าถึงหรือความเชื่อถือเท่าเทียมกับการเข้าถึงในเวลาทำการ

๖) องค์กรจะต้องเก็บรวบรวมข้อมูลที่เกี่ยวกับการรักษาความมั่นคงปลอดภัย

ระบบ Zero Trust ต้องมีการบันทึกเหตุการณ์ที่เกี่ยวข้องกับภัยด้านความมั่นคงปลอดภัยของระบบและสินทรัพย์ภายในองค์กรและเซสชันทั้งหมดอย่างต่อเนื่อง เพื่อใช้เป็นข้อมูลนำเข้าสำหรับส่วนขับเคลื่อนนโยบายและสำหรับการสอบสวนเหตุการณ์ (Forensics) ตามแนวทาง ISO/IEC 27037/27043

๗) การตรวจสอบสิทธิและการเข้าถึงเป็นแบบอัตโนมัติ

องค์กรต้องมุ่งเน้นการใช้ระบบอัตโนมัติในการตรวจสอบสิทธิและการบังคับใช้นโยบาย เพื่อให้การทำงานมีประสิทธิภาพ ลดความล่าช้าในการเข้าถึงและตอบสนองต่อภัยคุกคามได้อย่างรวดเร็ว

๒.๓.๒ การเน้นย้ำแนวคิดหลักเพื่อการเปลี่ยนผ่าน

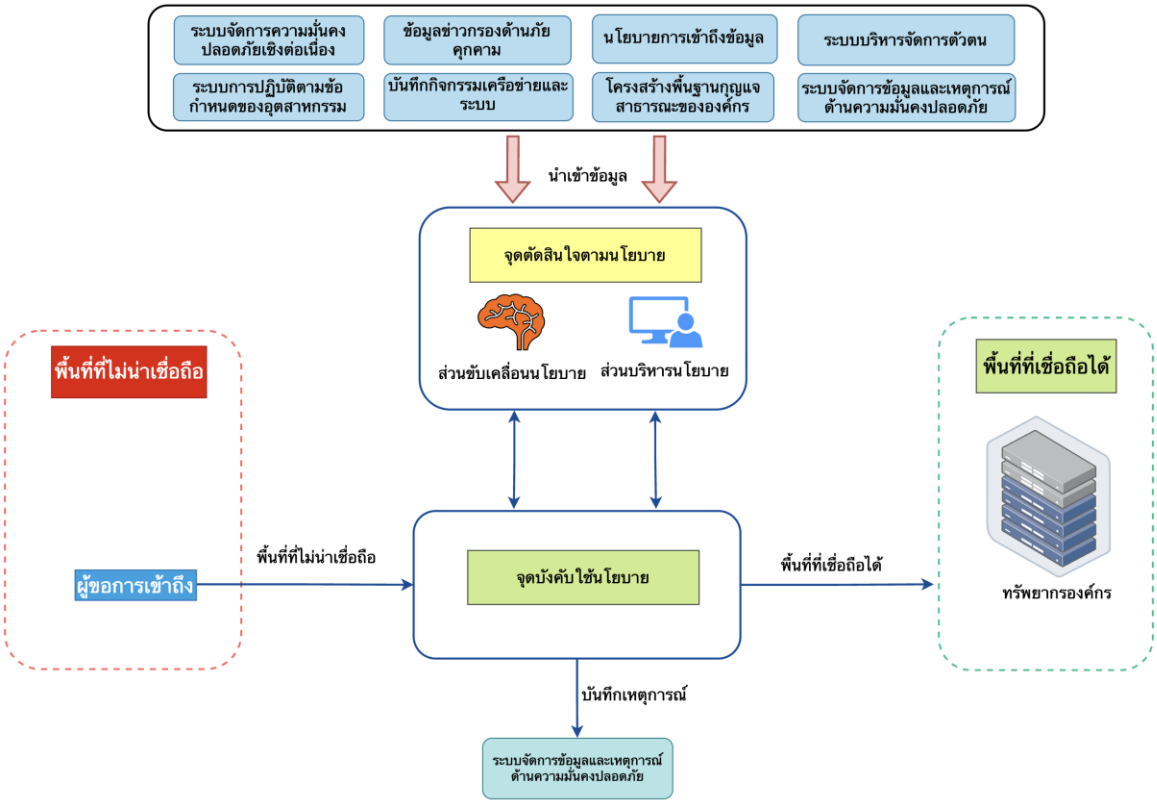
หลักการเหล่านี้ต้องถูกนำมาขยายความเพื่อเน้นย้ำความแตกต่างจากความมั่นคงปลอดภัยแบบเดิม ดังที่แสดงในตารางที่ ๖

ตารางที่ ๖ แสดงแนวคิดหลักเพื่อการเปลี่ยนผ่านสู่ Zero Trust

หลักการ (Zero Trust Tenet)	ความสำคัญที่ต้องเน้นในแนวทางปฏิบัติประเทศ	การเชื่อมโยงทางปฏิบัติ
“อย่าเชื่อทันทีจงตรวจสอบเสมอ”	เน้นว่าหลักการนี้ใช้กับทุกสิ่ง ไม่ใช่แค่ผู้ใช้ภายนอก แต่รวมถึงผู้ใช้ภายในด้วย	การเข้าถึงทุกอย่างต้องเริ่มต้นด้วยการยืนยันตัวตนแบบหลายปัจจัย (MFA) และการตรวจสอบสถานะของอุปกรณ์ (Device Posture)
การกำหนดสิทธิการเข้าถึงเท่าที่จำเป็น	การให้สิทธิการเข้าถึงแบบจำกัดตามความจำเป็นของงาน (Need-to-know) และจำกัดเวลา (Time-bound Access) เท่านั้น	เป็นกลไกทางเทคนิคที่สำคัญในการปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) และ ISO/IEC 27701 เพื่อปกป้องข้อมูลส่วนบุคคล
การตรวจสอบอย่างต่อเนื่อง	การตรวจสอบต้องทำอย่างต่อเนื่องตลอดระยะเวลาของเซสชันไม่ใช่แค่ตอนเริ่มต้นเข้าสู่ระบบเท่านั้น	ส่วนขับเคลื่อนนโยบายต้องสามารถยกเลิกเซสชันได้ทันที เมื่อสถานะความเสี่ยงของผู้ใช้ หรืออุปกรณ์เปลี่ยนไป เช่น อุปกรณ์ถูกตรวจพบไวรัส

๒.๔ องค์ประกอบเชิงตรรกะพร้อมตัวอย่าง

สถาปัตยกรรม Zero Trust ประกอบด้วยองค์ประกอบเชิงตรรกะที่ทำงานประสานกันเพื่อบังคับใช้หลักการ Zero Trust โดยเฉพาะอย่างยิ่งการบังคับใช้นโยบายแบบไดนามิก (Dynamic PolicyEnforcement) องค์ประกอบเหล่านี้กำหนดบทบาทในการรับส่งข้อมูล การตัดสินใจ และการบังคับใช้นโยบาย ดังแสดงในรูปที่ ๓



รูปที่ ๓ องค์ประกอบเชิงตรรกะ

๒.๔.๑ องค์ประกอบหลักของสถาปัตยกรรม Zero Trust

ตารางที่ ๗ แสดงองค์ประกอบหลักของสถาปัตยกรรม Zero Trust

องค์ประกอบเชิงตรรกะ	หน้าที่หลัก	ตัวอย่างการทำงาน
ส่วนขับเคลื่อนนโยบาย (Policy Engine: PE)	ศูนย์กลางการตัดสินใจรับผิดชอบในการให้หรือปฏิเสธการเข้าถึงทรัพยากร โดยพิจารณาจากนโยบายที่ได้รับ (Policies) และข้อมูลบริบท จากแหล่งข้อมูลต่างๆ	ประเมินความเสี่ยงแบบเรียลไทม์ (Realtime Risk Assessment) หากผู้ใช้ล็อกอินจากตำแหน่งทางภูมิศาสตร์ที่มีความเสี่ยงสูง (อ้างอิงจากข้อมูลข่าวกรองด้านภัยคุกคาม) ส่วนขับเคลื่อนนโยบายอาจปฏิเสธการเข้าถึงทันที
ส่วนบริหารนโยบาย (Policy Administrator: PA)	ส่วนบริหารนโยบายรับผิดชอบในการสื่อสารคำสั่งไปยังจุดบังคับใช้นโยบาย เพื่อเปิดหรือปิดการเชื่อมต่อตามการตัดสินใจของส่วนขับเคลื่อนนโยบาย	เมื่อส่วนขับเคลื่อนนโยบายตัดสินใจ “อนุญาต” ส่วนบริหารนโยบายจะสั่งให้จุดบังคับใช้นโยบาย อนุญาตการเชื่อมต่อที่จำกัดระยะเวลาและประสานงานกับระบบบริหารจัดการตัวตน (Identity Management: IdM) เพื่อยืนยันตัวตนใหม่
จุดบังคับใช้นโยบาย (Policy Enforcement Point: PEP)	จุดบังคับใช้นโยบายรับผิดชอบในการเปิดปิด หรือหยุดเซสชันการเชื่อมต่อตามคำสั่งของส่วนบริหารนโยบาย	ทำหน้าที่เป็นเกตเวย์ ไฟร์วอลล์ หรือเกตเวย์การแบ่งส่วนเครือข่ายแบบย่อย เพื่อควบคุมการเข้าถึงในระดับเครือข่ายหรือแอปพลิเคชัน โดยบังคับใช้นโยบายที่ได้รับจากส่วนบริหารนโยบาย

๒.๔.๒ องค์ประกอบสนับสนุนและแหล่งข้อมูล

การตัดสินใจของส่วนขับเคลื่อนนโยบายจะมีประสิทธิภาพก็ต่อเมื่อได้รับข้อมูลบริบทที่ครบถ้วนและเชื่อถือได้จากแหล่งข้อมูลเหล่านี้ ดังที่แสดงในตารางที่ ๘

ตารางที่ ๘ แสดงองค์ประกอบสนับสนุนและแหล่งข้อมูล

องค์ประกอบสนับสนุน	หน้าที่	การเชื่อมโยงกับ Zero Trust กระบวนการตัดสินใจ (Decision-Making)
ระบบจัดการความมั่นคงปลอดภัยเชิงต่อเนื่อง (Continuous Diagnostics and Mitigation: CDM)	ระบบตรวจสอบสถานะ ทำหน้าที่เก็บข้อมูลและประเมินสถานะของอุปกรณ์ และความเสี่ยงอย่างต่อเนื่อง	รายงานว่าอุปกรณ์ของผู้ใช้มีการอัปเดตแพตช์ล่าสุดหรือไม่ หรือมีซอฟต์แวร์ป้องกันไวรัสทำงานอยู่หรือไม่ ไปยังส่วนขับเคลื่อนนโยบายก่อนอนุญาตการเข้าถึง
ระบบบริหารจัดการตัวตน (Identity Management System: IdM)	จัดการบัญชี การยืนยันตัวตนแบบหลายปัจจัยและเก็บข้อมูลคุณสมบัติของผู้ใช้	เป็นแหล่งข้อมูลหลักในการยืนยันตัวตนของผู้ร้องขอการเข้าถึง
ข้อมูลข่าวกรองด้านภัยคุกคาม (Threat Intelligence)	ข้อมูลภัยคุกคามภายนอก เช่น ที่อยู่ไอพีที่ติดแบล็คลิสต์ หรือตัวบ่งชี้การบุกรุก (Indicators of Compromise: IOCs)	ส่วนขับเคลื่อนนโยบายใช้ข้อมูลนี้ในการประเมินความเสี่ยงเชิงรุก โดยเป็นไปตามหลักการลดความเสี่ยงตาม ISO/IEC 27005
ฐานข้อมูลการบริหารจัดการการตั้งค่า (Configuration Management Database: CMDB)	ข้อมูลเกี่ยวกับสินทรัพย์ สถานะแพตช์ ความสมบูรณ์ของอุปกรณ์ และการตั้งค่าของอุปกรณ์	ใช้เป็นข้อมูลเพื่อยืนยันว่าสินทรัพย์ที่ร้องขอการเข้าถึงนั้นมีการกำหนดค่าที่ถูกต้องหรือไม่
ระบบจัดการข้อมูลและเหตุการณ์ด้านความมั่นคงปลอดภัย (SIEM)	บันทึกการเข้าถึงและเหตุการณ์ทั้งหมด เพื่อใช้ในการตรวจสอบอย่างต่อเนื่องและเป็นหลักฐานดิจิทัล	ข้อมูลนี้มีความสำคัญสำหรับการสอบสวนเหตุการณ์และใช้เป็นพยานหลักฐานดิจิทัลตามแนวทาง ISO/IEC 27037/27043

องค์ประกอบเหล่านี้ทำงานร่วมกันในรูปแบบวงปิด (Closed Loop) โดยมีส่วนขับเคลื่อนนโยบายเป็นศูนย์กลางในการตัดสินใจตามหลักการ “อย่าเชื่อทันที จงตรวจสอบเสมอ” ในทุกจุดเข้าถึงทรัพยากร

๒.๕ รูปแบบการติดตั้งใช้งาน และกรณีการใช้งาน

การนำสถาปัตยกรรม Zero Trust มาใช้สามารถแบ่งออกเป็นรูปแบบการใช้งาน (Deployment Models) หลักได้หลายรูปแบบ โดยขึ้นอยู่กับบริบท ความเร่งด่วน และลำดับความสำคัญขององค์กร การกำหนดรูปแบบที่เหมาะสมจะช่วยให้องค์กรสามารถย้ายไปสู่ Zero Trust ได้อย่างเป็นขั้นตอนและมีประสิทธิภาพ

๒.๕.๑ รูปแบบการใช้งาน Zero Trust

รูปแบบหลักของการใช้งาน Zero Trust มักแบ่งตามจุดควบคุมหลัก ซึ่งเป็นไปตามแนวทางปฏิบัติสากล ดังที่แสดงในตารางที่ ๙

ตารางที่ ๙ แสดงรูปแบบการใช้งาน Zero Trust

รูปแบบ (Deployment Model)	จุดเน้นหลัก (Focus)	กลไกสำคัญที่ใช้งาน	กรณีการใช้งานหลัก (Use Case)
โมเดลที่เน้นตัวตนเป็นศูนย์กลาง (Identity-centric Model)	มุ่งเน้นการตรวจสอบตัวตนเป็นศูนย์กลางของการควบคุม (Center of Control)	การยืนยันตัวตนแบบหลายปัจจัย นโยบายการเข้าถึงแบบมีเงื่อนไข (Conditional Access Policy)	ความมั่นคงปลอดภัยของการทำงานแบบไฮบริด หรือแบบการทำงานจากระยะไกล บังคับใช้การตรวจสอบตัวตนอย่างเข้มงวด โดยไม่คำนึงถึงสถานที่ตั้งอยู่ของผู้ใช้
โมเดลเน้นเครือข่ายเป็นศูนย์กลาง (Network-centric Model)	เน้นการแบ่งเครือข่ายเป็นเครือข่ายย่อย เพื่อควบคุมการโจมตีแบบการเคลื่อนตัวในเครือข่าย	การแบ่งส่วนเครือข่ายแบบย่อยที่จุดบังคับใช้นโยบาย	การป้องกันมัลแวร์เรียกค่าไถ่โดยการจำกัดการเชื่อมต่อระหว่างเครื่องแม่ข่ายด้วยกันเอง เพื่อหยุดยั้งการโจมตีแบบการเคลื่อนตัวในเครือข่ายของมัลแวร์
โมเดลที่เน้นแอปพลิเคชันเป็นศูนย์กลาง	มุ่งเน้นการควบคุมการเข้าถึงในระดับแอปพลิเคชัน หรือเกตเวย์ API	SASE/SSE เกตเวย์ API	การกำหนดสิทธิเท่าที่จำเป็นสำหรับข้อมูลอ่อนไหว ควบคุมการเข้าถึงข้อมูลอ่อนไหวสูง เช่น PII ตามหลักการ PDPA และ ISO/IEC 27701
โมเดลที่เน้นข้อมูลเป็นศูนย์กลาง (Data-centric Model)	เน้นที่ความสามารถในการฟื้นคืนสภาพของข้อมูล (การกู้คืน)	การป้องกันการแก้ไขข้อมูล (Data anti-tampering) การตรวจจับและการแยกข้อมูล	การจัดเก็บและสำรองข้อมูล เพื่อการป้องกันล้มเหลว ต้องมั่นใจว่าข้อมูลไม่ถูกแก้ไข ตามหลักการ ๓-๒-๑-๑-๐ ข้อมูลมีความสะอาดและมีประสิทธิภาพ และสามารถกู้คืนได้อย่างรวดเร็วและปลอดภัย

๒.๕.๒ กรณีการใช้งานหลัก

การติดตั้งใช้งาน Zero Trust ในรูปแบบต่าง ๆ มีวัตถุประสงค์เพื่อแก้ปัญหาภัยคุกคามที่ระบุไว้ในหัวข้อ ๒.๑ ได้อย่างเป็นรูปธรรม

การสนับสนุนการทำงานแบบไฮบริดหรือแบบการทำงานจากระยะไกลอย่างมั่นคงปลอดภัย ปัญหาที่แก้ไข ความเสี่ยงจากการเข้าถึงทรัพยากรองค์กรจากอุปกรณ์ส่วนตัวหรือเครือข่ายสาธารณะที่ขาดการควบคุมความมั่นคงปลอดภัยกลไก Zero Trust ใช้โมเดลที่เน้นตัวตนเป็นศูนย์กลางร่วมกับกรอบ SASE/SSE หรือเกตเวย์ ZTNA เพื่อบังคับใช้การตรวจสอบตัวตนและสถานะของอุปกรณ์ก่อนอนุญาตการเข้าถึงแอปพลิเคชันหรือข้อมูลที่ต้องการโดยไม่ขึ้นอยู่กับสถานที่ตั้งทางกายภาพ

การป้องกันการแพร่กระจายของภัยคุกคาม

ปัญหาที่แก้ไข การแพร่กระจายของผู้โจมตีจากจุดที่เข้าสู่ระบบเบื้องต้นไปยังทรัพยากรอื่น ๆ ภายในเครือข่าย กลไก Zero Trust ใช้การแบ่งส่วนเครือข่ายแบบย่อย เพื่อจำกัดการสื่อสารระหว่างเครื่องแม่ข่าย เวิร์กโหลด และสินทรัพย์ให้เป็นแบบจำกัดตามความจำเป็นของงานเท่านั้น ทำให้การเคลื่อนที่ระหว่างเครื่องถูกหยุดยั้งสามารถลดขอบเขตความเสียหายได้อย่างมาก

การบังคับใช้การกำหนดสิทธิเท่าที่จำเป็นสำหรับบุคคลภายนอกและห่วงโซ่อุปทาน

ปัญหาที่แก้ไข ความเสี่ยงจากการถูกคุกคามจากห่วงโซ่อุปทานที่ผ่านการเชื่อมต่อที่น่าเชื่อถือกลไก Zero Trust ใช้หลักการกำหนดสิทธิการเข้าถึงเท่าที่จำเป็นอย่างเข้มงวด โดยเฉพาะกับบุคคลภายนอกเพื่อให้สามารถเข้าถึงทรัพยากรได้เฉพาะที่จำเป็นและถูกยกเลิกสิทธิทันทีหลังเสร็จสิ้นภารกิจ

การป้องกันข้อมูลสูญหายและการกู้คืนที่รวดเร็ว

ปัญหาที่แก้ไข โครงสร้างพื้นฐานทั้งหมดตกเป็นเป้าหมายของการโจมตีด้วยมัลแวร์เรียกค่าไถ่และระบบมีความเสี่ยงที่จะล้มเหลว กลไก Zero Trust มีการสร้างสภาพแวดล้อมความมั่นคงปลอดภัยที่ข้อมูลถูกแยกออกจากกันทางกายภาพ เพื่อรับประกันว่าสำเนาข้อมูลจะไม่ถูกแก้ไขและเนื้อหามีความสะอาดและมีประสิทธิภาพ กลไกนี้สามารถใช้เพื่อกู้คืนหรือสร้างระบบบริการขึ้นใหม่ได้อย่างรวดเร็ว

๒.๕.๓ วิวัฒนาการของหลักการสำรองข้อมูลสู่ความสามารถในการเตรียมตัวและตอบสนองต่อภัยคุกคามทางไซเบอร์ (Cyber Resilience)

ตารางที่ ๑๐ แสดงวิวัฒนาการของหลักการสำรองข้อมูล

หลักการ	องค์ประกอบที่เพิ่มเข้ามา	วัตถุประสงค์หลัก	ความเกี่ยวข้องกับ Zero Trust
๓-๒-๑	พื้นฐาน	ป้องกันภัยพิบัติทางกายภาพหรือความล้มเหลวของอุปกรณ์ (Physical Disasters or Hardware Failure)	ต่ำ (เน้นที่ความพร้อมใช้งานของข้อมูล)
๓-๒-๑-๑	+ ๑ ไม่สามารถเปลี่ยนแปลงได้หรือออฟไลน์ (Immutable or Offline)	ป้องกันภัยคุกคามไซเบอร์ (Cyber Threats)	เริ่มต้น (เน้นการไม่เชื่อถือระบบเครือข่าย)
๓-๒-๑-๑-๐	+ ๐ ไม่มีความผิดพลาด (Zero Errors)	รับประกันความสามารถในการกู้คืน (Guaranteed Recoverability) และความเชื่อถือ	สูงสุด (เน้นการตรวจสอบและยืนยันทุกครั้ง)

วิวัฒนาการหลักการสำรองข้อมูลจาก **๓-๒-๑** ไปสู่ **๓-๒-๑-๑-๐** เพื่อแสดงให้เห็นถึงความจำเป็นทางธุรกิจและทางเทคนิคในการยกระดับกลยุทธ์การปกป้องข้อมูลได้อย่างชัดเจน ดังนี้

๑. จุดเริ่มต้น หลักการสำรองข้อมูล ๓-๒-๑

หลักการสำรองข้อมูล ๓-๒-๑ มุ่งเน้นไปที่ความหลากหลายของสำเนา สื่อ และที่ตั้ง เพื่อป้องกันความล้มเหลวทางกายภาพหรือความเสียหายที่เกิดขึ้นกับอุปกรณ์

“๓” สำรอง: รับประกันว่าแม้สำเนาหลักจะเสียหายก็ยังมีสำรอง ๒ ชุด

“๒” ชนิดสื่อ: ลดความเสี่ยงที่ความล้มเหลวของเทคโนโลยีจัดเก็บประเภทเดียวจะส่งผลกระทบต่อข้อมูลสำรองทั้งหมด (เช่น ถ้า Hard Disk ล้มเหลว ก็ยังมี Tape หรือ คลาวด์)

“๑” ที่ตั้งภายนอก: ป้องกันเหตุการณ์ภัยพิบัติในพื้นที่เดียว (เช่น ไฟไหม้ น้ำท่วม)

จุดอ่อนที่นำไปสู่การพัฒนา

หลักการ ๓-๒-๑ ไม่ได้ออกแบบมาเพื่อรับมือกับมัลแวร์เรียกค่าไถ่โดยเฉพาะ หากผู้โจมตีเข้าถึงเครือข่ายได้ พวกเขาสามารถเข้าถึงและเข้ารหัส หรือลบสำเนาสำรองทั้งหมดที่เชื่อมต่อกับเครือข่ายได้ทันที

๒. การต่อยอด หลักการสำรองข้อมูล ๓-๒-๑-๑ ป้องกันมัลแวร์เรียกค่าไถ่

การเพิ่มเลข “๑” ตัวที่สองเข้ามา เป็นการแก้ไขจุดอ่อนของหลักการ ๓-๒-๑ โดยตรง ซึ่งเป็นก้าวแรกที่สำคัญสู่แนวคิด Zero Trust

“๑” สำเนาที่ไม่สามารถเปลี่ยนแปลงได้หรือสำเนาที่แยกจากระบบ (Immutable or Air-Gapped Copy):

Immutable (ไม่สามารถเปลี่ยนแปลงได้) เป็นการกำหนดค่าทางซอฟต์แวร์ที่ล็อกข้อมูลสำรองไว้ตามเวลาที่กำหนด ไม่ให้ใครมาแก้ไขหรือลบได้แม้แต่ผู้ดูแลระบบเอง

Air-Gapped (แยกจากระบบ) เป็นการแยกการเชื่อมต่อทางกายภาพหรือตรรกะออกจากเครือข่ายการดำเนินงานหลัก (Production Network)

วัตถุประสงค์ สร้าง **“ปราการสุดท้าย”** ของสำเนาที่ถูกแยกออก เพื่อให้มั่นใจว่าหากภัยคุกคามสามารถทะลุผ่านระบบป้องกันอื่น ๆ เข้ามาได้ก็จะไม่สามารถเข้าถึงสำเนาชุดนี้ได้ ทำให้องค์กรมีจุดกู้คืนที่ "สะอาด" เสมอ

ความเกี่ยวข้องกับ Zero Trust

เป็นจุดที่หลักการสำรองข้อมูลเริ่มสอดคล้องกับ Zero Trust โดยใช้หลักการ “อย่าเชื่อถือเครือข่าย และระบบดำเนินงานหลัก (Never Trust the Production Environment)” จึงต้อง “แยก” ข้อมูลสำรองเพื่อสร้างสภาพแวดล้อมที่ปลอดภัยและถูกควบคุมอย่างเข้มงวด

๓. จุดสูงสุด: หลักการสำรองข้อมูล ๓-๒-๑-๑-๐ (Guaranteed Recoverability and ZeroTrust)

การเพิ่มเลข “๐” เข้ามา เป็นการเปลี่ยนมุมมองจากการมีสำเนาไปสู่การ **“รับประกันความสามารถในการกู้คืน”** มีรายละเอียดแสดงในตารางที่ ๑๑

ตารางที่ ๑๑ แสดงรายละเอียดหลักการสำรองข้อมูล ๓-๒-๑-๑-๐

ตัวเลข	ความหมาย	รายละเอียด
“๓”	**“๓” สำเนา**	ต้องมีสำเนาของข้อมูลอย่างน้อย **๓ ชุด** (๑ ชุดใช้งานหลัก และ ๒ ชุดสำรอง)
“๒”	**“๒” ชนิดสื่อ**	ต้องเก็บสำเนาไว้ในสื่อหรือประเภทของที่เก็บข้อมูลที่แตกต่างกันอย่างน้อย **๒ ประเภท** เช่น ดิสก์ NAS คลาวด์ฯลฯ เพื่อป้องกันความเสียหายจากความล้มเหลวของสื่อบันทึกประเภทเดียว
“๑”	**“๑” สำเนาภายนอกสถานที่**	ต้องมีสำเนาอย่างน้อย ๑ ชุด จัดเก็บไว้นอกสถานที่ (Off-Site) เช่น ในศูนย์ข้อมูลอื่น หรือคลาวด์ เพื่อป้องกันภัยพิบัติทางกายภาพในสถานที่ตั้งหลัก (เช่น ไฟไหม้ น้ำท่วม)
“๑”	**“๑” สำเนาที่ไม่สามารถเปลี่ยนแปลงได้ หรือสำเนาที่แยกจากระบบ**	ต้องมีสำเนาอย่างน้อย **๑ ชุด** ที่เป็นแบบ **ไม่สามารถเปลี่ยนแปลงได้** หรือ **สำเนาที่แยกจากระบบ** ซึ่งเป็นกุญแจสำคัญใน

ตัวเลข	ความหมาย	รายละเอียด
		การป้องกันมัลแวร์เรียกค่าไถ่ ไม่ให้เข้าถึงและเข้ารหัสหรือลบสำเนาข้อมูลสำรองได้
“๐”	**“๐” ข้อผิดพลาด (Errors)**	ต้องมั่นใจว่าการกู้คืนข้อมูลสำรองนั้น **ไม่มีข้อผิดพลาด** โดยต้องมีการทดสอบการกู้คืนข้อมูลโดยอัตโนมัติและสม่ำเสมอ (Verified Backups) เพื่อให้แน่ใจว่าข้อมูลสำรองสามารถใช้งานได้อย่างสมบูรณ์

“๐” Errors ไม่มีข้อผิดพลาด และทดสอบการกู้คืน (Zero Errors - Verified Backups)

วัตถุประสงค์ แก้ไขปัญหาใหญ่ที่สุดของการสำรองข้อมูลคือ **“ข้อมูลสำรองใช้ไม่ได้จริงเมื่อจำเป็นต้องกู้คืน”**

หลักการนี้กำหนดให้มี**การทดสอบการกู้คืน (Recovery Verification)** โดยอัตโนมัติและสม่ำเสมอ เพื่อให้มั่นใจว่าสำเนาที่เก็บไว้ไม่ว่าจะอยู่บนสื่อใดก็ตาม เช่น ดิสก์ คลาวด์ พื้นที่จัดเก็บที่ไม่สามารถเปลี่ยนแปลงได้ (Immutable Storage) สามารถนำไปสร้างระบบใหม่ (Rebuild) ได้อย่างสมบูรณ์แบบ

หากการทดสอบล้มเหลว ถือว่าสำเนาชุดนั้นมี **“ข้อผิดพลาด”** และต้องดำเนินการแก้ไขทันที

ความเกี่ยวข้องกับ Zero Trust

เป็นการประยุกต์ใช้หลักการ **“ตรวจสอบเสมอ (Always Verify)”** ของ Zero Trust เข้ากับกระบวนการกู้คืนโดยตรง

Zero Trust คือ การตรวจสอบทุกการเข้าถึง ๓-๒-๑-๑-๐ คือการ **ตรวจสอบทุกสำเนา**

การยืนยันว่าข้อมูลสำรอง “สะอาด” และ “ใช้งานได้” คือ ไม่เชื่อถือว่ากระบวนการสำรองจะสมบูรณ์แบบเสมอไป แต่ต้องมีการ **“พิสูจน์”** ด้วยการทดสอบจริงก่อนทุกครั้ง

๒.๖ แนวทางปฏิบัติ มาตรฐาน และกรอบการทำงานระหว่างประเทศ

Zero Trust ไม่ได้เป็นมาตรฐานใหม่ที่แยกจากแนวทางปฏิบัติ มาตรฐาน และกรอบการทำงาน แต่เป็นกลยุทธ์ ที่ถูกนำมาใช้เพื่อบังคับใช้และเสริมสร้างมาตรการควบคุม (Controls) ในมาตรฐานสากลที่มีอยู่เดิมได้อย่างเข้มงวดและต่อเนื่อง

๒.๖.๑ เอกสารรากฐานและสถาปัตยกรรม (Foundational Document and Architecture)

NIST Special Publication 800-207 "Zero Trust Architecture" เอกสารนี้คือรากฐานที่กำหนดนิยาม "Zero Trust Architecture (ZTA)" อย่างเป็นทางการ และกำหนด ๗ หลักการ (Tenets) และ องค์ประกอบเชิงตรรกะ (Logical Components) ที่สำคัญ

สถานะ "De facto Standard": แม้ NIST จะเป็นหน่วยงานของสหรัฐฯ แต่เอกสารนี้ได้รับการยอมรับและอ้างอิงจากผู้ผลิต องค์กร และรัฐบาลทั่วโลก จนมีสถานะเป็น "มาตรฐานโดยพฤตินัย"

(De facto Standard) สำหรับสถาปัตยกรรม Zero Trust ความจำเป็นในการคงไว้ในแนวทางปฏิบัติเนื่องจาก ณ ปี ๒๕๖๘ ISO/IEC ยังไม่มีมาตรฐานเฉพาะ ที่กำหนดสถาปัตยกรรม Zero Trust ที่เทียบเท่าโดยตรง การอ้างอิง NIST SP 800-207 จึงเป็นสิ่งจำเป็นเพื่อประกันว่าแนวทางปฏิบัติระดับชาติสอดคล้องกับเกณฑ์มาตรฐานอุตสาหกรรมระดับโลก

๒.๖.๒ การบูรณาการ Zero Trust เข้ากับมาตรฐานระบบการจัดการ (Management Systems)

Zero Trust ทำหน้าที่เป็นกลไกสำคัญในการนำมาตรฐานระบบการจัดการมาปฏิบัติใช้จริง ISO/IEC 27001 (ISMS): Zero Trust เป็นกลยุทธ์ในการนำ ISMS มาปฏิบัติ โดย Zero Trust ควรถูกจัดประเภทเป็นมาตรการลดความเสี่ยง (Risk Mitigation) ต่อภัยคุกคามหลักในองค์กร เช่น มัลแวร์เรียกค่าไถ่ หรือภัยคุกคามจากคนภายใน

ISO/IEC 27002:2022 (Information Security Controls): Zero Trust ช่วยบังคับใช้มาตรการควบคุมที่สำคัญอย่างเข้มงวด เช่น A.5.15 (Access Control), A.8.3 (Information access restriction) และ A.8.5 (Secure authentication)

ISO/IEC 27005 (Risk Management): การกำกับดูแล Zero Trust (Zero Trust Governance) และการจัดการความเสี่ยง (Risk Management) ต้องบูรณาการเข้ากับกระบวนการบริหารความเสี่ยง โดย Zero Trust เป็นมาตรการบรรเทาความเสี่ยง

ISO 22301 (BCM) และ ISO/IEC 20000-1 (ITSM): Zero Trust สนับสนุนความต่อเนื่องทางธุรกิจ (Business Continuity) และการจัดการบริการที่มั่นคงปลอดภัย โดยควบคุมการเข้าถึงระบบสำรองหรือระบบบริการที่สำคัญอย่างเข้มงวด

๒.๖.๓ กรอบการทำงานที่เกี่ยวข้องกับโดเมนเฉพาะทาง

ตารางที่ ๑๒ แสดงกรอบการทำงานที่เกี่ยวข้องกับโดเมนเฉพาะทาง

โดเมน (Domain)	มาตรฐาน/กรอบการทำงาน (Standard/Framework)	บทบาทของ Zero Trust
การคุ้มครองข้อมูลส่วนบุคคล	ISO/IEC 27701 (PIMS)	Zero Trust ช่วยบังคับใช้การกำหนดสิทธิเท่าที่จำเป็นและจำกัดตามความจำเป็นของงาน เพื่อปกป้องข้อมูลส่วนบุคคล
ความมั่นคงปลอดภัยคลาวด์	ISO/IEC 27017, Cloud Security Alliance (CSA)	Zero Trust จัดให้มีการควบคุมการเข้าถึงที่เข้มงวดแก่ทรัพยากรบนคลาวด์ โดยไม่เชื่อถือขอบเขตเครือข่าย

โดเมน (Domain)	มาตรฐาน/กรอบการทำงาน (Standard/Framework)	บทบาทของ Zero Trust
ความมั่นคงปลอดภัย AI	ISO/IEC 42001 (AIMS)	Zero Trust ช่วยรักษาความมั่นคงปลอดภัยของ โมเดล AI และข้อมูล โดยการควบคุมการเข้าถึงตามนโยบาย
การกำกับดูแล	ISO 38500, COBIT และ ISO 31000	Zero Trust เป็นกลยุทธ์เชิงเทคนิคที่ถูกขับเคลื่อนโดยกระบวนการกำกับดูแลและการจัดการความเสี่ยงเหล่านี้

๒.๖.๔ แนวทางปฏิบัติและกฎหมายระหว่างประเทศที่เกี่ยวข้อง

GDPR (EU): Zero Trust เป็นเครื่องมือสำคัญในการบังคับใช้หลักการความเป็นส่วนตัวโดยการออกแบบ (Privacy by Design) เพื่อปฏิบัติตามข้อกำหนดทางเทคนิคของการปกป้องข้อมูล

NIS2 Directive (EU) และ ENISA: Zero Trust เสริมสร้างความยืดหยุ่น (Resilience) และความมั่นคงปลอดภัยของโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure: CII)

Zero Trust Maturity Model (ZTMM)[๓]: ZTMM (เช่น ของ CISA) ถูกใช้เป็นเครื่องมือในการประเมินระดับความพร้อมขององค์กรในการนำ Zero Trust ไปใช้ โดยแบ่งการประเมินออกเป็น ๕ เสาหลัก คือ ตัวตน อุปกรณ์ เครือข่าย แอปพลิเคชันและเวิร์กโหลด และข้อมูล

๒.๗ แนวทางปฏิบัติและกฎหมายที่เกี่ยวข้องในประเทศไทย (Related Guidelines and Regulations in Thailand)

การนำ Zero Trust มาใช้ในประเทศไทยเป็นกลยุทธ์สำคัญที่สนับสนุนการปฏิบัติตามกฎหมายหลักของประเทศ และข้อกำหนดของหน่วยงานกำกับดูแลเฉพาะทาง (Sector Regulators) ในกลุ่มโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII)

๒.๗.๑ กฎหมายความมั่นคงปลอดภัยพื้นฐานของประเทศ

ตารางที่ ๑๓ แสดงกฎหมายความมั่นคงปลอดภัยพื้นฐานของประเทศ

ชื่อกฎหมาย/ข้อกำหนด	หลักการที่เกี่ยวข้องกับ Zero Trust	บทบาทของ Zero Trust ในการสนับสนุน
พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒	การป้องกันและรับมือภัยคุกคามไซเบอร์ต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) และการลดความเสี่ยง	Zero Trust เน้นการแบ่งส่วนเครือข่ายแบบย่อย เพื่อควบคุมการโจมตีแบบการเคลื่อนตัวในเครือข่าย ทำให้การป้องกัน CII มีความยืดหยุ่นสูงขึ้น
พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (PDPA)	กำหนดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสมเพื่อปกป้องข้อมูลส่วนบุคคล	Zero Trust บังคับใช้หลักการกำหนดสิทธิเท่าที่จำเป็น และจำกัดตามความจำเป็นของงาน ในการควบคุมการเข้าถึงข้อมูลส่วนบุคคล
พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม	ป้องกันการเข้าถึงระบบ หรือข้อมูลโดยไม่ชอบ (Unauthorized Access)	โมเดลที่เน้นตัวตนเป็นศูนย์กลาง ช่วยเสริมการตรวจสอบ และการยืนยันตัวตนอย่างเข้มงวด ลดความเสี่ยงในการทำผิดตามมาตรา ๕-๗

๒.๗.๒ การเชื่อมโยงกับหน่วยงานกำกับดูแลด้านเทคโนโลยีดิจิทัล

ตารางที่ ๑๔ แสดงการเชื่อมโยงกับหน่วยงานกำกับดูแลด้านเทคโนโลยีดิจิทัล

หน่วยงานกำกับดูแล	ข้อกำหนด/แนวทางปฏิบัติที่เกี่ยวข้อง (ตัวอย่าง)	บทบาทของ Zero Trust ในการสนับสนุน
ETDA (สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์)	ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ (เช่น ขมธอ. ๒๐-๒๕๖๑ ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย การยืนยันตัวตน) และการกำกับดูแลธุรกิจบริการ Digital ID	Zero Trust ใช้ระดับความน่าเชื่อถือของการยืนยันตัวตน (Authentication Assurance Level: AAL) ที่กำหนดโดย ETDA เป็นข้อมูลหลัก (Data Source) สำหรับส่วนขับเคลื่อนนโยบายในการตัดสินใจให้สิทธิเข้าถึง
DGA (สำนักงานพัฒนารัฐบาลดิจิทัล)	มาตรฐานรัฐบาลดิจิทัล (ว่าด้วยการยืนยันตัวตน การกำหนดสิทธิและบัญชี	Zero Trust ช่วยบังคับใช้หลักการยืนยันตัวตน การตรวจสอบสิทธิ อย่าง

หน่วยงานกำกับดูแล	ข้อกำหนด/แนวทางปฏิบัติที่เกี่ยวข้อง (ตัวอย่าง)	บทบาทของ Zero Trust ในการสนับสนุน
	การใช้งาน) และมาตรฐานความมั่นคงปลอดภัยเว็บไซต์ภาครัฐ	ต่อเนื่อง และเข้มงวดสำหรับการเข้าถึงบริการและข้อมูลของภาครัฐ
NCSA (สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ)	คำแนะนำมาตรฐานการรักษาความมั่นคงปลอดภัยระบบคลาวด์[๗] และแนวทางการรักษาความมั่นคงปลอดภัยสำหรับปัญญาประดิษฐ์[๘]	Zero Trust เป็นกลไกสำคัญในการควบคุมการเข้าถึงทรัพยากรบนคลาวด์ และการปกป้องโมเดล AI และข้อมูลชุดฝึก (Training Data) ตามแนวทางของ สกมช.

๒.๗.๓ การเชื่อมโยงกับหน่วยงานกำกับดูแลเฉพาะทาง

ตารางที่ ๑๕ แสดงการเชื่อมโยงกับหน่วยงานกำกับดูแลเฉพาะทาง

หน่วยงานกำกับดูแล	ชื่อกฎหมาย/ข้อกำหนด/ประกาศที่เกี่ยวข้อง (ตัวอย่าง)	บทบาทของ Zero Trust ในการสนับสนุน
ธนาคารแห่งประเทศไทย (ธปท.)	ประกาศธนาคารแห่งประเทศไทย เรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและหนังสือเวียนด้านความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการควบคุมการเข้าถึง	การแบ่งส่วนเครือข่ายย่อยและการกำหนดสิทธิเท่าที่จำเป็น ช่วยให้สถาบันการเงินสามารถควบคุมการเข้าถึงระบบหลัก (Core Banking Systems) และข้อมูลลูกค้าได้อย่างเคร่งครัดตามข้อกำหนดของ ธปท.
สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (ก.ล.ต.) และตลาดหลักทรัพย์แห่งประเทศไทย (ตลท.)	ประกาศคณะกรรมการ ก.ล.ต. ว่าด้วยหลักเกณฑ์ เงื่อนไข และวิธีการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ และข้อกำหนดหรือประกาศของ ตลท. ที่เกี่ยวข้องกับการจัดการความเสี่ยงด้านสารสนเทศ	Zero Trust เสริมความมั่นคงปลอดภัยในการเข้าถึงระบบซื้อขายและข้อมูลนักลงทุน โดยเฉพาะการจำกัดสิทธิของบุคคลภายนอกและการทำธุรกรรมที่มีความสำคัญ
กระทรวงสาธารณสุข (สธ.)	พระราชบัญญัติสุขภาพแห่งชาติ พ.ศ. ๒๕๕๐ (มาตราที่เกี่ยวข้องกับการปกป้องข้อมูลสุขภาพ) และ PDPA	โมเดลที่เน้นแอปพลิเคชันเป็นศูนย์กลางช่วยให้มีการควบคุมการเข้าถึงข้อมูลประวัติผู้ป่วย (Protected Health Information:

หน่วยงานกำกับดูแล	ชื่อกฎหมาย/ข้อกำหนด/ประกาศที่เกี่ยวข้อง (ตัวอย่าง)	บทบาทของ Zero Trust ในการสนับสนุน
		PHI) ที่อ่อนไหวอย่างจำกัดสิทธิตามความจำเป็นของงาน
สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (กสทช.)	ประกาศ กสทช. ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของโครงข่ายโทรคมนาคม (โดยเฉพาะกลุ่ม CII) และข้อกำหนดด้านการปกป้องข้อมูลผู้ใช้บริการ	Zero Trust ช่วยรักษาความมั่นคงปลอดภัยของโครงสร้างพื้นฐานโทรคมนาคมผ่านการแบ่งส่วนเครือข่ายแบบย่อยและควบคุมการเข้าถึงข้อมูลส่วนบุคคลของผู้ใช้บริการ

๒.๘ การกำกับดูแลและการบริหารความเสี่ยงเฉพาะทางสำหรับ Zero Trust

การนำ Zero Trust มาปฏิบัติอย่างยั่งยืนและมีประสิทธิภาพในองค์กร จำเป็นต้องอาศัยกรอบการทำงาน GRC (Governance, Risk and Compliance) ที่ชัดเจน โดย Zero Trust ทำหน้าที่เป็นกลไกทางเทคนิคในการขับเคลื่อนหลักการเหล่านี้

๒.๘.๑ การกำกับดูแลและการบริหารจัดการ (Governance and COBIT, ISO 38500)

๑) การกำกับดูแล Zero Trust คือ การทำให้ผู้บริหารมั่นใจว่า Zero Trust สร้างมูลค่าและจัดการความเสี่ยงได้อย่างมีประสิทธิภาพ โดยอ้างอิงหลักการระดับสูง

๒) กรอบหลัก ใช้ ISO/IEC 38500 (Governance of IT) เป็นรากฐานในการกำกับดูแล โดยเน้นหลักการความรับผิดชอบ และประสิทธิภาพ

๒.๑) ความรับผิดชอบของผู้บริหาร ต้องรับผิดชอบสูงสุดในการอนุมัติกลยุทธ์ Zero Trust และกำหนดความเสี่ยงที่ยอมรับได้ (Risk Acceptance)

๓) การกำหนดวงจรชีวิตของนโยบาย ใช้ COBIT 2019[๙] ในการกำหนดวงจรชีวิตนโยบาย Zero Trust ที่ประกอบไปด้วย การจัดทำ การทดสอบ การประกาศใช้ (Enforce) การเฝ้าระวัง การปรับปรุงให้เหมาะสม เพื่อให้เกิดความต่อเนื่องและการกำกับดูแล

๒.๘.๒ การบริหารความเสี่ยงและการบูรณาการ (Risk Management and Integration)

การบริหารความเสี่ยง Zero Trust คือ การจัดให้ Zero Trust เป็นกลไกสำคัญในการควบคุมความเสี่ยงด้านความมั่นคงปลอดภัย โดยต้องบูรณาการเข้ากับระบบการจัดการความเสี่ยงที่มีอยู่

๑) การลดความเสี่ยง Zero Trust ต้องถูกจัดประเภทเป็นมาตรการลดความเสี่ยงที่สำคัญสำหรับภัยคุกคามหลักในองค์กร เช่น มัลแวร์เรียกค่าไถ่หรือภัยคุกคามจากบุคคลภายใน ตามแนวทาง ISO/IEC 27005 (Information Security Risk Management)

๒) การประเมินความเสี่ยงอย่างต่อเนื่อง (Continuous Risk Assessment) Zero Trust อาศัยการประเมินความเสี่ยงแบบเรียลไทม์กับผู้ใช้และอุปกรณ์ เช่น สถานะของอุปกรณ์ ในการตัดสินใจให้สิทธิการเข้าถึง ซึ่งสอดคล้องกับหลักการจัดการความเสี่ยงตามมาตรฐาน ISO 31000

๓) การจัดการเหตุการณ์ Zero Trust สนับสนุนกระบวนการจัดการเหตุการณ์โดยส่วนขับเคลื่อนนโยบายและจุดบังคับใช้นโยบายและมีการบันทึกเหตุการณ์การเข้าถึงทรัพยากรทั้งหมด ซึ่งใช้เป็นหลักฐานในการสืบสวนและตอบสนองต่อเหตุการณ์ไซเบอร์ ตามแนวทาง ISO/IEC 27035 (Information Security Incident Management)

๔) การบูรณาการกับ ISMS: Zero Trust เป็นกลยุทธ์ในการนำมาตรการควบคุมของ ISO/IEC 27001 (ISMS) และ ISO/IEC 27002 มาปฏิบัติใช้ โดยเฉพาะการควบคุมการเข้าถึง (Access Control)

๒.๘.๓ การปฏิบัติตามข้อกำหนดและการวัดผล (Compliance and Measurement)

การปฏิบัติตามข้อกำหนดเป็นสิ่งสำคัญในการกำกับดูแล Zero Trust เพื่อให้มั่นใจว่าการบังคับใช้นโยบาย Zero Trust สอดคล้องกับข้อกำหนดทางกฎหมายและมาตรฐาน

๑) กฎหมายและข้อบังคับ นโยบาย Zero Trust ต้องสอดคล้องกับการกำหนดสิทธิเท่าที่จำเป็นในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) และพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์[๖] (CII Protection)

๑.๑) การวัดผลการปกฎหมายและข้อบังคับ ใช้หลักการ COBIT ในการประเมินความสอดคล้องของการควบคุม Zero Trust กับข้อกำหนดทางกฎหมายอย่างสม่ำเสมอ

๒) การประเมินความพร้อมต้องใช้ Zero Trust Maturity Model (ZTMM) เพื่อประเมินระดับความพร้อมและความสมบูรณ์และกำหนดตัวชี้วัดความเสี่ยง (Key Risk Indicators: KRIs) ที่เชื่อมโยงกับ ๕ เสาหลักของ Zero Trust คือ ตัวตน อุปกรณ์ เครือข่าย แอปพลิเคชันและเวิร์กโหลด และข้อมูล

๓) การตรวจสอบ ต้องกำหนดให้มีกระบวนการตรวจสอบนโยบาย และการปฏิบัติงานอย่างสม่ำเสมอ โดยผู้ตรวจสอบจะทำการตรวจสอบว่าจุดบังคับใช้นโยบายของ Zero Trust ได้มีการบังคับใช้นโยบายตามที่ระบุไว้ในเอกสารกำกับดูแลหรือไม่

๒.๙ การกำหนดบทบาทและความรับผิดชอบ (Defining Roles and Responsibilities)

สถาปัตยกรรม Zero Trust เปลี่ยนกระบวนทัศน์จากการรักษาความมั่นคงปลอดภัยที่ขอบเขตไปสู่การควบคุมที่ทรัพยากรโดยตรง ดังนั้นการกำหนดบทบาทและความรับผิดชอบจึงต้องเปลี่ยนไป โดยเน้นการสร้างความรับผิดชอบในการกำหนดนโยบายการเข้าถึงแบบกำหนดสิทธิเท่าที่จำเป็น ให้แก่เจ้าของทรัพยากร การกำหนดบทบาทเหล่านี้เป็นไปตามหลักการกำกับดูแลและการบริหารความเสี่ยง ที่กล่าวถึงในหัวข้อ ๒.๘ และสอดคล้องกับมาตรฐาน ISO/IEC 27001:2022 (A.5.1 Roles and Responsibilities) ดังที่แสดงในตารางที่ ๑๖

ตารางที่ ๑๖ แสดงการกำหนดบทบาท และความรับผิดชอบ

ระดับ	บทบาทหลัก (Role)	ความรับผิดชอบหลักต่อ Zero Trust (Responsibility)	การอ้างอิงมาตรฐาน
ระดับกำกับดูแล (Governance Level)	คณะกรรมการและผู้บริหารระดับสูง (Executive Management/Board)	กำหนดทิศทาง และ ประเมินกลยุทธ์ Zero Trust อนุมัติการลงทุน และยอมรับความเสี่ยงคงเหลือ (Residual Risk)	ISO/IEC 38500, COBIT 2019 (EDM)
ระดับกลยุทธ์หรือนโยบาย (Strategy or Policy Level)	ผู้บริหารระดับสูงด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ (CISO) คณะกรรมการด้านความมั่นคงปลอดภัย และผู้บริหารระดับสูงด้านการรักษาความมั่นคงปลอดภัยและความเป็นส่วนตัว (CSPO)	พัฒนาสถาปัตยกรรม Zero Trust กำหนดนโยบายความมั่นคงปลอดภัย โดยรวม กำหนดเกณฑ์ความเสี่ยง (Risk Criteria) และวัดระดับความพร้อม และความสมบูรณ์ (ZTMM)	COBIT 2019 (APO), ISO/IEC 27001
ระดับเจ้าของ (Owner or Accountable)	เจ้าของข้อมูลและเจ้าของสินทรัพย์ (Data Owner and Asset Owner)	รับผิดชอบสูงสุด ในการกำหนดว่าใคร เมื่อใด และอย่างไร ที่จะสามารถเข้าถึงทรัพยากรของตนได้ ตามหลักการ ความจำเป็นของงาน และการกำหนดสิทธิเท่าที่จำเป็น	ISO/IEC 27001 (A.5.15)
ระดับปฏิบัติการ (Operational or Technical Level)	ผู้ดูแลระบบและเจ้าหน้าที่ฝ่ายไอที (System Administrator and IT Officer)	ติดตั้ง (Implementation) และบำรุงรักษา องค์ประกอบ Zero Trust หลัก เช่น การติดตั้งจุดบังคับใช้นโยบาย ผู้ให้บริการยืนยันตัวตน และการดำเนินการแบ่งส่วนเครือข่ายแบบย่อย	COBIT 2019 (BAI)

ระดับ	บทบาทหลัก (Role)	ความรับผิดชอบหลักต่อ Zero Trust (Responsibility)	การอ้างอิงมาตรฐาน
ระดับเฝ้าระวัง (Monitoring Level)	เจ้าหน้าที่ศูนย์ปฏิบัติการความมั่นคงปลอดภัยไซเบอร์ (SOC Team)	เฝ้าระวังอย่างต่อเนื่อง (Continuous Monitoring) และตอบสนองต่อเหตุการณ์ (Incident Response) โดยใช้ข้อมูลเหตุการณ์และการวิเคราะห์ข้อมูลจากหลายแหล่ง (Telemetry) ที่ถูกรวบรวมผ่านกลไก Zero Trust	ISO/IEC 27035

๒.๙.๑ บทบาทที่สำคัญในการเปลี่ยนผ่านสู่ Zero Trust

๑) การโอนถ่ายความรับผิดชอบ (Shift of Accountability) ความสำเร็จของ Zero Trust ขึ้นอยู่กับการโอนถ่ายความรับผิดชอบในการกำหนดสิทธิการเข้าถึงจากทีมไอทีและเครือข่าย ไปยังเจ้าของข้อมูล หรือเจ้าของสินทรัพย์ซึ่งเข้าใจความอ่อนไหวของข้อมูลอย่างแท้จริง

๒) การวัดผล (Measurement) บุคลากรในทุกระดับต้องมีบทบาทและส่วนร่วมและบทบาทในการประเมิน ZTMM เพื่อให้มั่นใจว่าการดำเนินการสอดคล้องกับกลยุทธ์ที่กำหนดโดย CISO หรือผู้บริหารระดับสูง

๒.๙.๒ RACI Matrix: การกำหนดบทบาทและความรับผิดชอบใน Zero Trust

ตารางที่ ๑๗ RACI นี้แสดงความรับผิดชอบในกระบวนการ Zero Trust ที่สำคัญ โดยเน้นการโอนถ่ายความรับผิดชอบไปสู่เจ้าของทรัพยากร

ตารางที่ ๑๗ แสดงการกำหนดบทบาทและความรับผิดชอบใน Zero Trust ตามโมเดล RACI

กระบวนการ Zero Trust ที่สำคัญ	เจ้าของข้อมูล (Data/Asset Owner)	ส่วนบริหารนโยบาย (IT Security)	ผู้บริหารระดับสูงด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ (CISO)	เจ้าหน้าที่ตรวจสอบการปฏิบัติตามข้อกำหนด (Compliance Officer / Auditor)	ผู้บริหารระดับสูง (Executive Management)	ผู้ใช้งาน (End-Users)
๑. การกำหนดข้อกำหนดนโยบายการเข้าถึง	A	R	C	C	I	I
๒. การติดตั้งและบังคับใช้นโยบาย	I	A	C	I	I	I
๓. การอนุมัติกลยุทธ์ Zero Trust และจัดสรรงบประมาณ	I	C	R	I	A	I
๔. การตรวจสอบและทบทวนนโยบาย	C	R	A	R	I	I
๕. การตอบสนองต่อเหตุการณ์	C	C	A	I	I	I
๖. การใช้การยืนยันตัวตนแบบหลายปัจจัย และรักษาสถานะของอุปกรณ์	I	C	I	I	I	R / A

คำจำกัดความสำหรับตาราง RACI

R (Responsible) ผู้ปฏิบัติงานจริง เพื่อให้ภารกิจสำเร็จ

A (Accountable) ผู้รับผิดชอบหลักต่อผลลัพธ์ (มีได้เพียงคนเดียว)

C (Consulted) ผู้ที่ต้องให้คำปรึกษาหรือข้อมูลก่อนการตัดสินใจ

I (Informed) ผู้ที่ต้องรับทราบผลลัพธ์หรือการดำเนินการหลังเสร็จสิ้นแล้ว

๒.๑๐ การสื่อสาร การฝึกอบรม และการสร้างวัฒนธรรมความมั่นคงปลอดภัย

การเปลี่ยนผ่านไปสู่ Zero Trust เป็นการเปลี่ยนแปลงทางวัฒนธรรมและความคิด (Mindset Shift) ที่สำคัญ จากการเชื่อถือในขอบเขตเครือข่ายเป็นการ “อย่าเชื่อทันที จงตรวจสอบเสมอ” การเปลี่ยนแปลงนี้จะไม่สำเร็จหากขาดการจัดการการเปลี่ยนแปลง (Change Management) ที่ดี ซึ่งสอดคล้องกับข้อกำหนดของ ISO/IEC 27001 (Clause 7.3 Awareness) และ ISO/IEC 27002 (A.6.3 Information Security Awareness, Education and Training)

๒.๑๐.๑ แผนการสื่อสาร

แผนการสื่อสารต้องถูกปรับให้เหมาะสมกับผู้รับสารแต่ละกลุ่ม เพื่อให้ผู้เกี่ยวข้องเข้าใจว่า Zero Trust จะส่งผลกระทบ และให้ประโยชน์ต่อการทำงานอย่างไร ดังที่แสดงในตารางที่ ๑๘

ตารางที่ ๑๘ แสดงแผนการสื่อสาร

กลุ่มเป้าหมาย (Target Audience)	จุดเน้นการสื่อสาร (Key Focus)	การเชื่อมโยงกับการกำกับดูแล
ผู้บริหารระดับสูง (Executive Management)	ทำไมต้องใช้ Zero Trust เน้นการเชื่อมโยง Zero Trust กับการลดความเสี่ยงทางธุรกิจ และการปฏิบัติตามกฎหมาย	รายงานความคืบหน้าของ ZTMM และผลกระทบต่อความเสี่ยงโดยรวม
ผู้ใช้งานทั่วไป (General Users)	วิธีการใช้งาน Zero Trust ในชีวิตประจำวัน เน้นการยืนยันตัวตนแบบหลายปัจจัย และผลกระทบของการเข้าถึงที่ถูกปฏิเสธเมื่ออุปกรณ์ไม่เป็นไปตามข้อกำหนด	เน้นบทบาทของผู้ใช้ในการเป็นจุดป้องกันด่านแรก
ทีมงานด้านเทคนิค (Technical Teams)	อะไร คือ การเปลี่ยนแปลงทางสถาปัตยกรรม และขั้นตอนการเปลี่ยนผ่าน เน้นบทบาทใหม่ในการบริหาร ขับเคลื่อนนโยบาย และบังคับใช้นโยบาย	การฝึกอบรมเชิงเทคนิค และการจัดการการเปลี่ยนแปลง

๒.๑๐.๒ แผนการฝึกอบรมแบบบูรณาการ (Integrated Training Roadmap)

แผนการฝึกอบรมต้องมีความแตกต่าง (Differentiated) ตามบทบาทและความรับผิดชอบ และบูรณาการเข้ากับระบบการจัดการอื่นๆ ขององค์กร ดังที่แสดงในตารางที่ ๑๙

ตารางที่ ๑๙ แสดงแผนการฝึกอบรมแบบบูรณาการ

กลุ่มเป้าหมาย	หัวข้อการฝึกอบรมหลัก (Key Training Topics)	การเชื่อมโยงกับมาตรฐาน/กฎหมาย
ผู้ใช้งานทั่วไป (General Users)	การสร้างความตระหนักรู้และทักษะแก่ผู้ใช้งาน (User Awareness Training): การยืนยัน	ISO/IEC 27002 (A.8.5) (Secure Authentication)

กลุ่มเป้าหมาย	หัวข้อการฝึกอบรมหลัก (Key Training Topics)	การเชื่อมโยงกับมาตรฐาน/กฎหมาย
	ตัวตนแบบหลายปัจจัย การรายงานภัยคุกคาม และการจัดการอุปกรณ์ให้มีความมั่นคงปลอดภัย	
เจ้าของนโยบายหรือเจ้าของข้อมูล (Policy Owners or Data Owners)	การฝึกอบรมด้านการกำหนดนโยบาย (Policy Definition Training): การทำความเข้าใจหลักการกำหนดสิทธิเท่าที่จำเป็น วิธีการกำหนดข้อกำหนดและนโยบายการเข้าถึงข้อมูลที่ละเอียดอ่อน	PDPA และ ISO/IEC 27701 (PIMS)
ทีมเทคนิคและศูนย์ปฏิบัติการความมั่นคงปลอดภัยไซเบอร์ (Technical and SOC Teams)	การอบรมเชิงเทคนิค (Technical Training) การกำหนดค่าส่วนขับเคลื่อนนโยบาย การตั้งค่าเครือข่ายย่อย และการวิเคราะห์เหตุการณ์ที่ได้จากจุดบังคับใช้นโยบาย	ISO/IEC 27035 (Incident Management) และ ISO/IEC 20000-1 (ITSM)

๒.๑๐.๓ การสร้างวัฒนธรรมด้านความมั่นคงปลอดภัย (Building a Security Culture)

การเปลี่ยนผ่านสู่ Zero Trust ต้องได้รับการสนับสนุนจากวัฒนธรรมองค์กร โดยเน้นหลักการสำคัญดังนี้

๑) การปรับเปลี่ยนกระบวนทัศน์กรอบแนวคิด Zero Trust ปลูกฝังแนวคิดที่ว่า “อย่าเชื่อทันทีจงตรวจสอบเสมอ” เพื่อให้เกิดการตรวจสอบทุกกิจกรรมที่เข้าถึงทรัพยากร

๒) วัฒนธรรมการตรวจสอบอย่างต่อเนื่อง (Culture of Continuous Verification) ส่งเสริมให้ผู้ใช้งานยอมรับว่าการถูกยืนยันตัวตนซ้ำ (Re-authentication) หรือการตรวจสอบสถานะของอุปกรณ์ (Device Checks) เป็นเรื่องปกติและจำเป็น

๓) วงจรป้อนกลับ (Feedback Loops) และปรับปรุงให้เหมาะสม (Optimization): สร้างกลไกให้ผู้ใช้งานสามารถรายงานความยุ่งยากหรือข้อผิดพลาดของนโยบาย Zero Trust ได้ เพื่อให้ส่วนบริหารนโยบายสามารถนำไปปรับปรุง ซึ่งเป็นส่วนหนึ่งของวงจรชีวิตนโยบาย Zero Trust

๔) การวัดผล ใช้ Zero Trust Maturity Model (ZTMM) ในการประเมินองค์ประกอบที่เกี่ยวข้องกับคน (People) เช่น อัตราการใช้งานการยืนยันตัวตนแบบหลายปัจจัยและความเร็วในการอัปเดตแพตช์อุปกรณ์ เพื่อสะท้อนการเปลี่ยนแปลงทางวัฒนธรรมและรายงานต่อผู้บริหารตามหลัก COBIT

๒.๑๐.๔ RACI Matrix: การสร้างวัฒนธรรมความมั่นคงปลอดภัย Zero Trust

ตารางที่ ๒๐ แสดงการสร้างวัฒนธรรมความมั่นคงปลอดภัย Zero Trust ตามโมเดล RACI

กระบวนการ Zero Trust ที่สำคัญ	ผู้บริหารระดับสูงด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ (CISO)	ฝ่ายทรัพยากรบุคคล / ฝ่ายการเรียนรู้และพัฒนาบุคลากร (HR / Learning & Dev.)	ส่วนบริหารนโยบาย/ IT Security	เจ้าหน้าที่ตรวจสอบการปฏิบัติตามข้อกำหนด (Compliance Officer)	ผู้บริหารระดับสูง (Executive Management)	ผู้ใช้งาน (End-Users)
๑. การกำหนดแผนแม่บทการฝึกอบรม (Training Roadmap)	A (อนุมัติกลยุทธ์)	R (ดำเนินการจัดทำ)	C (ให้ข้อมูลเทคนิค)	C (ด้านกฎหมาย/ PDPA)	I	I
๒. การจัดทำแผนการสื่อสาร (Communication Plan)	A	R	C	C	I	I
๓. การดำเนินการฝึกอบรมด้านความตระหนักรู้ (User Awareness)	C	A	R (เนื้อหาเทคนิค)	C	I	R
๔. การประเมินความตระหนัก	A	R	C	C (ด้านความสอดคล้อง)	I	R
๕. การบูรณาการกรอบแนวคิด Zero Trust เข้ากับวัฒนธรรม	A	R	C	I	C (ให้การสนับสนุน)	I

คำจำกัดความสำหรับตาราง RACI

R (Responsible) ผู้ปฏิบัติงานจริง เพื่อให้ภารกิจสำเร็จ

A (Accountable) ผู้รับผิดชอบหลักต่อผลลัพธ์ (มีได้เพียง ๑ ราย)

C (Consulted) ผู้ที่ต้องให้คำปรึกษาหรือข้อมูลก่อนการตัดสินใจ

I (Informed) ผู้ที่ต้องรับทราบผลลัพธ์หรือการดำเนินการหลังเสร็จสิ้นแล้ว

๒.๑๑ การจัดการความเสี่ยงด้านอธิปไตยข้อมูลและข้อกำหนดทางกฎหมายนอกอาณาเขต

สถาปัตยกรรม Zero Trust ถูกนำมาใช้เป็นกลยุทธ์หลักในการรักษา**อธิปไตยข้อมูล (Data Sovereignty)** และ**ความยืดหยุ่นทางไซเบอร์ (Cyber Resilience)** สำหรับข้อมูล ระบบ หรือบริการที่มีความสำคัญอย่างยิ่ง เพื่อป้องกันผลกระทบจากการเข้าถึงหรือระงับการให้บริการโดยอำนาจทางกฎหมายของต่างประเทศ โดยมีแนวทางดำเนินการตามหลัก CIA Triad และความเป็นส่วนตัว แสดงในตารางที่ ๒๑ และมีรายละเอียดดังนี้

๑. การรักษาความลับ (Confidentiality) และความเป็นส่วนตัว

การถือครองกุญแจรหัสด้วยตนเอง (Hold Your Own Key: HYOK): องค์กรต้องเข้ารหัสข้อมูลก่อนจัดเก็บบนคลาวด์และบริหารจัดการกุญแจเข้ารหัส (Encryption Keys) สำหรับอุปกรณ์ที่ควบคุมเองและตั้งอยู่ในประเทศ เพื่อประกันว่าข้อมูลจะยังคงเป็นความลับแม้ผู้ให้บริการคลาวด์จะถูกบังคับด้วยกฎหมายให้ส่งมอบข้อมูล

การกระจายเขตอำนาจศาล (Diversified Jurisdiction): เลือกใช้สถาปัตยกรรมหลายคลาวด์ (Multi-Cloud) โดยกระจายข้อมูลไปยังผู้ให้บริการที่อยู่ภายใต้เขตอำนาจศาลที่แตกต่างกัน เพื่อลดความเสี่ยงจากการถูกกระบวนการทางกฎหมายชุดเดียวกันบังคับใช้ทั้งหมด

การบังคับใช้นโยบายแบบให้สิทธิเท่าที่จำเป็น (Least Privilege): บังคับใช้การเข้าถึงข้อมูลส่วนบุคคล ตามหลักการ “ความจำเป็นของงาน” (Need-to-know) และ “จำกัดเวลา” (Time-Bound) เพื่อให้สอดคล้องกับ PDPA และลดโอกาสที่ข้อมูลจะถูกเข้าถึงโดยไม่ได้รับอนุญาตในวงกว้าง

๒. การรักษาความถูกต้องของข้อมูล (Integrity)

การตรวจสอบสถานะของอุปกรณ์และความสมบูรณ์ (Continuous Verification) ใช้กลไก Zero Trust ตรวจสอบว่าข้อมูลและแอปพลิเคชันบนคลาวด์ไม่ถูกเปลี่ยนแปลงหรือแก้ไขโดยไม่ได้รับอนุญาต ไม่ว่าจะจากมัลแวร์หรือเจ้าหน้าที่ของผู้ให้บริการที่มีสิทธิสูง (Privileged Users)

การบันทึกหลักฐานดิจิทัลที่เปลี่ยนแปลงไม่ได้ (Immutable Logging) ใช้ระบบ SIEM บันทึกเหตุการณ์การเข้าถึงทั้งหมดเพื่อใช้เป็นหลักฐานในการสืบสวน และยืนยันความถูกต้องของข้อมูลตามแนวทาง ISO/IEC 27037/27043

๓. การรักษาความพร้อมใช้งาน (Availability) และความต่อเนื่องของกระบวนการ

การวางแผนรับมือการระงับการประมวลผล (Process Redundancy) วางแผนให้เวิร์กโหลดสำคัญสามารถย้ายไปประมวลผลบนผู้ให้บริการรายอื่น (Alternative CSP) ได้ทันทีหากรายแรกถูกสั่งระงับการให้บริการ (Process Suspension) โดยอำนาจกฎหมายต่างชาติ เพื่อให้ธุรกิจดำเนินต่อไปได้อย่างไร้รอยต่อ (Business Continuity Management: BCM)

หลักการสำรองข้อมูล ๓-๒-๑-๑-๐ (Data Resiliency) มี ๑ สำเนาที่แยกส่วน (Air-Gapped/Isolated) ต้องมีอย่างน้อย ๑ ชุดที่เก็บแบบออฟไลน์ภายใต้เขตอำนาจศาลไทย เพื่อเป็น “ปราการสุดท้าย”

“๐” ข้อผิดพลาด (Zero Errors) ทดสอบการกู้คืนโดยอัตโนมัติเพื่อให้มั่นใจว่าข้อมูลสำรองสามารถนำกลับมาใช้บนระบบใหม่ได้ทันทีหากระบบบนคลาวด์หลักล้มเหลว

ตารางที่ ๒๑ สรุปการดำเนินการตามหลัก Confidentiality Integrity and Availability และความเป็นส่วนตัว

เป้าหมาย	แนวทางการดำเนินการ (Actions)	ผลลัพธ์ต่อความเสี่ยงกฎหมายต่างชาติ
การรักษาความลับและความเป็นส่วนตัว	การถือครองกุญแจรหัสด้วยตนเอง สถาปัตยกรรมแบบหลายคลาวด์ (ภายใต้เขตอำนาจศาลที่แตกต่าง) การปกปิดข้อมูล	ป้องกันการถอดรหัสและการเข้าถึงข้อมูลโดยอาศัยอำนาจนอกอาณาเขต
การรักษาความถูกต้องของข้อมูล	ระบบจัดการความมั่นคงปลอดภัยเชิงต่อเนื่อง การบันทึกหลักฐานดิจิทัลที่แก้ไขไม่ได้	มั่นใจว่าข้อมูลไม่ถูกแอบแก้ไขหรือแทรกแซงจากภายนอก
การรักษาความพร้อมใช้	ระบบสำรองเวิร์กโหลดข้อมูลผู้ให้บริการคลาวด์ (Multi-Cloud Workload Failover) หลักการสำรองข้อมูล ๓-๒-๑-๑-๐	ประกันความต่อเนื่องแม้ถูกสั่งระงับการให้บริการหรือถูกโจมตีด้วยมัลแวร์เรียกค่าไถ่ (Ransomware)

เอกสารอ้างอิง

๑) S. Rose, O. Borchert, S. Mitchell, and S. Connelly, “Zero Trust Architecture”, NIST Special Publication 800-207, 2020.

๒) Gartner Research, "Defining SASE (Secure Access Service Edge)" and "SSE (Security Service Edge)".

๓) Cybersecurity and Infrastructure Security Agency (CISA), *Zero Trust Maturity Model*, Version 2.0, 2023.

๔) ISO/IEC, “ISO/IEC 27002:2022 — Information security, cybersecurity and privacy protection Information security controls” 2022.

๕) Thailand, Personal Data Protection Act 2019, Royal Thai Government Gazette, 2019.

๖) Thailand, Cybersecurity Act 2019, Royal Thai Government Gazette, 2019.

๗) National Cyber Security Agency (NCSA), “Cybersecurity Standards for Cloud Systems,” Notification of National Cyber Security Committee, 2024.

๘) National Cyber Security Committee (NCSC)/National Cyber Security Agency (NCSA), “Guideline for the Security of Artificial Intelligence,” National Cyber Security Committee Notification, 2025.

๙) ISACA, “COBIT 2019 Framework: Governance and Management Objectives,” ISACA, 2019.

๑๐) ISO/IEC, “ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection — Information security management systems,” 2022.

บทที่ ๓
แนวทางการเปลี่ยนผ่านสู่ Zero Trust และการดำเนินงานระบบ Zero Trust

๓.๑ แนวทางปฏิบัติในการติดตั้งและนำไปใช้งานระบบ Zero Trust แบบ ๕ ขั้นตอน

การเปลี่ยนผ่านสู่สถาปัตยกรรม Zero Trust อย่างเป็นระบบและบรรลุผลสำเร็จ จำเป็นต้องอาศัยแนวทางการดำเนินงานที่ชัดเจน การกำหนดกรอบการดำเนินงานแบ่งเป็น ๕ ขั้นตอน[๓] เป็นแนวทางเพื่อสนับสนุนให้องค์กรสามารถยกระดับความมั่นคงปลอดภัยไซเบอร์ได้อย่างเป็นรูปธรรมและยั่งยืน

ขั้นตอนที่ ๑ การกำหนดพื้นที่ป้องกัน (Protect Surface) และวางกลยุทธ์ที่อิงตามความเสี่ยง

ขั้นตอนนี้มีวัตถุประสงค์เพื่อปรับเปลี่ยนแนวคิดจากการมุ่งเน้นการตอบสนองภัยคุกคามไปสู่การให้ความสำคัญกับการระบุและปกป้องสินทรัพย์ที่มีความสำคัญหรือที่มีความละเอียดอ่อนสูงขององค์กรเป็นลำดับแรก องค์กรต้องดำเนินการระบุ จัดประเภท และจัดทำเอกสารพื้นที่ป้องกันอย่างชัดเจน เพื่อใช้เป็นข้อมูลอ้างอิงพื้นฐานในการออกแบบและบังคับใช้มาตรการ Zero Trust ในขั้นตอนถัดไป

ขั้นตอนการกำหนดพื้นที่ป้องกัน โดยทั่วไปประกอบด้วยองค์ประกอบหลัก ๔ ด้าน เรียกว่า DAAS ได้แก่ ข้อมูล แอปพลิเคชัน สินทรัพย์ และบริการ โดยมีรายละเอียดดังนี้

ข้อมูล ข้อมูลสำคัญและข้อมูลอ่อนไหว เช่น ข้อมูลบัตรที่ใช้ในการชำระเงิน (Payment Card Industry Data: PCI Data) ข้อมูลสุขภาพ (Protected Health Information: PHI) ข้อมูลส่วนบุคคลที่สามารถใช้ระบุตัวตนได้ (Personally Identifiable Information: PII) ทรัพย์สินทางปัญญา (Intellectual Property: IP) ซึ่งหากถูกละเมิดหรือรั่วไหลอาจสร้างความเสียหายอย่างรุนแรง

แอปพลิเคชัน ซอฟต์แวร์ที่มีปฏิสัมพันธ์กับข้อมูลอ่อนไหวหรือทำหน้าที่ควบคุมสินทรัพย์และกระบวนการที่สำคัญทางธุรกิจ เช่น ระบบบริหารจัดการความสัมพันธ์ลูกค้า ระบบบริหารกระบวนการทางธุรกิจ (Business Process Management System)

สินทรัพย์ อุปกรณ์ด้านเทคโนโลยีสารสนเทศ (IT) อุปกรณ์เทคโนโลยีเชิงปฏิบัติการ (OT) หรืออุปกรณ์ IoT เช่น เครื่องรับชำระเงิน ณ จุดขาย (Point of Sale: POS) ระบบควบคุมและเก็บข้อมูลอุตสาหกรรม (SCADA) อุปกรณ์การแพทย์ที่เชื่อมต่อเครือข่าย

บริการ บริการโครงสร้างพื้นฐาน (Infrastructure Services) และโปรโตคอลที่สำคัญต่อการดำเนินงาน เช่น ระบบชื่อโดเมน (Domain Name System: DNS) โปรโตคอลการกำหนดค่าโฮสต์แบบไดนามิก (Dynamic Host Configuration Protocol: DHCP) แอคทีฟไดเรกทอรี (Active Directory: AD) โปรโตคอลเวลาของเครือข่าย (Network Time Protocol: NTP)

เพื่อให้การปรับใช้ Zero Trust เป็นไปอย่างมีประสิทธิภาพ องค์กรควรให้ความสำคัญกับปัจจัยหลัก ๒ ประการ ได้แก่ การกำหนดพื้นที่ป้องกันที่ชัดเจน และการบริหารจัดการระยะเวลาของการเปลี่ยนผ่านสู่ Zero Trust ซึ่งควรถูกออกแบบให้เป็นกระบวนการที่ดำเนินไปอย่างต่อเนื่องและสามารถปรับเปลี่ยนได้ตามบริบทขององค์กร การจำแนกประเภทข้อมูล (Data Classification) ถือเป็น

จุดเริ่มต้น ที่มีความสำคัญอย่างยิ่ง โดยองค์กรควรเริ่มจากพื้นที่ป้องกันที่มีข้อมูลสำคัญต่ำ หรือมีความอ่อนไหวน้อย เช่น สภาพแวดล้อมสำหรับการพัฒนา (Development) สภาพแวดล้อมสำหรับการทดสอบเพื่อการยอมรับโดยผู้ใช้ (User Acceptance Testing) หรือระบบที่ไม่สำคัญต่อการดำเนินงานหลัก (Non-Production) เพื่อเปิดโอกาสให้สามารถทดสอบ ปรับปรุงกระบวนการและเรียนรู้ข้อจำกัด โดยไม่ก่อให้เกิดผลกระทบต่อธุรกิจ

เมื่อเกิดความเข้าใจและความมั่นใจในแนวทางการดำเนินงานแล้ว องค์กรจึงควรขยายขอบเขตการดำเนินงานไปยังพื้นที่ป้องกันที่มีข้อมูลสำคัญสูงและมีความอ่อนไหวสูงขึ้นตามลำดับ ทั้งนี้ควรหลีกเลี่ยงการเริ่มต้นกับสินทรัพย์ที่มีความสำคัญหรือมีข้อมูลสำคัญสูงสุด (Most Critical Assets) ในระยะแรก เพื่อจำกัดความเสี่ยงและผลกระทบที่อาจเกิดขึ้น แนวทางการดำเนินงานแบบค่อยเป็นค่อยไป (Phased Approach) ดังกล่าว ช่วยสร้างความชัดเจนและความเชื่อมั่นในการประยุกต์ใช้หลักการ Zero Trust ก่อนการขยายไปยังข้อมูล ระบบที่มีความสำคัญ ระบบที่มีความอ่อนไหวสูงขึ้นฯลฯ จนครอบคลุมองค์ประกอบสำคัญทั้งหมด เพื่อสร้างสภาพแวดล้อม Zero Trust ที่สมบูรณ์และยั่งยืนในระยะยาว

ขั้นตอนที่ ๒ การจัดทำแผนผังแสดงลำดับขั้นตอนของธุรกรรม (Transaction Flows)

วัตถุประสงค์ของขั้นตอนนี้เพื่อการทำให้องค์กรและผู้มีส่วนเกี่ยวข้องเข้าใจการทำงานของระบบในเชิงลึก โดยเฉพาะการปฏิสัมพันธ์ระหว่างองค์ประกอบของพื้นที่ป้องกันในมุมมองของความมั่นคงปลอดภัยไซเบอร์โดยรวม องค์กรควรจัดทำแผนผังแสดงลำดับขั้นตอนของธุรกรรมสำหรับแต่ละพื้นที่ป้องกัน เพื่อแสดงให้เห็นว่าองค์ประกอบของข้อมูล แอปพลิเคชัน สินทรัพย์ และบริการมีการสื่อสารและเชื่อมโยงกันอย่างไรในกระบวนการทำงานของระบบ

แผนผังแสดงลำดับขั้นตอนของธุรกรรมดังกล่าวมีบทบาทสำคัญในการอธิบายรูปแบบการทำงานของระบบ และใช้เป็นข้อมูลพื้นฐานในการระบุตำแหน่งที่เหมาะสมสำหรับการกำหนด และบังคับใช้มาตรการควบคุมด้านความมั่นคงปลอดภัย (Security Controls) เพื่อปกป้องข้อมูลและทรัพยากรที่สำคัญ ซึ่งถือเป็นพื้นฐานที่สำคัญต่อการออกแบบสถาปัตยกรรม Zero Trust โดยรวมเมื่อจัดทำแผนผังแสดงลำดับขั้นตอนของธุรกรรมเสร็จสมบูรณ์แล้ว องค์กรควรดำเนินการจัดลำดับความสำคัญของธุรกรรมแต่ละรายการ เนื่องจากมีผลโดยตรงต่อการกำหนดสิทธิการเข้าถึงและเงื่อนไขต่าง ๆ ภายในสถาปัตยกรรม Zero Trust โดยพิจารณาจากทรัพยากรที่มีอยู่ เช่น บุคลากร เวลา งบประมาณ และเทคโนโลยี ควบคู่กับระดับความสำคัญและความอ่อนไหวของข้อมูลที่เกี่ยวข้อง เพื่อให้การจัดสรรทรัพยากรถูกมุ่งเน้นไปยังจุดที่มีความเสี่ยงสูงและส่งผลกระทบต่อธุรกิจมากที่สุดเป็นลำดับต้น ทั้งนี้เพื่อให้การเปลี่ยนผ่านเป็นไปอย่างราบรื่น องค์กรควรเริ่มต้นจากกระบวนการทางธุรกิจที่มีความเสี่ยงต่ำ หรือมีผลกระทบต่อการดำเนินงานในระดับจำกัด ก่อนขยายขอบเขตไปยังกระบวนการที่มีระดับความสำคัญสูงขึ้นตามลำดับ

ขั้นตอนที่ ๓ การสร้างสถาปัตยกรรม Zero Trust

การนำสถาปัตยกรรม Zero Trust ไปใช้งานโดยเริ่มจากการกำหนดพื้นที่ป้องกัน เป็นกระบวนการที่ต้องอาศัยทั้งการปรับเปลี่ยนโครงสร้างพื้นฐานด้านเทคโนโลยี และการปรับปรุงกระบวนการดำเนินงานที่มีอยู่เดิมขององค์กรให้สอดคล้องกับหลักการของ Zero Trust อย่างเป็นรูปธรรม

การออกแบบระบบรักษาความมั่นคงปลอดภัยพื้นที่ป้องกันควรครอบคลุมกิจกรรมสำคัญ ได้แก่ การจัดทำแผนผังแสดงลำดับขั้นตอนของธุรกรรม การกำหนดมาตรการควบคุมความมั่นคงปลอดภัย และการกำหนดพื้นที่ป้องกันรอง (Secondary Protect Surfaces) รวมถึงการออกแบบระบบหรือแนวทางที่เหมาะสมสำหรับการนำไปใช้งานจริงในขั้นตอนสุดท้าย ซึ่งทั้งหมดนี้เป็นองค์ประกอบพื้นฐานของการออกแบบสถาปัตยกรรม Zero Trust

ในสภาพแวดล้อมปัจจุบันขององค์กร การเปลี่ยนผ่านไปสู่สถาปัตยกรรม Zero Trust โดยอาศัยการปรับเปลี่ยนเทคโนโลยีทั้งหมดเพียงครั้งเดียวอาจไม่เหมาะสม องค์กรจึงจำเป็นต้องปรับปรุงกระบวนการดำเนินงานเดิมให้สอดคล้องกับหลักการของ Zero Trust ควบคู่ไปกับการปรับใช้เทคโนโลยีให้เหมาะสม แม้การเปลี่ยนแปลงในบางส่วนจะเป็นเพียงการปรับเปลี่ยนเพียงเล็กน้อย แต่สามารถช่วยเพิ่มประสิทธิภาพและลดความเสี่ยงในการดำเนินงานได้ ระดับและรูปแบบของการปรับเปลี่ยนขึ้นอยู่กับสถานะด้านความมั่นคงปลอดภัยไซเบอร์ และบริบทการดำเนินงานในปัจจุบันขององค์กร เพื่อให้สามารถออกแบบและดำเนินการสถาปัตยกรรม Zero Trust ได้อย่างเหมาะสม องค์กรจำเป็นต้องมีความเข้าใจอย่างชัดเจนเกี่ยวกับองค์ประกอบหลัก ดังต่อไปนี้

๑) สินทรัพย์ขององค์กร ทั้งในรูปแบบทางกายภาพและเสมือน

๒) บุคลากรที่เกี่ยวข้อง รวมถึงบทบาทและสิทธิการเข้าถึง

๓) กระบวนการทางธุรกิจที่มีความสำคัญต่อองค์กร

แม้ว่าพื้นที่ป้องกันที่มีสินทรัพย์สำคัญหรือมีข้อมูลที่มีความอ่อนไหวสูงสุดจะเป็นบริเวณที่ต้องการการป้องกันตามหลัก Zero Trust มากที่สุด และเป็นจุดที่ควรให้ความสำคัญ พื้นที่ดังกล่าวมักเกี่ยวข้องกับผู้มีส่วนได้ส่วนเสียหลายฝ่ายและต้องผ่านกระบวนการอนุมัติที่ซับซ้อน ซึ่งอาจทำให้การดำเนินงานใช้เวลานานและอาจส่งผลให้เกิดความเสี่ยง และผลกระทบทางธุรกิจ

ในมุมมองเชิงกลยุทธ์องค์กรควรให้ความสำคัญกับการสร้างความสำเร็จในระยะสั้น (Quick Wins) ก่อน เพื่อเสริมสร้างความเชื่อถือและการยอมรับภายในองค์กร โดยเริ่มจากพื้นที่ป้องกันที่ต้องการขั้นตอนการอนุมัติน้อย มีระยะเวลาในการดำเนินการสั้น หรือมีผลกระทบต่อธุรกิจในระดับต่ำ แนวทางดังกล่าวช่วยให้องค์กรสามารถเริ่มต้นจากสิ่งที่ดำเนินการได้ง่าย และเห็นผลลัพธ์ได้อย่างรวดเร็ว

อีกหนึ่งกลยุทธ์ที่สำคัญ คือ การพิจารณาพื้นที่ป้องกันที่สามารถพัฒนาเป็นบริการที่สามารถใช้ร่วมกัน (Shared Services) หรือสามารถนำเทคโนโลยีมารวมศูนย์ (Technology Centralization) ได้

เมื่อองค์กรสามารถดำเนินการในส่วนนี้ได้สำเร็จ จะช่วยลดระยะเวลาและเพิ่มประสิทธิภาพในการดำเนินงานในพื้นที่ป้องกันถัดไป

ตัวอย่างที่เห็นได้ชัดของการรวมศูนย์เทคโนโลยี คือ การรวมศูนย์ผู้ให้บริการยืนยันตัวตน (Identity Provider: IdP) โดยเฉพาะในองค์กรขนาดใหญ่ หรือองค์กรที่ยังมีระบบดั้งเดิม และมีแอปพลิเคชันจำนวนมาก ทั้งนี้แนวทางดังกล่าวหากทำสำเร็จสามารถสร้างประโยชน์ที่ชัดเจน ได้แก่

๑) การบริหารจัดการที่ง่ายขึ้น (Simplified Management)

๒) ประสบการณ์ของผู้ใช้งานที่ดีขึ้น (Improved User Experience)

๓) ความสามารถในการปฏิบัติตามกฎหมายและปฏิบัติตามข้อกำหนดที่ดีขึ้น (Improved Compliance)

กรอบการทำงานของ Zero Trust ไม่ได้ผูกติดกับเทคโนโลยีหรือแนวทางใดเป็นการเฉพาะ จึงเปิดโอกาสให้องค์กรสามารถเลือกและปรับใช้มาตรการด้านความมั่นคงปลอดภัยให้สอดคล้องกับความต้องการในการปกป้องสินทรัพย์ขององค์กรได้อย่างยืดหยุ่น การแบ่งส่วนเครือข่ายออกเป็นส่วนย่อยที่แยกจากกันอย่างชัดเจน เป็นหนึ่งในแนวทางสำคัญที่ช่วยจำกัดขอบเขตการเข้าถึง ลดผลกระทบจากเหตุการณ์ด้านความมั่นคงปลอดภัยและเพิ่มประสิทธิภาพในการควบคุมข้อมูลภายในองค์กร

โดยทั่วไปองค์กรสามารถนำแนวทางที่หลากหลายมาประยุกต์ใช้ในการออกแบบสถาปัตยกรรม Zero Trust โดยเลือกเน้นองค์ประกอบ กฎข้อบังคับ และนโยบายที่เหมาะสมกับบริบทขององค์กร แนวทางเหล่านี้อาจประกอบด้วย

๑) แนวทางการกำกับดูแลตัวตนขั้นสูง

๒) การแบ่งส่วนเครือข่าย

๓) การแบ่งส่วนเครือข่ายแบบย่อย

๔) การใช้บริการแบบคลาวด์

๕) แนวทางแบบผสมหรือไฮบริด

แนวทาง Zero Trust แบบครบวงจรมักประกอบด้วยหลายแนวทางร่วมกัน ระดับความเหมาะสมของแต่ละแนวทางขึ้นอยู่กับทิศทางเชิงกลยุทธ์ของธุรกิจและระดับความเสี่ยงที่องค์กรยอมรับได้ ซึ่งควรถูกนำมาพิจารณาในการออกแบบและเลือกแนวทางที่เหมาะสม ทั้งนี้การเลือกใช้แนวทางหนึ่งไม่ได้หมายความว่าแนวทางอื่นจะไม่สามารถนำมาใช้ร่วมกันได้ ในหลายกรณีแนวทางที่มีความท้าทายในการนำไปปฏิบัติมากกว่า อาจสอดคล้องกับเป้าหมายเชิงกลยุทธ์ระยะยาวขององค์กรได้ดีกว่า การประยุกต์ใช้ Zero Trust จึงอาจแตกต่างกันไปในแต่ละองค์กร โดยองค์กรสามารถเลือกปรับให้เหมาะสมกับกระบวนการทางธุรกิจที่แตกต่างกัน เพื่อให้การดำเนินงานเป็นไปตามหลักการ Zero Trust อย่างครอบคลุมและยั่งยืน

ขั้นตอนที่ ๔ การกำหนดนโยบาย Zero Trust

นโยบาย Zero Trust ถือเป็นรากฐานสำคัญของสถาปัตยกรรม Zero Trust ที่มีความมั่นคงปลอดภัย ในระยะเริ่มต้นนโยบายอาจมีลักษณะเป็นแบบสแตติก (Static) อย่างไรก็ตามนโยบายควรถูกออกแบบให้สามารถพัฒนาไปสู่รูปแบบไดนามิก (Dynamic) ได้ เพื่อให้สอดคล้องกับบริบทของการดำเนินงาน การเติบโตขององค์กร และการยกระดับสถาปัตยกรรม Zero Trust ให้มีความสมบูรณ์ยิ่งขึ้นในระยะยาว

เพื่อสนับสนุนการนำแนวคิด Zero Trust ไปปรับใช้ภายในองค์กรอย่างมีประสิทธิภาพ องค์กรควรใช้หลักการ ๕W๑H (Who, What, When, Where, Why, How) เป็นกรอบในการกำหนดนโยบาย แนวทางดังกล่าวช่วยให้สามารถกำหนดการควบคุมการเข้าถึงได้อย่างละเอียด และช่วยให้สามารถพิจารณาปัจจัยที่เกี่ยวข้องกับการเข้าถึงทรัพยากรแต่ละประเภทได้อย่างรอบด้าน อีกทั้งยังเอื้อต่อการจัดทำนโยบายและขั้นตอนปฏิบัติที่มีความชัดเจน และสอดคล้องกับบริบทของพื้นที่ป้องกันแต่ละส่วน

องค์ประกอบ ๕W๑H ในการสร้างนโยบาย Zero Trust

๑) Who (ใคร) ระบุตัวตนของผู้ที่ต้องการเข้าถึงทรัพยากร ไม่ใช่เพียงแค่ผู้ใช้ แต่รวมถึงอุปกรณ์ (Device) ทั้งนี้ต้องมีการยืนยันตัวตน และตรวจสอบสถานะอย่างต่อเนื่องตามบริบท (Continuous and Contextual Verification)

๒) What (อะไร) ระบุเป้าหมายหรือทรัพยากรที่ต้องการเข้าถึง เช่น ข้อมูล แอปพลิเคชัน หรือบริการ เพื่อกำหนดขอบเขตการเข้าถึงให้ชัดเจน

๓) When (เมื่อไร) กำหนดเงื่อนไขด้านเวลาหรือช่วงเวลาที่อนุญาตให้เข้าถึง เช่น เฉพาะเวลาทำการ หรือช่วงเวลาที่กำหนด เพื่อจำกัดความเสี่ยงจากการเข้าถึงที่ไม่จำเป็น

๔) Where (ที่ไหน) ระบุตำแหน่งที่อนุญาต เช่น เครือข่ายภายใน อุปกรณ์จากที่อยู่ไอพีที่กำหนดหรือขอบเขตทางภูมิศาสตร์ (Geo-Fencing) เพื่อป้องกันการเข้าถึงจากพื้นที่ที่มีความเสี่ยง

๕) Why (ทำไม) ระบุความจำเป็นทางธุรกิจ โดยยึดหลักให้สิทธิเท่าที่จำเป็นและสอดคล้องกับบทบาทหน้าที่

๖) How (อย่างไร) กำหนดวิธีการและมาตรการควบคุมทางเทคนิคที่ต้องบังคับใช้ เช่น การเชื่อมต่อแบบเข้ารหัส การยืนยันตัวตนแบบหลายปัจจัย หรือการบังคับใช้นโยบายด้านความมั่นคงปลอดภัยของอุปกรณ์ปลายทางเพื่อให้สอดคล้องกับระดับความเสี่ยง

ขั้นตอนที่ ๕ การเฝ้าระวังและบำรุงรักษาอย่างต่อเนื่อง

ตามกรอบ CISA: Zero Trust Maturity Model (ZTMM) องค์ประกอบด้านการมองเห็นและการวิเคราะห์ ถือเป็นปัจจัยสำคัญในการยกระดับและรักษาประสิทธิภาพของการดำเนินงานตามแนวคิด Zero Trust การรับรู้สถานะปัจจุบัน รวมถึงการปรับเปลี่ยนมาตรการด้านความมั่นคงปลอดภัยในแต่ละพื้นที่ป้องกันภายในเครือข่าย หรือสภาพแวดล้อมขององค์กรให้เหมาะสม เป็นพื้นฐานสำคัญในการตรวจจับและตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัย

การดำเนินงานในขั้นตอนนี้เกี่ยวข้องโดยตรงกับการบันทึกเหตุการณ์ การเฝ้าระวัง และการแจ้งเตือนอย่างทันท่วงที (Prompt Alerting) ซึ่งเป็นกลไกหลักในการสนับสนุนการปรับปรุงอย่างต่อเนื่อง (Continuous Improvement) และการจัดการเหตุการณ์อย่างเป็นระบบ โดยอาศัยวงจรป้อนกลับที่ชัดเจน การตรวจจับที่มีความแม่นยำ รวมถึงแผนการตอบสนองต่อเหตุการณ์ที่เหมาะสม จะช่วยให้องค์กรสามารถปรับปรุงนโยบาย Zero Trust ให้สอดคล้องกับสภาพแวดล้อมและภัยคุกคามที่เปลี่ยนแปลงอยู่เสมอ

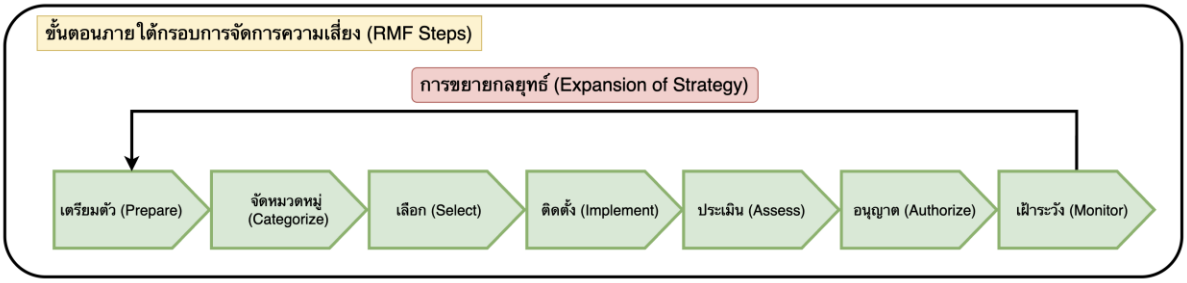
นอกจากนี้ องค์กรควรมีการทบทวนและปรับปรุงพื้นที่ป้องกัน รวมถึงนโยบาย Zero Trust อย่างสม่ำเสมอ เช่น ทุก ๆ ไตรมาส โดยการทบทวนควรครอบคลุมองค์ประกอบสำคัญ ได้แก่ ตัวตน อุปกรณ์ การเข้าถึง นโยบาย และพื้นที่ป้องกัน ที่เกี่ยวข้องทั้งหมด

ด้วยการเฝ้าระวังและขยายขอบเขตการป้องกันอย่างต่อเนื่อง องค์กรจะสามารถเสริมสร้างความมั่นคงปลอดภัยให้สูงขึ้น (Incremental Security) การกำกับดูแลอย่างต่อเนื่องนี้ไม่เพียงช่วยลดความเสี่ยงด้านความมั่นคงปลอดภัยเท่านั้น แต่ยังสนับสนุนการเพิ่มประสิทธิภาพการดำเนินงาน ความคล่องตัวในการเข้าถึงทรัพยากร และความยืดหยุ่นของระบบ ซึ่งส่งผลเชิงบวกต่อประสิทธิภาพในการทำงาน (Productivity) ขององค์กรโดยรวม

การสื่อสารผลการดำเนินการและคุณค่าที่ได้รับจากการลงทุนด้าน Zero Trust ต่อผู้บริหารระดับสูงอย่างสม่ำเสมอ เป็นปัจจัยสำคัญในการสร้างแรงผลักดัน และสนับสนุนกลยุทธ์ Zero Trust ในระยะยาว

๓.๒ การวิเคราะห์ช่องว่าง (Gap Analysis)

การวิเคราะห์ช่องว่างก่อนการนำ Zero Trust มาใช้จริง สามารถออกแบบให้สอดคล้องกับ “กรอบการจัดการความเสี่ยง (Risk Management Framework: RMF)”[๑] เพื่อให้การวิเคราะห์ช่องว่างครอบคลุมทั้งมิติด้านกลยุทธ์ การบริหารและจัดการความเสี่ยง และการดำเนินงานจริง โดยไม่จำกัดอยู่เพียงการเปรียบเทียบเทคโนโลยีที่มีอยู่กับเทคโนโลยีเป้าหมาย โดยรูปที่ ๔ แสดงขั้นตอนของ RMF ที่สามารถนำมาใช้เป็นแนวทางในการวิเคราะห์และวางแผนได้อย่างเป็นระบบ



รูปที่ ๔ แสดงขั้นตอนภายใต้กรอบการจัดการความเสี่ยง

ความพร้อมเชิงกลยุทธ์และการกำกับดูแล

ในขั้นตอนเตรียมตัว การวิเคราะห์ช่องว่างมุ่งเน้นไปที่การกำหนดจุดเริ่มต้นของ Zero Trust ในระดับองค์กร โดยพิจารณาว่า Zero Trust ถูกวางบทบาทเป็นสถาปัตยกรรมเชิงความเสี่ยง หรือเป็นเพียงโครงการด้านเทคนิค ช่องว่างในขั้นตอนนี้มักสะท้อนผ่านประเด็นสำคัญ เช่น

๑) การขาดกลยุทธ์ Zero Trust หรือแผนงานที่ชัดเจน

๒) การไม่กำหนดขอบเขตของระบบและภารกิจ หรือกระบวนการทางธุรกิจที่ต้องได้รับการปกป้องเป็นลำดับแรก

๓) การขาดการเชื่อมโยงกับผู้บริหารในการตัดสินใจด้านความเสี่ยง

หากช่องว่างในขั้นตอนเตรียมตัวไม่ได้รับการแก้ไข การติดตั้ง Zero Trust ในขั้นตอนต่อไปมักจะเกิดการขาดการเชื่อมโยง และไม่สามารถขยายผลในระดับองค์กรได้

การทำความเข้าใจสินทรัพย์ ข้อมูล และผลกระทบ

ในขั้นตอนจัดหมวดหมู่ ช่วยให้การวิเคราะห์ช่องว่างของ Zero Trust ในมุมมองที่มีข้อมูลและสินทรัพย์เป็นศูนย์กลางมากขึ้น โดยพิจารณาว่าการจัดหมวดหมู่ระบบและข้อมูลสะท้อนผลกระทบต่อภารกิจหรือไม่ ช่องว่างที่พบได้บ่อย เช่น

๑) การจัดระดับความสำคัญของระบบโดยไม่เชื่อมโยงกับผลกระทบทางธุรกิจ

๒) การขาดความเข้าใจเรื่องเส้นทางการไหลของข้อมูล และขอบเขตความน่าเชื่อถือ

๓) การมองว่าสินทรัพย์ทุกระบบในองค์กรมีระดับความเสี่ยงเดียวกัน

ช่องว่างในขั้นตอนนี้ส่งผลโดยตรงต่อความถูกต้องของนโยบาย Zero Trust เนื่องจากการตัดสินใจด้านความน่าเชื่อถือควรแตกต่างกันตามบริบทของทรัพยากร

ความสอดคล้องระหว่างหลักการ Zero Trust กับมาตรการควบคุม

ในขั้นตอนเลือก การวิเคราะห์ช่องว่างจะตรวจสอบว่ามาตรการควบคุมที่องค์กรเลือกใช้นั้นสนับสนุนหลักการของ Zero Trust อย่างแท้จริงหรือไม่ โดยมักพิจารณาจากประเด็นดังนี้

๑) การเลือกเทคโนโลยีที่ยังคงยึดแนวคิด การป้องกันในระดับขอบของเครือข่าย

๒) การเลือกเทคโนโลยีตามแนวโน้ม (Trend) มากกว่าการอิงความเสี่ยง

๓) ความไม่สอดคล้องระหว่างนโยบายกับเทคโนโลยีที่เลือกใช้

ในขั้นตอนนี้สะท้อนถึงช่องว่างระหว่างแนวคิด Zero Trust กับการนำไปใช้จริงในระดับสถาปัตยกรรม

ช่องว่างระหว่างการออกแบบและการดำเนินงาน

เมื่อเข้าสู่ขั้นตอนติดตั้ง (Implement) การวิเคราะห์ช่องว่างในขั้นตอนนี้จะเน้นไปที่ความแตกต่างระหว่างสิ่งที่ออกแบบไว้กับสิ่งที่นำไปใช้จริง โดยเฉพาะการบูรณาการองค์ประกอบหลักของ Zero Trust เช่น ตัวตน อุปกรณ์ และการควบคุมการเข้าถึง ช่องว่างที่พบได้บ่อย เช่น การนำ Zero Trust ไปใช้แบบแยกส่วน (Silo) จากระบบอื่น การขาดการจัดการการเปลี่ยนแปลงและการสื่อสารกับผู้ใช้งาน การที่มาตรการควบคุมมีโอกาสถูกเลี่ยงผ่าน (Bypass) ได้ในทางปฏิบัติ

ในขั้นตอนนี้ การวิเคราะห์ช่องว่างช่วยชี้ให้เห็นว่า ปัญหาหลักไม่ใช่การขาดเทคโนโลยี แต่เป็นการขาดการเชื่อมโยงระหว่าง Zero Trust กับกระบวนการทำงาน

การประเมินประสิทธิผลของ Zero Trust

ขั้นตอนประเมิน ช่วยยกระดับการวิเคราะห์ช่องว่าง จากการประเมินการปฏิบัติตามข้อกำหนดไปสู่การประเมินเชิงประสิทธิผล โดยพิจารณาว่ามาตรการควบคุมของ Zero Trust สามารถลดความเสี่ยงได้หรือไม่ ประเด็นที่สะท้อนช่องว่างในขั้นตอนนี้ เช่น

๑) การประเมินแบบครั้งคราวแทนการประเมินแบบต่อเนื่อง

๒) การขาดตัวชี้วัดที่สะท้อนความสมบูรณ์ของ Zero Trust

๓) การประเมินที่ไม่เชื่อมโยงกับบริบทที่ภัยคุกคามมีการเปลี่ยนแปลงอยู่เสมอ

ช่องว่างในขั้นตอนประเมินมักชี้ให้เห็นว่าการติดตั้ง Zero Trust ยังไม่เชื่อมโยงกับหลักการตรวจสอบอยู่เสมอหรือการตรวจสอบอย่างต่อเนื่อง

การตัดสินใจด้านความเสี่ยงภายใต้ Zero Trust

ในขั้นตอนอนุญาต นั้น การวิเคราะห์ช่องว่างจะเชื่อมโยง Zero Trust เข้ากับกระบวนการตัดสินใจของผู้บริหารและองค์กร โดยพิจารณาว่าการอนุญาตให้เข้าถึงทรัพยากรนั้นสะท้อนระดับความเสี่ยงที่เหลืออยู่ภายหลังการติดตั้งระบบ Zero Trust หรือไม่ ช่องว่างที่พบได้ เช่น

๑) การอนุญาตเป็นช่วงเวลาโดยไม่พิจารณาบริบทที่เปลี่ยนไป

๒) การขาดความเข้าใจในเรื่องความเสี่ยงที่เหลืออยู่ในสภาพแวดล้อม Zero Trust

๓) การตรวจสอบและการอนุญาตที่ไม่ได้ใช้ข้อมูลจากการประเมินและการเฝ้าระวัง

ความต่อเนื่องและการปรับตัวของ Zero Trust

ขั้นตอนเฝ้าระวัง ทำให้การวิเคราะห์ช่องว่างไม่จบลงเพียงหลังจากการติดตั้ง แต่สามารถดำเนินการต่อเนื่องไปในระยะยาว โดยพิจารณาว่าข้อมูลจากการเฝ้าระวังและเหตุการณ์ที่เกิดขึ้นถูกนำมาใช้ในการปรับปรุงนโยบายและมาตรการควบคุมได้หรือไม่ ช่องว่างในขั้นตอนนี้ที่มักปรากฏ เช่น

๑) การเฝ้าระวังเพื่อแจ้งเตือน แต่ไม่ได้นำไปปรับปรุงนโยบาย

๒) การแยกการทำงานระหว่างศูนย์ปฏิบัติการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (SOC) กับระบบควบคุมการเข้าถึง

๓) การที่ Zero Trust ไม่สามารถปรับตัวตามบริบทใหม่ได้

การวิเคราะห์ช่องว่างโดยอิงกรอบการจัดการความเสี่ยง (RMF) ช่วยให้การติดตั้งและนำไปใช้งาน Zero Trust เป็นกระบวนการเชิงระบบที่ช่วยให้องค์กรสามารถมองเห็นช่องว่างทั้งในเชิงกลยุทธ์ นโยบาย และการดำเนินงาน นำไปสู่การวางแผนที่สอดคล้องกับบริบทและความเสี่ยงขององค์กรอย่างแท้จริง

๓.๓ แนวทางปฏิบัติในการดำเนินการ (Operation) ระบบ Zero Trust

เมื่อองค์กรประเมินภูมิทัศน์เทคโนโลยี (Technology Landscape)[๓] ที่เกี่ยวข้องกับ Zero Trust อย่างครบถ้วนแล้ว ขั้นตอนถัดไป คือ การระบุระบบหรือทรัพยากรเป้าหมายในการนำหลักการ Zero Trust มาประยุกต์ใช้ เพื่อยกระดับหรือขยายมาตรการควบคุมด้านความมั่นคงปลอดภัยจากที่มีอยู่เดิมให้สอดคล้องกับความเสี่ยงและบริบทขององค์กรในปัจจุบันและอนาคต

เพื่อสนับสนุนการยกระดับและการเปลี่ยนผ่านสู่แนวทาง Zero Trust องค์กรจำเป็นต้องปรับปรุง หรือเพิ่มเติมเทคโนโลยีด้านความมั่นคงปลอดภัยให้ครอบคลุมหลายมิติ โดยเทคโนโลยีสำคัญที่ควรพิจารณา ได้แก่

๑) การยืนยันตัวตนและการควบคุมสิทธิอย่างต่อเนื่อง (Continuous Authentication and Authorization)

๒) การวิเคราะห์พฤติกรรมผู้ใช้และเอนทิตี (User and Entity Behavior Analytics)

๓) จุดบังคับใช้นโยบายแบบไดนามิก (Dynamic Policy Enforcement Points)

๔) ระบบอัตโนมัติและการจัดการประสานงาน (Automation and Orchestration: AO)

พื้นที่ปฏิบัติการทั่วไปที่ได้รับผลกระทบจากกลยุทธ์ Zero Trust

การนำ Zero Trust ไปใช้จะส่งผลต่อการดำเนินงานในหลายด้านขององค์กร โดยส่วนงานสำคัญที่จะเกิดการเปลี่ยนแปลงในด้านกระบวนการ ได้แก่

การบริหารจัดการระบบ (System Administration)

การจัดการเครือข่าย (Network Management)

การจัดการข้อมูล (Data Management)

การเฝ้าระวังด้านประสิทธิภาพ (Performance Monitoring)

ฝ่ายช่วยเหลือและสนับสนุน (Helpdesk and Support)

DevOps และลำดับขั้นตอนการทำงานของการเข้าถึง (Access Workflow)

การนำ Zero Trust ไปใช้อย่างมีประสิทธิภาพจำเป็นต้องได้รับการยอมรับในทุกระดับขององค์กร การให้ความรู้แก่พนักงานและผู้บริหารระดับสูงจึงมีความสำคัญ เพื่อให้สามารถเข้าใจคุณค่า และ

สื่อสารเป้าหมายของ Zero Trust ได้อย่างชัดเจน ซึ่งจะช่วยสนับสนุนการตัดสินใจของคณะกรรมการ และทำให้กลยุทธ์ Zero Trust สอดคล้องกับทิศทางเชิงกลยุทธ์ขององค์กร

ในสภาพแวดล้อมด้านความมั่นคงปลอดภัยที่มีการเปลี่ยนแปลงอยู่ตลอดเวลา โมเดลความมั่นคงปลอดภัยแบบดั้งเดิมไม่สามารถตอบสนองต่อความซับซ้อนของภัยคุกคามในปัจจุบันได้อย่างเพียงพอ แนวคิด Zero Trust จึงถูกนำเสนอในฐานะกรอบแนวคิดเชิงรุกและครอบคลุม องค์กรจำเป็นต้องตระหนักถึงข้อกำหนดทางกฎหมาย และข้อบังคับที่แตกต่างกันในแต่ละประเทศหรือภูมิภาค และปรับกลยุทธ์ Zero Trust ให้สอดคล้องกับบริบทดังกล่าว สำหรับองค์กรที่ยังใช้ระบบดั้งเดิม อาจจำเป็นต้องนำโซลูชันสำเร็จรูปจากผู้ให้บริการมาใช้ เพื่อสร้างลำดับขั้นตอนการทำงานแบบอัตโนมัติและบูรณาการองค์ประกอบของสถาปัตยกรรม Zero Trust เข้าด้วยกัน การยกระดับการประสานการทำงานแบบอัตโนมัติ เช่น การเชื่อมโยงระหว่างการควบคุมการเข้าถึงและการเฝ้าระวัง จะช่วยลดความซับซ้อนของการปฏิบัติงาน และเอื้อต่อการนำไปสู่การปรับใช้ในสภาพแวดล้อมจริงได้อย่างมีประสิทธิภาพมากยิ่งขึ้น

ประสบการณ์ผู้ใช้ (User Experience: UX) และวิศวกรรมความน่าเชื่อถือได้ของไซต์ (Site Reliability Engineering: SRE)

ประสบการณ์ผู้ใช้และวิศวกรรมความน่าเชื่อถือได้ของไซต์ เป็นองค์ประกอบสนับสนุนที่มีบทบาทสำคัญต่อความสำเร็จในการนำสถาปัตยกรรม Zero Trust ไปปรับใช้ในทางปฏิบัติ การออกแบบการควบคุมด้านความมั่นคงปลอดภัยให้สอดคล้องกับประสบการณ์การใช้งานที่คุ้นเคย ช่วยลดแรงต้านในการใช้งาน และส่งเสริมการยอมรับจากผู้ใช้และทีมปฏิบัติการ

ในขณะเดียวกันแนวทางของ SRE ซึ่งเน้นระบบอัตโนมัติ การทำงานที่ขับเคลื่อนด้วยโค้ด และการเฝ้าระวังอย่างต่อเนื่อง สนับสนุนหลักการของ Zero Trust ในด้านการบังคับใช้นโยบายอย่างสม่ำเสมอ ลดการพึ่งพากระบวนการแบบแมนวล และลดความเสี่ยงจากข้อผิดพลาดของมนุษย์ (Human Error)

ในบริบทดังกล่าวหัวข้อย่อยต่อไปนี้ จะอธิบายประเด็นสำคัญด้านการดำเนินงานที่องค์กรควรพิจารณาในการนำ Zero Trust ไปปรับใช้อย่างยั่งยืน

๓.๓.๑ การเปลี่ยนแปลงทางวัฒนธรรมและโครงสร้างองค์กร

การนำสถาปัตยกรรม Zero Trust ไปปรับใช้อย่างมีประสิทธิผล มิได้เป็นประเด็นด้านเทคโนโลยีเพียงอย่างเดียว หากแต่จำเป็นต้องอาศัยการปรับเปลี่ยนด้านวัฒนธรรม และโครงสร้างองค์กรให้สอดคล้องกับบริบททางธุรกิจ วิสัยทัศน์ และทิศทางเชิงกลยุทธ์ที่กำหนดโดยคณะกรรมการขององค์กร

การสร้างวัฒนธรรม Zero Trust ที่แข็งแกร่งต้องอาศัยองค์ประกอบสำคัญดังต่อไปนี้

(๑) เน้นที่บุคลากร กระบวนการ และมิติด้านการบริหารองค์กร (Organizational Dimensions) มากกว่าการมุ่งเน้นเพียงการจัดหาเทคโนโลยี

(๒) ส่งเสริมให้เกิดการเฝ้าระวัง การบันทึกเหตุการณ์ และการตอบสนองต่อเหตุการณ์อย่างต่อเนื่องและรวดเร็ว

การสนับสนุนและรับรองจากผู้บริหารระดับสูง

๑) การสนับสนุนและการรับรองอย่างเป็นทางการจากผู้บริหารสำหรับโครงการ Zero Trust เพื่อแสดงให้เห็นถึงความมุ่งมั่นของผู้นำ

๒) พัฒนาแผนการสื่อสารเพื่อสร้างความเข้าใจที่สอดคล้องกันระหว่างผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้อง กับเป้าหมายของการประยุกต์ใช้ Zero Trust

การปลูกฝังวัฒนธรรมการจัดการความเสี่ยงอย่างต่อเนื่อง

๑) ประเมิน และวัดความเสี่ยงอย่างต่อเนื่อง ทั้งเชิงปริมาณ และเชิงคุณภาพ เพื่อใช้เป็นแนวทางในการตัดสินใจที่สอดคล้องกับระดับความเสี่ยงที่องค์กรยอมรับได้ (Risk Appetite)

๓.๓.๒ การฝึกอบรมและการให้ความรู้

โครงการฝึกอบรม และการให้ความรู้ด้าน Zero Trust ควรถูกออกแบบอย่างเป็นระบบ เพื่อสนับสนุนให้บุคลากรทุกระดับขององค์กรเข้าใจแนวคิดเชิงหลักการของ Zero Trust อย่างถูกต้อง และสามารถนำหลักการไปประยุกต์ใช้ได้ตามบทบาท และความรับผิดชอบของตน โดยกลุ่มเป้าหมายหลักประกอบด้วย พนักงานด้านไอที ผู้บริหารระดับสูง และผู้จัดการสายงานธุรกิจ การฝึกอบรมควรครอบคลุมเนื้อหาดังต่อไปนี้

การเสริมสร้างความเข้าใจในระดับผู้บริหาร

ผู้บริหารที่มีความเข้าใจใน Zero Trust จะมีบทบาทสำคัญในการสื่อสารคุณค่าทางธุรกิจของ Zero Trust และเชื่อมโยงการดำเนินงานด้านความมั่นคงปลอดภัยเข้ากับเป้าหมายเชิงกลยุทธ์ขององค์กร โดยเฉพาะอย่างยิ่งในการสร้างการยอมรับ และการสนับสนุนจากคณะกรรมการบริหาร

การให้ความรู้แก่พนักงานทั่วไป

การฝึกอบรมสำหรับพนักงานทุกระดับควรมุ่งเน้นความเข้าใจหลักการพื้นฐานของ Zero Trust โดยแยกแนวคิดออกจากการมองว่าเป็นเพียงเครื่องมือทางเทคโนโลยี การฝึกอบรมควรช่วยให้พนักงานตระหนักถึงบทบาท หน้าที่ และความรับผิดชอบที่เปลี่ยนแปลงไปภายใต้กรอบแนวคิด Zero Trust รวมถึงผลกระทบต่อกระบวนการทำงาน

การมีส่วนร่วมของหน่วยงานตรวจสอบ

หน่วยงานตรวจสอบขององค์กรทั้งภายใน และภายนอกควรมีส่วนร่วมในการฝึกอบรม ผู้ตรวจสอบจำเป็นต้องเข้าใจถึงระดับความมั่นคงปลอดภัย ความยืดหยุ่น และแนวทางการควบคุมที่องค์กรได้รับจากการนำ Zero Trust ไปใช้ เพื่อให้สามารถประเมิน และให้ข้อเสนอแนะได้อย่างเหมาะสม และสอดคล้องกับกรอบ Zero Trust

การบูรณาการการฝึกอบรมเกี่ยวกับ Zero Trust

การผนวกรวม Zero Trust เข้าเป็นส่วนหนึ่งของโปรแกรมการฝึกอบรมที่มีอยู่เดิมขององค์กรสำหรับพนักงานทุกคน เพื่อให้มั่นใจว่าการปรับปรุง การกำหนดตารางเวลา และการทบทวนที่จำเป็นในอนาคต จะได้รับการดำเนินการอย่างต่อเนื่อง และไม่ถูกละเลยโดยหน่วยงานฝึกอบรมขององค์กร

๓.๓.๓ การเปลี่ยนแปลงด้านกฎระเบียบและการปฏิบัติตามข้อกำหนด

ภาพรวมของข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์มีการเปลี่ยนแปลงอย่างต่อเนื่อง อันเป็นผลจากความซับซ้อน และความถี่ที่เพิ่มขึ้นของภัยคุกคามไซเบอร์ แนวทางความมั่นคงปลอดภัยแบบดั้งเดิมที่มุ่งเน้นการป้องกันขอบเขตเครือข่ายไม่เพียงพอต่อการคุ้มครองข้อมูลและระบบที่สำคัญในบริบทปัจจุบัน ส่งผลให้หน่วยงานภาครัฐและหน่วยงานกำกับดูแลในหลายอุตสาหกรรม เริ่มผลักดันให้มีการนำกรอบแนวคิดเชิงรุกและเป็นระบบ เช่น Zero Trust มาใช้เป็นแนวทางในการยกระดับการควบคุมด้านความมั่นคงปลอดภัย

ในสภาพแวดล้อมด้านไซเบอร์ที่มีการเปลี่ยนแปลงอย่างต่อเนื่อง กฎหมาย ระเบียบ และมาตรฐานด้านการปฏิบัติตามข้อกำหนดที่สำคัญ เช่น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) และพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ มีแนวโน้มได้รับการปรับปรุง เพื่อกำหนดให้มีการบังคับใช้มาตรการควบคุมด้านความมั่นคงปลอดภัยที่สอดคล้องกับหลักการของ Zero Trust มากยิ่งขึ้น โดย PDPA มุ่งเน้นการคุ้มครองข้อมูลส่วนบุคคล และความเป็นส่วนตัวของพลเมืองไทย ด้าน พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์มุ่งเน้นด้านความมั่นคงปลอดภัยไซเบอร์

แนวโน้มนี้มีความเด่นชัดในภาคการเงิน หน่วยงานด้านสาธารณสุข และภาครัฐ เนื่องจากความอ่อนไหวของข้อมูลส่วนบุคคลที่จัดเก็บไว้ ทำให้ความจำเป็นในการปรับใช้นโยบายมีความสำคัญมากขึ้น แม้ว่ากฎระเบียบในปัจจุบันอาจยังไม่บังคับใช้หลักการ Zero Trust โดยตรง แต่แนวโน้มนี้มีความชัดเจนในอุตสาหกรรมที่มีการกำกับดูแลที่เข้มงวด ซึ่งการปฏิบัติตามข้อกำหนดทางด้าน Zero Trust เป็นกลไกสำคัญในการลดความเสี่ยงและเสริมสร้างการป้องกันภัยคุกคามไซเบอร์อย่างต่อเนื่อง

องค์กรจำเป็นต้องติดตามและประเมินข้อกำหนดทางกฎหมาย รวมถึงข้อบังคับที่เกี่ยวข้องในประเทศ และภูมิภาค เนื่องจากการประกาศหรือการปรับปรุงกฎระเบียบใหม่มักส่งผลให้เกิดการประเมิน การตรวจสอบ และการรับรองตามข้อกำหนดเฉพาะ โดยเฉพาะในช่วงของการเปลี่ยนผ่านสู่สถาปัตยกรรม Zero Trust ซึ่งอาจมีผลกระทบต่อกระบวนการและการควบคุมด้านความมั่นคงปลอดภัยเดิมขององค์กร

ความท้าทายหลัก คือ การจัดการกับสภาพแวดล้อมดั้งเดิม ที่มักมีข้อจำกัดด้านความยืดหยุ่น ทำให้การปรับเปลี่ยนสถาปัตยกรรม และการปฏิบัติตามข้อกำหนดใหม่เป็นเรื่องยาก หรือใช้เวลานาน องค์กรจึงควรประเมินสถานะปัจจุบัน วางแผนอย่างเป็นขั้นตอน และกำหนดมาตรการรองรับอย่างรอบคอบ เพื่อให้สามารถปฏิบัติตามกฎหมายได้อย่างต่อเนื่องและมีประสิทธิภาพ

๓.๓.๔ ระบบและโครงสร้างพื้นฐานเก่า

เทคโนโลยีเฉพาะทางที่ยังใช้ในระบบดั้งเดิม เช่น อุปกรณ์เทคโนโลยีเชิงปฏิบัติการ (OT) อุปกรณ์ IoT หรืออุปกรณ์ควบคุมในงานอุตสาหกรรม (Industrial Control Systems) มักอยู่ในโครงสร้างพื้นฐานที่สำคัญ และมีข้อจำกัดด้านเทคนิคชัดเจนหลายประการ เช่น การจัดการแพตช์และการควบคุมการเข้าถึง เพื่อให้บรรลุเป้าหมาย Zero Trust สำหรับเทคโนโลยีเหล่านี้ จำเป็นต้องนำกลยุทธ์และเทคโนโลยีการควบคุมการเข้าถึงระดับไมโครเพอริมิเตอร์มาใช้

องค์กรที่ยังคงพึ่งพาระบบดั้งเดิม และโมเดลการตรวจสอบความเชื่อถือแบบดั้งเดิม มักเผชิญกับความท้าทายในการนำแนวทาง Zero Trust มาใช้ โดยเฉพาะอย่างยิ่งในประเด็นการมองเห็นเครือข่าย และสินทรัพย์ที่มีข้อจำกัด และการบูรณาการการทำงานกับระบบดั้งเดิม การเปลี่ยนผ่านสู่ Zero Trust จะแตกต่างกันไปตามคุณลักษณะเฉพาะของแต่ละองค์กร ทั้งระดับความพร้อม ภารกิจ และความท้าทายเฉพาะตัว การปรับปรุงระบบดั้งเดิมไปเป็น Zero Trust ไม่จำเป็นต้องทำพร้อมกันทั้งระบบในทันที แต่การปรับปรุงใด ๆ ควรได้รับการวางแผนเชิงกลยุทธ์ เพื่อรับมือกับภัยคุกคามที่เกิดขึ้นใหม่ และปรับปรุงระบบให้ทันสมัยต่อการรับมือภัยคุกคามในทุกประเภท

การนำโมเดล Zero Trust มาใช้ ตัวอย่างเช่น การเฝ้าระวังด้านความมั่นคงปลอดภัยสารสนเทศอย่างต่อเนื่อง (Information Security Continuous Monitoring: ISCM) ต้องการระบบที่มีความยืดหยุ่นเพื่อจัดการกระบวนการทำงานและการเคลื่อนย้ายของข้อมูล ความไม่ยืดหยุ่นของระบบดั้งเดิมจึงเป็นอุปสรรคสำคัญต่อการนำโมเดลดังกล่าวไปประยุกต์ใช้ นอกจากนี้ประสบการณ์ขององค์กรในการใช้โปรแกรมการวัดผล (Measurement Program) ยังส่งผลต่อความสามารถในการนำ Zero Trust มาใช้ โดยองค์กรที่มีความพร้อมและประสบการณ์ในการวัดผลมากกว่าจะสามารถปรับตัวในการนำ Zero Trust มาใช้ได้ง่ายกว่าองค์กรที่มีความสามารถในการวัดผลน้อย

๓.๓.๕ ความง่ายในการใช้งานและการยอมรับ (Usability and Adoption)

ประสบการณ์ผู้ใช้ (UX) และแนวทางวิศวกรรมความน่าเชื่อถือได้ของไซต์ (SRE) มีบทบาทสำคัญในการส่งเสริมการนำสถาปัตยกรรม Zero Trust มาใช้ การปรับปรุง UX ให้ใช้งานง่าย และสอดคล้องกับกระบวนการทำงาน จะช่วยเพิ่มการยอมรับหลักการ Zero Trust ขณะเดียวกันการเปลี่ยนไปสู่แนวทางการขับเคลื่อนด้วยระบบอัตโนมัติที่ขับเคลื่อนด้วยโค้ด (Code-Driven Automation) ช่วยลดภาระงานที่ต้องทำด้วยตนเองและลดข้อผิดพลาดที่เกิดขึ้นจากมนุษย์ ซึ่งส่งผลให้แนวทาง SRE มีประสิทธิภาพมากยิ่งขึ้น ความร่วมมือระหว่าง UX และ SRE ทำให้มาตรการความมั่นคงปลอดภัยมีประสิทธิผล ช่วยยกระดับความมั่นคงปลอดภัยขององค์กรและส่งเสริมให้ปฏิบัติงานดีขึ้น

กุญแจสำคัญในการสร้างความยอมรับต่อ Zero Trust ในหมู่พนักงาน คือ การออกแบบ UX ที่เป็นมิตรต่อผู้ใช้และการผลักดันให้แนวทางต่าง ๆ ถูกนำไปใช้ผ่านระบบอัตโนมัติ ซึ่งจะเพิ่มการสนับสนุนจากทีมงานและช่วยยกระดับผลลัพธ์ด้าน SRE ไปพร้อมกัน

๓.๓.๕.๑ ประสบการณ์ผู้ใช้ (User Experience: UX)

การให้ความสำคัญกับประสบการณ์ผู้ใช้ เป็นปัจจัยสำคัญในการเพิ่มการยอมรับและการนำ Zero Trust มาใช้ในองค์กร

ประสบการณ์ผู้ใช้ที่ออกแบบมาอย่างดีทำให้มาตรการความมั่นคงปลอดภัยทั้งแข็งแกร่งและใช้งานง่าย ส่งผลให้เกิดสภาพแวดล้อมการทำงานที่มั่นคงปลอดภัยและมีประสิทธิภาพสูง

๓.๓.๕.๒ วิศวกรรมความน่าเชื่อถือได้ของไซต์ (Site Reliability Engineering: SRE)

วิศวกรรมความน่าเชื่อถือได้ของไซต์ คือ การผสมผสานระหว่างวิศวกรรมซอฟต์แวร์เข้ากับการดำเนินงานด้านไอที เพื่อสร้างระบบที่สามารถปรับขนาดได้ (Scalable) และมีความน่าเชื่อถือ โดยเน้นการจัดการเชิงรุกผ่านการเฝ้าระวังอย่างต่อเนื่อง ระบบอัตโนมัติ การจัดการประสานงาน (Orchestration) และความสามารถในการปรับขนาด การวางแผนด้าน SRE เป็นส่วนสำคัญของความมั่นคงปลอดภัยของ Zero Trust ซึ่งช่วยรักษาความถูกต้องสมบูรณ์ (Integrity) และความยืดหยุ่นของระบบ รวมถึงการตรวจสอบช่องโหว่เป็นประจำอยู่เสมอและการจัดการทรัพยากรอย่างมีประสิทธิภาพ

การนำ SRE มาประยุกต์ใช้กับ Zero Trust สามารถนำมาประยุกต์ใช้ได้ทั้งในสภาพแวดล้อมแบบคลาวด์และการติดตั้งภายในองค์กร เพื่อช่วยเพิ่มความน่าเชื่อถือของระบบได้อย่างครอบคลุม ไม่ว่าจะอยู่ในสภาพแวดล้อมแบบใด

ระบบอัตโนมัติและการจัดการประสานงาน เป็นปัจจัยขับเคลื่อนที่สำคัญในการปรับปรุง และบำรุงรักษาสถาปัตยกรรม Zero Trust ให้มีประสิทธิภาพสูงสุด โดยมีบทบาทใน ๒ ด้านหลักดังนี้

(๑) การปรับปรุงการควบคุมและนโยบาย โดยการใช้ข้อมูลป้อนกลับแบบอัตโนมัติ (Automated Feedback) ซึ่งช่วยปรับปรุงการควบคุมการเข้าถึง นโยบาย และการบังคับใช้โดยอิงตามข้อมูลป้อนกลับ

(๒) การจัดการโครงสร้างพื้นฐาน ด้วยการนำแนวทางโครงสร้างพื้นฐานแบบโค้ด (Infrastructure as Code: IaC) มาประยุกต์ร่วมกับการตรวจสอบความสอดคล้องตามข้อกำหนดแบบอัตโนมัติ ช่วยให้สคริปต์และเครื่องมือสามารถตรวจสอบความสอดคล้องกับระบบตามนโยบายของ Zero Trust ได้อย่างต่อเนื่อง ทำให้สามารถตรวจพบความเบี่ยงเบนใด ๆ และแก้ไขได้อย่างรวดเร็ว

การใช้โครงสร้างพื้นฐานแบบโค้ดช่วยให้สามารถตอบสนองต่อภัยคุกคามที่ตรวจพบได้อย่างรวดเร็ว โดยปรับการควบคุมการเข้าถึงและการกำหนดค่าของเครือข่ายโดยอัตโนมัติแบบเรียลไทม์ นอกจากนี้ IaC ยังช่วยป้องกันปัญหาการเบี่ยงเบนของโครงสร้างพื้นฐาน (Infrastructure Drift) ซึ่งเกิดขึ้นเมื่อสถานะจริงของเครือข่ายแตกต่างไปจากสถานะที่กำหนดไว้โดยโค้ด การรักษาความสอดคล้องของโครงสร้างพื้นฐานอย่างต่อเนื่องจึงมีความสำคัญต่อการคงความถูกต้องตามนโยบาย Zero Trust

๓.๓.๕.๒.๑ การเฝ้าระวังและความเข้าใจเกี่ยวกับการถูกบุกรุกระบบ

ในการรักษาความมั่นคงปลอดภัยแบบ Zero Trust การติดตามชุดเทคโนโลยี (Technology Stack) อย่างต่อเนื่องถือเป็นสิ่งสำคัญอย่างยิ่งสำหรับการตรวจหาช่องโหว่และจุดอ่อน โดย SRE ช่วยเสริมกระบวนการนี้ผ่านการเฝ้าระวังระบบและการบันทึกข้อมูลเหตุการณ์อย่างต่อเนื่อง วิธีนี้ช่วยให้สามารถระบุการละเมิดที่อาจเกิดขึ้นได้อย่างรวดเร็วและสนับสนุนมาตรการความมั่นคงปลอดภัยเชิงรุก

นอกจากนี้ SRE ยังช่วยให้เกิดความเข้าใจเชิงลึกในการละเมิดระบบ ผ่านการวิเคราะห์หลังเหตุการณ์ (Postmortem Analysis) และการเรียนรู้จากความล้มเหลว ซึ่งสำคัญต่อการฟื้นฟูระบบอย่างมั่นคงปลอดภัย และเสริมสร้างความยืดหยุ่นของระบบ (System Resilience) แนวปฏิบัติ เช่น การจัดทำเอกสารเหตุการณ์อย่างละเอียด และการวิเคราะห์หลังเหตุการณ์แบบไม่โทษหรือตำหนิที่ตัวบุคคล (Blameless Postmortems) ช่วยให้ทีมทำความเข้าใจสาเหตุของปัญหา และเสริมความแข็งแกร่งในการป้องกันระบบในระยะยาว

๓.๓.๕.๒.๒ การจัดการทรัพยากร และโครงสร้างพื้นฐานที่ไม่เปลี่ยนแปลง

ในบริบทของความมั่นคงปลอดภัยแบบ Zero Trust การนำทรัพยากรที่ไม่เปลี่ยนแปลง (Immutable Resources) มาใช้เป็นสิ่งสำคัญ ทรัพยากรที่ไม่เปลี่ยนแปลง หมายถึง ส่วนประกอบโครงสร้างพื้นฐานที่เมื่อถูกนำไปใช้งานแล้วจะไม่ถูกแก้ไข หากต้องมีการเปลี่ยนแปลงจะต้องสร้างตัวทรัพยากรใหม่ (New Instance) ขึ้นมาแทน SRE ช่วยอำนวยความสะดวกในกระบวนการนี้ โดยทำให้การทำงานเป็นไปแบบอัตโนมัติ ทำให้มั่นใจได้ว่าตัวทรัพยากรใหม่มีความสอดคล้องเชื่อถือได้และสามารถตรวจสอบได้ วิธีการนี้ช่วยลดความเสี่ยงจากการเบี่ยงเบนของการตั้งค่า (Configuration Drift) และการเปลี่ยนแปลงที่ไม่ได้รับอนุญาต ซึ่งสอดคล้องกับหลักการ Zero Trust การเน้นระบบอัตโนมัติและการตรวจสอบความเชื่อถือได้ของ SRE ทำให้การใช้งานทรัพยากรที่ไม่เปลี่ยนแปลงเป็นไปอย่างมีประสิทธิภาพและมีความมั่นคงปลอดภัย สามารถตอบสนองอย่างเด็ดขาด และรวดเร็วเมื่อส่วนประกอบของระบบถูกละเมิดหรือถูกบุกรุก แนวทางนี้คล้ายกับการปลดระวาง (Decommissioning) และเปลี่ยนใหม่เพื่อทดแทน (Replacing) อย่างรวดเร็วในทันที โดยการลบส่วนประกอบที่ถูกละเมิดออก และแทนที่ด้วยตัวใหม่ที่มั่นคงปลอดภัย

SRE สนับสนุนกลยุทธ์การตอบสนองอย่างรวดเร็วผ่านแนวทาง เช่น โครงสร้างพื้นฐานแบบโค้ด และกระบวนการปรับใช้ระบบอัตโนมัติแบบเป็นลำดับขั้น (Automated Deployment Pipelines) แนวทางเหล่านี้ช่วยให้สามารถนำทรัพยากรที่ได้รับผลกระทบกลับมาใช้งานใหม่ได้อย่างรวดเร็ว ลดช่วงเวลาที่ระบบหยุดทำงาน (Downtime) และลดความเสี่ยงจากภัยคุกคาม จึงถือได้ว่า SRE ช่วยให้การตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยมีความรวดเร็วและเชื่อถือได้

บทสรุป

การรักษาความมั่นคงปลอดภัยด้วยหลักการ Zero Trust จำเป็นต้องผสานรวมการมีส่วนร่วมเชิงกลยุทธ์ในหลายระดับ ระดับสูงสุด คือ กลยุทธ์ขององค์กรซึ่งกำหนดทิศทางและการตัดสินใจในภาพรวม ขณะที่ระดับถัดมา คือ กลยุทธ์ Zero Trust ที่นิยามแนวคิดความน่าเชื่อถือใหม่ โดยเน้นการตรวจสอบอย่างต่อเนื่อง บนสมมติฐานว่าการละเมิดหรือบุกรุกระบบอาจเกิดขึ้นได้เสมอ (Assume Breach)

การทำให้แนวทาง Zero Trust สอดคล้องกับค่านิยมขององค์กร จำเป็นต้องเข้าใจปัจจัยขับเคลื่อนหลักในการนำไปใช้ เช่น ข้อกำหนดด้านกฎหมาย การเพิ่มความมั่นคงปลอดภัย การสร้างข้อได้เปรียบทางการแข่งขัน และการลดต้นทุนในระยะยาว การบริหารความเสี่ยงเป็นหัวใจสำคัญ ต้องให้ความสำคัญกับการปกป้องสินทรัพย์ดิจิทัล กำหนดผู้รับผิดชอบที่ชัดเจน และจัดการความเสี่ยงอย่างเป็นระบบ

การจัดทำกรณีศึกษาทางธุรกิจ (Business Case) เพื่อขับเคลื่อน Zero Trust เกี่ยวข้องกับการประเมินผลกระทบทางการเงินและประสิทธิภาพ พร้อมกับการรับความเห็นจากผู้มีส่วนได้ส่วนเสียข้ามสายงาน (Cross-Functional Stakeholders) และปรับให้สอดคล้องกับกลยุทธ์ การออกแบบความมั่นคงปลอดภัยที่บูรณาการภายในองค์กร และการจัดการสิทธิในการเข้าถึงอย่างเข้มงวด

ความสำเร็จของ Zero Trust จำเป็นต้องอาศัยการเปลี่ยนแปลงทางวัฒนธรรมองค์กร ซึ่งครอบคลุมถึงการจัดการความเสี่ยงอย่างต่อเนื่อง การสนับสนุนจากผู้บริหารระดับสูง และการสร้างความตระหนักรู้ในทุกระดับขององค์กร นอกจากนี้องค์กรต้องปรับตัวให้สอดคล้องกับกฎระเบียบที่เปลี่ยนแปลงอยู่เสมอ Zero Trust เป็นแนวทางด้านความมั่นคงปลอดภัยไซเบอร์ที่ต้องอาศัยการปรับกลยุทธ์ การวางแผน และการดำเนินการที่รอบด้านและบูรณาการ เพื่อให้สามารถบรรลุประสิทธิผลสูงสุดจาก Zero Trust ได้

เอกสารอ้างอิง

๑) S. Rose, O. Borchert, S. Mitchell, and S. Connelly, “Zero Trust Architecture”, NIST Special Publication 800-207, 2020.

๒) Cybersecurity and Infrastructure Security Agency (CISA), Zero Trust Maturity Model, Version 2.0, 2023.

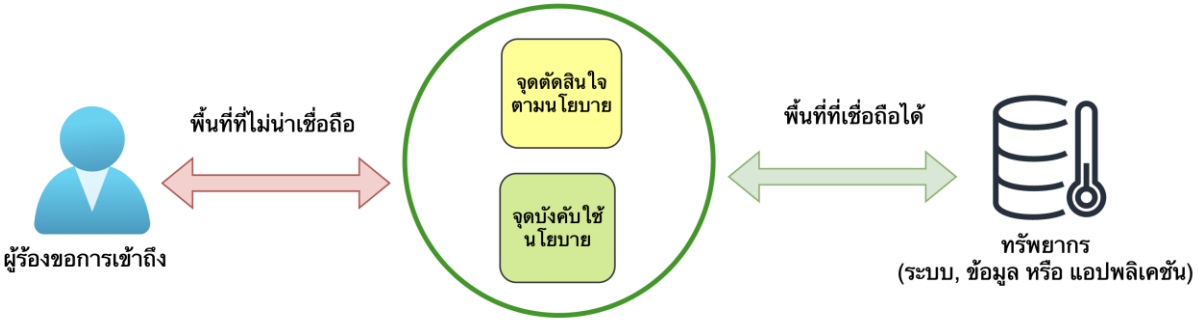
๓) Cloud Security Alliance (CSA), “Zero Trust Strategy Certificate of Competence in Zero Trust”, Version Number: 20250219, 2025.

บทที่ ๔
สถาปัตยกรรมของ Zero Trust และรูปแบบการใช้งาน

การประยุกต์ใช้ Zero Trust เป็นก้าวสำคัญในการยกระดับความมั่นคงปลอดภัยขององค์กร จากรูปแบบป้องกันที่ยึดขอบเขตเครือข่าย ไปสู่สถาปัตยกรรมที่ตรวจสอบความไว้วางใจทุกครั้งที่มีการเข้าถึงทรัพยากรไม่ว่าจะเป็นผู้ใช้ อุปกรณ์ หรือบริการทั้งภายในและภายนอกองค์กร โดยเน้นการยืนยันตัวตน การกำหนดสิทธิเท่าที่จำเป็นและการตรวจสอบอย่างต่อเนื่อง เพื่อลดความเสี่ยงด้านการโจมตีแบบการเคลื่อนตัวในเครือข่ายของผู้โจมตี ซึ่งในบทนี้ได้นำเสนอแนวทางปฏิบัติในการติดตั้ง ประยุกต์ใช้งาน Zero Trust อย่างเป็นขั้นตอน ช่วยให้องค์กรนำหลักการ Zero Trust ไปประยุกต์ใช้ได้จริงในสภาพแวดล้อมที่หลากหลายและซับซ้อน เพื่อให้การนำไปปฏิบัติมีความชัดเจนยิ่งขึ้น

๔.๑ องค์ประกอบเชิงตรรกะของสถาปัตยกรรม Zero Trust

ในการปรับใช้สถาปัตยกรรม Zero Trust ในองค์กรประกอบด้วยองค์ประกอบเชิงตรรกะหลายส่วนที่ทำงานร่วมกัน ซึ่งสามารถติดตั้งภายในองค์กร (On-premises) หรือให้บริการผ่านระบบคลาวด์ได้ (On-Cloud) โมเดลกรอบแนวคิดในรูปที่ ๕ แสดงความสัมพันธ์พื้นฐานระหว่างองค์ประกอบต่าง ๆ และรูปแบบการทำงานระหว่างกัน ทั้งนี้โมเดลดังกล่าวเป็นการนำเสนอในเชิงอุดมคติ เพื่อใช้เป็นแนวทางทำความเข้าใจองค์ประกอบเชิงตรรกะของระบบ



รูปที่ ๕ องค์ประกอบพื้นฐานของระบบ Zero Trust

จากรูปที่ ๕ เมื่อ “ผู้ร้องขอการเข้าถึง” ต้องการเข้าถึงทรัพยากรขององค์กร ก่อนที่จะเข้าถึงได้ต้องผ่านจุดตรวจสองจุด คือ จุดตัดสินใจตามนโยบายและจุดบังคับใช้นโยบาย ซึ่งทำหน้าที่คล้ายประตูสองชั้นที่ไม่ปล่อยให้ใครเดินผ่านไปได้โดยอัตโนมัติ

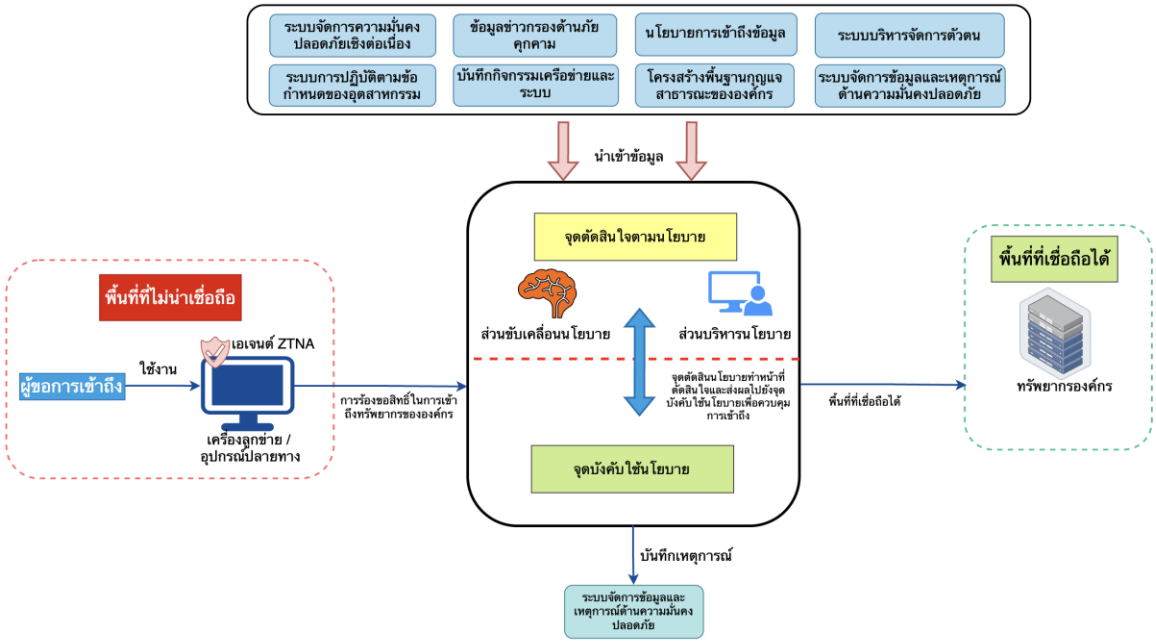
ระบบต้องประเมินการร้องขอเพื่อเข้าถึงข้อมูลทุกครั้ง เช่น

๑) มั่นใจแค่ไหนว่าผู้ร้องขอเป็นตัวจริง?

๒) สิ่งที่ร้องขอการเข้าถึงเหมาะสมกับ ความน่าเชื่อถือนี้หรือไม่?

๓) อุปกรณ์ที่ใช้ มีสภาพความมั่นคงปลอดภัยเพียงพอหรือไม่?

๔) ปัจจัยอื่นๆ เช่น สถานที่ เวลา หรือสภาพความมั่นคงปลอดภัยของอุปกรณ์ มีผลให้ความน่าเชื่อถือลดลงหรือไม่?



รูปที่ ๖ องค์ประกอบหลักเชิงตรรกะของ Zero Trust

รูปที่ ๖ แสดงองค์ประกอบหลักเชิงตรรกะของ Zero Trust โดยมีคำอธิบายองค์ประกอบดังนี้

๑) จุดตัดสินใจตามนโยบาย (Policy Decision Point: PDP) องค์ประกอบนี้เป็นบทบาทเชิงตรรกะ ที่ทำหน้าที่เป็นศูนย์กลางในการตัดสินใจด้านการเข้าถึงในสถาปัตยกรรม Zero Trust โดยจุดตัดสินใจตามนโยบายประกอบไปด้วยส่วนขับเคลื่อนนโยบายและส่วนบริหารนโยบาย ซึ่งในทางสถาปัตยกรรมจะถูกแยกบทบาทออกเป็น ๒ ส่วน คือ ส่วนขับเคลื่อนนโยบายและส่วนบริหารนโยบาย เพื่อให้การตัดสินใจและการบังคับใช้เป็นไปอย่างเป็นระบบและตรวจสอบได้

๒) ส่วนขับเคลื่อนนโยบาย (Policy Engine: PE) เป็นศูนย์กลางในการตัดสินใจขั้นสุดท้ายว่าผู้ร้องขอการเข้าถึง จะได้รับอนุญาตให้เข้าถึงทรัพยากรขององค์กรหรือไม่ การตัดสินใจของส่วนขับเคลื่อนนโยบาย อ้างอิงจากนโยบายขององค์กร รวมถึงข้อมูลจากระบบภายนอก เช่น ระบบจัดการความมั่นคงปลอดภัยเชิงต่อเนื่องหรือบริการข้อมูลข่าวกรองด้านภัยคุกคาม ข้อมูลทั้งหมดจะถูกนำเข้าสู่กระบวนการประเมินความน่าเชื่อถือ (Trust Algorithm) เพื่อให้ผลการตัดสินใจคือ “อนุญาต” “ปฏิเสธ” หรือ “เพิกถอนการเข้าถึงบางส่วน” ส่วนขับเคลื่อนนโยบายจะทำงานประสานกับองค์ประกอบส่วนบริหารนโยบาย โดยจะทำ

หน้าที่เฉพาะด้านการตัดสินใจและจัดเก็บบันทึกเหตุการณ์ ขณะที่ส่วนบริหารนโยบายจะเป็นผู้ดำเนินงานตามคำตัดสินดังกล่าวต่อไป

๓) ส่วนบริหารนโยบาย (Policy Administrator: PA) มีหน้าที่จัดตั้งหรือยุติเส้นทางการสื่อสารระหว่างผู้ร้องขอการเข้าถึงและทรัพยากรขององค์กร โดยออกคำสั่งไปยังจุดบังคับใช้นโยบายที่เกี่ยวข้อง นอกจากนี้ส่วนบริหารนโยบายยังรับผิดชอบการสร้างข้อมูลรับรองเซสชัน เช่น โทเค็นหรือข้อมูลยืนยันตัวตนที่จำเป็นสำหรับการเข้าถึงทรัพยากร ส่วนบริหารนโยบาย ทำงานสัมพันธ์โดยตรงกับส่วนขับเคลื่อนนโยบายและทำงานตามผลการตัดสินใจของส่วนขับเคลื่อนนโยบายในทุกกรณี หากเซสชันได้รับอนุญาตและผ่านการยืนยันตัวตน ส่วนบริหารนโยบายจะทำการส่งข้อมูลหรือคำสั่งไปยังจุดบังคับใช้นโยบาย เพื่อให้เซสชันสามารถเริ่มต้นและดำเนินการได้ ในทางกลับกัน หากการเข้าถึงถูกปฏิเสธส่วนบริหารนโยบายจะแจ้งให้ยุติหรือไม่อนุญาตให้มีการสร้างเซสชันดังกล่าว

๔) จุดบังคับใช้นโยบาย (Policy Enforcement Point: PEP) ทำหน้าที่เปิดใช้งาน ตรวจสอบและยุติการเชื่อมต่อระหว่างผู้ร้องขอการเข้าถึงและทรัพยากรขององค์กร โดยเป็นจุดที่มีการบังคับใช้การตัดสินใจเชิงนโยบายอย่างแท้จริง ส่วนบริหารนโยบายจะสื่อสารกับจุดบังคับใช้นโยบาย เพื่อส่งคำสั่งอนุญาตให้เข้าถึงและอัปเดตนโยบายการเข้าถึงที่ใช้ในปัจจุบัน จุดบังคับใช้นโยบายอาจถูกแบ่งออกเป็น ๒ องค์ประกอบ ได้แก่

๕) ฝั่งเครื่องลูกข่าย (Client) เช่น เอเจนต์ (Agent) ที่ติดตั้งบนอุปกรณ์ปลายทาง

๖) ฝั่งทรัพยากร ทำหน้าที่ควบคุมการเข้าถึงทรัพยากรขององค์กร

แต่ในการใช้งานจริงจุดบังคับใช้นโยบายส่วนใหญ่จะเป็นองค์ประกอบฝั่งทรัพยากรแต่เพียงอย่างเดียว โดยเอเจนต์ในฝั่งเครื่องลูกข่ายจะทำหน้าที่แค่เพียงเก็บสถานะของอุปกรณ์ แต่อาจจะมีการตอบสนองต่อคำสั่งที่สั่งโดยจุดตัดสินใจตามนโยบาย ในบางกรณีจุดบังคับใช้นโยบายอาจเป็นแบบพอร์ทัลรวมศูนย์ ที่ทำหน้าที่เป็นจุดควบคุมหลักสำหรับการเข้าถึงทรัพยากรทั้งหมด พอร์ทัลรวมศูนย์เป็นตัวกลางในการเข้าถึงทรัพยากรแทนผู้ใช้ โดยหลังผ่านพอร์ทัลรวมศูนย์ไปจะเข้าสู่พื้นที่ที่เรียกว่า พื้นที่ที่เชื่อถือได้ (Trust Zone) ซึ่งเป็นบริเวณที่ตั้งของทรัพยากรและบริการต่าง ๆ ขององค์กร ซึ่งพอร์ทัลรวมศูนย์จะนิยมใช้กับรูปแบบที่เครื่องลูกข่ายไม่ใช้เอเจนต์ (Agentless) นอกจากองค์ประกอบหลักของสถาปัตยกรรม Zero Trust แล้วยังมีแหล่งข้อมูลหลายแห่งตามรูปที่ ๖ ที่ให้ข้อมูลและระเบียบข้อกำหนดต่าง ๆ ที่ส่วนขับเคลื่อนนโยบายภายในจุดตัดสินใจตามนโยบายใช้ในการตัดสินใจ ซึ่งรวมถึงแหล่งข้อมูลภายนอกองค์กร (ที่ไม่ได้ควบคุมหรือสร้างโดยองค์กร) สถาปัตยกรรม Zero Trust สามารถรับข้อมูลจากองค์ประกอบดังที่แสดงในตารางที่ ๒๒ ดังนี้

ตารางที่ ๒๒ แสดงองค์ประกอบหลักเชิงตรรกะของ Zero Trust

องค์ประกอบ	บทบาทเชิงหน้าที่ (Functional Role)
ระบบจัดการความมั่นคงปลอดภัยเชิงต่อเนื่อง (Continuous Diagnostics and Mitigations)	ประเมินความถูกต้องสมบูรณ์ของสินทรัพย์ (Asset Integrity) รวมทั้งสถานะการปฏิบัติตามกฎระเบียบและข้อบังคับทางเทคนิค เช่น การแพตช์ ความสมบูรณ์ของซอฟต์แวร์ฯลฯ
ระบบการปฏิบัติตามข้อกำหนดของอุตสาหกรรม (Industry Compliance System)	การกำหนดระเบียบและข้อกำหนดที่จำเป็นให้สอดคล้องกับการปฏิบัติตามข้อกำหนดทางกฎหมายและข้อกำหนดภายในองค์กร
ข้อมูลข่าวกรองด้านภัยคุกคาม (Threat Intelligence Feeds)	ให้ข้อมูลบริบทภัยคุกคามแบบไดนามิก เพื่อใช้ในการประเมินความเสี่ยง และปฏิเสธการเข้าถึงจากแหล่งที่ระบุว่าอันตรายหรือมีช่องโหว่ใหม่
บันทึกกิจกรรมเครือข่ายและระบบ (Network and System Activity Logs)	ให้ข้อมูลสถานะความมั่นคงปลอดภัยแบบเรียลไทม์ ผ่านการรวบรวมบันทึกกิจกรรมและเหตุการณ์เครือข่าย เพื่อตรวจสอบการดำเนินการบนเครือข่ายและการเข้าถึงทรัพยากร
นโยบายการเข้าถึงข้อมูล (Data Access Policies)	กำหนดกฎการอนุญาต (Authorization Rules) พื้นฐาน และแอตทริบิวต์การเข้าถึงสำหรับ ข้อมูลตัวตน แอปพลิเคชัน และบริการ โดยอิงตามความต้องการของภารกิจ
โครงสร้างพื้นฐานกุญแจสาธารณะขององค์กร (Enterprise Public Key Infrastructure)	สนับสนุนการยืนยันตัวตน (Identification) อุปกรณ์ ทรัพยากร และผู้ร้องขอการเข้าถึง ผ่านการออกและจัดการใบรับรองดิจิทัล
ระบบบริหารจัดการตัวตน (ID Management System)	จัดการข้อมูลตัวตน (Identity Data) ของผู้ใช้ (เช่น ชื่อผู้ใช้งาน บทบาท แอตทริบิวต์การเข้าถึง) ซึ่งใช้เป็นอินพุตหลักในกระบวนการอนุญาตให้เข้าถึงทรัพยากร
ระบบจัดการข้อมูลและเหตุการณ์ด้านความมั่นคงปลอดภัย (Security Information and Event Management)	เป็นระบบสำหรับรวบรวมและวิเคราะห์ข้อมูลด้านความมั่นคงปลอดภัย เพื่อปรับปรุงนโยบาย ตรวจจับการโจมตี และเฝ้าระวังภัยคุกคาม

๔.๒ แนวทางการพัฒนาตามสถาปัตยกรรม Zero Trust

องค์กรสามารถนำสถาปัตยกรรม Zero Trust มาประยุกต์ใช้กับนโยบายความมั่นคงปลอดภัยขององค์กรได้หลายแนวทาง โดยแต่ละแนวทางจะแตกต่างกันทั้งในแง่ขององค์ประกอบที่ใช้รวมถึงการรองรับกฎระเบียบข้อบังคับ และนโยบายที่องค์กรกำหนด โดยแต่ละแนวทางแม้ว่าจะเน้นองค์ประกอบที่ต่างกัน แต่ทุกแนวทางยังคงยึดหลักการพื้นฐานของ Zero Trust เหมือนกัน แนวทางที่ใช้ในการพัฒนาสถาปัตยกรรม Zero Trust สามารถแบ่งได้เป็น ๓ กลุ่มหลัก ได้แก่

๑) แนวทางการขับเคลื่อนด้วยการกำกับดูแลตัวตนขั้นสูง (Enhanced Identity Governance-Driven)

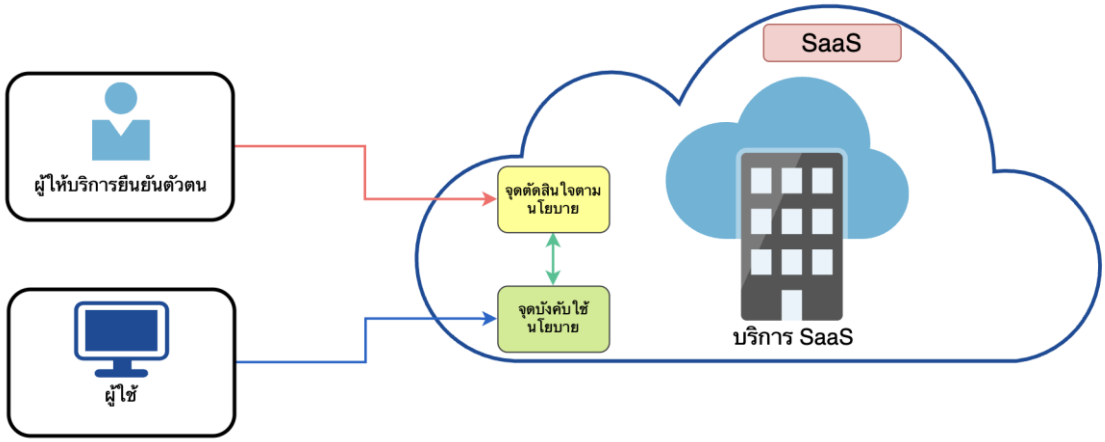
๒) แนวทางการแบ่งส่วนเครือข่ายแบบย่อย (Logical Micro-segmentation)

๓) แนวทางการแบ่งขอบเขตเครือข่ายที่กำหนดด้วยซอฟต์แวร์ (Software-Defined Perimeter)

องค์กรอาจพบว่าระบบในปัจจุบันและนโยบายที่มีอยู่เดิมอาจเหมาะสมสอดคล้องกับแบบใดแบบหนึ่ง แต่ Zero Trust ที่สมบูรณ์อาจจะต้องผสานองค์ประกอบจากทั้ง ๓ แนวทางตามความเหมาะสมและบริบทขององค์กร แม้แนวทางใดแนวทางหนึ่งจะเป็นจุดเริ่มต้นหลัก แต่แนวทางอื่นก็สามารถช่วยเสริมและยกระดับความมั่นคงปลอดภัยโดยรวมให้กับองค์กร

๔.๒.๑ แนวทางการกำกับดูแลตัวตนขั้นสูง (Enhanced Identity Governance)

แนวทางนี้ใช้ “ตัวตน” ของผู้ร้องขอการเข้าถึงเป็นศูนย์กลางของการกำหนดนโยบาย โดยนโยบายการเข้าถึงจะถูกสร้างขึ้นตามแอตทริบิวต์และสิทธิของผู้ร้องขอการเข้าถึงแต่ละราย แม้ตัวตนจะเป็นองค์ประกอบหลักแต่ปัจจัยอื่น เช่น ประเภทของอุปกรณ์ สถานที่ เวลาที่เชื่อมต่อ และบริบทแวดล้อมสามารถส่งผลต่อการประเมินระดับ “ความเชื่อมั่น (Confidence Level)” ในการอนุญาตให้เข้าถึง ซึ่งจะนำไปสู่การอนุญาตแบบเต็มสิทธิ จำกัดสิทธิบางส่วน หรือปฏิเสธการเข้าถึงโดยสิ้นเชิง โดยจุดบังคับใช้นโยบายที่ทำหน้าที่ปกป้องทรัพยากรต้องสามารถตรวจสอบตัวตนได้โดยตรง หรือส่งคำขอไปยังส่วนขับเคลื่อนนโยบายเพื่อทำการประเมินและอนุมัติการเข้าถึงก่อนเปิดให้ใช้งาน ดังรูปที่ ๗



รูปที่ ๗ รูปแบบการทำงานของสถาปัตยกรรม Zero Trust แบบแนวทางการกำกับดูแลตัวตนขั้นสูง

ลักษณะเด่นและการใช้งานที่เหมาะสม

แนวทางนี้เหมาะกับสภาพแวดล้อมที่มีลักษณะ “เครือข่ายแบบเปิด (Open Network)” หรือองค์กรที่มักมี

๑) อุปกรณ์ที่ไม่ใช่ขององค์กรเชื่อมต่อเข้ามาบ่อยครั้ง

๒) การเชื่อมต่อจากบุคคลภายนอก

๓) การทำงานที่ต้องใช้ทรัพยากรร่วมกันระหว่างหลายหน่วยงาน

๔) ไม่สามารถติดตั้งเอเจนต์สำหรับการเชื่อมต่อแบบ Zero Trust

โดยทั่วไป “การเข้าถึงเครือข่ายพื้นฐาน” อาจเปิดกว้างสำหรับทุกอุปกรณ์ แต่การเข้าถึง “ทรัพยากรขององค์กร” ต้องถูกควบคุมอย่างเข้มงวดตามสิทธิของผู้ใช้

ข้อเสีย คือ การเปิดให้เชื่อมต่อกับทรัพยากรได้โดยตรง เป็นช่องทางให้ผู้ไม่ประสงค์ดีทำการสำรวจเป้าหมาย (Reconnaissance) หรือโจมตีเพื่อทำให้ระบบไม่สามารถให้บริการได้ (Denial of Service) รวมถึงรูปแบบที่ไม่ใช้เอเจนต์มีข้อจำกัดในการตรวจสอบสถานะความมั่นคงปลอดภัยของอุปกรณ์ (Security posture) ดังนั้นยังจำเป็นต้องมีการเฝ้าระวังและมีระบบความมั่นคงปลอดภัยที่ตอบสนองต่อภัยคุกคามได้ทันที

แนวทางนี้ใช้งานร่วมกับโมเดลเข้าถึงทรัพยากรผ่านพอร์ทัลได้เป็นอย่างดี และยังเหมาะสำหรับองค์กรที่ใช้บริการคลาวด์ เช่น ซอฟต์แวร์ในรูปแบบบริการ (Software-as-a-Service: SaaS) ที่ไม่สามารถติดตั้งอุปกรณ์เพิ่มเติมสำหรับการทำ Zero Trust ได้โดยตรง ต้องอาศัยการกำกับดูแลตัวตนเป็นหลัก กลไกทางด้าน Zero Trust (จุดตัดสินใจตามนโยบายและจุดบังคับใช้นโยบาย) มักเป็นบริการ หรือความสามารถที่ผนวกรวม (Native) มากับ SaaS

ข้อจำกัดและข้อเสียของแนวทางการกำกับดูแลตัวตนขั้นสูง

แนวทางนี้เป็นแนวทางที่สามารถเริ่มต้นได้ง่าย แต่มีข้อจำกัดที่สำคัญดังนี้

๑) มีความเสี่ยงจากการรวมศูนย์การยืนยันตัวตน (Identity-centric Single Point of Failure) หากบัญชีผู้ใช้ถูกขโมยสิทธิ ผู้โจมตีอาจได้รับสิทธิของผู้ใช้ทั้งหมด เนื่องจากระบบพึ่งพาการยืนยันตัวตนเป็นหลัก

๒) ไม่สามารถทำการแบ่งส่วนเครือข่าย (Segmentation) ได้ โดยแนวทางการกำกับดูแลตัวตนขั้นสูง สามารถควบคุมสิทธิได้ดีแต่ไม่สามารถปิดกั้นการเคลื่อนที่ภายในเครือข่าย (Network Movement) ได้

๓) มีความซับซ้อนด้านการบริหารสิทธิ ซึ่งต้องทำการเชื่อมโยงแอตทริบิวต์ และบริการ มากเกินไปทำให้เกิดปัญหา เช่น

๓.๑) ความซับซ้อนของนโยบายความมั่นคงปลอดภัยที่มากเกินไป ทำให้เกิดความเสี่ยงต่อการตั้งค่าที่ผิดพลาด (Misconfiguration) และลดประสิทธิภาพของ Zero Trust

๓.๒) ความผิดพลาดในการกำหนดสิทธิการเข้าถึงทรัพยากร

๓.๓) การอนุญาตเกินความจำเป็น (Privilege Creep)

๔) เพิ่มความเสี่ยงจากการเปิดพื้นที่การโจมตีที่ระดับเครือข่าย (Reconnaissance Exposure) จาก

๔.๑) การสแกนพอร์ต (Port Scanning)

๔.๒) การสำรวจเป้าหมายเพื่อการโจมตีภายหลัง

๔.๓) การโจมตีเพื่อขัดขวางการให้บริการแบบกระจาย (Distributed Denial of Service: DDoS)

เนื่องจากมีโอกาสถูกโจมตีดังกล่าว จึงควรมีระบบป้องกันหรือใช้บริการทางด้านความมั่นคงปลอดภัยอื่น ๆ เพิ่มตามระดับความเสี่ยง

๕) ไม่เหมาะกับอุปกรณ์เทคโนโลยีเชิงปฏิบัติการ (OT) หรือ อุปกรณ์ IoT ที่ไม่ใช่บุคคล (Human Identity) เช่น เครื่องจักร หุ่นยนต์ ฯลฯ ซึ่งอุปกรณ์ดังกล่าวรองรับการยืนยันตัวตนผ่านใบรับรองดิจิทัลเท่านั้น

๖) ไม่รองรับการตรวจสอบสถานะของอุปกรณ์ (Posture Check) ซึ่งจำเป็นจะต้องติดตั้ง เอเจนต์บนเครื่องลูกข่าย

๔.๒.๒ แนวทางการแบ่งส่วนเครือข่ายแบบย่อย (Micro-Segmentation)

แนวทางนี้เน้นการแบ่งแยกทรัพยากรออกเป็นส่วนย่อย เพื่อจำกัดการเข้าถึงเฉพาะทรัพยากรที่จำเป็น องค์กรจะวางทรัพยากรเดี่ยวหรือกลุ่มทรัพยากรในแต่ละเครือข่ายย่อย ซึ่งถูกป้องกันโดยเกตเวย์ เช่น

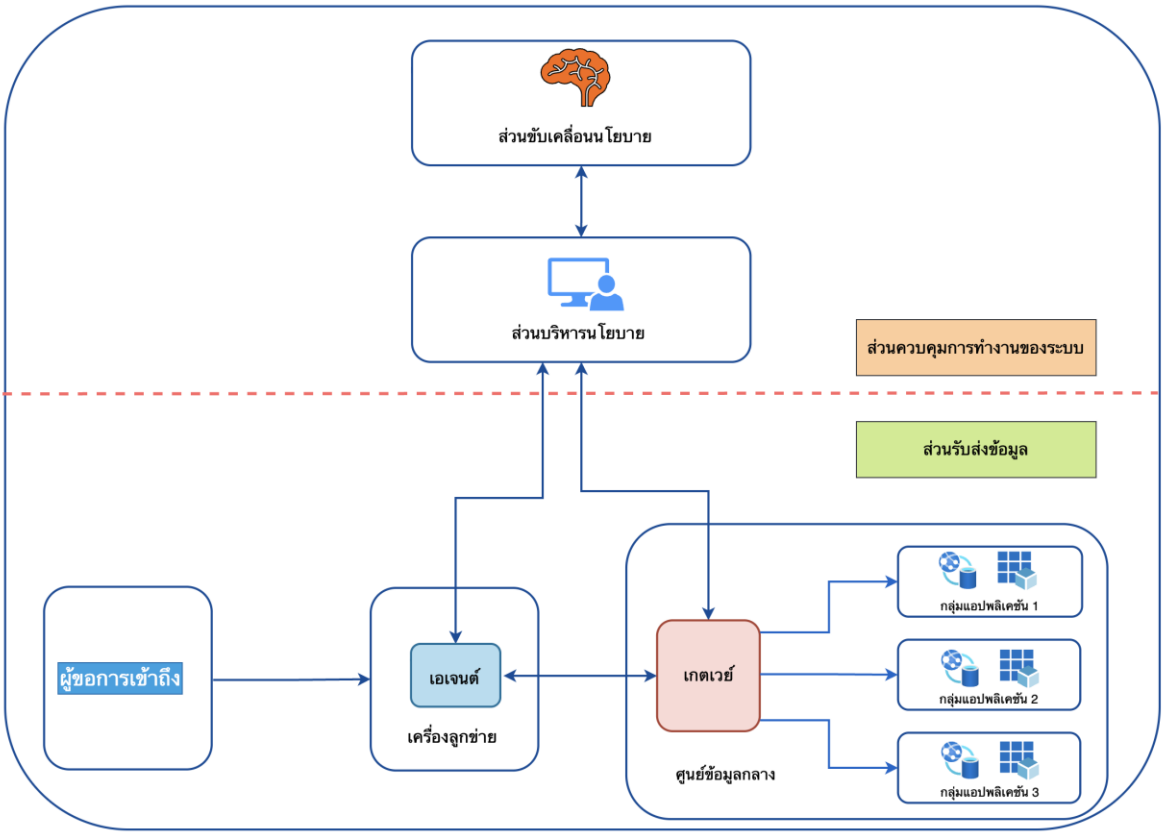
๑) สวิตช์หรือเราเตอร์อัจฉริยะ (Intelligent Switches or Routers)

๒) เน็กซ์เจเนอเรชันไฟร์วอลล์ (NGFW) ที่มีความสามารถตรวจสอบความมั่นคงปลอดภัยขั้นสูง

๓) อุปกรณ์เกตเวย์เฉพาะทาง (Special Purpose Gateway)

๔) การแบ่งส่วนเครือข่ายแบบย่อยบนตัวโฮสต์ (Host-Based) ผ่านซอฟต์แวร์เอเจนต์

องค์ประกอบเหล่านี้ทำหน้าที่เป็นจุดบังคับใช้นโยบายที่ตรวจสอบคำขอ และอนุญาตการเข้าถึงแบบไดนามิกสำหรับแต่ละทรัพยากรที่อยู่ในเครือข่ายย่อย ดังรูปที่ ๘ ซึ่งแนวทางนี้นิยมเรียกว่า Zero Trust Network Access (ZTNA) ในปัจจุบัน โดยมีการผนวกรวมแนวทางการกำกับดูแลตัวตนขั้นสูงไว้ด้วย ซึ่งในแนวทางปฏิบัติฉบับนี้จะกล่าวถึงแนวทาง ZTNA เป็นหลักต่อไป



รูปที่ ๘ รูปแบบการแบ่งส่วนเครือข่ายแบบย่อย

ลักษณะเด่นและการใช้งานที่เหมาะสม

แนวทางนี้เหมาะสำหรับสถานการณ์ที่ต้องการ

๑) การควบคุมย่อยในระดับกลุ่มของทรัพยากร โดยแบ่งตามบริการและผูกกับกลุ่มผู้ใช้งานเท่าที่จำเป็น

๒) การจำกัดการโจมตีแบบการเคลื่อนตัวในเครือข่าย โดยเฉพาะในศูนย์ข้อมูลกลางหรือคลาวด์

๓) ความสามารถในการตอบสนองแบบเรียลไทม์ต่อภัยคุกคาม

การปฏิบัติตามหลักการ Zero Trust

๑) ทุกการเชื่อมต่อถือว่าไม่ปลอดภัยจนกว่าจะผ่านการตรวจสอบสถานะของอุปกรณ์อย่างครบถ้วน

๒) บังคับใช้การตรวจสอบตัวตนและสถานะของอุปกรณ์ทุกครั้งตามหลัก “อย่าเชื่อทันที จงตรวจสอบเสมอ”

๓) อนุญาตให้เข้าถึงเฉพาะทรัพยากรตามนโยบายที่กำหนดไว้สำหรับแต่ละส่วนเครือข่ายย่อย (Segment) ควบคุมโดยเกตเวย์ ZTNA

๔) อำพราง (Obfuscate) ทรัพยากรเพื่อป้องกันการสแกนและการโจมตีโดยตรง

๕) บริหารจัดการสิทธิและนโยบายโดยใช้แนวทางเดียวกับการกำกับดูแลตัวตนขั้นสูง

ตัวเลือกการใช้งาน

ZTNA อาจอยู่ในรูปแบบ

๑) การติดตั้งอุปกรณ์ภายในองค์กร เช่น ภายในศูนย์ข้อมูลกลาง

๒) คลาวด์ของผู้ให้บริการประเภท IaaS

๓) ไฮบริด ซึ่งผสมทั้ง ๒ แบบเข้าด้วยกัน

ข้อสรุป

แนวทางการแบ่งส่วนเครือข่ายแบบย่อย หรือ ZTNA เป็นแนวทางที่ออกแบบมาเพื่อรองรับผู้ใช้ที่อยู่นอกขอบเขตเครือข่ายอย่างปลอดภัย โดยยกระดับจากเครือข่ายส่วนตัวเสมือนแบบดั้งเดิมผ่านการบังคับใช้การเข้าถึงแบบการกำหนดสิทธิเท่าที่จำเป็น และการตรวจสอบตัวตนตามบริบท องค์ประกอบหลักประกอบด้วย (๑) เอเจนต์เพื่อยืนยันตัวตนและตรวจสอบสถานะของอุปกรณ์ (๒) เกตเวย์ ZTNA ที่ติดตั้งก่อนเข้าถึงแอปพลิเคชัน ทำหน้าที่เป็นตัวกลางในการตรวจสอบตัวตน ควบคุมการเข้าถึง และลดความเสี่ยงต่อภัยคุกคาม เช่น การสแกนพอร์ต การโจมตีเพื่อขัดขวางการให้บริการแบบกระจาย ฯลฯ รวมถึงจำกัดการเข้าถึงเฉพาะแอปพลิเคชันที่อนุญาต (Per-Application Access) ช่วยลดการโจมตีแบบการเคลื่อนตัวในเครือข่ายและป้องกันผู้ใช้ที่มีพฤติกรรมผิดปกติ

โดยสรุป ZTNA เหมาะสำหรับการควบคุมการเข้าถึงระดับผู้ใช้ และสามารถใช้ทดแทนเครือข่ายส่วนตัวเสมือนได้ โดยเพิ่มความมั่นคงปลอดภัยผ่านการจำกัดขอบเขตการเข้าถึงตามแอปพลิเคชัน ลดพื้นที่การโจมตีและป้องกันภัยคุกคาม ผ่านการแบ่งส่วนเครือข่ายเป็นเครือข่ายย่อยตามแอปพลิเคชัน ทำให้รองรับสภาพแวดล้อมการทำงานสมัยใหม่ได้อย่างมีประสิทธิภาพ

๔.๒.๓ แนวทางการแบ่งขอบเขตเครือข่ายที่กำหนดด้วยซอฟต์แวร์ (Software-Defined Perimeter: SDP)

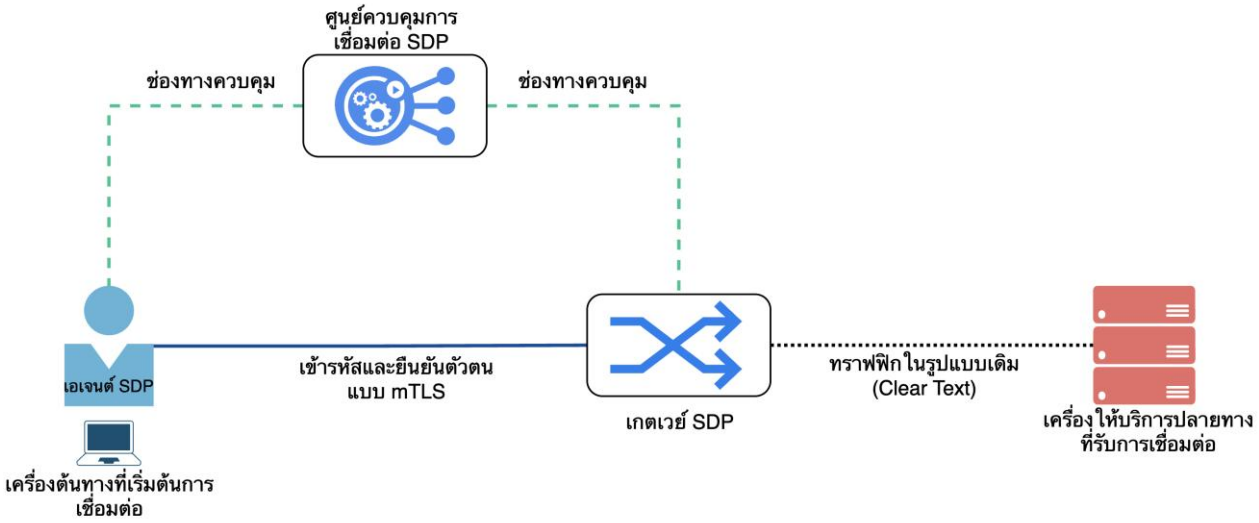
แนวทางการแบ่งขอบเขตเครือข่ายที่กำหนดด้วยซอฟต์แวร์ หรือ SDP เป็นสถาปัตยกรรมการควบคุมการเข้าถึงเครือข่ายที่บังคับใช้หลักการ Zero Trust ในระดับการเชื่อมต่อ ตามแนวคิดของ CSA[๑] โดยยึดหลักการสำคัญคือ “การทำให้บริการทั้งหมดไม่ปรากฏตัวต่อสาธารณะ (Service Cloaking) เป็นค่าเริ่มต้น” เครื่องต้นทางจะไม่สามารถมองเห็นหรือเข้าถึงบริการใดๆ บนเครือข่ายได้จนกว่าจะได้รับการอนุญาตตามสิทธิที่กำหนดไว้ โดยพอร์ต (Port) หรือบริการจะถูกซ่อนไว้จนกว่าจะได้รับอนุญาตผ่านกระบวนการอนุญาตสิทธิด้วยแพ็กเก็ตเดียว (Single Packet Authorization: SPA)

โดยทั่วไป SPA จะประกอบด้วยข้อมูลที่ถูกเข้ารหัส พร้อมกลไกตรวจสอบความถูกต้องของแพ็กเก็ต เช่น MAC/HMAC สำหรับการยืนยันแหล่งที่มาและความถูกต้องของข้อมูล กลไกป้องกันการโจมตี (เช่น ค่าที่สุ่มขึ้นและใช้ได้ครั้งเดียว (Nonce) หรือ ตราประทับเวลา (Timestamp) เพื่อป้องกันการโจมตีโดยการนำข้อมูลเดิมมาใช้ซ้ำ (Replay attack)) ข้อมูลที่ผูกกับตัวตนของเครื่องต้นทาง และข้อมูลที่ระบุบริการที่ต้องการเข้าถึง โดยเครื่องต้นทางจะส่งแพ็กเก็ตที่ถูกเข้ารหัสนี้ไปยังศูนย์ควบคุมการเชื่อมต่อ SDP

(SDP Controller) เพื่อยืนยันตัวตนและตรวจสอบสิทธิเบื้องต้น หากข้อมูลถูกต้องจึงจะอนุญาตให้มีการเชื่อมต่อและเปิดให้เข้าถึงทรัพยากรได้ กลไกนี้ช่วยป้องกันไม่ให้บริการภายในถูกค้นพบหรือถูกสแกนจากบุคคลที่ไม่ได้รับอนุญาต ทำให้การเข้าถึงเป็นแบบถูกเปิดเผยเมื่อได้รับสิทธิเท่านั้น และการเชื่อมต่อที่ได้รับอนุญาตจะถูกปกป้องด้วยการเข้ารหัสแบบการยืนยันตัวตนแบบสองทางด้วย TLS (mTLS) ที่มีการตรวจสอบใบรับรองดิจิทัลทั้งฝั่งต้นทางและฝั่งปลายทาง (ในกรณีนี้คือเกตเวย์ SDP) เพื่อยืนยันตัวตนทั้งสองทางและสร้างความมั่นใจว่าการเชื่อมต่อถูกต้องและเชื่อถือได้ตลอดระยะเวลาของเซสชัน (Session)

องค์ประกอบสำคัญของ SDP[๒] คือ ศูนย์ควบคุมการเชื่อมต่อ SDP ซึ่งทำหน้าที่ตรวจสอบตัวตน อุปกรณ์ และบริบทเชิงนโยบาย ก่อนอนุญาตให้สร้างการเชื่อมต่อระหว่างเครื่องต้นทางที่เริ่มต้นการเชื่อมต่อ (Initiating Host: IH) กับเครื่องปลายทางที่รับการเชื่อมต่อ (Accepting Host: AH) หรือผู้ให้บริการโดยมีกระบวนการตรวจสอบล่วงหน้า (Pre-Vetting) เพื่อยืนยันความถูกต้องและความน่าเชื่อถือของคำร้องตามที่แสดงในรูปที่ ๙ ก่อนที่จะอนุญาตให้มองเห็นทรัพยากรหรือมีการรับส่งข้อมูลใด ๆ ระหว่างกัน

ด้วยแนวคิดการทำให้บริการทั้งหมดไม่ปรากฏตัวต่อสาธารณะ และการเปิดเฉพาะการเชื่อมต่อที่ได้รับอนุญาตหลังการยืนยันตัวตน ทำให้ SDP สามารถลดพื้นที่การถูกโจมตี (Attack Surface) ได้อย่างมีนัยสำคัญ ซึ่งช่วยให้การบังคับใช้นโยบาย Zero Trust ในระดับเครือข่ายมีความแม่นยำและปลอดภัยสูง



รูปที่ ๙ สถาปัตยกรรม SDP และกระบวนการตรวจสอบล่วงหน้า

องค์ประกอบของสถาปัตยกรรม SDP

สถาปัตยกรรม SDP ประกอบด้วย ๕ องค์ประกอบหลัก:

๑. เครื่องต้นทางที่เริ่มต้นการเชื่อมต่อ เช่น เครื่องคอมพิวเตอร์โน้ตบุ๊ก หรืออุปกรณ์เคลื่อนที่ (Mobile Device) ที่เป็นผู้ร้องขอการเชื่อมต่อ

๒. เอเจนต์ SDP เป็นซอฟต์แวร์บนเครื่องต้นทางทำหน้าที่เริ่มการเชื่อมต่อเข้าใช้งานแบบเข้ารหัส พร้อมจัดเตรียมแพ็คเก็ต SPA สำหรับทำการยืนยันตัวตนและตรวจสอบสิทธิก่อนเข้าใช้งาน

๓. ศูนย์ควบคุมการเชื่อมต่อ SDP ทำหน้าที่ตรวจสอบตัวตน ยืนยันอุปกรณ์ และควบคุมกระบวนการตรวจสอบล่วงหน้า ซึ่งเป็นขั้นตอนที่ศูนย์ควบคุมการเชื่อมต่อ SDP ใช้ตรวจสอบว่า ตัวตนของผู้ใช้และอุปกรณ์มีความถูกต้องและมีสิทธิเพียงพอ ก่อนที่ระบบจะให้เริ่มต้นเซสชัน หรือเปิดเผยบริการ

๔. เครื่องปลายทางที่รับการเชื่อมต่อ หรือบริการที่จะได้รับอนุญาตให้เข้าใช้ หลังผ่านการตรวจสอบและเป็นทรัพยากรที่ถูกปกป้องด้วยสถาปัตยกรรม SDP

๕. เกตเวย์ SDP คือจุดบังคับใช้นโยบายและควบคุมการเชื่อมต่อไปยังบริการที่ไม่ปรากฏตัวต่อสาธารณะ เพื่อให้ผู้ใช้และอุปกรณ์ที่ได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงบริการที่ได้รับการปกป้องตามหลักการ “ปฏิเสธทุกการเข้าถึงเป็นค่าเริ่มต้น และอนุญาตเฉพาะการเชื่อมต่อที่ผ่านการตรวจสอบแล้วเท่านั้น” พร้อมรองรับการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยและการบันทึกการเชื่อมต่อ

การปฏิบัติตามหลักการ Zero Trust ใน SDP

แนวทางของ SDP สอดคล้องกับ Zero Trust ตามประเด็นสำคัญดังต่อไปนี้

๑) ใช้เกตเวย์แบบปฏิเสธทุกการเข้าถึงเป็นค่าเริ่มต้นเป็นจุดบังคับใช้นโยบาย และเปิดช่องทางเชื่อมต่อเฉพาะเมื่อกระบวนการ SPA ยืนยันแล้วว่าเป็นเครื่องต้นทางที่ได้รับสิทธิอย่างถูกต้อง

๒) การตรวจสอบตัวตนและสิทธิการเข้าถึงต้องเกิดขึ้นและสำเร็จก่อนการมองเห็นหรือเชื่อมต่อไปยังเครื่องปลายทางที่ให้บริการ โดยบริการของเครื่องปลายทางที่รับการเชื่อมต่อ จะไม่ปรากฏหรือไม่สามารถเข้าถึงได้ จนกว่าจะได้รับการอนุญาตจากศูนย์ควบคุมการเชื่อมต่อ SDP

๓) การกำกับสิทธิให้จำกัดเฉพาะเท่าที่จำเป็นต่อการใช้งานแต่ละบริการ โดยแต่ละบริการมีนโยบายกำกับของตนเอง ทำให้สามารถกำหนดสิทธิได้ละเอียดและสามารถป้องกันการเข้าถึงทรัพยากรที่ไม่เกี่ยวข้องได้

๔) เกตเวย์ SDP ทำงานประสานกับศูนย์ควบคุมการเชื่อมต่อ SDP เพื่อทำหน้าที่เป็นศูนย์รวมข้อมูล ช่วยให้การตรวจสอบพฤติกรรม การเก็บบันทึกเหตุการณ์ และการวิเคราะห์ความมั่นคงปลอดภัยเป็นไปอย่างครบถ้วน

ลักษณะเฉพาะของ SDP

๑) ใช้กระบวนการ SPA ในการยืนยันตัวตน โดยการอนุญาตเกิดขึ้นในระดับเครือข่ายก่อนที่ฝั่งต้นทางจะเห็นหรือเข้าถึงบริการบนเครื่องปลายทาง ส่งผลให้ลดพื้นที่การถูกโจมตีและป้องกันการสแกนหรือค้นหาทรัพยากรที่ไม่ได้รับอนุญาตได้อย่างมีนัยสำคัญ

๒) ทำการเข้ารหัสการเชื่อมต่อด้วยรูปแบบ mTLS ทำให้สามารถยืนยันตัวตนทั้งสองฝั่ง สร้างความมั่นใจว่าการสื่อสารจะเกิดขึ้นระหว่างผู้รับและผู้ส่งที่เชื่อถือได้เท่านั้น

๓) ต้องติดตั้งเอเจนต์เพื่อสร้างการเชื่อมต่อแบบ mTLS ไม่รองรับการทำงานในแบบไม่ใช้เอเจนต์และไม่สามารถทำงานร่วมกับระบบอื่นที่ไม่รองรับ mTLS

จากเอกสารอ้างอิงของ CSA สถาปัตยกรรม SDP มุ่งเน้นไปที่การตรวจสอบล่วงหน้าจึงมีข้อจำกัดในการตรวจสอบสถานะความมั่นคงปลอดภัยของอุปกรณ์แบบต่อเนื่องระหว่างเซสชัน ซึ่งเป็นความสามารถสำคัญของ Zero Trust ยุคใหม่ ทำให้สถาปัตยกรรม SDP ตามแนวทางของ CSA ไม่สอดคล้องกับความต้องการขององค์กรที่ต้องการนำ Zero Trust ไปใช้งานอย่างเต็มรูปแบบ แต่อย่างไรก็ตามในปัจจุบันผู้ผลิต SDP บางราย ได้มีการนำคุณสมบัตินี้เพิ่มเข้ามาในสถาปัตยกรรม SDP ของตน หรืออาจมีการเพิ่มเติมในภายหลัง ทำให้ SDP มีความคล้ายคลึงกับ ZTNA และกลายเป็นอีกทางเลือกหนึ่งที่มีความมั่นคงปลอดภัยตามแนวคิด Zero Trust อย่างสมบูรณ์

๔.๒.๔ บทสรุปแนวทางของสถาปัตยกรรม Zero Trust

ในยุคที่สถาปัตยกรรม Zero Trust กลายเป็นแนวปฏิบัติหลักในการออกแบบระบบความมั่นคงปลอดภัยไซเบอร์ องค์กรจำเป็นต้องประเมินแนวทางการควบคุมการเข้าถึง (Access Control Models) ที่เหมาะสมกับองค์กรของตน ซึ่งสามารถสรุปข้อดีข้อเสียของแต่ละแนวทางได้ดังต่อไปนี้

ตารางที่ ๒๓ แสดงข้อดีข้อเสียของสถาปัตยกรรม Zero Trust แต่ละแนวทาง

แนวทาง Zero Trust	กลไกการบังคับใช้หลัก	ข้อดี (Pros)	ข้อเสีย (Cons)
๑. แนวทางการกำกับดูแลตัวตนขั้นสูง	ตัวตนของผู้ใช้ นโยบายการเข้าถึง และการกำกับดูแล	๑) เป็นไปตามหลักการ Zero Trust ขั้นพื้นฐานที่ต้องรู้จักตัวตนผู้ใช้ก่อน ๒) การเริ่มต้นเปลี่ยนผ่านไปยัง Zero Trust ทำได้ง่าย เพราะความสามารถ Zero Trust ฝั่งเกตเวย์มักเป็นบริการที่ฝังอยู่ใน SaaS ที่ง่ายต่อการนำไปใช้งาน	๑) ไม่เหมาะสมกับอุปกรณ์หรือบริการที่ไม่สามารถยืนยันตัวตนได้ ๒) ขาดความสามารถในการป้องกันการโจมตีแบบการเคลื่อนตัวในเครือข่าย

แนวทาง Zero Trust	กลไกการบังคับใช้หลัก	ข้อดี (Pros)	ข้อเสีย (Cons)
๒. แนวทางการแบ่งส่วนเครือข่ายแบบย่อย	การแบ่งเครือข่ายด้วยเกตเวย์ ZTNA และแท็ก ZTNA หรือสถานะของอุปกรณ์	๑) ใช้แนวทางการแบ่งส่วนเครือข่ายแบบย่อยในการจำกัดการเข้าถึงแต่ละ ๒) แอปพลิเคชัน (Application-Specific Access) แทนที่การเข้าถึงเครือข่ายทั้งหมด ๓) จำกัดการโจมตีแบบการเคลื่อนตัวในเครือข่าย ๔) ตอบสนองต่อภัยคุกคามแบบเรียลไทม์	๑) ต้องมีการติดตั้งเกตเวย์ ZTNA และแบ่งเครือข่ายให้เหมาะสม ซึ่งจะมีความยุ่งยากถ้าเป็นระบบขนาดใหญ่ ๒) ต้องติดตั้งเอเจนต์ ZTNA บนอุปกรณ์เครื่องลูกข่ายเพื่อรวบรวมข้อมูลสถานะของอุปกรณ์
๓. แนวทางการแบ่งขอบเขตเครือข่ายที่กำหนดด้วยซอฟต์แวร์ (ตามแนวทางของ CSA)	การซ่อนและจำกัดการมองเห็นทรัพยากร (Resource Cloaking)	๑) ทรัพยากรจะไม่ปรากฏต่อผู้ใช้จนกว่าจะได้รับสิทธิอย่างชัดเจน ซึ่งช่วยลดพื้นที่การโจมตีได้อย่างมีนัยสำคัญ	๑) มีข้อจำกัดในการตรวจสอบสถานะของอุปกรณ์ และการตรวจสอบสถานะของอุปกรณ์แบบต่อเนื่องในระหว่างเซสชัน (Continuous Posture Assessment) ส่งผลให้ไม่สามารถตรวจพบความเสี่ยงต่าง ๆ ที่อาจเกิดขึ้น ระหว่างการใช้งานได้อย่างมีประสิทธิภาพ ๒) ต้องติดตั้งเอเจนต์ SDP บนอุปกรณ์ที่ต้องการเข้าถึงทรัพยากร เพื่อสร้างการเชื่อมต่อแบบ mTLS จึงมีข้อจำกัดด้านความยืดหยุ่นในรูปแบบการนำไปใช้และการรองรับอุปกรณ์ที่มีความหลากหลาย ๓) มีความยุ่งยากในการจัดการใบรับรองดิจิทัลให้กับทั้งสองฝั่ง

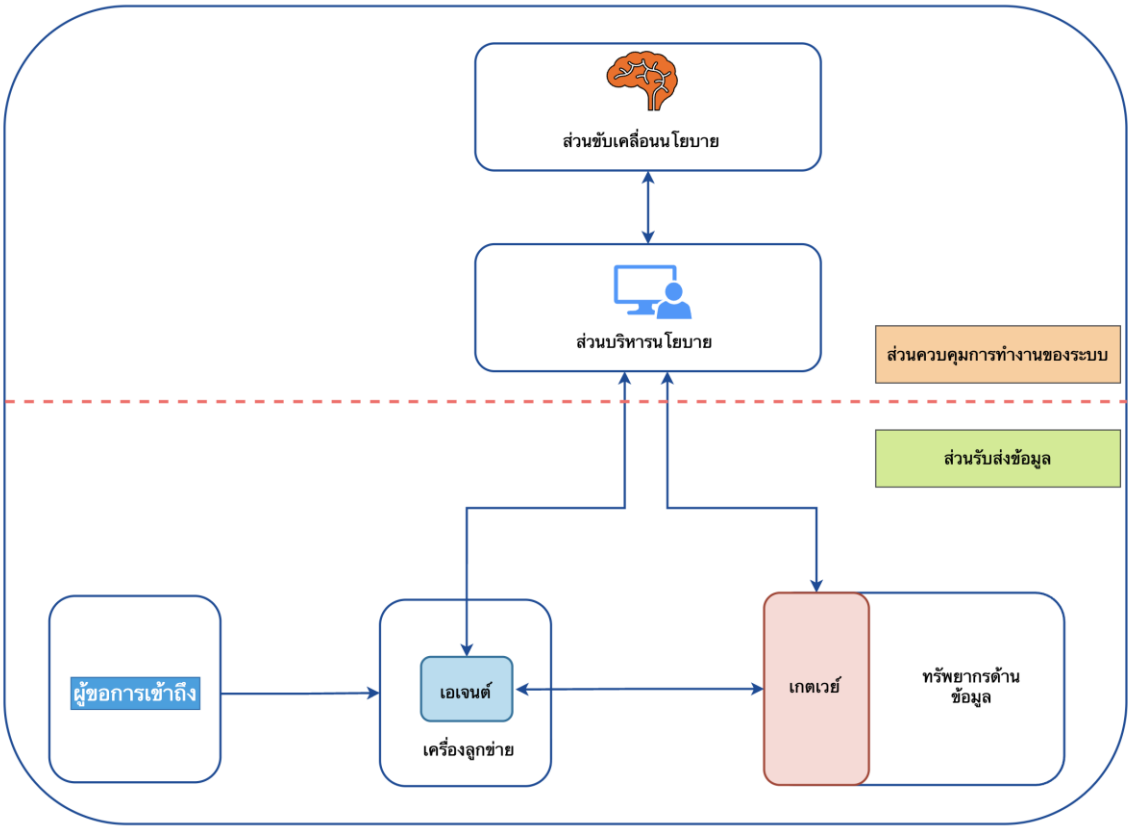
จากตารางด้านบนเป็นข้อมูลสนับสนุนเชิงเทคนิคว่าทำไมองค์กรควรใช้ **“แนวทางการแบ่งส่วนเครือข่ายแบบย่อย”** ที่พัฒนามาเป็น ZTNA ในปัจจุบัน ซึ่งจะกล่าวถึงรายละเอียดในบทที่ **๕ แนวทางปฏิบัติในการติดตั้งและนำไปใช้งานระบบ Zero Trust”** ต่อไป

๔.๓ รูปแบบการนำไปใช้งาน (Deployment) ของสถาปัตยกรรมเชิงนามธรรม

การปรับใช้สถาปัตยกรรม Zero Trust ในระดับองค์กรไม่จำกัดอยู่เพียงสถาปัตยกรรมเชิงตรรกะ (Logical Architecture) เท่านั้น แต่ต้องคำนึงถึงวิธีการนำไปใช้งานจริงให้เหมาะสมกับระบบเดิม ประเภทของทรัพยากร และความสามารถในการบริหารจัดการอุปกรณ์ขององค์กร องค์ประกอบเชิงตรรกะของ Zero Trust หนึ่งองค์ประกอบอาจทำหน้าที่หลายบทบาท เช่น ทำหน้าที่เป็นทั้งส่วนขับเคลื่อนนโยบายและส่วนบริหารนโยบาย หรือกระจายบทบาทเดียวให้ทำงานบนหลายอุปกรณ์เพื่อเพิ่มความพร้อมใช้งานและกระจายความเสี่ยง และรองรับการบังคับใช้นโยบายในสภาพแวดล้อมที่ต้องกระจายการทำงานของระบบออกไปหลายจุด หรือหลายไซต์

ด้วยเหตุนี้จึงมีการพัฒนารูปแบบการนำไปใช้งาน (Deployment Variations)[๓] ในองค์กรเป็นหลายรูปแบบ ซึ่งแต่ละรูปแบบตอบสนองระดับความสามารถในการบังคับใช้นโยบาย การบริหารจัดการ และระดับความเข้มข้นด้านความมั่นคงปลอดภัยที่ต่างกันดังนี้

๔.๓.๑ การติดตั้งแบบเอเจนต์และเกตเวย์ (Device Agent and Gateway)



รูปที่ ๑๐ รูปแบบเอเจนต์บนอุปกรณ์ปลายทาง และเกตเวย์

โมเดลนี้วางจุดบังคับใช้นโยบายไว้ที่เกตเวย์ ซึ่งอยู่ก่อนเข้าถึงแต่ละทรัพยากร ตามที่แสดงในรูปที่ ๑๐ โดยคำร้องทั้งหมดถูกเริ่มต้นจากเอเจนต์บนเครื่องลูกข่าย โดยเอเจนต์จะทำหน้าที่รวบรวมข้อมูลการยืนยันตัวตนและสถานะของอุปกรณ์ แล้วส่งต่อไปยังจุดตัดสินใจตามนโยบายที่ประกอบด้วยส่วนขับเคลื่อนนโยบายและส่วนบริหารนโยบาย ในขั้นตอนนี้ส่วนบริหารนโยบายจะเป็นผู้รับคำร้องจากเอเจนต์และส่งให้ส่วนขับเคลื่อนนโยบายประเมินสิทธิตามตัวตน อุปกรณ์ และบริบทตามนโยบายขององค์กร

หากได้รับอนุญาตส่วนบริหารนโยบายที่อยู่ในชั้นควบคุม (Control Plane) จะสั่งให้เกตเวย์เปิดช่องทางการสื่อสารแบบเข้ารหัสระหว่างเอเจนต์กับเกตเวย์เพื่อเข้าใช้ทรัพยากรที่ได้รับสิทธิ พร้อมกำหนดค่าเชิงเทคนิค เช่น ที่อยู่ไอพี พอร์ต คีย์เข้ารหัส หรือข้อมูลประกอบอื่นที่จำเป็นสำหรับการสร้างเซสชันที่ปลอดภัย การเชื่อมต่อนี้จะถูกใช้งานจนกว่ากระบวนการทำงานจะเสร็จสิ้น หรือจนกว่าจะถูกยกเลิกตามคำสั่งจากส่วนบริหารนโยบาย เช่น เซสชันหมดอายุ การตรวจสอบตัวตนล้มเหลว หรือเกิดเหตุการณ์ความเสี่ยงด้านความมั่นคงปลอดภัยขึ้น

สถาปัตยกรรมนี้ทำให้การควบคุมการเข้าถึงแต่ละทรัพยากรมีความมั่นคงปลอดภัย และกำหนดสิทธิตามระดับผู้ใช้และอุปกรณ์ได้อย่างมีประสิทธิภาพ

ลักษณะเด่นของรูปแบบเอเจนต์และเกตเวย์

๑) รองรับนโยบายแบบไดนามิกและต่อยอดไปสู่ ZTNA สมัยใหม่

๒) สามารถทำการตรวจสอบสถานะของอุปกรณ์รวมถึงควบคุมเซสชันได้อย่างละเอียด

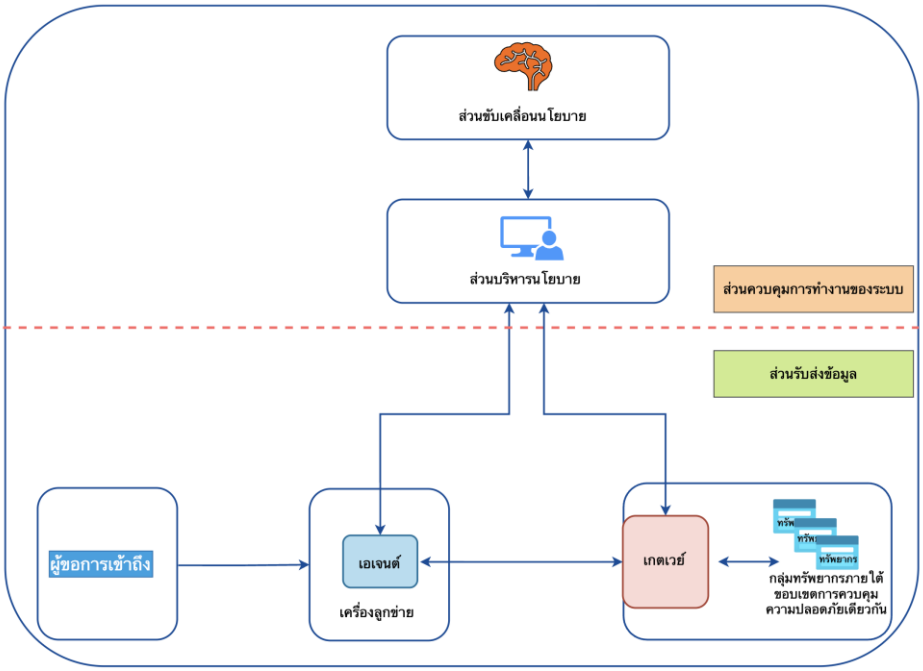
ข้อเสีย

๑) จะต้องมีเกตเวย์สำหรับแต่ละทรัพยากร ซึ่งเป็นไปได้ยากในการนำไปใช้จริง

๒) ต้องติดตั้งเอเจนต์บนอุปกรณ์ฝั่งผู้ใช้เพื่อให้สามารถตรวจสอบตัวตน สถานะ และความถูกต้องของอุปกรณ์ และสร้างช่องทางเชื่อมต่อที่ได้รับอนุญาต

๔.๓.๒ การใช้เกตเวย์ร่วม (Enclave-Based)

รูปแบบนี้จะเหมาะกับองค์กรที่ไม่สามารถติดตั้งเกตเวย์ให้ทรัพยากรแต่ละตัวได้ เช่น ระบบงานดั้งเดิม (Legacy System) ที่ไม่สามารถปรับเปลี่ยนสถาปัตยกรรมได้ หรือบริการที่ผูกกับสภาพแวดล้อมการทำงานเดิม จึงย้ายเกตเวย์ไปอยู่ที่ส่วนหน้าหรือขอบของกลุ่มทรัพยากร (Enclave) ที่สามารถป้องกันระบบหรือทรัพยากรทั้งหมดได้ในจุดเดียว ตามที่แสดงในรูปที่ ๑๑ แนวคิดนี้ช่วยลดความซับซ้อนของการติดตั้งเกตเวย์จำนวนมาก โดยอาศัยกลไกควบคุมการเข้าถึงผ่านจุดบังคับใช้นโยบายที่ระดับเครือข่ายที่ทำหน้าที่ควบคุมการเข้าถึงทรัพยากรในขอบเขตเดียวกัน



รูปที่ ๑๑ แสดงการใช้เกตเวย์ร่วม ในการป้องกันกลุ่มทรัพยากร

ลักษณะเด่นของรูปแบบการใช้เกตเวย์ร่วม

๑) เหมาะกับสภาพแวดล้อมที่มีศูนย์ข้อมูลกลางแบบดั้งเดิม และมีข้อจำกัดด้านการปรับแต่งสถาปัตยกรรมที่ทำให้การออกแบบหรือปรับเปลี่ยนใหม่ทำได้ยาก

๒) ลดภาระในการติดตั้งเกตเวย์ให้กับแต่ละทรัพยากร โดยใช้เกตเวย์ร่วมกัน

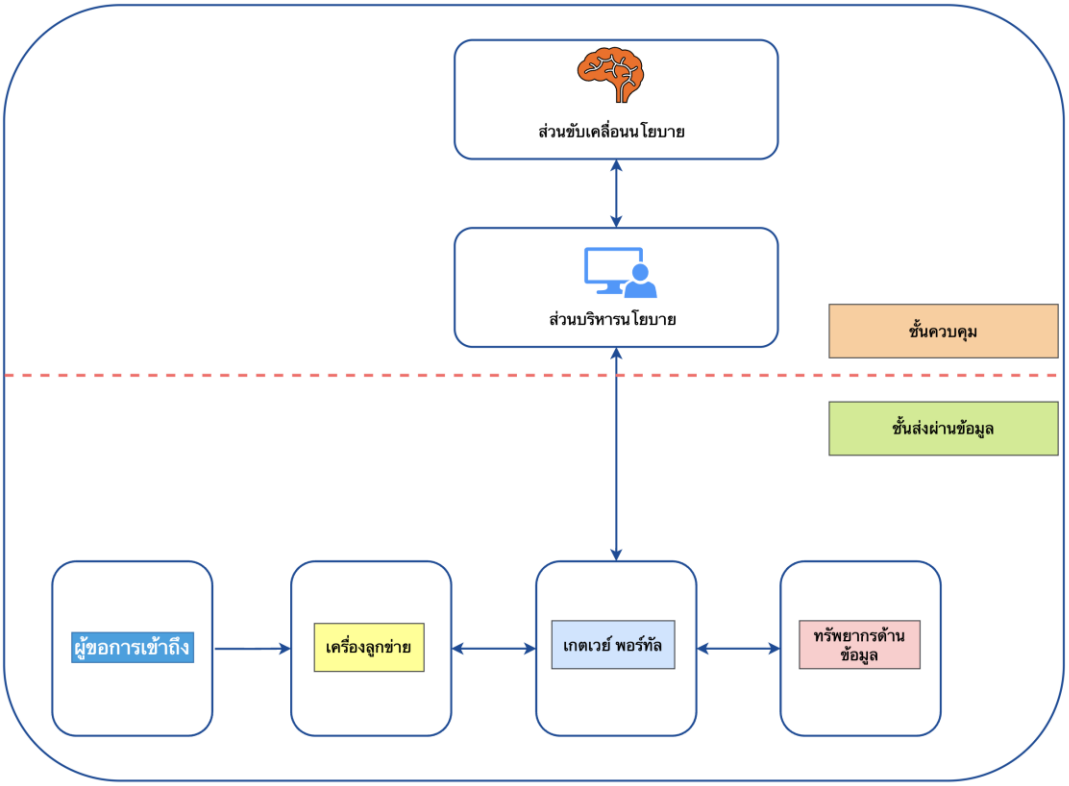
ข้อเสีย

ต้องติดตั้งเอเจนต์บนอุปกรณ์ฝั่งผู้ใช้เพื่อให้สามารถตรวจสอบตัวตน สถานะและความถูกต้องของอุปกรณ์ และสร้างช่องทางเชื่อมต่อที่ได้รับอนุญาต

๔.๓.๓ แบบผ่านพอร์ทัล (Portal-Based Deployment)

ในสถาปัตยกรรมนี้มีพอร์ทัลเป็นจุดทางเข้า (Portal) สำหรับการเข้าถึงทรัพยากรขององค์กร ผู้ใช้งานต้องเชื่อมต่อผ่านพอร์ทัลทุกครั้งก่อนเข้าถึงบริการหรือข้อมูล โดยเกตเวย์พอร์ทัลทำหน้าที่ตรวจสอบคำร้อง ยืนยันตัวตนและบังคับใช้นโยบายก่อนส่งต่อคำร้องไปยังทรัพยากรปลายทาง ดังรูปที่ ๑๒ การทำงานลักษณะนี้ช่วยให้ผู้ใช้เข้าถึงบริการได้โดยไม่จำเป็นต้องติดตั้งเอเจนต์บนเครื่องลูกข่าย จึงเหมาะกับสภาพแวดล้อมที่มีผู้ใช้งานหรืออุปกรณ์ที่หลากหลาย เช่น พนักงาน ลูกค้า คู่ค้า หรืออุปกรณ์ที่อยู่นอกการควบคุมขององค์กร

อย่างไรก็ตาม ความสามารถด้านการตรวจสอบสถานะของอุปกรณ์ยังคงมีข้อจำกัด เนื่องจากพอร์ทัลสามารถเห็นข้อมูลของอุปกรณ์เฉพาะในขณะที่มีการเชื่อมต่อหรือใช้งานเท่านั้น ไม่สามารถติดตามการเปลี่ยนแปลงด้านสถานะความมั่นคงปลอดภัยของอุปกรณ์หรือประเมินระดับความเสี่ยงได้เช่นเดียวกับการติดตั้งเอเจนต์บนอุปกรณ์ปลายทาง ที่ให้การตรวจสอบเชิงลึก และช่วยสนับสนุนให้สามารถปรับสิทธิแบบไดนามิกตลอดอายุการใช้งานของเซสชันได้



รูปที่ ๑๒ รูปแบบผ่านพอร์ทัล

ลักษณะเด่นของรูปแบบผ่านพอร์ทัล

๑) เพิ่มความยืดหยุ่นในการเข้าถึง พร้อมลดภาระการติดตั้งเอเจนต์

๒) รองรับผู้ใช้งานหลายประเภทได้ดี เช่น พนักงาน ลูกค้า คู่ค้า หรือบุคคลภายนอก

ข้อเสีย

๑) ไม่สามารถตรวจสอบสถานะของอุปกรณ์ปลายทางเชิงลึกได้

เอกสารอ้างอิง

- Cloud Security Alliance, Software Defined Perimeter Architecture, 2020.
- Cloud Security Alliance, Introduction to Software-Defined Perimeter (CCZT Study Guide), Version 20250219, 2025.
- S. Rose, O. Borchert, S. Mitchell, and S. Connelly, “Zero Trust Architecture”, NIST Special Publication 800-207, 2020.

บทที่ ๕
แนวทางปฏิบัติในการติดตั้งและนำไปใช้งานระบบ Zero Trust

๕.๑ แนวทางปฏิบัติในการติดตั้งและนำไปใช้งาน Zero Trust แบบ ZTNA

ZTNA เป็นแนวทางที่ทำให้องค์กรสามารถปกป้องทรัพยากรได้สอดคล้องกับวิถีการทำงานแบบไฮบริด ที่สามารถต่อสู้กับภัยคุกคามสมัยใหม่ ทั้งในสภาพแวดล้อมแบบคลาวด์ และภายในเครือข่ายขององค์กร ซึ่งการติดตั้ง ZTNA มีแนวทางปฏิบัติที่สำคัญ ดังต่อไปนี้

แนวทางตรวจสอบสถานะของอุปกรณ์ด้วยเอเจนต์ ZTNA

เอเจนต์ ZTNA (หรือเอเจนต์บนอุปกรณ์ปลายทาง) คือ ซอฟต์แวร์ที่ติดตั้งบนอุปกรณ์ปลายทางของผู้ใช้ในสถาปัตยกรรม Zero Trust บทบาทหลักของเอเจนต์คือการรวบรวมข้อมูลสถานะของอุปกรณ์ และการตรวจสอบสถานะของอุปกรณ์อย่างเข้มงวดก่อนและระหว่างการอนุญาตให้เข้าถึงทรัพยากร

การตรวจสอบต่อเซสชัน

การตรวจสอบต่อเซสชัน คือ การเริ่มต้นการประเมินความน่าเชื่อถือในทุกคำขอเข้าถึงทรัพยากร เอเจนต์มีบทบาทสำคัญในการจัดการกระบวนการนี้ร่วมกับส่วนขับเคลื่อนนโยบายและจุดบังคับใช้นโยบาย การตรวจสอบตัวตนของผู้ใช้เอเจนต์ช่วยให้มั่นใจว่าผู้ใช้ที่กำลังเข้าถึงทรัพยากรนั้นเป็นบุคคลที่กล่าวอ้างจริง และมีสิทธิในระดับที่เหมาะสม โดยสนับสนุนกลไกการยืนยันตัวตนที่หลากหลาย เช่น

๑) การยืนยันตัวตนแบบหลายปัจจัย เอเจนต์ยืนยันว่าผู้ใช้ได้ผ่านการยืนยันตัวตนอย่างน้อยสองปัจจัยขึ้นไป (เช่น รหัสผ่าน และโทเค็นมือถือหรือไบโอเมตริก (Biometric)) ก่อนได้รับอนุญาตให้เข้าถึงทรัพยากร

๒) การยืนยันตัวตนแบบไม่ใช้รหัสผ่าน (Passwordless) สนับสนุนเทคโนโลยีการยืนยันตัวตนสมัยใหม่ที่ไม่ใช้รหัสผ่าน (เช่น FIDO2) เพื่อเพิ่มความมั่นคงปลอดภัยและลดความเสี่ยงจากการโจมตีแบบฟิชชิง

๓) การยืนยันตัวตนครั้งเดียว (Single Sign-On: SSO) เอเจนต์ผสานรวมกับผู้ให้บริการยืนยันตัวตนขององค์กร เพื่อใช้ตัวตนของผู้ใช้อันเดียวกันในการเข้าถึงแอปพลิเคชันต่าง ๆ อย่างปลอดภัย โดยไม่ต้องป้อนข้อมูลหรือยืนยันตัวตนซ้ำ

๔) การยืนยันตัวตนโดยใช้ใบรับรองดิจิทัล ที่สามารถนำไปใช้ในการยืนยันตัวตนได้ทั้งบุคคลและอุปกรณ์ เช่น อุปกรณ์ OT และอุปกรณ์ IoT

การตรวจสอบสถานะของอุปกรณ์

นี่คือหัวใจสำคัญของการทำ Zero Trust โดยเอเจนต์จะรวบรวมข้อมูลสถานะด้านความมั่นคงปลอดภัยของอุปกรณ์ปลายทางแบบเรียลไทม์ เพื่อส่งให้ส่วนขับเคลื่อนนโยบายประเมินผล หน้าที่ที่สำคัญของเอเจนต์เช่น

๑) ยืนยันว่าอุปกรณ์ได้รับการลงทะเบียน (Registered) และเป็นขององค์กร (Owned/Managed) โดยมักใช้ใบรับรองดิจิทัลของเครื่องลูกข่าย (Device Certificate) หรือรหัสเฉพาะ (Unique ID)

๒) ตรวจสอบว่าระบบปฏิบัติการถูกอัปเดตให้อยู่ในเวอร์ชันที่ปลอดภัยตามข้อกำหนดขององค์กรหรือไม่ เพื่อหลีกเลี่ยงช่องโหว่ของระบบปฏิบัติการเวอร์ชั่นเก่า

๓) ตรวจสอบว่าซอฟต์แวร์ป้องกันไวรัสถูกติดตั้งทำงานอยู่ และได้รับการอัปเดตฐานข้อมูลล่าสุดแล้ว

๔) ตรวจสอบช่องโหว่ (Vulnerability Assessment) โดยการประเมินช่องโหว่พื้นฐานของอุปกรณ์ เพื่อให้แน่ใจว่าอุปกรณ์ไม่ได้มีช่องโหว่ร้ายแรงที่ยังไม่ได้รับการแก้ไข

จากตัวอย่างด้านบนเป็นแค่เพียงส่วนหนึ่งเท่านั้น องค์กรสามารถกำหนดการตรวจสอบสถานะเพิ่มเติม ตามความเสี่ยงและความเหมาะสมขององค์กรได้

การตรวจสอบอย่างต่อเนื่อง

เอเจนต์ ZTNA ไม่ได้หยุดการตรวจสอบเมื่อได้รับอนุญาตให้เข้าถึงแล้ว แต่ยังคงตรวจสอบสถานะด้านความมั่นคงปลอดภัยของอุปกรณ์ปลายทาง และพฤติกรรมของผู้ใช้ตลอดระยะเวลาของเซสชัน

๑) สถานะของอุปกรณ์ เอเจนต์ตรวจสอบปัจจัยด้านความมั่นคงปลอดภัยของอุปกรณ์ปลายทางอย่างละเอียดและต่อเนื่อง เช่น หากผู้ใช้ทำการปิดไฟร์วอลล์ หรือถอนการติดตั้งซอฟต์แวร์ป้องกันไวรัสระหว่างเซสชัน เอเจนต์จะรายงานข้อมูลนี้ไปยังส่วนขับเคลื่อนนโยบายทันที ซึ่งอาจส่งผลให้ส่วนขับเคลื่อนนโยบายสั่งการให้ส่วนบริหารนโยบาย เพิกถอนหรือลดสิทธิการเข้าถึง (Re-Authenticate or Revoke Access)

๒) พฤติกรรมผู้ใช้ (User Behavior) เอเจนต์ร่วมกับระบบวิเคราะห์พฤติกรรมผู้ใช้ในการตรวจสอบพฤติกรรมการใช้งานของผู้ใช้ เช่น หากผู้ใช้รายหนึ่งเริ่มดาวน์โหลดข้อมูลปริมาณมากอย่างผิดปกติ หรือเข้าถึงแอปพลิเคชันที่ไม่เคยใช้ ระบบจะทำการประเมินความเสี่ยงใหม่ และอาจสั่งให้เอเจนต์บังคับให้ผู้ใช้ยืนยันตัวตนซ้ำ หรือถูกจำกัดการเข้าถึงทรัพยากรโดยระบบ

การควบคุมแบบละเอียด (Granular Control)

เกตเวย์ ZTNA หรือจุดบังคับใช้นโยบายทำหน้าที่เป็นจุดควบคุมการเข้าถึงตามนโยบายขั้นสุดท้าย เพื่อจำกัดทรัพยากรที่ผู้ใช้และอุปกรณ์สามารถเข้าถึงได้จริง ตามหลักการได้รับสิทธิเท่าที่จำเป็น

๑) การอนุญาตให้เข้าถึงได้เฉพาะแอปพลิเคชันที่ได้รับสิทธิเท่านั้น เอเจนต์ ZTNA สร้างช่องทางการเชื่อมต่อแบบเข้ารหัส (Encrypted Tunnel) โดยตรงไปยังจุดบังคับใช้นโยบาย และหลังจากการตรวจสอบสิทธิและสถานะเรียบร้อยแล้ว ผู้ใช้จะสามารถเข้าถึงแอปพลิเคชันที่ได้รับอนุญาตเท่านั้น

๒) เกตเวย์ ZTNA หรือจุดบังคับใช้นโยบายจะรับคำสั่งจากส่วนบริหารนโยบาย เพื่อเปิดหรือปิดการเชื่อมต่อจากเอเจนต์ ทำให้มั่นใจว่าผู้ใช้เห็นและเข้าถึงได้เฉพาะแอปพลิเคชันที่จำเป็นต่อการทำงานเท่านั้น

เอเจนต์ ZTNA เป็นองค์ประกอบที่เป็นกลไกสำคัญที่ทำให้สถาปัตยกรรม Zero Trust สามารถดำเนินการได้อย่างสมบูรณ์ โดยให้ความสามารถในการตรวจสอบ การวัดระดับความมั่นคงปลอดภัยของอุปกรณ์ปลายทาง และการเฝ้าระวังพฤติกรรมอย่างต่อเนื่อง ข้อมูลเหล่านี้ช่วยให้เกตเวย์ ZTNA สามารถบังคับใช้การเข้าถึงแบบจำกัดสิทธิได้ในระดับแอปพลิเคชัน ซึ่งเป็นรากฐานสำคัญของสถาปัตยกรรม Zero Trust สำหรับองค์กรยุคใหม่

แนวทางการกำหนดนโยบาย Zero Trust

นโยบาย Zero Trust[๑] ทำหน้าที่เป็นกลไกควบคุมการเข้าถึง เพื่อให้เป็นไปตามหลักการกำหนดสิทธิเท่าที่จำเป็น ซึ่งมุ่งจำกัดสิทธิการเข้าถึงให้เฉพาะเท่าที่จำเป็นต่อการปฏิบัติงาน และจำกัดขอบเขตการเข้าถึงเฉพาะทรัพยากรหรือข้อมูลที่มีความเกี่ยวข้อง การพิจารณาการเข้าถึงจะทำที่จุดตัดสินใจตามนโยบาย ที่ทำหน้าที่นิยาม ตีความ ประเมิน ตัดสินใจตามนโยบายและบริหารนโยบายโดยส่วนขับเคลื่อนนโยบาย ก่อนส่งผลไปบังคับใช้บนจุดบังคับใช้นโยบายผ่านส่วนบริหารนโยบายต่อไป การทำงานจะยึดหลักไม่เชื่อถือโดยปริยายและตรวจสอบคำร้องด้วยบริบทหลายมิติ เช่น ตัวตน อุปกรณ์ เวลา ตำแหน่ง และระดับความเสี่ยงฯลฯ ทั้งยังต้องประเมินเซสชันอย่างต่อเนื่องผ่านการตรวจสอบสถานะและยืนยันตัวตนซ้ำ มีการตรวจสอบสถานะความมั่นคงปลอดภัยของเครื่องลูกข่ายและการตรวจจับพฤติกรรมผิดปกติอย่างต่อเนื่อง เพื่อให้สามารถลดสิทธิหรือยุติการเข้าถึงได้ทันทีเมื่อบริบทไม่สอดคล้องกับนโยบาย การออกแบบนโยบายและลำดับขั้นตอนการทำงาน (Workflow) จึงต้องผสมผสานข้อมูลและเหตุการณ์ด้านความมั่นคงปลอดภัยจากแหล่งต่าง ๆ เพื่อให้การตัดสินใจของระบบมีความแม่นยำและตอบสนองต่อความเสี่ยงได้แบบเรียลไทม์ องค์กรควรให้ความสำคัญกับตำแหน่งของจุดบังคับใช้นโยบายที่เหมาะสม รวมถึงการตรวจสอบการเข้าถึงอย่างต่อเนื่อง เพื่อให้การควบคุมสิทธิเป็นไปอย่างไดนามิก และสอดคล้องกับหลักการ Zero Trust

แนวทางปฏิบัติในการออกแบบนโยบาย Zero Trust

การออกแบบนโยบาย

๑) สร้างนโยบายแบบลำดับชั้นและเข้าใจง่าย

๒) ออกแบบนโยบายในระดับ “กลุ่มผู้ใช้ – กลุ่มแอปพลิเคชัน” เพื่อลดความซับซ้อน

๓) ผูกนโยบายเข้ากับระดับความเสี่ยงและการกำหนดสิทธิแบบไดนามิก

๔) ใช้ข้อมูลจากระบบจัดการบัญชีผู้ใช้ (User Directory) บทบาทการเข้าถึงระบบ สถานะของอุปกรณ์ และการวิเคราะห์พฤติกรรมผู้ใช้และเอนทิตี (User and Entity Behavior Analytics: UEBA) ในการตัดสินใจควบคุมการเข้าถึงที่แม่นยำ

การบังคับใช้และลำดับขั้นตอนการทำงาน (Enforcement & Workflow)

๑) วางจุดบังคับใช้นโยบายก่อนเข้าถึงแอปพลิเคชันหรือบริการสำคัญ และยึดหลักไม่เชื่อถือโดยปริยาย

๒) ตรวจสอบและเฝ้าระวังในระดับเซสชัน (Session Monitoring) อยู่ตลอดเวลา

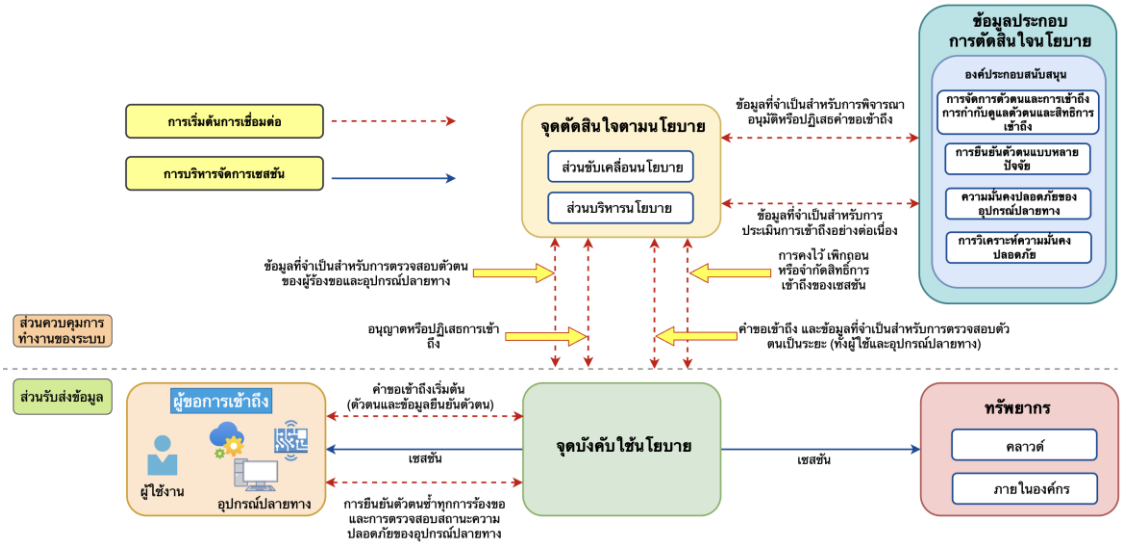
๓) กำหนดเงื่อนไขการเข้าถึงหรือยืนยันตัวตนใหม่ ตามระดับความเสี่ยงของการเข้าถึงหรือพฤติกรรมการใช้งานที่เปลี่ยนแปลงไป

๔) ตรวจสอบสถานะความมั่นคงปลอดภัยของอุปกรณ์ปลายทางอย่างต่อเนื่อง เพื่อยืนยันความมั่นคงปลอดภัย

การตรวจจับความเสี่ยงและตอบสนองต่อความผิดปกติ

๑) ใช้การวิเคราะห์พฤติกรรมผู้ใช้และเอนทิตี เพื่อตรวจจับพฤติกรรมที่เบี่ยงเบนจากรูปแบบปกติ

๒) ปรับลดสิทธิหรือยุติเซสชันทันทีเมื่อพบสัญญาณความเสี่ยง



รูปที่ ๑๓ องค์ประกอบของ Zero Trust และกระบวนการทำงานตามนโยบาย

สรุปข้อควรพิจารณาและการวางแผนนโยบาย

นโยบาย Zero Trust คือ กลไกที่ทำหน้าที่ตัดสินใจก่อนการเข้าถึงทุกครั้ง โดยการตั้ง “คำถามหลัก” กับทุกคำร้องขอ เช่น ผู้ใช้เป็นใคร อุปกรณ์ใด เวลาที่ขอเข้าถึงคือเมื่อใด มาจากเครือข่ายใด และมีสิทธิระดับใด คำถามเหล่านี้เป็นจุดตั้งต้นของกระบวนการกำหนดนโยบาย โดยข้อมูลที่ได้จะถูกนำมาใช้เป็นปัจจัยเชิงบริบทสำหรับการประเมินความเหมาะสมในการเข้าถึงทรัพยากร นโยบายจึงต้องออกแบบให้อิงบริบทหลายมิติ และสะท้อนระดับความเสี่ยง ณ เวลาปัจจุบัน

แนวคิดสำคัญ คือ การวางแผนต้องทำในระดับ “กลุ่มผู้ใช้และทรัพยากร” เพื่อให้ง่ายต่อการบริหารจัดการ ลดข้อผิดพลาด และตอบโจทย์การขยายระบบในอนาคต ส่วนการกำหนดนโยบายแบบรายบุคคลควรใช้เฉพาะในกรณีที่จำเป็นเท่านั้น

นโยบาย Zero Trust ควรมุ่งเน้นการออกแบบนโยบายอย่างเป็นโครงสร้าง พร้อมตระหนักว่านโยบายต้องทำงานแบบไดนามิก รองรับการปรับตามระดับความเสี่ยง สิทธิการเข้าถึง และสามารถตรวจสอบตามบริบทที่เปลี่ยนแปลงอยู่เสมอ ในเชิงการบังคับใช้นโยบายควรให้ความสำคัญกับการตรวจสอบการเข้าถึงอย่างต่อเนื่อง เช่น การตรวจสอบสถานะและการยืนยันตัวตนซ้ำตามเงื่อนไขที่กำหนด เพื่อหลีกเลี่ยงการคงความเชื่อถือไว้ตลอดอายุการเชื่อมต่อ นอกจากนี้ควรกำหนดกฎการตอบสนองต่อเหตุผิดปกติอย่างชัดเจน เพื่อให้ระบบสามารถลดระดับสิทธิ หรือยุติการเข้าถึงได้ทันทีเมื่อพบพฤติกรรมที่เบี่ยงเบนจากปกติ

ภาพรวมข้อดีและข้อจำกัดของแนวทางปฏิบัติในการติดตั้งและนำไปใช้งาน ZTNA แต่ละแนวทาง

การนำสถาปัตยกรรม ZTNA มาใช้งานเป็นกลไกสำคัญในการยกระดับความมั่นคงปลอดภัยไซเบอร์ในองค์กรยุคดิจิทัล ผู้ใช้งานอุปกรณ์และแอปพลิเคชันไม่ได้ถูกจำกัดอยู่ภายในขอบเขตเครือข่ายภายในองค์กรอีกต่อไป แนวคิด Zero Trust จึงมุ่งเน้นการตรวจสอบและควบคุมการเข้าถึงอย่างเข้มงวดในทุกคำขอเชื่อมต่อโดยยึดหลัก “อย่าเชื่อทันที จงตรวจสอบเสมอ” และ “การควบคุมการเข้าถึงตามบริบท” ในทางปฏิบัติ ZTNA สามารถนำไปใช้งานได้หลากหลายรูปแบบ ขึ้นอยู่กับโครงสร้างพื้นฐาน ความพร้อมขององค์กร และข้อกำหนดด้านกฎระเบียบ โดยหัวข้อนี้ได้นำเสนอแนวทางการติดตั้ง ZTNA ใน ๓ แนวทาง ได้แก่

๑) แบบการติดตั้งภายในองค์กร (On-Premises)

๒) แบบคลาวด์ (Cloud)

๓) แบบไฮบริด (Hybrid)

แต่ละรูปแบบมีข้อดี ข้อจำกัด และความเหมาะสมที่แตกต่างกัน การทำความเข้าใจข้อดีและข้อจำกัดของแต่ละแนวทางจะช่วยให้องค์กรสามารถเลือกสถาปัตยกรรม ZTNA ที่สอดคล้องกับกลยุทธ์ขององค์กร ความต้องการทางธุรกิจ และทิศทางการพัฒนาระบบในอนาคตได้อย่างมีประสิทธิภาพ ซึ่งจะกล่าวถึงรายละเอียดเพิ่มเติมในหัวข้อถัดไป โดยสามารถสรุปเป็นตารางดังแสดงในตารางที่ ๒๔

ตารางที่ ๒๔ แสดงการเปรียบเทียบข้อดีและข้อจำกัดของแต่ละแนวทาง

รูปแบบการติดตั้ง	ลักษณะเด่น	ข้อดี (Pros)	ข้อจำกัด (Cons)
ZTNA แบบติดตั้งภายในองค์กร	ใช้เน็กซ์เจเนอเรชันไฟร์วอลล์เป็นเกตเวย์ ZTNA ติดตั้งในศูนย์ข้อมูลกลางผสานกับเอเจนต์และระบบจัดการสถานะความมั่นคงปลอดภัยของอุปกรณ์ปลายทาง	๑) ลดความเสี่ยงจากการโจมตี โดยการแบ่งเครือข่ายในศูนย์ข้อมูลกลางเป็นเครือข่ายย่อย ๒) • มีความมั่นคงปลอดภัยสูงเหมาะกับองค์กรที่ต้องการเก็บทรัพยากรไว้ภายในองค์กรเอง	ไม่เหมาะกับองค์กรที่ใช้บริการ SaaS หรือ PaaS
ZTNA แบบคลาวด์	ให้บริการผ่านแพลตฟอร์ม SASE/SSE เน้นการทำงานบนคลาวด์เพื่อลดการพึ่งพาฮาร์ดแวร์	๑) บริหารจัดการง่ายแบบรวมศูนย์ ๒) สามารถขยายตัวได้ยืดหยุ่นไร้ข้อจำกัดด้านฮาร์ดแวร์ ๓) ลดการพึ่งพาศูนย์ข้อมูลกลาง ๔) ลดต้นทุนโครงสร้างพื้นฐานและการดำเนินการ ๕) ให้ความมั่นคงปลอดภัยที่สม่ำเสมอในทุกสถานที่	๑) มีค่าความหน่วงเวลาสูงและประสิทธิภาพการทำงานต่ำเมื่อจุดให้บริการ SASE/SSE อยู่ไกล ดังนั้นองค์กรควรออกแบบและเลือกจุดให้บริการที่เหมาะสมและใช้เทคโนโลยี SD-WAN เพื่อควบคุมเส้นทาง ๒) จุดให้บริการ SASE/SSE ต้องมีบริการทางด้านความมั่นคงปลอดภัยที่เพียงพอ เช่น บริการไฟร์วอลล์บนคลาวด์ บริการป้องกันภัยคุกคามอื่น ๆ การเข้ารหัสการสื่อสาร ฯลฯ และผ่านข้อตกลงระดับการให้บริการที่ได้มาตรฐาน
ZTNA แบบไฮบริด	ผสานเน็กซ์เจเนอเรชันไฟร์วอลล์ (อุปกรณ์หรือซอฟต์แวร์เฉพาะทาง) และคลาวด์ SASE/SSE เข้าด้วยกัน	๑) การเข้าถึงแอปพลิเคชันที่ผ่านเส้นทางที่เหมาะสมที่สุด ทำให้ได้ค่าความหน่วงเวลาที่ต่ำสุด ๒) รองรับการทำงานแบบไฮบริดโดยผู้ใช้ที่อยู่ในสาขาสามารถเข้าถึงแอปพลิเคชันภายในผ่านเกตเวย์	ระบบมีความซับซ้อนต้องอาศัยผู้เชี่ยวชาญในการออกแบบ ติดตั้ง บริหารจัดการ และบำรุงรักษา

รูปแบบการติดตั้ง	ลักษณะเด่น	ข้อดี (Pros)	ข้อจำกัด (Cons)
	โดยบริหารจัดการแบบรวมศูนย์	ZTNA ได้โดยตรงอย่างมีประสิทธิภาพผ่านเครือข่าย SD-WAN ๓) เพิ่มประสิทธิภาพการทำงานระหว่างสาขาและศูนย์ข้อมูลกลาง ๔) รองรับสถาปัตยกรรม Zero Trust แบบรวมศูนย์ (Unified Zero Trust Access) สำหรับทั้งระบบคลาวด์และศูนย์ข้อมูลกลาง ๕) เพิ่มความยืดหยุ่นในการออกแบบระบบ ๖) ลดความเสี่ยงจากระบบล่มในจุดใดจุดหนึ่ง และแบ่งภาระการทำงาน ๗) การสร้างและจัดการ Zero Trust แบบครบวงจร	

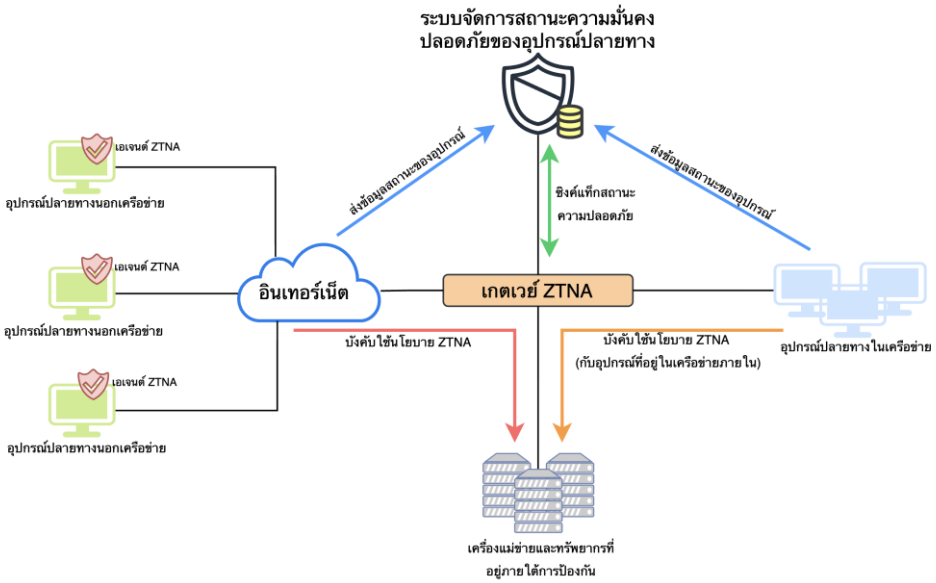
๕.๒ แนวทางปฏิบัติในการติดตั้งและนำไปใช้งาน ZTNA แบบการติดตั้งภายในองค์กร (On-Premises)

ในยุคปัจจุบันอุปกรณ์และผู้ใช้งานจำเป็นต้องเข้าถึงทรัพยากรขององค์กรจากทุกที่ ทำให้รูปแบบการเชื่อมต่อแบบเดิม เช่น ระบบเครือข่ายส่วนตัวเสมือน ไม่ตอบโจทย์ทั้งทางด้านความมั่นคงปลอดภัยและด้านการควบคุมการเข้าถึงตามบริบท (Context-Aware) อีกต่อไป

ZTNA เป็นกลไกที่ยกระดับการควบคุมการเข้าถึงตามหลักการ “อย่าเชื่อทันที จงตรวจสอบเสมอ” โดยการตรวจสอบผู้ใช้งาน อุปกรณ์ และสถานะความมั่นคงปลอดภัยของอุปกรณ์ปลายทางทุกครั้งก่อนการเข้าถึงทรัพยากรในศูนย์ข้อมูลกลาง

การทำงาน ZTNA รูปแบบนี้ผสานการทำงานของเกตเวย์ ZTNA และเอเจนต์ ZTNA บนเครื่องลูกข่ายและระบบจัดการสถานะความมั่นคงปลอดภัยของอุปกรณ์ปลายทาง (Endpoint Security Posture Management: ESPM[๒]) ที่ทำหน้าที่ประมวลผลข้อมูลที่ได้จากเอเจนต์ ZTNA และส่งข้อมูลหรือคำสั่งต่อไปยังจุดบังคับใช้นโยบาย (เกตเวย์ ZTNA) ที่ทำหน้าที่เป็นเกตเวย์ที่ช่วยให้ผู้ใช้งานที่อยู่ภายนอกองค์กรสามารถเข้าถึงแอปพลิเคชันภายในได้อย่างปลอดภัย โดยไม่ต้องสร้างระบบเครือข่ายส่วนตัวเสมือนแบบเดิม ลดความเสี่ยงจากการโจมตีและเพิ่มประสิทธิภาพการควบคุมบนระดับชั้นแอปพลิเคชัน (Application Layer)

สถาปัตยกรรม ZTNA แบบการติดตั้งภายในองค์กรโดยใช้เน็กซ์เจเนอเรชันไฟร์วอลล์เป็นเกตเวย์ ZTNA



รูปที่ ๑๔ สถาปัตยกรรม ZTNA แบบการติดตั้งภายในองค์กร

องค์ประกอบหลัก

จากรูปที่ ๑๔ ประกอบไปด้วยองค์ประกอบหลักหลายส่วนดังต่อไปนี้

๑) เกตเวย์ ZTNA เช่น เน็กซ์เจเนอเรชันไฟร์วอลล์ในศูนย์ข้อมูลกลาง ทำหน้าที่เป็นจุดบังคับใช้นโยบายที่บังคับใช้นโยบาย ZTNA โดยพิจารณาจาก การยืนยันตัวตน การตรวจสอบสถานะของอุปกรณ์ ใบรับรองดิจิทัล แท็ก ZTNA ฯลฯ

๒) เอเจนต์ ZTNA บนเครื่องลูกข่ายทำหน้าที่ส่งข้อมูลสถานะของอุปกรณ์ไปยังระบบจัดการสถานะความมั่นคงปลอดภัยของอุปกรณ์ปลายทาง ส่งใบรับรองดิจิทัลที่ใช้ยืนยันตัวตนไปยังเกตเวย์ ZTNA และสร้างการเชื่อมต่อแบบเข้ารหัสไปยังเกตเวย์ ZTNA ที่เลือก

๓) ระบบจัดการสถานะความมั่นคงปลอดภัยของอุปกรณ์ปลายทาง เป็นจุดตัดสินใจตามนโยบายทำหน้าที่ประมวลผลข้อมูลที่ได้จากการตรวจสอบสถานะของอุปกรณ์ปลายทางที่ได้จากเอเจนต์ ZTNA ออกใบรับรองดิจิทัลให้เครื่องลูกข่ายและประสานข้อมูลแท็ก ZTNA ให้เกตเวย์ ZTNA (เน็กซ์เจเนอเรชันไฟร์วอลล์) โดยแท็ก ZTNA จะได้จากการประมวลผลข้อมูลที่ได้จากเอเจนต์ ZTNA สรุปเป็นข้อมูลที่สามารถนำไปใช้ต่อโดยเกตเวย์ ZTNA เพื่อควบคุมการเชื่อมต่อจากเครื่องลูกข่าย ตัวอย่างของแท็ก ZTNA เช่น กลุ่มความเสี่ยงระดับต่ำ กลุ่มความเสี่ยงระดับกลาง กลุ่มความเสี่ยงระดับสูง ฯลฯ

๔) ผู้ให้บริการยืนยันตัวตน คือ ระบบหรือบริการที่ทำหน้าที่สนับสนุนการยืนยันตัวตนผู้ใช้ และจัดการข้อมูลตัวตน เพื่อให้ผู้ใช้สามารถล็อกอินได้อย่างปลอดภัยและรวมศูนย์

๕) แอปพลิเคชัน บริการที่อยู่ในศูนย์ข้อมูลกลาง เช่น เว็บไซต์ ระบบรองรับการเชื่อมต่อจากเดสก์ท็อประยะไกล (Remote Desktop) ระบบวางแผนทรัพยากรองค์กร (Enterprise Resource Planning: ERP) และแอปพลิเคชันอื่น ๆ ภายในองค์กร

ลำดับขั้นตอนการทำงานของ ZTNA แบบการติดตั้งภายในองค์กร

ขั้นตอนที่ ๑ เอเจนต์ ZTNA บนเครื่องลูกข่ายทำการเชื่อมต่อไปยังระบบจัดการสถานะความมั่นคงปลอดภัยของอุปกรณ์ปลายทาง เพื่อส่งข้อมูลสถานะของอุปกรณ์ เช่น ระบบปฏิบัติการ ซอฟต์แวร์ป้องกันไวรัส ข้อมูลการเข้ารหัสสื่อจัดเก็บข้อมูล ข้อมูลการปฏิบัติตามข้อกำหนดอื่นๆ ระบบจัดการสถานะความมั่นคงปลอดภัยของอุปกรณ์ปลายทางทำการประมวลผลข้อมูลสถานะอิงตามเงื่อนไขที่กำหนด และทำการกำหนดแท็ก ZTNA

ขั้นตอนที่ ๒ ระบบจัดการสถานะความมั่นคงปลอดภัยของอุปกรณ์ปลายทางเชื่อมต่อไปยังเกตเวย์ ZTNA เพื่อซิงโครไนซ์แท็ก ZTNA ไปยังเกตเวย์ ZTNA สำหรับบังคับใช้นโยบาย

ขั้นตอนที่ ๓ ผู้ใช้เข้าถึงแอปพลิเคชันภายในผ่านเกตเวย์ ZTNA เอเจนต์ ZTNA บนเครื่องลูกข่ายจะทำการสร้างการเชื่อมต่อแบบเข้ารหัสไปยังเกตเวย์ ZTNA เพื่อขอเข้าใช้บริการหรือแอปพลิเคชัน

ขั้นตอนที่ ๔ เกตเวย์ ZTNA ทำการตรวจสอบและพิจารณาการอนุญาตให้เข้าถึงจาก

๑) การยืนยันตัวตนผู้ใช้

๒) ใบรับรองดิจิทัลของเครื่องลูกข่าย

๓) นโยบายควบคุมการเข้าถึง

๔) แท็ก ZTNA ที่ได้จากระบบจัดการสถานะความมั่นคงปลอดภัยของอุปกรณ์ปลายทาง

๕) ข้อมูลสถานะอื่น ๆ ตามความเหมาะสมและความเสี่ยงขององค์กร

ขั้นตอนที่ ๕ การอนุญาตหรือปฏิเสธตามนโยบาย ZTNA ลักษณะสำคัญของรูปแบบนี้ คือ ไม่มีการเข้าถึงระดับเครือข่าย (Network Access) แต่เป็นการเข้าถึงเฉพาะแอปพลิเคชัน (Application Access) ซึ่งเป็นหัวใจของ Zero Trust โดยมีเกตเวย์ ZTNA เป็นตัวควบคุม

ข้อแนะนำในการนำไปประยุกต์ใช้งาน

แนวทางที่ ๑ การเข้าถึงแอปพลิเคชันภายใน (Private Application) เหมาะสำหรับองค์กรที่ต้องการใช้ ZTNA แทนระบบเครือข่ายส่วนตัวเสมือน สำหรับ

๑) เว็บพอร์ทัล (Web portal) และเว็บไซต์ภายใน

๒) ระบบวางแผนทรัพยากรองค์กร ระบบบริหารความสัมพันธ์ลูกค้า (Customer Relationship Management: CRM) ฯลฯ

๓) โปรโตคอลการเชื่อมต่อจากเดสก์ท็อประยะไกล (Remote Desktop Protocol: RDP) โปรโตคอลเชลล์ที่ปลอดภัย (Secure Shell: SSH) ฯลฯ

ประโยชน์

๑) กำหนดสิทธิการเข้าถึงแอปพลิเคชันภายในตามผู้ใช้และสถานะของผู้ใช้

๒) ไม่ต้องเปิดพอร์ตการเข้าถึงไว้เสมอ เพราะการอนุญาตให้เข้าถึงถูกกำหนดโดยเกตเวย์ ZTNA

๓) ผู้ใช้งานมีสิทธิใช้งานเฉพาะแอปพลิเคชันภายในที่จำเป็นเท่านั้น

แนวทางที่ ๒ บังคับการตรวจสอบสถานะก่อนเข้าถึงระบบภายใน

องค์กรสามารถกำหนดเงื่อนไขก่อนอนุญาตให้เข้าถึง เช่น

๑) ระบบปฏิบัติการต้องเป็นแพตช์ (Patch) ล่าสุด

๒) ต้องมีซอฟต์แวร์ป้องกันไวรัสเปิดใช้งานอยู่

๓) ต้องเปิดไฟร์วอลล์ของระบบปฏิบัติการ

๔) เครื่องลูกข่ายต้องไม่มีความระดับเสี่ยงสูง (High risk) เช่น ตรวจพบช่องโหว่รุนแรงในระบบปฏิบัติการหรือแอปพลิเคชันบนเครื่องลูกข่าย

หากเงื่อนไขข้างต้นใดไม่ผ่าน สามารถส่งการแจ้งเตือนไปยังเครื่องลูกข่ายได้ เช่น การแนะนำแนวทางปฏิบัติและจะอนุญาตให้ผู้ใช้เข้าถึงทรัพยากรได้ก็ต่อเมื่อเงื่อนไขทั้งหมดผ่านครบถ้วนแล้ว

แนวทางที่ ๓ การแบ่งส่วนเครือข่ายแบบย่อยในระดับรายแอปพลิเคชัน

ต่างจากระบบเครือข่ายส่วนตัวเสมือนแบบเดิมที่ให้การเข้าถึงที่กว้างเกินไป โดย ZTNA กำหนดให้

๑) เข้าถึงได้เฉพาะแอปพลิเคชันที่อยู่บนเครือข่ายย่อยที่ได้รับอนุญาต

๒) ไม่สามารถสแกนพอร์ตหรือสแกนเครือข่ายย่อยอื่นที่ไม่ได้รับอนุญาตให้เข้าถึงได้

๓) ลดความเสี่ยงด้านการโจมตีแบบการเคลื่อนตัวในเครือข่าย

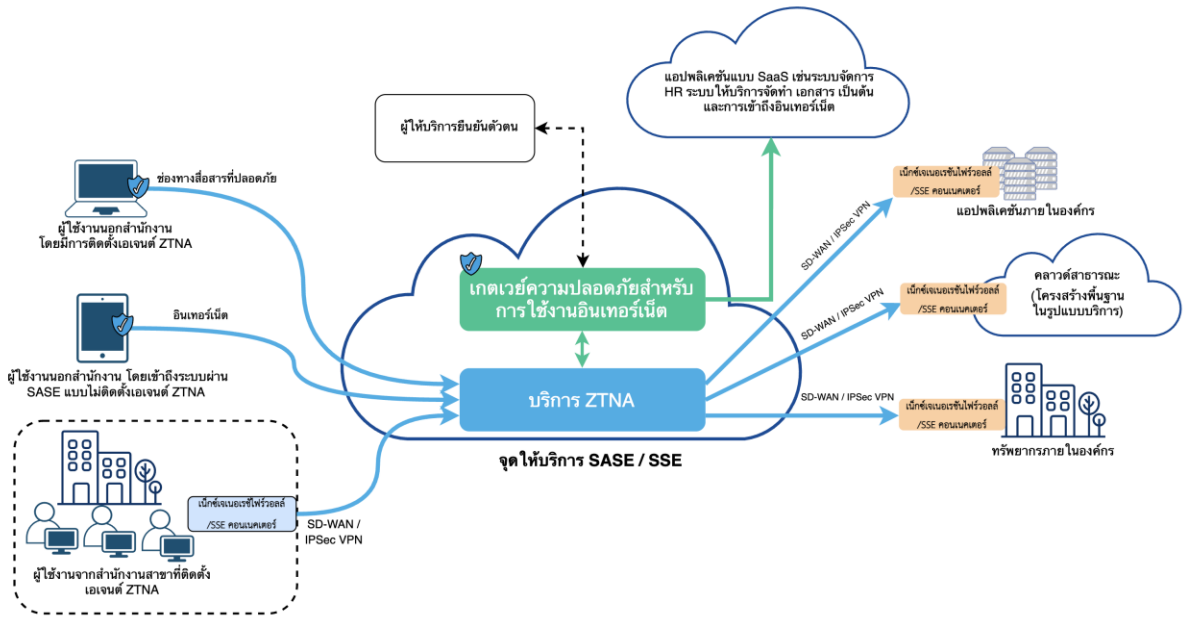
ZTNA แบบติดตั้งภายในองค์กรโดยใช้เน็กซ์เจเนอเรชันไฟร์วอลล์เป็นเกตเวย์ ZTNA เป็นสถาปัตยกรรมที่ตอบโจทย์องค์กรที่ต้องการความมั่นคงปลอดภัยระดับสูง โดยไม่ต้องพึ่งการเชื่อมต่อระบบเครือข่ายส่วนตัวเสมือนแบบเดิม ทำให้การเข้าถึงทรัพยากรภายในองค์กรมีความปลอดภัย มีการควบคุมตามสถานะของอุปกรณ์และสามารถแบ่งเครือข่ายในศูนย์ข้อมูลกลางเป็นเครือข่ายย่อย และเป็นไปตามแนวคิด Zero Trust อย่างแท้จริง

๕.๓ แนวทางปฏิบัติในการติดตั้งและนำไปใช้งาน ZTNA แบบคลาวด์ (Cloud)

โลกยุคดิจิทัลในปัจจุบันองค์กรต่าง ๆ มีการใช้งานระบบคลาวด์และมีลักษณะกระจายศูนย์มากขึ้น ผู้ใช้ไม่ได้อยู่ภายในเครือข่ายขององค์กรตลอดเวลา การใช้การเชื่อมต่อแบบระบบเครือข่ายส่วนตัวเสมือนแบบดั้งเดิม (เช่น SSL-VPN หรือ IPsec) เพื่อเข้าถึงทรัพยากรขององค์กรจากภายนอกมีข้อจำกัดในการควบคุมการเข้าถึงทรัพยากร และมีต้นทุนในการบำรุงรักษาสูง

แนวทางปฏิบัติ ZTNA แบบคลาวด์ภายใต้แพลตฟอร์ม SASE สามารถแก้ไขปัญหาเหล่านี้ หรือสามารถเลือกใช้ SSE เป็นอีกแนวทางเลือกหนึ่งในการเริ่มต้น โดยทั้ง SASE และ SSE จะรวมฟังก์ชันความมั่นคงปลอดภัยไว้บนคลาวด์ เช่น บริการ ZTNA บริการควบคุมความมั่นคงปลอดภัยการใช้งานเว็บไซต์ (Secure Web Gateway: SWG) บริการไฟร์วอลล์บนคลาวด์ (FWaaS) ฯลฯ แต่ SSE ยังคงโครงสร้างเครือข่ายแบบเดิมไว้โดยเน้นการเชื่อมต่อผ่านเอเจนต์จากเครื่องลูกข่ายไปยังจุดให้บริการ SSE เป็นหลัก จากจุดให้บริการ SSE ไปยังศูนย์ข้อมูลกลางจะเชื่อมต่อกันผ่าน SSE คอนเนคเตอร์ ส่วน SASE จะมีการควบรวมความสามารถทั้ง SSE กับ SD-WAN เอาไว้ในตัวเอง ทำให้สามารถสร้างเครือข่าย SD-WAN จากสาขาและศูนย์ข้อมูลกลางเชื่อมต่อกับ SASE ได้โดยตรงด้วยเน็กซ์เจเนอเรชันไฟร์วอลล์หรืออุปกรณ์ที่มีความสามารถด้าน SD-WAN และยังสามารถรองรับการทำงานร่วมกับเอเจนต์ได้เช่นเดียวกัน ในภาพรวม SASE ยังคงเป็นแนวทางหลักในการสร้างสถาปัตยกรรมความมั่นคงปลอดภัยที่รองรับอนาคต โดยให้ทั้งความยืดหยุ่น ความคล่องตัว ประสิทธิภาพ และการป้องกันที่สอดคล้องตามหลัก Zero Trust อย่างครบถ้วน

สถาปัตยกรรม ZTNA แบบคลาวด์บน **SASE/SSE**



รูปที่ ๑๕ สถาปัตยกรรม ZTNA แบบ SASE/SSE

ลำดับการทำงานของ ZTNA แบบคลาวด์ ตามรูปที่ ๑๕ ทราฟฟิกที่ถูกเข้ารหัสจะถูกส่งจากเอเจนต์ ZTNA บนเครื่องลูกข่ายไปยังจุดให้บริการ (Point of Presence: PoP) SASE หรือ SSE ในบางผู้ผลิต ต่อไปนี้จะเรียกรวมกันว่า SASE/SSE หลังจากนั้นทราฟฟิกที่ถูกเข้ารหัสจะถูกส่งจากจุดให้บริการ SASE/SSE ไปยังเน็กซ์เจเนอเรชันไฟร์วอลล์ (SSE คอนเนคเตอร์ในกรณีของ SSE) ที่อยู่ในศูนย์ข้อมูลกลางผ่านเครือข่ายส่วนตัวเสมือน เช่น เครือข่าย SD-WAN หรือ IPSec VPN โดยจุดบังคับใช้นโยบายจะอยู่ในจุดให้บริการ SASE/SSE เอง และระบบจัดการสถานะความมั่นคงปลอดภัยของอุปกรณ์ปลายทางจะอยู่ในจุดให้บริการ SASE/SSE หรือแยกออกมาอีกคลาวด์ต่างหากก็ได้แล้วแต่ผู้ผลิต ในสถาปัตยกรรม ZTNA แบบคลาวด์นี้ ทราฟฟิกที่เข้ารหัสจะต้องวิ่งผ่านจุดให้บริการ SASE/SSE ซึ่งทำให้เกิดค่าความหน่วงเวลาที่สูงขึ้น

องค์ประกอบหลัก

๑) จุดให้บริการ SASE/SSE ทำหน้าที่เป็นทั้งจุดบังคับใช้นโยบายและจุดตัดสินใจตามนโยบายที่

๑.๑) เป็นศูนย์กลางความมั่นคงปลอดภัยบนคลาวด์ในการจัดการเอเจนต์ ZTNA บนเครื่องลูกข่าย

๑.๒) เป็นระบบจัดการสถานะความมั่นคงปลอดภัยของอุปกรณ์ปลายทางบนคลาวด์ ทำหน้าที่จัดการเอเจนต์ ZTNA บนเครื่องลูกข่าย ออกใบรับรองดิจิทัล ประมวลผลข้อมูลสถานะจากเอเจนต์ ZTNA และส่งต่อแท็ก ZTNA ไปยังจุดบังคับนโยบายที่อยู่ในจุดให้บริการ SASE/SSE เอง

๒) เอเจนต์ ZTNA บนเครื่องลูกข่ายจะทำหน้าที่ตรวจสอบสถานะของอุปกรณ์และส่งข้อมูลสถานะไปยังระบบจัดการสถานะความมั่นคงปลอดภัยของอุปกรณ์ปลายทางที่อยู่ในจุดให้บริการ SASE/SSE พร้อมกับสร้างการเชื่อมต่อและส่งข้อมูลที่เข้ารหัสไปยังจุดให้บริการ SASE/SSE โดยยืนยันตัวตนผ่านใบรับรองดิจิทัล

๓) เน็กซ์เจเนอเรชันไฟร์วอลล์หรือ SSE คอนเนคเตอร์หรืออุปกรณ์ SD-WAN ที่ติดตั้งในศูนย์ข้อมูลกลาง ทำหน้าที่รับการเชื่อมต่อแบบเข้ารหัส (SD-WAN หรือ IPSec VPN) ที่มาจากจุดให้บริการ SASE/SSE อีกต่อหนึ่งก่อนที่จะส่งการร้องขอการใช้บริการไปที่แอปพลิเคชัน ในรูปแบบนี้ เน็กซ์เจเนอเรชันไฟร์วอลล์ (หรือ SSE คอนเนคเตอร์ หรืออุปกรณ์ SD-WAN) จะไม่ได้ทำหน้าที่เป็นจุดบังคับนโยบาย

๔) ผู้ให้บริการยืนยันตัวตน คือ ระบบหรือบริการที่ทำหน้าที่สนับสนุนการยืนยันตัวตนผู้ใช้ และจัดการข้อมูลตัวตน เพื่อให้ผู้ใช้สามารถล็อกอินได้อย่างปลอดภัยและรวมศูนย์

ลำดับขั้นตอนการทำงานของ ZTNA แบบคลาวด์บน SASE/SSE

ขั้นตอนที่ ๑ การลงทะเบียนเครื่องลูกข่ายและเก็บค่าสถานะของอุปกรณ์ปลายทาง (Endpoint Registration & Posture Collection)

ติดตั้งเอเจนต์ ZTNA บนเครื่องลูกข่ายและทำการลงทะเบียน จากนั้นเชื่อมต่อกับระบบจัดการสถานะความมั่นคงปลอดภัยของอุปกรณ์ปลายทางเพื่อส่งข้อมูลสถานะของอุปกรณ์ เช่น เวอร์ชันของระบบปฏิบัติการ สถานะซอฟต์แวร์ป้องกันไวรัส แพตช์ ฯลฯ

ขั้นตอนที่ ๒ การซิงโครไนซ์ (Synchronization) แท็ก ZTNA

ระบบจัดการสถานะความมั่นคงปลอดภัยของอุปกรณ์ปลายทางจะทำการซิงโครไนซ์แท็ก ZTNA ไปยังจุดบังคับใช้นโยบายที่อยู่ภายในจุดให้บริการ SASE/SSE เอง

ขั้นตอนที่ ๓ คำขอของผู้ใช้ไปยังแอปพลิเคชันส่วนตัว (User Request to Private App)

เมื่อผู้ใช้ต้องการเข้าถึงแอปพลิเคชันที่อยู่ในศูนย์ข้อมูลกลาง

๑) เอเจนต์ ZTNA บนเครื่องลูกข่ายจะเปลี่ยนเส้นทาง (Redirect) การเชื่อมต่อแบบเข้ารหัสไปยังจุดให้บริการ SASE/SSE ก่อน

๒) ผู้ใช้ไม่เห็นแอปพลิเคชันจริงโดยตรง แอปพลิเคชันถูก “ซ่อน (Stealth)” ตามหลักการ Zero Trust

ขั้นตอนที่ ๔ การตรวจสอบโดยจุดบังคับใช้นโยบายที่อยู่ภายในจุดให้บริการ SASE/SSE

โดยทั่วไปจุดบังคับใช้นโยบายที่อยู่ภายในจุดให้บริการ SASE/SSE จะทำการตรวจสอบส่วนหลักดังนี้

๑) ตัวตนผู้ใช้ ด้วยการยืนยันตัวตนผ่านโปรโตคอล เช่น LDAP RADIUS SAML ฯลฯ

๒) ใบรับรองดิจิทัลของเครื่องลูกข่าย

๓) แท็ก ZTNA ที่ได้จากการประมวลผลข้อมูลสถานะของอุปกรณ์ เช่น ช่องโหว่ระบบปฏิบัติการ การเปิดใช้งานซอฟต์แวร์ป้องกันไวรัส ฯลฯ

ขั้นตอนที่ ๕ การอนุญาตเป็นรายเซสชัน

หลังจากจุดบังคับใช้นโยบายที่อยู่ในจุดให้บริการ SASE/SSE ได้รับแท็ก ZTNA แล้ว จุดบังคับใช้นโยบายจะอนุญาตให้การร้องขอที่ส่งจากเครื่องลูกข่ายที่ได้รับอนุญาตผ่านการเชื่อมต่อแบบเข้ารหัส (SD-WAN หรือ IPSec VPN) ไปยังเน็กซ์เจเนอเรชันไฟร์วอลล์ (หรือ SSE คอนเนคเตอร์) ก่อนที่การร้องขอจะถูกส่งต่อไปยังแอปพลิเคชัน จุดบังคับใช้นโยบายในจุดให้บริการ SASE/SSE จะตรวจสอบและอนุญาตการร้องขอเป็นรายเซสชัน

ข้อแนะนำของ ZTNA เมื่อใช้งานบน SASE/SSE

แนวทางที่ ๑ การทำงานจากระยะไกลหรือการทำงานจากทุกที่

๑) พนักงานสามารถทำงานจากบ้านหรือระหว่างการเดินทาง

๒) เครื่องลูกข่ายเชื่อมต่อกับจุดให้บริการ SASE/SSE ผ่านเอเจนต์ ZTNA เพื่อเข้าถึงแอปพลิเคชันที่ต้องการ (อาจเป็นรูปแบบบริการ SaaS หรือแอปพลิเคชันภายใน) ได้อย่างปลอดภัย

๓) การใช้ ZTNA รูปแบบนี้จะช่วยลดความจำเป็นในการใช้ระบบเครือข่ายส่วนตัวเสมือนแบบเดิม และลดภาระศูนย์ข้อมูลกลาง (ไม่ต้องเชื่อมต่อทุกทราฟฟิกไปยังศูนย์ข้อมูลกลางก่อนเสมอ)

แนวทางที่ ๒ การเข้าถึงเครือข่ายส่วนตัวที่ปลอดภัย (Secure Private Access: SPA)

๑) การเข้าถึงแอปพลิเคชันภายในองค์กร (เครื่องแม่ข่ายอยู่บนศูนย์ข้อมูลกลางหรือคลาวด์ส่วนตัว)

๒) การเข้าถึงแอปพลิเคชันเป็นแบบส่วนตัว โดยแอปพลิเคชันถูกซ่อนไว้ (ไม่เปิดให้เห็นบนอินเทอร์เน็ต) และจะถูกเข้าถึงผ่านจุดให้บริการ SASE/SSE ก่อนที่จะถูกส่งต่อไปให้เน็กซ์เจเนอเรชันไฟร์วอลล์ (หรือ SSE คอนเนคเตอร์) ที่อยู่ในศูนย์ข้อมูลกลางผ่านการเชื่อมต่อแบบเข้ารหัส เมื่อผู้ใช้และอุปกรณ์ได้รับการตรวจสอบและได้รับอนุญาต

แนวทางที่ ๓ การเข้าถึงบริการ SaaS ที่ปลอดภัย (Secure SaaS Access: SSA)

๑) สำหรับแอปพลิเคชันแบบ SaaS ผู้ใช้จากทุกที่สามารถเข้าถึงได้ผ่าน SASE/SSE

๒) นโยบาย ZTNA สามารถถูกกำหนดเพื่ออนุญาตให้เฉพาะผู้ใช้และอุปกรณ์ที่ปฏิบัติตามข้อกำหนดเท่านั้นที่สามารถเข้าถึงแอปพลิเคชันแบบ SaaS ได้โดยทราฟฟิกต้องผ่านจุดให้บริการ SASE/SSE ก่อนเท่านั้น

แนวทางที่ ๔ การเข้าถึงอินเทอร์เน็ตที่ปลอดภัย (Secure Internet Access: SIA)

๑) ผู้ใช้อินเทอร์เน็ต (Web Browsing) เชื่อมต่อผ่านจุดให้บริการของ SASE/SSE เพื่อควบคุมความมั่นคงปลอดภัยการใช้งานเว็บไซต์ และป้องกันภัยคุกคามจากเว็บไซต์

๒) ZTNA ช่วยเสริมความมั่นคงปลอดภัยตามแนวคิด Zero Trust แบบรายเซสชัน โดยทราฟฟิกผู้ใช้งานอินเทอร์เน็ตถูกตรวจสอบและควบคุมผ่านจุดให้บริการ SASE/SSE

แนวทางที่ ๕ การตรวจสอบอย่างต่อเนื่องและควบคุมการเข้าถึงแบบปรับตามบริบท

๑) ระบบใช้การตรวจสอบอย่างต่อเนื่อง โดยตรวจสอบสถานะของอุปกรณ์เป็นระยะ เพื่อให้แน่ใจว่าอุปกรณ์ยังปลอดภัยก่อนให้สิทธิเข้าถึงแอปพลิเคชัน

๒) ถ้าอุปกรณ์ไม่ผ่านการตรวจสอบหรือไม่ปฏิบัติตามข้อกำหนด เช่น ซอฟต์แวร์ป้องกันไวรัสไม่เปิดใช้งาน อาจถูกจำกัดการเข้าถึงหรือถูกตัดสิทธิบางส่วนโดยทันที

แนวทางที่ ๖ ลดการพึ่งพาระบบเครือข่ายส่วนตัวเสมือนแบบเดิม

๑) ด้วย ZTNA ที่ฝังอยู่ใน SASE/SSE องค์กรสามารถลดการใช้ระบบเครือข่ายส่วนตัวเสมือนแบบดั้งเดิมที่เชื่อมต่อไปยังศูนย์ข้อมูลกลางโดยตรงได้ รวมถึงช่วยลดความเสี่ยงจากการแพร่กระจายการโจมตีไปยังระบบเครือข่ายภายในได้

๒) SASE/SSE รองรับการเปลี่ยนผ่าน (Migration) องค์กร โดยสามารถให้พนักงานเริ่มใช้ ZTNA ทีละส่วน ลดผลกระทบต่อผู้ใช้และองค์กร

แนวทาง ZTNA แบบคลาวด์ ช่วยให้องค์กรสามารถใช้งาน ZTNA และยังผสานการทำงานกับสถาปัตยกรรม SASE/SSE ได้อย่างราบรื่น เพื่อมอบการเข้าถึงแอปพลิเคชันที่ปลอดภัย ยืดหยุ่น และควบคุมตามหลัก Zero Trust อย่างเป็นระบบ โดยมีกรณีใช้งานสำคัญ เช่น การเข้าถึงเครือข่ายส่วนตัวที่ปลอดภัย การเข้าถึงบริการ SaaS ที่ปลอดภัย การเข้าถึงอินเทอร์เน็ตที่ปลอดภัย ฯลฯ

แนวทางนี้ยังแสดงให้เห็นถึงศักยภาพของ ZTNA บนโครงสร้าง SASE/SSE ในการแก้ปัญหาด้านความมั่นคงปลอดภัยและเพิ่มประสิทธิภาพการเชื่อมต่อ แม้จะยังมีความท้าทายด้านค่าความหน่วงเวลา และการจัดการการเปลี่ยนแปลง แต่ด้วยการออกแบบสถาปัตยกรรมที่เหมาะสมและการวางแผนเชิงกลยุทธ์ที่ดี องค์กรสามารถนำแนวทางนี้ไปใช้ได้อย่างมีประสิทธิผล ทั้งนี้แนวโน้มในอนาคตของ ZTNA บน SASE/SSE จะถูกพัฒนาไปสู่การวิเคราะห์เชิงพฤติกรรมของผู้ใช้และเครื่องลูกข่าย การบูรณาการกับบริการด้านความมั่นคงปลอดภัยอื่น ๆ เพิ่มมากขึ้น และการขยายโครงสร้าง SASE/SSE ให้ครอบคลุมมากยิ่งขึ้น

๕.๔ แนวทางปฏิบัติในการติดตั้งและนำไปใช้งาน ZTNA แบบไฮบริด (Hybrid)

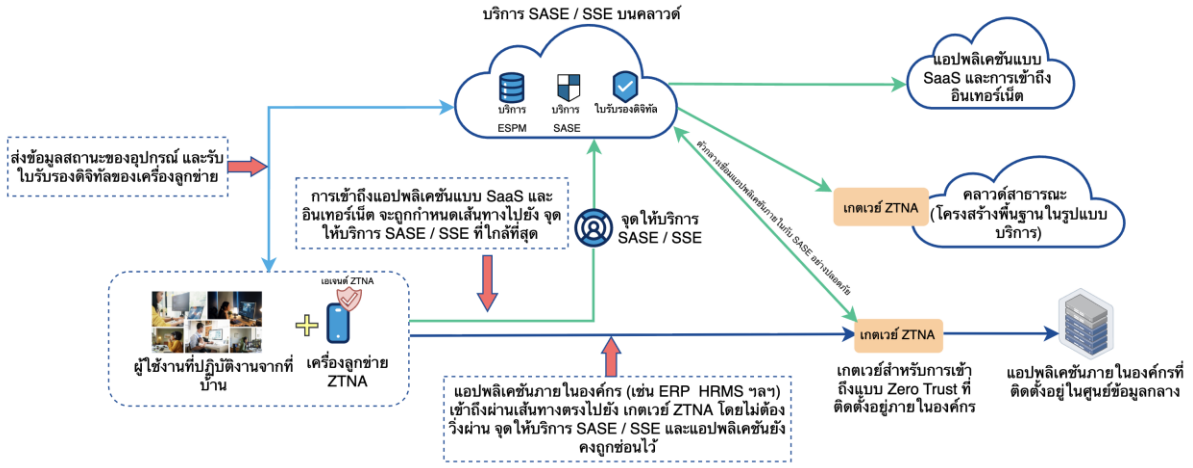
สถาปัตยกรรมด้านความมั่นคงปลอดภัยแบบไฮบริดเป็นแนวทางสำคัญสำหรับองค์กรที่กำลังเปลี่ยนผ่านไปสู่ Zero Trust แต่ยังต้องการผสานระบบที่ติดตั้งภายในองค์กรกับบริการความมั่นคงปลอดภัยบนคลาวด์อย่างมีประสิทธิภาพ แนวทางนี้เสนอ ZTNA ในลักษณะการประยุกต์ใช้ในรูปแบบแบบไฮบริด (Hybrid Deployment) เพื่อเพิ่มความยืดหยุ่นด้านการตรวจสอบอุปกรณ์ การยืนยันตัวตน และการควบคุมการเข้าถึงในระดับแอปพลิเคชัน

องค์กรยุคดิจิทัลมีความจำเป็นต้องรองรับผู้ใช้งานหลากหลายรูปแบบ ทั้งพนักงานภายใน ผู้ใช้งานที่เดินทาง และผู้ใช้งานจากสาขา ทำให้ความต้องการระบบความมั่นคงปลอดภัยแบบ Zero Trust เพิ่มสูงขึ้น อย่างไรก็ตาม หลายองค์กรยังคงมีระบบที่ติดตั้งภายในองค์กรที่ต้องควบคุมด้วยตนเอง เช่น ศูนย์ข้อมูล แอปพลิเคชันภายในที่มีความอ่อนไหว หรือกฎระเบียบที่ถูกกำกับดูแล ทำให้ไม่สามารถย้ายไปสู่คลาวด์ได้ทั้งหมด เพื่อตอบโจทย์นี้ได้มีการนำเสนอ ZTNA ในรูปแบบไฮบริด ซึ่งผสาน

๑) การติดตั้งเน็กซ์เจเนอเรชันไฟร์วอลล์ หรืออุปกรณ์อื่นที่มีความสามารถเป็นเกตเวย์ ZTNA ภายในองค์กร

๒) ระบบคลาวด์ SASE/SSE แบบ SaaS

ซึ่งทั้งสองส่วนจะทำงานตามแนวทางของ Zero Trust โดยสมบูรณ์ ทำให้สามารถควบคุมการเข้าถึงได้ทั้งที่ศูนย์ข้อมูลกลางและบนคลาวด์โดยใช้มาตรฐาน Zero Trust ได้อย่างปลอดภัย ทั้งสองส่วน จะใช้ส่วนบริหารและจัดการร่วมกันแบบรวมศูนย์ และยังคงให้ผู้ใช้เข้าถึงแอปพลิเคชันภายในองค์กรได้โดยตรงผ่านเกตเวย์ ZTNA (เน็กซ์เจเนอเรชันไฟร์วอลล์) ทำให้เส้นทางการเข้าถึงนั้นสั้นและปลอดภัยที่สุด ซึ่งเป็นจุดเด่นสำคัญของแบบไฮบริด



รูปที่ ๑๖ สถาปัตยกรรม ZTNA แบบไฮบริด

องค์ประกอบหลัก

สถาปัตยกรรมแบบไฮบริดประกอบด้วยส่วนหลัก ๒ ส่วนที่ทำงานร่วมกัน ได้แก่

๑) จุดให้บริการ SASE/SSE ทำหน้าที่ทั้งเป็นจุดตัดสินใจตามนโยบายและจุดบังคับใช้นโยบายส่วนคลาวด์

เพื่อทำหน้าที่ดังต่อไปนี้

๑) เป็นระบบจัดการสถานะความมั่นคงปลอดภัยของอุปกรณ์ปลายทาง

๒) จัดการเอเจนต์ ZTNA บนเครื่องลูกข่ายและออกใบรับรองดิจิทัล

๓) ประมวลผลข้อมูลสถานะของอุปกรณ์และกำหนดแท็ก ZTNA สำหรับการบังคับใช้นโยบายและส่งแท็ก ZTNA ต่อไปยังจุดบังคับใช้นโยบายที่อยู่ใน SASE/SSE เอง และที่เกตเวย์ ZTNA ในศูนย์ข้อมูลกลาง

๔) ทำการระบุและยืนยันตัวตนผ่านโปรโตคอล เช่น SAML เพื่อการยืนยันตัวตนแบบรวมศูนย์และยืนยันตัวตนเพียงครั้งเดียว (เช่น SSO)

๕) ให้บริการด้านการรักษาความมั่นคงปลอดภัยอื่น ๆ เช่น บริการเกตเวย์ควบคุมความมั่นคงปลอดภัยการใช้งานเว็บไซต์ บริการตัวกลางควบคุมความมั่นคงปลอดภัยการเข้าถึงบริการคลาวด์ (Cloud Access Security Broker: CASB) บริการไฟร์วอลล์บนคลาวด์ฯลฯ

๖) เป็นจุดบังคับนโยบายที่ทำหน้าที่เหมือนเกตเวย์ ZTNA บนคลาวด์ ที่จะถูกอธิบายหน้าที่โดยละเอียดในหัวข้อต่อไป

๒) เกตเวย์ ZTNA ในที่นี้คือ เน็กซ์เจเนอเรชันไฟร์วอลล์ (อุปกรณ์หรือซอฟต์แวร์เฉพาะทาง) ที่ติดตั้งอยู่ภายในศูนย์ข้อมูลกลาง เพื่อทำหน้าที่ดังต่อไปนี้

๑) เป็นจุดบังคับใช้นโยบายตามแท็ก ZTNA สำหรับเครื่องลูกข่ายทั้งภายในและภายนอกองค์กรที่มีความจำเป็นที่ต้องเชื่อมต่อกับแอปพลิเคชันที่อยู่ในศูนย์ข้อมูลกลางโดยตรง

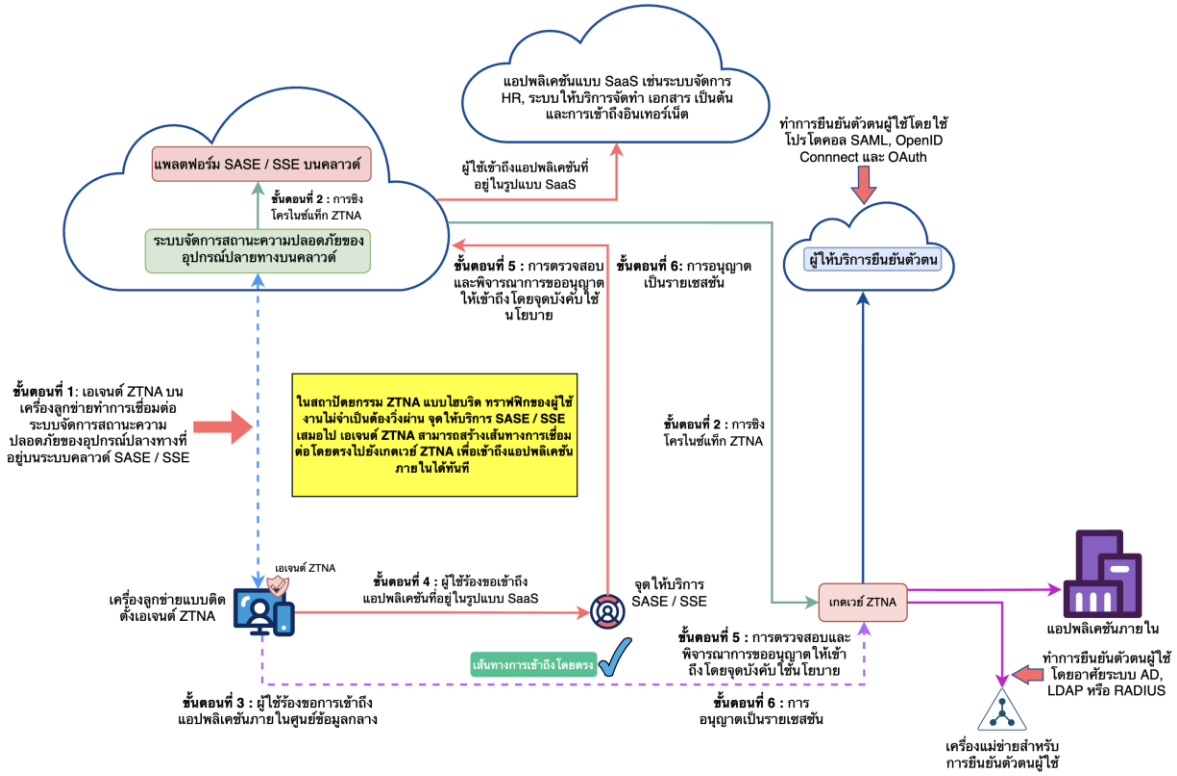
๒) รับแท็ก ZTNA จากระบบจัดการสถานะความมั่นคงปลอดภัยของอุปกรณ์ปลายทางบนคลาวด์ที่อยู่ในระบบ SASE/SSE แบบอัตโนมัติ

๓) ตรวจสอบใบรับรองดิจิทัลของเอเจนต์ ZTNA จากเครื่องลูกข่าย

๔) ตรวจสอบการเข้าถึงแบบรายเซสชันและรายแอปพลิเคชัน

๕) ทำการระบุและยืนยันตัวตนผ่านโปรโตคอล เช่น SAML ฯลฯ

การติดตั้งแบบไฮบริดจะช่วยให้ “ทราฟฟิก ZTNA บางส่วนที่ไปยังทรัพยากรภายในไม่ต้องเชื่อมต่อไปยังจุดให้บริการ SASE/SSE” ทำให้มีค่าความหน่วงเวลาต่ำแต่ยังคงความมั่นคงปลอดภัยไว้เหมือนเดิม



รูปที่ ๑๗ ลำดับขั้นตอนการทำงานของ ZTNA แบบไฮบริด

ลำดับขั้นตอนการทำงานของ ZTNA แบบไฮบริด อ้างอิงจากรูปที่ ๑๗

ขั้นตอนที่ ๑ เอเจนต์ ZTNA บนเครื่องลูกข่ายทำการเชื่อมต่อกับระบบจัดการสถานะความมั่นคงปลอดภัยของอุปกรณ์ปลายทางที่อยู่บนระบบ SASE/SSE

เอเจนต์ ZTNA บนเครื่องลูกข่ายทำการลงทะเบียนและเชื่อมต่อกับระบบจัดการสถานะความมั่นคงปลอดภัยของอุปกรณ์ปลายทาง เพื่อส่งข้อมูลสถานะของอุปกรณ์ไปประมวลผล โดยเอเจนต์จะมีหน้าที่หลักดังนี้

๑) ติดตั้งใบรับรองดิจิทัลที่ได้จากระบบจัดการสถานะความมั่นคงปลอดภัยของอุปกรณ์ปลายทางบนเครื่องลูกข่าย

๒) ตรวจสอบสถานะของอุปกรณ์และส่งข้อมูลไปยังระบบจัดการสถานะความมั่นคงปลอดภัยของอุปกรณ์ปลายทาง เพื่อใช้ในการประมวลผลและกำหนดแท็ก ZTNA

๓) เลือกจุดบังคับใช้นโยบายระหว่างจุดที่อยู่ในศูนย์ข้อมูลกลาง หรือจุดให้บริการ SASE/SSE ขึ้นอยู่กับตำแหน่งของแอปพลิเคชันปลายทาง

๔) เชื่อมต่อแบบเข้ารหัสไปยังจุดบังคับใช้นโยบายที่เลือกโดยอัตโนมัติเพื่อขอเข้าถึงแอปพลิเคชัน

ขั้นตอนที่ ๒ การซิงโครไนซ์แท็ก ZTNA

ระบบจัดการสถานะความมั่นคงปลอดภัยของอุปกรณ์ปลายทาง ทำการซิงโครไนซ์แท็ก ZTNA ไปยังจุดบังคับใช้นโยบายทั้งที่อยู่ในศูนย์ข้อมูลกลาง และในจุดให้บริการ SASE/SSE

ขั้นตอนที่ ๓ ผู้ใช้ร้องขอเข้าถึงแอปพลิเคชันภายในศูนย์ข้อมูลกลาง

ผู้ใช้ร้องขอการเข้าถึงแอปพลิเคชันที่อยู่ในศูนย์ข้อมูลกลางผ่านการเชื่อมต่อแบบเข้ารหัสจากเอเจนต์ ZTNA บนเครื่องลูกข่ายไปยังจุดบังคับใช้นโยบายบนเกตเวย์ ZTNA ที่อยู่ในศูนย์ข้อมูลกลาง

ขั้นตอนที่ ๔ ผู้ใช้ร้องขอเข้าถึงแอปพลิเคชันแบบ SaaS

ผู้ใช้ร้องขอการเข้าถึงแอปพลิเคชันแบบ SaaS ผ่านการเชื่อมต่อแบบเข้ารหัสจากเอเจนต์ ZTNA บนเครื่องลูกข่ายไปยังจุดบังคับใช้นโยบายที่อยู่ในระบบ SASE/SSE บนคลาวด์

ขั้นตอนที่ ๕ การตรวจสอบและพิจารณาการขออนุญาตเข้าถึงโดยจุดบังคับใช้นโยบาย

จุดบังคับใช้นโยบายจะทำหน้าที่เหมือนกับแนวทางปฏิบัติข้อ ๕.๒ แนวทางปฏิบัติในการติดตั้งและนำไปใช้งาน ZTNA แบบการติดตั้งภายในองค์กร (On-Premises) และ ๕.๓ แนวทางปฏิบัติในการติดตั้งและนำไปใช้งาน ZTNA แบบคลาวด์ (Cloud)

ขั้นตอนที่ ๖ การอนุญาตเป็นรายเซสชัน

จุดบังคับใช้นโยบายจะตรวจสอบและอนุญาตการร้องขอไปยังแอปพลิเคชันจากเครื่องลูกข่ายเป็นรายเซสชันตามแนวนโยบายที่กำหนด

สถาปัตยกรรมแบบไฮบริดเป็นการผสมผสานจุดเด่นของแต่ละสถาปัตยกรรมเข้าด้วยกัน และมีความยืดหยุ่นสามารถปรับให้เข้ากับองค์กรที่มีระบบที่ซับซ้อนหรือมีความหลากหลายได้เป็นอย่างดี

ข้อแนะนำในการนำไปประยุกต์ใช้งาน

แนวทางที่ ๑ การเข้าถึงบริการ SaaS และการเข้าถึงเครือข่ายส่วนตัวที่ปลอดภัย

๑) ทราฟฟิกที่ต้องการเข้าถึง SaaS จะถูกส่งไปยังจุดให้บริการ SASE/SSE

๒) ทราฟฟิกที่ต้องการเข้าถึงแอปพลิเคชันภายใน เช่น ระบบวางแผนทรัพยากร ฯลฯ จะถูกส่งผ่านเกตเวย์ ZTNA โดยตรง

ประโยชน์

ลดค่าความหน่วงเวลา ลดทราฟฟิกที่ผ่านภายในองค์กร และยังคงความสามารถ Zero Trust ไว้เช่นเดิม

แนวทางที่ ๒ การตรวจสอบสถานะของเครื่องลูกข่ายแบบรวมศูนย์บนระบบคลาวด์

๑) เหมาะสำหรับองค์กรที่ต้องการใช้ระบบจัดการสถานะความมั่นคงปลอดภัยของเครื่องลูกข่ายแบบคลาวด์ แต่ไม่ต้องการดูแลเครื่องแม่ข่ายเอง และยังคงต้องการเก็บข้อมูลสำคัญไว้ในศูนย์ข้อมูลกลาง

๒) การประมวลผลสถานะของอุปกรณ์ทำบนคลาวด์ทั้งหมด แต่การเข้าถึงแอปพลิเคชันภายในจะเชื่อมต่อผ่านเกตเวย์ ZTNA โดยตรง

แนวทางที่ ๓ การเข้าถึงแบบไฮบริดจากพนักงานในสาขา (Branch)

๑) เมื่อใช้ร่วมกับ SD-WAN ทราฟฟิกจากสาขาสามารถเชื่อมต่อผ่าน SD-WAN ไปยัง SASE หรือ ศูนย์ข้อมูลกลาง ตามเส้นทางที่ดีที่สุดไปยังแอปพลิเคชัน

แนวทางที่ ๔ ไฮบริดมัลติคลาวด์

เหมาะสำหรับองค์กรที่มีทรัพยากรที่อยู่ในทั้ง

๑) ศูนย์ข้อมูลกลาง

๒) คลาวด์ส่วนตัว

๓) คลาวด์สาธารณะ

ZTNA ไฮบริดสามารถกำหนดว่าทราฟฟิกที่เข้าถึงทรัพยากรใด ต้องเชื่อมต่อผ่านจุดบังคับใช้นโยบายจุดใด เช่น

๑) แอปพลิเคชันที่ติดตั้งภายในศูนย์ข้อมูลกลางผ่านเกตเวย์ ZTNA

๒) คลาวด์แอปพลิเคชันผ่านจุดให้บริการ SASE/SSE

สถาปัตยกรรม ZTNA แบบไฮบริดเป็นสถาปัตยกรรมที่มีความยืดหยุ่น ช่วยให้องค์กรสามารถปกป้องทรัพยากรสำคัญโดยไม่ลดประสิทธิภาพในการทำงาน ซึ่งเป็นแนวทางที่ผสานข้อดีของทั้งสองแบบเข้าด้วยกัน

เอกสารอ้างอิง

๑) Cloud Security Alliance, Introduction to Zero Trust Architecture (CCZT Study Guide), Version 20250219, 2025.

๒) Endpoint Security Posture Management (ESPM) aligns with National Institute of Standards and Technology (NIST) guidance by providing tools and processes to meet specific controls within the NIST Cybersecurity Framework (CSF 2.0), 2024 and NIST Special Publication 800-53, 2020 /800-171, 2020.

ภาคผนวก

ผนวก ก รายการตรวจสอบความมั่นคงปลอดภัยแบบ Zero Trust

ส่วนที่ ๑ ตัวตน (Identity)

ตารางที่ ๒๕ แสดงรายการตรวจสอบของตัวตน

รหัส	ระดับรายการตรวจสอบ	รายการตรวจสอบ	สถานะ
IDT-01	ขั้นพื้นฐาน	มีการยืนยันตัวตนแบบหลายปัจจัยร่วมกับรหัสผ่าน	☐
IDT-01 RE1	ขั้นสูง	มีการยืนยันตัวตนแบบหลายปัจจัยในขั้นสูง เช่น แบบไม่ใช้รหัสผ่านด้วย FIDO2	☐
IDT-02	ขั้นพื้นฐาน	มีการจัดการแหล่งเก็บข้อมูลยืนยันตัวตนทั้งบนระบบภายในองค์กรและระบบคลาวด์อย่างปลอดภัย แต่ยังไม่มีการรวมศูนย์และบูรณาการจากหลายแหล่งเข้าด้วยกัน	☐
IDT-02 RE1	ขั้นสูง	มีการจัดการแหล่งเก็บข้อมูลยืนยันตัวตนทั้งบนระบบภายในองค์กรและระบบคลาวด์อย่างปลอดภัย และสามารถทำงานรวมศูนย์และบูรณาการจากหลายแหล่งเข้าด้วยกันเพื่อสนับสนุน SSO	☐
IDT-03	ขั้นพื้นฐาน	มีการประเมินความเสี่ยงของตัวตนเบื้องต้น เช่น มีการตรวจสอบเหตุการณ์ด้านความมั่นคงปลอดภัยของการยืนยันตัวตน เพื่อค้นหาบัญชีผู้ใช้ใดถูกละเมิดด้วยการโจมตี เช่น บรูทฟอร์ซ และระงับการเข้าถึงด้วยการกำหนดกฎแบบสแตติก เช่น ปิดใช้งานบัญชีผู้ใช้รายนั้น	☐
IDT-03 RE1	ขั้นสูง	มีการประเมินความเสี่ยงของตัวตนแบบอัตโนมัติตามพฤติกรรมของผู้ใช้ และระงับการเข้าถึงแบบกฎไดนามิก เช่น กำหนดนโยบายว่า หากบัญชีผู้ใช้ใดหรือการเข้าสู่ระบบของผู้ใช้ใดมีความเสี่ยงสูง ให้ระงับการเข้าถึง หรือกำหนดค่าควบคุมกักกันการเข้าสู่ระบบชั่วระยะเวลาหนึ่งได้ เช่น กักกันไม่ให้เข้าระบบเป็นระยะเวลา 30 นาที	☐
IDT-04	ขั้นพื้นฐาน	มีการกำหนดสิทธิการใช้งานที่อนุมัติการเข้าถึงแบบจำกัดเวลา กำหนดเวลาหมดอายุที่ชัดเจน และเมื่อครบเวลาสามารถระงับ	☐

รหัส	ระดับรายการตรวจสอบ	รายการตรวจสอบ	สถานะ
		สิทธิได้แบบอัตโนมัติ เช่น หลังจากทำการยืนยันตัวตนเรียบร้อย สามารถเข้าใช้งานเป็นเวลา 1 ชั่วโมง เมื่อครบเวลาต้องกลับไปทำการขออนุมัติการเข้าถึงอีกครั้ง	
IDT-04 RE1	ขั้นสูง	มีการกำหนดสิทธิการใช้งานแบบจำกัดเวลา อนุมัติการเข้าถึงเฉพาะที่จำเป็นตามเซสชันที่ใช้งานได้	☐
IDT-05	ขั้นพื้นฐาน	มีระบบเก็บบันทึกเหตุการณ์ การใช้งานของผู้ใช้และมีการวิเคราะห์ข้อมูลแบบอัตโนมัติได้บางระบบ แต่ไม่สามารถเชื่อมโยงและวิเคราะห์ความสัมพันธ์ของบันทึกเหตุการณ์ได้	☐
IDT-05 RE1	ขั้นสูง	ระบบเก็บบันทึกเหตุการณ์ สามารถวิเคราะห์ข้อมูลอัตโนมัติและสามารถเชื่อมโยงบันทึกเหตุการณ์หลายประเภทร่วมกันเพื่อวิเคราะห์ความสัมพันธ์ของบันทึกเหตุการณ์ได้	☐
IDT-06	ขั้นพื้นฐาน	มีความสามารถในการจัดการบัญชีผู้ใช้อย่างเป็นระบบ เพื่อลดความเสี่ยงในการเข้าใช้งาน เช่น มีเครื่องมือสำหรับ เพิ่มบัญชีผู้ใช้เมื่อพนักงานเข้าใหม่ ลบบัญชีผู้ใช้เมื่อพนักงานลาออก ปิดบัญชีผู้ใช้เมื่อไม่มีการเข้าระบบเกิน 180 วัน ฯลฯ โดยระบบภายในขององค์กรต้องสามารถจัดการได้ครบทุกบัญชี	☐
IDT-06 RE1	ขั้นสูง	มีระบบจัดการบัญชีผู้ใช้แบบอัตโนมัติครบทุกบัญชี เช่น ตรวจสอบบัญชีผู้ใช้อย่างต่อเนื่อง ในกรณีที่ไม่มีการเข้าระบบเกิน 180 วัน สามารถปิดบัญชีผู้ใช้เมื่อครบกำหนดได้ทันที เพื่อลดความเสี่ยงในการเข้าใช้งาน และการซิงโครไนซ์บัญชีผู้ใช้ทั้งระบบภายในองค์กรและระบบคลาวด์	☐
IDT-07	ขั้นพื้นฐาน	มีนโยบายระดับองค์กรที่ชัดเจน ในการใช้รหัสผ่านและการยืนยันตัวตน เช่น ต้องมีการตั้งรหัสผ่านที่แข็งแรง ต้องมีการใช้ MFA ต้องมีการเปลี่ยนรหัสผ่านทุก 120 วัน และต้องมีการบังคับใช้และทบทวนนโยบาย	☐
IDT-07 RE1	ขั้นสูง	มีนโยบายองค์กรที่ชัดเจนในการใช้รหัสผ่าน การยืนยันตัวตน พร้อมบังคับใช้ (Enforcement) และมีการแจ้งเตือนเป็นระยะแบบอัตโนมัติ	☐

ส่วนที่ ๒ อุปกรณ์ (Devices)

ตารางที่ ๒๖ แสดงรายการตรวจสอบของอุปกรณ์

รหัส	ระดับรายการตรวจสอบ	รายการตรวจสอบ	สถานะ
DVS-01	ขั้นพื้นฐาน	สามารถตรวจสอบสถานะของอุปกรณ์ โดยเก็บข้อมูลรายงานอุปกรณ์เบื้องต้น เช่น คีย์ โทเค็น ผู้ใช้งาน ที่มีการใช้งานบนแต่ละอุปกรณ์ และมีกระบวนการบังคับใช้ซอฟต์แวร์เฉพาะที่อนุญาตเท่านั้น รวมถึงส่งการอัปเดตระบบปฏิบัติการ (OS) ให้อยู่ในเวอร์ชันที่ปลอดภัยบนอุปกรณ์ต่าง ๆ ได้	☐
DVS-01 RE1	ขั้นสูง	มีระบบตรวจสอบอุปกรณ์ได้ก่อนเชื่อมต่อ และมีการอัปเดตระบบปฏิบัติการให้อยู่ในเวอร์ชันที่ปลอดภัยอัตโนมัติ และตรวจสอบสถานะของอุปกรณ์แบบต่อเนื่อง	☐
DVS-02	ขั้นพื้นฐาน	มีการบันทึกและติดตามสินทรัพย์ทางกายภาพทั้งหมดและสินทรัพย์เสมือนบางส่วน และจัดการความเสี่ยงของสินทรัพย์โดยการกำหนดนโยบายและเกณฑ์พื้นฐานในการประเมินความเสี่ยงของสินทรัพย์ทั้งหมด โดยใช้กรอบการทำงานที่ปลอดภัย	☐
DVS-02 RE1	ขั้นสูง	มีการบันทึกและติดตามสินทรัพย์ทางกายภาพและสินทรัพย์เสมือนทั้งหมดแบบอัตโนมัติ สามารถทำงานร่วมกับผู้ผลิตหลายราย เพื่อจัดการความเสี่ยงของสินทรัพย์และประเมินความเสี่ยงของสินทรัพย์ได้	☐
DVS-03	ขั้นพื้นฐาน	มีการนำข้อมูลอุปกรณ์และลักษณะเฉพาะของอุปกรณ์ มาใช้ในการอนุญาตเพื่อเข้าถึงระบบ เช่น อุปกรณ์ที่มีระบบปฏิบัติการเป็น Windows 10 และ Windows 11 อนุญาตให้เข้าถึงทรัพยากรในศูนย์ข้อมูลกลางได้	☐
DVS-03 RE1	ขั้นสูง	มีการใช้ข้อมูลและลักษณะเฉพาะของอุปกรณ์หลายอย่างร่วมกัน รวมถึงข้อมูลสำหรับประเมินความเสี่ยงของอุปกรณ์เพื่อนำมากำหนดเงื่อนไขในการพิจารณาว่า เป็นอุปกรณ์ที่ผ่านการตรวจสอบตามนโยบายขององค์กรแล้ว และอนุญาตให้	☐

รหัส	ระดับรายการตรวจสอบ	รายการตรวจสอบ	สถานะ
		เข้าถึงระบบได้ เช่น อุปกรณ์ที่ผ่านการตรวจสอบการปฏิบัติตามข้อกำหนด ต้องมีคุณสมบัติดังนี้ จึงเข้าระบบได้ ๑) มีระบบปฏิบัติการเป็น Windows 10 และ Windows 11 ๒) มีการใช้งานซอฟต์แวร์ป้องกันภัยคุกคาม ๓) ไม่มีช่องโหว่ระดับรุนแรงของซอฟต์แวร์ที่ใช้งานบนอุปกรณ์	
DVS-04	ขั้นพื้นฐาน	อุปกรณ์มีการติดตั้งซอฟต์แวร์ป้องกันภัยคุกคามที่สามารถอัปเดตได้อัตโนมัติ	☐
DVS-04 RE1	ขั้นสูง	มีแนวทางแบบรวมศูนย์สำหรับการป้องกันภัยคุกคามบนอุปกรณ์ การบังคับใช้นโยบายและการตรวจสอบการปฏิบัติตามข้อกำหนดสำหรับอุปกรณ์ทั้งหมด	☐
DVS-05	ขั้นพื้นฐาน	มีการมองเห็นและวิเคราะห์รายการสินทรัพย์ทั้งหมดจากหมายเลขเครื่อง (MAC Address) เพื่อตรวจจับอุปกรณ์ที่ไม่ได้รับอนุญาต	☐
DVS-05 RE1	ขั้นสูง	ดำเนินการรวบรวมและวิเคราะห์รายการสินทรัพย์ของผู้ใช้ทั้งหมดแบบอัตโนมัติ เช่น คอมพิวเตอร์ตั้งโต๊ะ คอมพิวเตอร์พกพา เพื่อตรวจจับอุปกรณ์ที่ไม่ได้รับอนุญาต	☐
DVS-06	ขั้นพื้นฐาน	มีเครื่องมือเพื่อทำให้กระบวนการจัดเตรียม การลงทะเบียนและการยกเลิกลงทะเบียนของอุปกรณ์ที่ถูกใช้งานเป็นไปโดยอัตโนมัติ	☐
DVS-06 RE1	ขั้นสูง	มีระบบตรวจจับและแยกอุปกรณ์ที่ไม่เป็นไปตามระเบียบข้อบังคับแบบอัตโนมัติ เช่น อุปกรณ์มีช่องโหว่ ไม่มีใบรับรองดิจิทัล อุปกรณ์ที่ไม่ได้ลงทะเบียน จะต้องถูกแยกออกจากเครือข่ายปกติโดยอัตโนมัติ	☐
DVS-07	ขั้นพื้นฐาน	มีการกำกับดูแลอุปกรณ์ โดยการบังคับใช้นโยบายสำหรับการจัดซื้ออุปกรณ์ใหม่ และการบริหารวงจรชีวิตของอุปกรณ์ ระบบมีความสามารถในการจัดการอุปกรณ์ การอัปเดตอุปกรณ์ในระบบ แก้ไขช่องโหว่ ตรวจจับและทำการกำจัดภัย	☐

รหัส	ระดับรายการตรวจสอบ	รายการตรวจสอบ	สถานะ
		คุกคาม เพื่อให้มั่นใจว่าอุปกรณ์ที่ใช้งานนั้นไม่เป็นอุปกรณ์ที่ล้าสมัยและไม่มีช่องโหว่ระดับรุนแรง เป็นการลดความเสี่ยงเมื่อเข้าใช้งานภายในองค์กร	
DVS-07 RE1	ขั้นสูง	มีการกำกับดูแลอุปกรณ์ โดยบังคับใช้และบริหารวงจรชีวิตของอุปกรณ์แบบรวมศูนย์ โดยผู้ดูแลระบบสามารถบริหารจัดการอุปกรณ์แบบรวมศูนย์ ในการสั่งอัปเดตอุปกรณ์ในระบบ แก้ไขช่องโหว่ ตรวจจับและทำการกำจัดภัยคุกคาม เพื่อให้มั่นใจว่าอุปกรณ์ที่ใช้งานนั้นไม่เป็นอุปกรณ์ที่ล้าสมัยและไม่มีช่องโหว่ระดับรุนแรง เป็นการลดความเสี่ยงเมื่อเข้าใช้งานภายในองค์กร	☐

ส่วนที่ ๓ ระบบเครือข่าย (Networks)

ตารางที่ ๒๗ แสดงรายการตรวจสอบของระบบเครือข่าย

รหัส	ระดับรายการตรวจสอบ	รายการตรวจสอบ	สถานะ
NWS-01	ขั้นพื้นฐาน	การแบ่งส่วนเครือข่าย ใช้ VLAN หรือ ACL ในการแบ่งแยกเครือข่ายบางส่วน	☐
NWS-01 RE1	ขั้นสูง	การแบ่งส่วนเครือข่ายแบบย่อยใช้แอปพลิเคชันเป็นเกณฑ์ในการแบ่งแยกเครือข่าย เพื่อจำกัดการเข้าถึงเฉพาะทรัพยากรที่จำเป็น	☐
NWS-02	ขั้นพื้นฐาน	การเข้ารหัสทราฟฟิกที่เชื่อมต่อจากภายนอกองค์กรทั้งหมด	☐
NWS-02 RE1	ขั้นสูง	การเข้ารหัสทราฟฟิกทุกช่องทางทั้ง ภายนอกและภายในองค์กรทั้งหมด	☐
NWS-03	ขั้นพื้นฐาน	ควบคุมการเข้าถึงเครือข่าย โดยการตรวจสอบอุปกรณ์ก่อนเชื่อมต่อ เช่น หมายเลขเครื่อง ใบรับรองดิจิทัล ฯลฯ	☐
NWS-03 RE1	ขั้นสูง	ควบคุมการเข้าถึงเครือข่าย โดยใช้ข้อมูลตัวตน (Identity-based Access) ในการอนุญาต	☐

รหัส	ระดับรายการตรวจสอบ	รายการตรวจสอบ	สถานะ
NWS-04	ขั้นพื้นฐาน	สามารถเก็บรวบรวมบันทึกเหตุการณ์ จากหลายแหล่ง เช่น ไฟร์วอลล์ อุปกรณ์ในระบบเครือข่าย อุปกรณ์ปลายทาง เครื่องแม่ข่าย ฯลฯ	☐
NWS-04 RE1	ขั้นสูง	ตรวจจับและบันทึกเหตุการณ์ที่ผิดปกติแบบเรียลไทม์ สามารถวิเคราะห์ความสัมพันธ์ของบันทึกเหตุการณ์ร่วมกัน เพื่อแจ้งเตือนเหตุการณ์ที่ไม่ปลอดภัยหรือผิดปกติให้ผู้ดูแลระบบได้	☐
NWS-04 RE2	ขั้นสูง	มีการกำกับดูแลและมีความสามารถในการมองเห็นการติดต่อสื่อสารในระบบเครือข่ายและทุกสภาพแวดล้อมขององค์กร และมีความสามารถในการแบ่งปันข้อมูลการตรวจสอบสถานะของอุปกรณ์ไปยังจุดบังคับใช้นโยบาย (Policy Enforcement Point) พร้อมกันได้ทั้งหมด	☐
NWS-05	ขั้นพื้นฐาน	สามารถตรวจจับภัยคุกคามด้วย IDS/IPS	☐
NWS-05 RE1	ขั้นสูง	สามารถตรวจจับและตอบสนองต่อภัยคุกคามในระดับเครือข่ายได้ (Network Detection & Response) โดยวิเคราะห์พฤติกรรมที่ผ่านเครือข่าย เพื่อมองเห็นและหยุดยั้งภัยคุกคามที่ซับซ้อน	☐
NWS-05 RE2	ขั้นสูง	สามารถรับมือกับภัยคุกคามได้อย่างมีประสิทธิภาพ โดยมีกระบวนการทำงานที่ชัดเจนและเป็นระบบ ตั้งแต่การรวบรวมข้อมูล การวิเคราะห์ ไปจนถึงการตอบสนองแบบอัตโนมัติ (Security Orchestration, Automation, and Response) โดยสามารถตอบสนองได้อย่างทันท่วงทีผ่าน playbooks ได้	☐
NWS-06	ขั้นพื้นฐาน	มีการจัดการการตั้งค่าและบังคับใช้นโยบายของอุปกรณ์ในระบบเครือข่าย เช่น การกำหนดกฎและนโยบายความมั่นคงปลอดภัยในการเข้าถึงทรัพยากรขององค์กร ฯลฯ	☐
NWS-06 RE1	ขั้นสูง	มีวิธีแบบอัตโนมัติในการจัดการการตั้งค่าและบังคับใช้นโยบายของอุปกรณ์ในระบบเครือข่ายแบบรวมศูนย์ เช่น การกำหนดกฎและนโยบายความมั่นคงปลอดภัยในการเข้าถึงทรัพยากรขององค์กร ฯลฯ	☐

รหัส	ระดับรายการตรวจสอบ	รายการตรวจสอบ	สถานะ
NWS-07	ขั้นพื้นฐาน	มีการกำกับดูแลเครือข่ายด้วยนโยบายพื้นฐาน (การเข้าถึงโปรโตคอล การแบ่งส่วน การแจ้งเตือน และการแก้ไข) โดยมุ่งเน้นที่การป้องกันขอบเขตของเครือข่าย รวมถึงมีการเก็บบันทึกเหตุการณ์ และการตรวจสอบการเปลี่ยนแปลง	☐
NWS-07 RE1	ขั้นสูง	มีการกำกับดูแลเครือข่ายด้วยนโยบายในระดับองค์กรที่สนับสนุนการกำหนดมาตรการควบคุมการเข้าถึงของหน่วยงานย่อยตามความเหมาะสม สามารถปรับปรุงเปลี่ยนแปลงได้แบบไดนามิก และรองรับการเชื่อมต่อกับระบบภายนอกอย่างปลอดภัย โดยอ้างอิงตามรูปแบบการทำงานของแอปพลิเคชันและผู้ใช้งาน	☐

ส่วนที่ ๔ แอปพลิเคชันและเวิร์กโหลด (Applications and Workloads)

ตารางที่ ๒๘ แสดงรายการตรวจสอบของแอปพลิเคชันและเวิร์กโหลด

รหัส	ระดับรายการตรวจสอบ	รายการตรวจสอบ	สถานะ
APW-01	ขั้นพื้นฐาน	อนุญาตการเข้าถึงแอปพลิเคชันตามข้อมูลบริบท (เช่น ข้อมูลประจำตัว การปฏิบัติตามข้อกำหนดของอุปกรณ์) พร้อมกำหนดระยะเวลาจำกัดการเข้าถึงแอปพลิเคชันได้ เช่น อนุญาตให้เข้าถึงแอปพลิเคชันได้ไม่เกิน 60 นาที	☐
APW-01 RE1	ขั้นสูง	อนุญาตการเข้าถึงแอปพลิเคชันตามบริบทแบบหลายมิติ และเป็นการเข้าถึงแบบได้รับสิทธิเฉพาะตามความจำเป็นในการใช้งานเท่านั้น	☐
APW-02	ขั้นพื้นฐาน	แอปพลิเคชันที่สำคัญต้องมีระบบป้องกันภัยคุกคาม (Threat Protections)	☐
APW-02 RE1	ขั้นสูง	แอปพลิเคชันทั้งหมดต้องมีระบบป้องกันภัยคุกคามขั้นสูง (Advanced Threat Protections)	☐
APW-03	ขั้นพื้นฐาน	เริ่มเปิดให้เข้าใช้แอปพลิเคชันผ่านเครือข่ายสาธารณะ โดยมีการควบคุมความมั่นคงปลอดภัย	☐

รหัส	ระดับรายการตรวจสอบ	รายการตรวจสอบ	สถานะ
APW-03 RE1	ขั้นสูง	แอปพลิเคชันส่วนใหญ่เข้าถึงได้อย่างปลอดภัยตามหลักการ Zero Trust	☐
APW-04	ขั้นพื้นฐาน	มีโครงสร้างพื้นฐานแยกสำหรับทีมพัฒนาแอปพลิเคชันโดยเฉพาะ และนำหลักการ DevOps มาเพิ่มความมั่นคงปลอดภัยในการพัฒนาแอปพลิเคชัน	☐
APW-04 RE1	ขั้นสูง	ทีมงานมีการประสานงานกันในเรื่องการพัฒนา (Development) ความมั่นคงปลอดภัย (Security) และการดำเนินงาน (Operation) และแยกบทบาทชัดเจน โดยกระบวนการนำแอปพลิเคชันที่พัฒนาขึ้นไปยังระบบจริงต้องผ่าน CI/CD pipeline ทั้งหมด	☐
APW-05	ขั้นพื้นฐาน	ทดสอบความมั่นคงปลอดภัยของแอปพลิเคชัน โดยใช้การตรวจสอบแบบสแตติก (SAST) และการตรวจสอบแบบไดนามิกบางส่วน	☐
APW-05 RE1	ขั้นสูง	ทดสอบความมั่นคงปลอดภัยของแอปพลิเคชัน โดยใช้การทดสอบแบบไดนามิกทั้งหมด และประสานการทดสอบนี้เข้ากับ CI/CD pipeline ของกระบวนการนำแอปพลิเคชันที่พัฒนาขึ้นไปยังระบบจริง	☐
APW-06	ขั้นพื้นฐาน	ตรวจสอบโปรไฟล์ของแอปพลิเคชัน (เช่น สถานะ สุขภาพ และประสิทธิภาพ) และการตรวจสอบความมั่นคงปลอดภัยแบบอัตโนมัติ เพื่อรวบรวมบันทึกข้อมูลเกี่ยวกับการทำงานของแอปพลิเคชัน	☐
APW-06 RE1	ขั้นสูง	สามารถมองเห็นแอปพลิเคชันส่วนใหญ่หรือทั้งหมดขององค์กร มีการวิเคราะห์แนวโน้มสถานะและความมั่นคงปลอดภัยต่างๆ แบบอัตโนมัติ	☐
APW-07	ขั้นพื้นฐาน	ทำการปรับปรุงการตั้งค่าแอปพลิเคชันเป็นระยะ เพื่อให้แอปพลิเคชันมีความมั่นคงปลอดภัยอย่างเหมาะสม	☐
APW-07 RE1	ขั้นสูง	ปรับแต่งค่าด้านความมั่นคงปลอดภัยแบบอัตโนมัติอย่างเหมาะสม เมื่อสภาพแวดล้อมเปลี่ยน เช่น เมื่อพบช่องโหว่ใหม่	☐

รหัส	ระดับรายการตรวจสอบ	รายการตรวจสอบ	สถานะ
		ของแอปพลิเคชัน สามารถทำการแก้ไขช่องโหว่นั้นได้แบบอัตโนมัติ	
APW-08	ขั้นพื้นฐาน	บังคับใช้นโยบายกำกับดูแลแอปพลิเคชันแบบอัตโนมัติสำหรับแอปพลิเคชันบางส่วนตามความเสี่ยง โดยครอบคลุมการพัฒนาแอปพลิเคชัน การติดตั้งใช้งาน การจัดการสินทรัพย์ซอฟต์แวร์ การทดสอบความมั่นคงปลอดภัย การประเมิน และการแก้ไขข้อบกพร่อง	☐
APW-08 RE1	ขั้นสูง	ใช้นโยบายกำกับดูแลแอปพลิเคชันแบบอัตโนมัติทั่วทั้งองค์กรและครอบคลุมทุกแอปพลิเคชัน	☐

ส่วนที่ ๕ ข้อมูล (Data)

ตารางที่ ๒๙ แสดงรายการตรวจสอบของการรักษาความมั่นคงปลอดภัยของข้อมูล

รหัส	ระดับรายการตรวจสอบ	รายการตรวจสอบ	สถานะ
DAT-01	ขั้นพื้นฐาน	มีการจัดประเภทของข้อมูลในบางระบบ และติดป้ายกำกับข้อมูล (Label)	☐
DAT-01 RE1	ขั้นสูง	จัดประเภทของข้อมูลและติดป้ายกำกับข้อมูลแบบอัตโนมัติกับข้อมูลส่วนใหญ่ตามความเสี่ยง	☐
DAT-02	ขั้นพื้นฐาน	ควบคุมการเข้าถึงข้อมูลของผู้ใช้ (เช่น สิทธิในการอ่าน เขียน คัดลอก) ผ่านการควบคุมการเข้าถึงด้วยการกำหนดกฎแบบสแตติก	☐
DAT-02 RE1	ขั้นสูง	ควบคุมการเข้าถึงข้อมูลด้วยวิธีอัตโนมัติ โดยพิจารณาคุณลักษณะต่าง ๆ เช่น ตัวตน ความเสี่ยงของอุปกรณ์แอปพลิเคชัน ประเภทข้อมูลฯลฯ และมีระยะเวลาจำกัดตามความเหมาะสม	☐
DAT-03	ขั้นพื้นฐาน	ใช้การป้องกันข้อมูลด้วยการเข้ารหัส ผสมผสานกับการใช้ระบบป้องกันการสูญหายของข้อมูล (Data Loss Prevention: DLP)	☐

รหัส	ระดับรายการตรวจสอบ	รายการตรวจสอบ	สถานะ
		กับข้อมูลบางส่วน เช่น ข้อมูลที่สำคัญ และห้ามการแชร์ข้อมูลสำคัญออกไปภายนอก	
DAT-03 RE1	ขั้นสูง	ใช้ DLP ครอบคลุมข้อมูลทั้งหมด เพื่อตรวจจับและป้องกันข้อมูลรั่วไหล	☐
DAT-04	ขั้นพื้นฐาน	ใช้ DLP เฉพาะบางช่องทางสำคัญ เช่น อีเมลหรืออุปกรณ์ปลายทาง	☐
DAT-04 RE1	ขั้นสูง	ใช้ DLP ครอบคลุมทุกช่องทางข้อมูล รวมทั้งคลาวด์ API อุปกรณ์ปลายทางฯลฯ	☐
DAT-05	ขั้นพื้นฐาน	มีการสำรองข้อมูลบางส่วนจากภายในองค์กรเก็บไว้นอกสถานที่ เช่น คลาวด์ เพื่อให้มีความพร้อมใช้งานสูง (Highly Available) ในการเข้าถึงข้อมูล เมื่อเกิดเหตุการณ์ที่ส่งผลกระทบทำให้ไม่สามารถเข้าถึงข้อมูลจากแหล่งจัดเก็บข้อมูลหลักได้ ต้องสามารถทำการเข้าถึงข้อมูลจากแหล่งเก็บข้อมูลสำรองแทนได้	
DAT-05 RE1	ขั้นสูง	มีการสำรองข้อมูลทั้งหมดจากภายในองค์กรเก็บไว้นอกสถานที่ เช่น คลาวด์ เพื่อให้มีความพร้อมใช้งานสูง (Highly Available) ในการเข้าถึงข้อมูล เมื่อเกิดเหตุการณ์ที่ส่งผลกระทบทำให้ไม่สามารถเข้าถึงข้อมูลจากแหล่งจัดเก็บข้อมูลหลักได้ ต้องสามารถทำการเข้าถึงข้อมูลจากแหล่งเก็บข้อมูลสำรองแทนได้ รวมถึงสามารถเข้าถึงข้อมูลย้อนหลัง (Historical Data) ได้	
DAT-06	ขั้นพื้นฐาน	เก็บรวบรวมและวิเคราะห์บันทึกเหตุการณ์ จากแหล่งเก็บข้อมูลและแอปพลิเคชันบางส่วนตามความเสี่ยง	☐
DAT-06 RE1	ขั้นสูง	วิเคราะห์การเข้าถึงข้อมูลทั้งองค์กร พร้อมตรวจสอบความผิดปกติ	☐
DAT-07	ขั้นพื้นฐาน	ใช้นโยบายจัดการวงจรชีวิตของข้อมูล ทำการลบข้อมูลบางส่วนเมื่อข้อมูลอยู่ในระบบจนครบกำหนด เพื่อลดความเสี่ยงของข้อมูลรั่วไหลออกไปภายนอก	☐
DAT-07 RE1	ขั้นสูง	มีลำดับขั้นตอนการทำงานแบบอัตโนมัติในการจัดการวงจรชีวิตของข้อมูลกับข้อมูลทุกแหล่งจัดเก็บในองค์กร	☐

รหัส	ระดับรายการตรวจสอบ	รายการตรวจสอบ	สถานะ
DAT-08	ขั้นพื้นฐาน	นำนโยบายวงจรชีวิตของข้อมูลและความมั่นคงปลอดภัยของข้อมูลมาใช้ในองค์กร เช่น การเข้าถึง การใช้งาน การจัดเก็บ การเข้ารหัส การกำหนดค่า การป้องกัน การสำรองข้อมูล การจัดหมวดหมู่ การล้างข้อมูล ฯลฯ	☐
DAT-08 RE1	ขั้นสูง	นำนโยบายวงจรชีวิตของข้อมูลและความมั่นคงปลอดภัยของข้อมูลมาใช้ด้วยวิธีการอัตโนมัติเป็นหลักสำหรับข้อมูลขององค์กรส่วนใหญ่	☐
DAT-09	ขั้นพื้นฐาน	มีนโยบายกลางด้านการกำกับดูแลข้อมูล เช่น นโยบายการเก็บรักษาข้อมูล นโยบายการแบ่งปันข้อมูล ฯลฯ	☐
DAT-09 RE1	ขั้นสูง	บูรณาการการบังคับใช้นโยบายวงจรชีวิตของข้อมูลทั่วทั้งองค์กร ส่งผลให้สามารถกำหนดนโยบายการกำกับดูแลข้อมูลได้อย่างเป็นหนึ่งเดียวกัน	☐

ส่วนที่ ๖ ความสามารถเชิงบูรณาการ (Cross-Cutting Capabilities)

ตารางที่ ๓๐ แสดงรายการตรวจสอบของความสามารถเชิงบูรณาการ

รหัส	ระดับรายการตรวจสอบ	รายการตรวจสอบ	สถานะ
CCC-01	ขั้นพื้นฐาน	ดำเนินการรวบรวมและวิเคราะห์บันทึกเหตุการณ์ และเหตุการณ์ต่าง ๆ โดยอัตโนมัติสำหรับฟังก์ชันที่สำคัญต่อภารกิจขององค์กร	☐
CCC-01 RE1	ขั้นสูง	ขยายการรวบรวมบันทึกเหตุการณ์โดยอัตโนมัติให้ครอบคลุมสภาพแวดล้อมทั่วทั้งองค์กร เพื่อการวิเคราะห์แบบรวมศูนย์ที่เชื่อมโยงข้อมูลกันระหว่างหลายแหล่งที่มา เช่น คลาวด์ อุปกรณ์ปลายทางฯลฯ	☐
CCC-02	ขั้นพื้นฐาน	ดำเนินการแบบอัตโนมัติกับการประสานงานและการตอบสนองต่อภัยคุกคาม เพื่อสนับสนุนภารกิจที่สำคัญ	☐
CCC-02 RE1	ขั้นสูง	ดำเนินการประสานงานและตอบสนองกิจกรรมต่าง ๆ ทั่วทั้งองค์กรโดยอัตโนมัติ โดยใช้ประโยชน์จากข้อมูลเชิงบริบทจากหลายแหล่งในการประกอบการตัดสินใจ	☐
CCC-03	ขั้นพื้นฐาน	กำหนดและเริ่มดำเนินการนโยบายสำหรับการบังคับใช้การกำกับดูแลทั่วทั้งองค์กร	☐
CCC-03 RE1	ขั้นสูง	กำหนดและบังคับใช้นโยบายแบบแบ่งระดับและปรับให้เหมาะสมตามบริบทและความเสี่ยงทั่วทั้งองค์กร พร้อมทั้งนำระบบอัตโนมัติมาใช้เพื่อสนับสนุนการบังคับใช้นโยบายเท่าที่สามารถดำเนินการได้ การพิจารณานโยบายด้านการเข้าถึงระบบจะอาศัยข้อมูลเชิงบริบทจากหลายแหล่งมาประกอบ การตัดสินใจ	☐

ผนวก ข แนวทางในการกำหนดขอบเขตของงานขั้นต่ำของระบบรักษาความมั่นคงปลอดภัยแบบ Zero Trust

การกำหนดข้อกำหนดในขอบเขตของงาน (Terms of Reference: TOR) ควรครอบคลุมข้อกำหนดอย่างน้อยดังตัวอย่างที่นำเสนอในหัวข้อนี้ ทั้งนี้แต่ละองค์กรสามารถปรับลด หรือเพิ่มเติมข้อกำหนดตามความเสี่ยงขององค์กร โดยสามารถเลือกข้อกำหนดที่เหมาะสมเพิ่มเติมได้จาก หัวข้อ ๖.๑ และ ๖.๓ ของภาคผนวก

ตารางที่ ๓๑ แสดงแนวทางในการกำหนดขอบเขตของงานขั้นต่ำของระบบรักษาความมั่นคงปลอดภัยแบบ Zero Trust

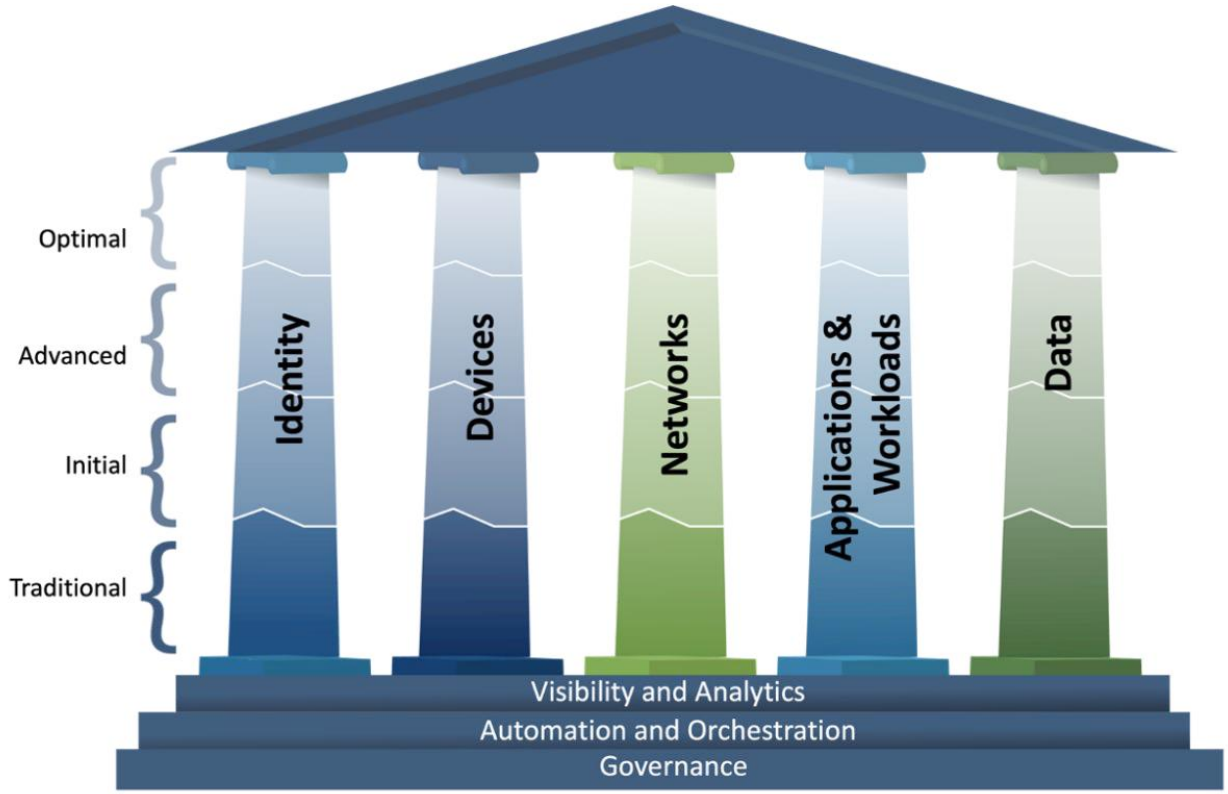
ข้อกำหนดที่	รหัสอ้างอิง
๑. คุณสมบัติการยืนยันตัวตน (Identity) มีคุณสมบัติดังนี้	
๑.๑ สามารถทำงานร่วมกับระบบยืนยันตัวตนแบบรวมศูนย์ขององค์กร เพื่อกำหนดสิทธิและการจัดการสิทธิที่แตกต่างกันในระดับบัญชีผู้ใช้และกลุ่มบัญชีผู้ใช้ หรือเสนอระบบยืนยันตัวตนแบบรวมศูนย์เพิ่มในโครงการได้	IDT-02 RE1 IDT-06 RE1
๑.๒ สามารถกำหนดนโยบายการตั้งรหัสผ่านแบบซับซ้อน พร้อมคุณสมบัติยืนยันตัวตนแบบหลายปัจจัยร่วมกับรหัสผ่าน และสามารถเลือกแบบไม่ใช้รหัสผ่าน (Passwordless) ได้	IDT-01 IDT-07 IDT-01 RE1
๑.๓ มีคุณสมบัติการกำหนดนโยบายในระดับองค์กร โดยสามารถเลือกกำหนดนโยบายยืนยันตัวตน วิธีการยืนยันตัวตนแบบหลายปัจจัย และนโยบายการตั้งรหัสผ่านที่แตกต่างกันแบ่งตามบัญชีผู้ใช้ และกลุ่มบัญชีผู้ใช้ได้	IDT-07
๑.๔ มีคุณสมบัติทำหน้าที่เป็นศูนย์กลางระบบบริหารจัดการบัญชีผู้ใช้ และคุณสมบัติยืนยันตัวตนแบบหลายปัจจัย พร้อมรองรับการทำงานร่วมกับระบบอื่น ๆ ผ่าน โปรโตคอลมาตรฐาน เช่น SAML (IdP/SP) RADIUS (Client/Server) LDAP (Client/Server) OAuth ฯลฯ	IDT-06 IDT-06 RE2
๑.๕ มีระบบรวบรวมบันทึกเหตุการณ์ พร้อมแสดงรายงานการใช้งานที่แสดงข้อมูลการยืนยันตัวตน การตรวจสอบอุปกรณ์ และการเข้าถึงเครือข่ายตามแบบ Zero Trust ได้แบบรวมศูนย์ พร้อมคุณสมบัติการแสดงรายงานเชิงวิเคราะห์ความสัมพันธ์ได้แบบอัตโนมัติ	IDT-05 IDT-05 RE1 NWS-04 NWS-04 RE1
๒. คุณสมบัติการตรวจสอบอุปกรณ์ (Devices) มีคุณสมบัติดังนี้	
๒.๑ มีคุณสมบัติตรวจสอบสถานะของอุปกรณ์ (Posture Check) ก่อนเข้าถึงเครือข่ายและระหว่างใช้งานเครือข่ายแบบรวมศูนย์ เช่น สถานะช่องโหว่ ใบรับรองดิจิทัล ระบบปฏิบัติการ ฯลฯ	DVS-01 RE1 DVS-02 RE1 DVS-03 DVS-05
๒.๒ สามารถกำหนดนโยบายการเข้าถึงเครือข่ายแบ่งตามความเสี่ยงของอุปกรณ์และตามข้อมูลที่ตรวจพบได้ โดยทำงานร่วมกับอุปกรณ์หรือระบบในระดับเกตเวย์ และเป็นการตรวจสอบระดับเซสชัน (Session) อย่างต่อเนื่องตามแนวทาง Zero Trust ครอบคลุมการใช้งานจากสาขา (ถ้ามี) ใช้งานจากภายใน และใช้งานจากภายนอกองค์กร	IDT-03 RE1 DVS-03 RE1 DVS-06 NWS-03

ข้อกำหนดที่	รหัสอ้างอิง
	NWS-05 NWS-06
๒.๓ มีการติดตั้งระบบที่สามารถอัปเดตซอฟต์แวร์ได้อัตโนมัติ และมีการบริหารจัดการแบบรวมศูนย์ รวมถึงสามารถเชื่อมโยงการทำงานร่วมกับคุณสมบัติตรวจสอบสถานะของอุปกรณ์ (Posture check) ขององค์กรได้	DVS-04 DVS-04 RE1 DVS-01 RE1
๒.๔ มีคุณสมบัติในการตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยที่เกี่ยวข้องกับการยืนยันตัวตน การตรวจสอบสถานะของอุปกรณ์ และการเข้าถึงเครือข่ายแบบ Zero Trust ได้แบบอัตโนมัติ เช่น ตรวจพบเหตุการณ์ที่มีอุปกรณ์เข้าถึงเครือข่ายและพบว่ามีช่องโหว่รุนแรงภายในอุปกรณ์ สามารถกักกันอุปกรณ์ออกจากเครือข่ายปกติได้แบบอัตโนมัติ รวมถึงสามารถทำงานร่วมกับระบบที่เสนอในโครงการหรือระบบที่ใช้อยู่ในปัจจุบันได้ โดยเขียนกำหนดเป็นสคริปต์หรือขั้นตอนการทำงาน (Playbook) ได้	IDT-06 RE1 DVS-06 DVS-06 RE1 NWS-05 RE2
๓. คุณสมบัติการตรวจสอบเครือข่าย (Networks) มีคุณสมบัติดังนี้	
๓.๑ ระบบที่เสนอมีคุณสมบัติแบ่งเครือข่ายออกเป็นส่วนย่อย (Zone Based) และสามารถกำหนดนโยบายการเข้าถึงเครือข่ายย่อยตามความเสี่ยงของอุปกรณ์และตามข้อมูลที่ตรวจพบได้ สามารถตรวจสอบระดับเซสชัน (Session) อย่างต่อเนื่องตามแนวทาง Zero Trust	DVS-01 RE1 DVS-03 RE1 NWS-01 NWS-03 NWS-03 RE1 IDT-04 RE1
๓.๒ กรณีที่มีการเข้าถึงจากผู้ใช้ที่อยู่ภายนอกหรือมีการเชื่อมต่อกันระหว่างไซต์ ต้องมีการเข้ารหัสแบบ TLS 1.2 หรือดีกว่า และต้องมีแนวทางเพื่อรองรับการเชื่อมต่อกรณีที่เครื่องของผู้ใช้ปลายทางไม่ใช้เอเจนต์ได้ (Agentless)	NWS-02 NWS-02 RE1
๓.๓ มีคุณสมบัติตรวจจับ (IDS) และป้องกันการโจมตีในระดับเครือข่าย (IPS) โดยรองรับการอัปเดตฐานข้อมูลลักษณะเฉพาะของภัยคุกคามได้ตลอดระยะเวลารับประกัน พร้อมรองรับการนำเข้าทราฟฟิคของเครือข่ายผ่านการ SPAN/Mirror เพื่อตรวจสอบบางส่วนของเครือข่ายเพิ่มเติมได้	NWS-05 NWS-05 RE1
๓.๔ กรณีที่มีอุปกรณ์หรือจุดบังคับใช้นโยบายในระดับเกตเวย์หลายส่วน ต้องมีระบบบริหารจัดการจากศูนย์กลาง เพื่อทำหน้าที่กำหนดนโยบายการเข้าถึงเครือข่าย และ	NWS-07 NWS-07 RE1

ข้อกำหนดที่	รหัสอ้างอิง
สามารถบันทึกตรวจสอบและเปรียบเทียบความแตกต่างของนโยบายในแต่ละเวอร์ชันที่มีการเปลี่ยนแปลงได้	
๓.๕ มีคุณสมบัติซิงโครไนซ์ข้อมูล (Synchronize) ที่ได้จากการตรวจสอบสถานะของอุปกรณ์ เพื่อทำงานร่วมกับจุดบังคับใช้นโยบาย (Policy Enforcement Point) ในการป้องกันสินทรัพย์ดิจิทัลที่สำคัญขององค์กร เช่น บริการ และแอปพลิเคชัน ฯลฯ ได้แบบสอดคล้องกันทุกสภาพแวดล้อมที่มีทรัพยากรขององค์กรอยู่ เช่น ในระบบคลาวด์ และศูนย์ข้อมูลกลาง ฯลฯ	NWS-04 RE2
๔. คุณสมบัติการตรวจสอบแอปพลิเคชันและเวิร์กโหลด (Applications and Workloads) มีคุณสมบัติดังนี้	
๔.๑ มีคุณสมบัติตรวจสอบการเข้าถึงแอปพลิเคชันตามแนวทาง Zero Trust โดยสามารถตรวจสอบการเข้าถึงแอปพลิเคชัน ทั้งจากผู้ใช้ที่อยู่ภายนอกและผู้ใช้ที่อยู่ภายในองค์กรได้ และสามารถกำหนดนโยบายการเข้าถึงแอปพลิเคชันตามความเสี่ยงของอุปกรณ์ รวมถึงเป็นการตรวจสอบระดับเซสชัน (Session) เพื่อรับสิทธิเฉพาะตามความจำเป็นในการใช้งานเท่านั้น	APW-01 RE1 APW-03 RE1 DVS-03 RE1
๔.๒ มีคุณสมบัติป้องกันภัยคุกคามขั้นสูง โดยสามารถป้องกันไวรัส (Antivirus) ตรวจจับ (IDS) และป้องกันการโจมตีในระดับเครือข่าย (IPS) สำหรับการเข้าถึงแอปพลิเคชันได้ โดยรองรับการอัปเดตฐานข้อมูลลักษณะเฉพาะของภัยคุกคามได้ตลอดระยะเวลารับประกัน	APW-02 APW-02 RE1
๔.๓ กรณีมีแอปพลิเคชันหลายส่วน ต้องมีระบบบริหารจัดการจากศูนย์กลางสำหรับจุดบังคับใช้นโยบาย (Policy Enforcement Point) เพื่อทำหน้าที่กำหนดนโยบายการเข้าถึงแอปพลิเคชัน และรวบรวมบันทึกเหตุการณ์การเข้าถึงแอปพลิเคชันได้	APW-03 RE1 APW-06
๕. คุณสมบัติการรักษาความมั่นคงปลอดภัยของข้อมูล (Data) มีคุณสมบัติดังนี้	
๕.๑ มีคุณสมบัติตรวจสอบการเข้าถึงข้อมูล โดยสามารถกำหนดนโยบายควบคุมการเข้าถึงข้อมูลตามคุณลักษณะต่าง ๆ เช่น ตัวตน และความเสี่ยงของอุปกรณ์ รวมถึงมีระยะเวลาจำกัดในการเข้าถึง เพื่อรับสิทธิเฉพาะตามความจำเป็นในการใช้งานเท่านั้น	DAT-02 RE1 DVS-03 RE1 IDT-01
๕.๒ มีคุณสมบัติป้องกันการสูญหายของข้อมูล (Data Loss Prevention: DLP) ในระดับเกตเวย์หรือเครือข่ายเป็นอย่างน้อย เพื่อตรวจจับและป้องกันข้อมูลรั่วไหล และรองรับการทำงานร่วมกับระบบติดป้ายกำกับข้อมูล (Label) ได้	DAT-01 RE1 DAT-03 RE1 DAT-04

ข้อกำหนดที่	รหัสอ้างอิง
๕.๓ ระบบต้องรองรับการจัดเก็บข้อมูลสำรองที่มีความคงสภาพ (Data Immutability) และความซ้ำซ้อนตามมาตรฐานสากล เพื่อป้องกันมัลแวร์เรียกค่าไถ่ในการแก้ไขหรือทำลายข้อมูล และรับประกันความถูกต้องของข้อมูลสำรอง (Data Integrity)	DAT-03 DAT-07
๕.๔ ระบบต้องมีความสามารถในการตรวจจับมัลแวร์เรียกค่าไถ่ และสามารถประสานงานกับระบบเครือข่ายเพื่อจำกัดขอบเขตผลกระทบ หรือแยกส่วนข้อมูลสำคัญ (Isolation) โดยอัตโนมัติเมื่อตรวจพบพฤติกรรมที่ผิดปกติ	NWS-05 RE2 CCC-02
๕.๕ ระบบต้องมีกลไกตรวจสอบความสมบูรณ์ของข้อมูลสำรองแบบอัตโนมัติ และรองรับการทดสอบการกู้คืนระบบ (Recovery Testing) เพื่อยืนยันความพร้อมในการฟื้นฟูธุรกิจได้ตามเงื่อนไขที่กำหนด	DAT-05 RE1 DAT-07
๖. คุณสมบัติความสามารถเชิงบูรณาการ (Cross-Cutting Capabilities) มีคุณสมบัติดังนี้	
๖.๑ มีคุณสมบัติประสานงานระหว่างสภาพแวดล้อมที่ครอบคลุมทั่วทั้งองค์กร เช่น คลาวด์ อุปกรณ์ปลายทาง ระบบป้องกันภัยคุกคามทางเครือข่าย ระบบป้องกันการโจมตีเว็บไซต์ ฯลฯ เพื่อกำหนดนโยบายสำหรับบังคับใช้การกำกับดูแลแบบสองคล้องกันได้ทั่วทั้งองค์กร	CCC-02 RE1 CCC-03
๖.๒ มีคุณสมบัติกำหนดนโยบายแบบแบ่งระดับตามบริบทหรือความเสี่ยงที่เหมาะสมกับแต่ละสภาพแวดล้อมและบริบทขององค์กรได้	CCC-03 RE1
๖.๓ มีคุณสมบัติรวบรวมเหตุการณ์ที่เชื่อมโยงกันระหว่างหลายแหล่งที่มา เพื่อวิเคราะห์แบบรวมศูนย์ได้	CCC-01 RE1

ผนวก ค แนวทางปฏิบัติตาม Zero Trust Maturity Model Version 2.0 ของ Cybersecurity & Infrastructure Security Agency (CISA)



รูปที่ ๑๘ แสดงให้เห็นถึงแนวคิดพื้นฐานของ Zero Trust Maturity Model

แนวคิดพื้นฐานของ ZTMM

โมเดลนี้ได้รับอิทธิพลจากหลักการ ๗ ข้อของ NIST SP 800-207 ที่กล่าวถึงในหัวข้อ ๒.๓ หลักการพื้นฐานของ Zero Trust

๑. ภาพรวมของ ZTMM

ZTMM[๑] ของ CISA Version 2.0 นำเสนอแนวทางในการพัฒนา Zero Trust แบบค่อยเป็นค่อยไป เพื่อให้องค์กรสามารถวางแผน ยกระดับ และประเมินความพร้อมด้าน Zero Trust ได้อย่างเป็นระบบ โมเดลนี้ประกอบด้วย ๕ เสาหลัก (Pillars) ของสถาปัตยกรรม Zero Trust ได้แก่

๑) ตัวตน (Identity)

๒) อุปกรณ์ (Devices)

๓) เครือข่าย (Networks)

๔) แอปพลิเคชันและเวิร์กโหลด (Applications and Workloads)

๕) ข้อมูล (Data)

และประกอบด้วย ๔ ระดับความสมบูรณ์ (Maturity Stages) ซึ่งสะท้อนระดับความสามารถขององค์กร ตั้งแต่ระดับพื้นฐานจนถึงระดับอัตโนมัติ และสามารถนำไปปรับปรุงได้

๑) ดั้งเดิม (Traditional)

๒) เริ่มต้น (Initial)

๓) พัฒนาแล้ว (Advanced)

๔) ปรับปรุงให้เหมาะสม (Optimal)

๒. เสาหลักของ Zero Trust

ตัวตน (Identity)

ตัวตน หมายถึง คุณลักษณะหรือชุดของคุณลักษณะที่ใช้ระบุความเป็นเอกลักษณ์ ของผู้ใช้หรือเอนทิตีใด ๆ ภายในองค์กร โดยไม่ได้จำกัดเฉพาะบุคคลเท่านั้นแต่ยังครอบคลุมถึง เอนทิตีที่ไม่ใช่บุคคล เช่น บริการ ระบบอัตโนมัติ แอปพลิเคชัน บอท (Bot) เครื่องแม่ข่าย อุปกรณ์ IoT หรือระบบที่ทำงานแทนมนุษย์

เสาหลักด้านตัวตน มุ่งเน้นการยืนยันตัวตน และการได้รับสิทธิสำหรับทั้งผู้ใช้งานและเอนทิตีที่ไม่ใช่บุคคล (Non-Person Entities – NPEs) เช่น ระบบ บริการ แอปพลิเคชัน และเวิร์กโหลด

แนวคิดหลัก

๑) ทุกบุคคลและบริการที่ร้องขอการเข้าถึงทรัพยากรต้องได้รับการยืนยันตัวตน และได้รับสิทธิตามหลักการได้รับสิทธิเท่าที่จำเป็น

๒) ไม่มีสิทธิใด ๆ ที่ถือว่าได้รับโดยปริยายแม้จะอยู่ภายในเครือข่ายองค์กร

ขอบเขตของเสาหลักด้านตัวตน

๑) การจัดการตัวตน

๒) การยืนยันตัวตนแบบหลายปัจจัย

๓) การจัดการสิทธิของผู้ใช้และผู้มีสิทธิสูง

๔) การตรวจสอบสิทธิอย่างต่อเนื่อง

สาระสำคัญตาม ZTMM

๑) องค์กรควรใช้ การจัดการตัวตนแบบรวมศูนย์และเชื่อมโยงกัน (Federated Identity) เพื่อให้สามารถควบคุมและบังคับใช้นโยบายได้อย่างสม่ำเสมอ

๒) ในระดับความสมบูรณ์ที่สูงขึ้นบัญชีผู้ใช้และบัญชีบริการทั้งหมดควรใช้การยืนยันตัวตนแบบหลายปัจจัย ร่วมกับการวิเคราะห์พฤติกรรมเพื่อประเมินระดับความเสี่ยง

๓) ในระดับความสมบูรณ์สูงสุด ระบบสามารถปรับนโยบายการเข้าถึงโดยอัตโนมัติตามบริบท (Context-Aware Policy) เช่น ตัวตนผู้ใช้ อุปกรณ์ ตำแหน่งที่ตั้ง และพฤติกรรมการใช้งานแบบเรียลไทม์

อุปกรณ์ (Devices)

ในบริบทของ Zero Trust คำว่า “อุปกรณ์” หมายถึงทรัพย์สินทุกประเภทที่สามารถเชื่อมต่อกับเครือข่ายได้ ไม่ว่าจะเป็นฮาร์ดแวร์ ซอฟต์แวร์ หรือเฟิร์มแวร์ เช่น เครื่องแม่ข่าย เดสก์ท็อป และโน้ตบุ๊ก โทรศัพท์มือถือ และแท็บเล็ต เครื่องพิมพ์ เราเตอร์ และอุปกรณ์เครือข่าย อุปกรณ์ OT และ IoT ซึ่งอุปกรณ์เหล่านี้อาจเป็นทรัพย์สินของหน่วยงาน (Agency-owned Devices) หรืออุปกรณ์ส่วนตัวของพนักงาน (Bring Your Own Device: BYOD)

เสาหลักด้านอุปกรณ์ มุ่งเน้นการจัดการ ระบุตัวตน และประเมินสถานะและความสมบูรณ์ของอุปกรณ์ทั้งอุปกรณ์ทางกายภาพและอุปกรณ์เสมือน (Physical & Virtual Devices) ที่ใช้ในการเข้าถึงทรัพยากรขององค์กร

แนวคิดหลัก

๑) องค์กรต้องสามารถระบุและทราบอุปกรณ์ทั้งหมดที่เชื่อมต่อหรือร้องขอการเข้าถึงระบบ และให้เฉพาะอุปกรณ์ที่ผ่านการตรวจสอบและเชื่อถือได้เท่านั้น ที่สามารถเข้าถึงทรัพยากร

๒) Zero Trust ต้องอาศัยข้อมูลสถานะของอุปกรณ์ เช่น ระดับแพตช์ ระบบป้องกันมัลแวร์ การเข้ารหัสดิสก์ การตั้งค่าความมั่นคงปลอดภัย ฯลฯ

ขอบเขตของเสาหลักด้านอุปกรณ์

๑) การค้นหาและจัดทำบัญชีอุปกรณ์

๒) การบังคับใช้นโยบายด้านความมั่นคงปลอดภัยและการปฏิบัติตามข้อกำหนด

๓) การยืนยันตัวตนอุปกรณ์

สาระสำคัญตาม ZTMM

๑) ในระดับความสมบูรณ์ที่สูงขึ้น อุปกรณ์ทุกเครื่องต้องได้รับการตรวจสอบสุขภาพและสถานะความมั่นคงปลอดภัยแบบเรียลไทม์ (Real-time Device Health Validation)

๒) ในระดับความสมบูรณ์สูงสุด ระบบสามารถบังคับใช้ ปรับเปลี่ยน หรือเพิกถอนสิทธิการเชื่อมต่อโดยอัตโนมัติ เมื่อพบว่าอุปกรณ์มีความเสี่ยงหรือไม่เป็นไปตามนโยบาย

เครือข่าย (Networks)

เสาหลักด้านเครือข่าย มุ่งเน้นการออกแบบเครือข่ายที่ควบคุมการเข้าถึงในระดับย่อยและลดการพึ่งพาการป้องกันแบบอิงขอบเขตเครือข่ายแบบดั้งเดิมไปสู่การควบคุมแบบ Zero Trust

แนวคิดหลัก

๑) Zero Trust ไม่ยอมรับแนวคิด “เครือข่ายภายในที่เชื่อถือได้โดยอัตโนมัติ” (No trusted internal network)

๒) ทุกการเชื่อมต่อในเครือข่ายต้องได้รับการตรวจสอบ ยืนยันตัวตน และเข้ารหัสการสื่อสาร

ขอบเขตของเสาหลักด้านเครือข่าย

๑) การแบ่งส่วนเครือข่าย

๒) การเข้ารหัสข้อมูลระหว่างการสื่อสาร

๓) การควบคุมการเข้าถึงเครือข่ายตามแนวคิด Zero Trust

สาระสำคัญตาม ZTMM

๑) ในระดับเริ่มต้น องค์กรอาจยังพึ่งพาระบบเครือข่ายส่วนตัวเสมือนและการเข้ารหัสด้วย TLS เป็นหลัก

๒) ในระดับพัฒนาแล้ว จะเริ่มใช้ ZTNA ที่อ้างอิงตัวตนและบังคับใช้การเข้ารหัสการสื่อสารอย่างครอบคลุมทั่วทั้งระบบ

๓) ในระดับปรับปรุงให้เหมาะสมจะใช้ การควบคุมเส้นทางและการเข้าถึงเครือข่ายสามารถปรับเปลี่ยนตามบริบทแบบเรียลไทม์ โดยอิงจากตัวตน อุปกรณ์ สถานะความเสี่ยง และพฤติกรรมการใช้งาน

แอปพลิเคชันและเวิร์กโหลด (Applications and Workloads)

เสาหลักด้านแอปพลิเคชันและเวิร์กโหลด มุ่งเน้นการนำแนวคิด Zero Trust ไปประยุกต์ใช้กับแอปพลิเคชันแบบ SaaS รวมถึงเวิร์กโหลด โดยไม่ขึ้นกับสถานที่ติดตั้ง ไม่ว่าจะเป็น สภาพแวดล้อมแบบภายในองค์กร แบบระบบคลาวด์ หรือแบบไฮบริด

แนวคิดหลัก

๑) แอปพลิเคชันและเวิร์กโหลดทุกประเภทต้องได้รับการปกป้องตามหลัก Zero Trust โดยไม่ถือว่าสภาพแวดล้อมหรือเครือข่ายใดมีความน่าเชื่อถือโดยอัตโนมัติ

๒) การควบคุมความมั่นคงปลอดภัยต้องอ้างอิงตัวตน บริบท และนโยบาย มากกว่าการพึ่งพาการป้องกันในระดับเครือข่าย

๓) แอปพลิเคชันและเวิร์กโหลดไม่ว่าจะอยู่ในสภาพแวดล้อมแบบติดตั้งภายในองค์กร อุปกรณ์เคลื่อนที่ หรือคลาวด์ล้วนต้องได้รับการตรวจสอบ ควบคุม และบังคับใช้นโยบายตามหลัก Zero Trust

๔) แอปพลิเคชันทุกตัวต้องถูกมองว่า “อย่าเชื่อถือโดยปริยาย (Never Trust by Default)” และต้องได้รับการป้องกันในระดับแอปพลิเคชันอย่างแน่นหนาจากระบบอื่น

๕) การอนุญาตการเข้าถึงต้องอิงตามบริบท เช่น ตัวตนของผู้ใช้ สถานะของอุปกรณ์ ระดับความเสี่ยง และรูปแบบการใช้งาน ฯลฯ

๖) กระบวนการพัฒนาผ่าน CI/CD Pipeline ต้องฝังมาตรการด้านความมั่นคงปลอดภัยในทุกขั้นตอน พร้อมการทดสอบและการผสานกลไกป้องกันภัยคุกคามเข้ากับกระบวนการพัฒนาอย่างเป็นระบบ

ขอบเขตของเสาหลักด้านแอปพลิเคชันและเวิร์กโหลด

๑) การรักษาความมั่นคงปลอดภัยของแอปพลิเคชันตลอดวงจรชีวิต

๒) การจัดการและการยืนยันตัวตนของเวิร์กโหลด

๓) การรักษาความมั่นคงปลอดภัยของการเชื่อมต่อและบริการผ่าน API

สาระสำคัญตาม ZTMM

๑) ในระดับความสมบูรณ์ที่สูงขึ้น องค์กรจะเริ่มใช้นโยบายความมั่นคงปลอดภัยในรูปแบบโค้ด (Policy-as-Code) เพื่อให้สามารถบังคับใช้นโยบายได้อย่างสม่ำเสมอและอัตโนมัติ

๒) ในระดับความสมบูรณ์สูงสุด ระบบสามารถตรวจสอบและบังคับใช้นโยบายความมั่นคงปลอดภัยในขณะทำงานจริง (Runtime Enforcement) และควบคุมการสื่อสารกับเวิร์กโหลด และระหว่างเวิร์กโหลดได้โดยตรง โดยไม่ต้องพึ่งพาความเชื่อถือในระดับเครือข่าย

ข้อมูล (Data)

เสาหลักด้านข้อมูลมุ่งเน้นการปกป้องข้อมูลตลอดวงจรชีวิต การสร้าง การจัดเก็บ การใช้งาน การแบ่งปัน ไปจนถึงการทำลาย โดยอาศัยการระบุรายการข้อมูล การจัดหมวดหมู่ข้อมูล การเข้ารหัสข้อมูล และการควบคุมการเข้าถึง

แนวคิดหลัก

๑) ข้อมูลต้องได้รับการปกป้องอย่างเหมาะสมตลอดทุกช่วงของวงจรชีวิต ครอบคลุมวงจรชีวิตของข้อมูลอย่างครบถ้วน ตั้งแต่การสร้าง การจัดเก็บ การใช้งาน การแบ่งปัน และ การทำลาย และในทุกสถานะ ได้แก่ ขณะจัดเก็บ (At Rest) ระหว่างส่ง (In Transit) และขณะใช้งาน (In Use)

๒) องค์กรต้องมีการจัดหมวดหมู่ข้อมูลและการติดป้ายกำกับข้อมูล (Labeling) อย่างเป็นระบบ เพื่อให้สามารถบังคับใช้นโยบายได้อย่างอัตโนมัติ

๓) แนวคิด Zero Trust กำหนดให้การเข้าถึงข้อมูลต้องถูกควบคุมโดยอิงบริบท เช่น ตัวตนของผู้ใช้ สถานะของอุปกรณ์ แอปพลิเคชัน ประเภทข้อมูล และระดับความเสี่ยง ณ ขณะนั้น

๔) องค์กรควรเข้ารหัสข้อมูลโดยเฉพาะข้อมูลที่สำคัญ และตรวจสอบการเข้าถึงอย่างต่อเนื่อง เพื่อป้องกันการเข้าถึงหรือการรั่วไหลที่ไม่ได้รับอนุญาต

๕) การเข้าถึงข้อมูลต้องยึดหลักให้สิทธิเท่าที่จำเป็น และมีการตรวจสอบและประเมินอย่างต่อเนื่อง

ขอบเขตของเสาหลักด้านข้อมูล

๑) การค้นหา ระบุ และจัดประเภทข้อมูล

๒) การป้องกันข้อมูลทั้งขณะจัดเก็บ ขณะมีการใช้งาน และขณะเคลื่อนที่

๓) การกำกับดูแลและควบคุมการเข้าถึงข้อมูล

สาระสำคัญตาม ZTMM

๑) ในระดับความสมบูรณ์ที่สูงขึ้น องค์กรสามารถใช้ระบบอัตโนมัติในการจำแนกข้อมูลและบังคับใช้นโยบายการเข้าถึงแบบปรับตามบริบท

๒) ในระดับความสมบูรณ์สูงสุด ระบบสามารถเข้ารหัสหรือจำกัดการเข้าถึงข้อมูลที่มีความอ่อนไหวโดยอัตโนมัติ เช่น เมื่อมีการส่งข้อมูลออกนอกขอบเขตที่ได้รับอนุญาต หรือเมื่อระดับความเสี่ยงเปลี่ยนแปลง

สรุปแนวทางจาก CISA

๑) Zero Trust ไม่ใช่จุดหมายปลายทาง แต่เป็นกระบวนการพัฒนาอย่างต่อเนื่อง องค์กรต้องปรับปรุงและยกระดับแนวทางด้าน Zero Trust อยู่ตลอดเวลา เพื่อให้สอดคล้องกับภัยคุกคามและบริบทที่เปลี่ยนแปลงไป

๒) องค์กรควรประเมินระดับความสมบูรณ์ของแต่ละเสาหลัก จากนั้นกำหนดแผนการพัฒนาและยกระดับความสามารถแบบเป็นลำดับขั้น โดยไม่จำเป็นต้องยกระดับทุกเสาพร้อมกัน

๓) การบูรณาการ Zero Trust อย่างมีประสิทธิภาพต้องอาศัยมากกว่าเทคโนโลยี แต่ต้องผสานนโยบาย เทคโนโลยี และวัฒนธรรมองค์กร เพื่อให้ Zero Trust ถูกนำไปใช้งานได้จริงและยั่งยืน

๓. ระดับความสมบูรณ์

การเปลี่ยนผ่านสู่ Zero Trust เป็นกระบวนการพัฒนาแบบเป็นลำดับขั้น โดยองค์กรจะค่อย ๆ พัฒนาจากระดับ**ดั้งเดิม**ไปสู่**เริ่มต้น พัฒนาแล้ว** และ**ปรับปรุงให้เหมาะสม**

ตารางที่ ๓๒ แสดงระดับความสมบูรณ์

ระดับความสมบูรณ์	ลักษณะสำคัญ
ดั้งเดิม	การตั้งค่าทั้งหมดแบบแมนวล ระบบแยกกัน ไม่มีการบูรณาการระหว่างเสา ใช้หลักการได้รับสิทธิเท่าที่จำเป็น ตั้งแต่การกำหนดสิทธิเริ่มต้น ไม่มีการตอบสนองแบบอัตโนมัติ
เริ่มต้น	เริ่มนำระบบอัตโนมัติมาใช้ในงานบางส่วน มีการเชื่อมโยงบางส่วนระหว่างเสาหลัก มีการรวบรวมบันทึกเหตุการณ์ และเริ่มมองเห็นภาพรวมของระบบ
พัฒนาแล้ว	ระบบส่วนใหญ่เริ่มบูรณาการร่วมกัน สามารถประเมินความเสี่ยง และปรับเปลี่ยนสิทธิการเข้าถึงแบบอัตโนมัติ มีการมองเห็นจากศูนย์กลาง และการตอบสนองตามนโยบาย
ปรับปรุงให้เหมาะสม	ระบบทำงานอัตโนมัติเต็มรูปแบบ การให้สิทธิเข้าถึงเฉพาะช่วงเวลาที่จำเป็นและการให้สิทธิเท่าที่จำเป็นต่อการปฏิบัติงาน สามารถตรวจจับ ปรับเปลี่ยน และเพิกถอนสิทธิแบบเรียลไทม์ มีการเชื่อมโยงข้อมูลข้ามทุกเสาหลักและมีการมองเห็นแบบครบวงจรทั่วทั้งองค์กร

กล่าวโดยสรุป ZTMM ช่วยให้องค์กรค่อย ๆ พัฒนาไปสู่ Zero Trust แบบเต็มรูปแบบได้อย่างเป็นขั้นเป็นตอน โดยไม่จำเป็นต้องยกระดับทุกเสาหลักพร้อมกัน แต่สามารถพัฒนาแต่ละเสาให้ก้าวหน้า ตามบริบทความพร้อม และลำดับความสำคัญขององค์กร

การประเมินและการพัฒนา

ก่อนเริ่มลงทุนหรือขยายการใช้งานเทคโนโลยี Zero Trust องค์กรควรดำเนินการดังต่อไปนี้

๑) ประเมินสถานะปัจจุบัน โดยครอบคลุมระบบ บุคลากร โครงสร้างพื้นฐาน และกระบวนการทำงานที่มีอยู่

๒) ระบุความสามารถที่มีอยู่แล้ว เพื่อใช้เป็นฐานในการต่อยอดสู่ Zero Trust

๓) วิเคราะห์และระบุช่องว่างที่ต้องได้รับการพัฒนาเพิ่มเติมในแต่ละเสาหลัก

๔) วางแผนการพัฒนาแบบบูรณาการเพื่อให้เสาหลักต่าง ๆ ทำงานประสานกัน และสามารถบังคับใช้การควบคุมสิทธิตามหลักการได้รับสิทธิเท่าที่จำเป็น เพื่อลดความเสี่ยงโดยรวมขององค์กร ทั้งนี้รายละเอียดของแนวทางดังกล่าวแสดงไว้ในตารางที่ ๓๓

ตารางที่ ๓๓ แสดงแนวทางปฏิบัติสำหรับ ๕ เสาหลัก

ระดับ	ตัวตน	อุปกรณ์	เครือข่าย	แอปพลิเคชันและเวิร์กโหลด	ข้อมูล
ดั้งเดิม	• ใช้รหัสผ่านหรือการยืนยันตัวตนแบบหลายปัจจัย • เก็บข้อมูลตัวตนภายในองค์กร • ประเมินความเสี่ยงตัวตนผู้ใช้แบบจำกัด • สิทธิเข้าถึงแบบถาวรพร้อมการทบทวนเป็นรอบ	• ติดตามบัญชีอุปกรณ์แบบแมนวล • การมองเห็นการปฏิบัติตามข้อกำหนดจำกัด • ไม่มีการกำหนดเกณฑ์ของอุปกรณ์ที่เข้าถึงทรัพยากร • ใช้การป้องกันภัยคุกคามในบางอุปกรณ์แบบแมนวล	• การแบ่งส่วนเครือข่ายขนาดใหญ่ • ความยืดหยุ่นจำกัด จัดการชุดกฎเกณฑ์ และการตั้งค่าแบบแมนวล • เข้ารหัสการรับส่งข้อมูลน้อยและจัดการกุญแจการเข้ารหัสแบบเฉพาะกิจ	• แอปพลิเคชันสำคัญเข้าถึงผ่านเครือข่ายส่วนตัว • การป้องกันมีการบูรณาการน้อยมาก • แยกสภาพแวดล้อมการพัฒนาทดสอบ และใช้งานจริงแบบเฉพาะกิจ	• ทำบัญชีและจัดหมวดหมู่ข้อมูลแบบแมนวล • การควบคุมการเข้าถึงแบบสแตติก • เข้ารหัสข้อมูลน้อยมากและจัดการกุญแจการเข้ารหัสแบบเฉพาะกิจ
เริ่มต้น	• การยืนยันตัวตนแบบหลายปัจจัยด้วยรหัสผ่าน • แหล่งเก็บข้อมูลตัวตนที่ผู้ใช้สามารถจัดการเองได้ • ประเมินความเสี่ยงตัวตนผู้ใช้แบบแมนวล • สิทธิการเข้าถึงหมดอายุด้วยการทบทวนแบบอัตโนมัติ	• เริ่มมีการติดตามสินทรัพย์ทางกายภาพทั้งหมด • บังคับใช้การปฏิบัติตามข้อกำหนดและการควบคุมอุปกรณ์ในวงจำกัด • การป้องกันบางส่วนสามารถผ่านระบบอัตโนมัติ	• เริ่มแยกส่วนเวิร์กโหลดที่สำคัญ • จัดการความต้องการในด้านพร้อมใช้งานของเครือข่ายให้กับแอปพลิเคชันมากขึ้น • การตั้งค่าแบบไดนามิกในบางส่วนของเครือข่าย	• มีลำดับการทำงานที่สำคัญบางส่วนซึ่งมีการบูรณาการระบบป้องกันความมั่นคงปลอดภัย และสามารถเข้าถึงได้ผ่านเครือข่ายสาธารณะจากผู้ใช้งานที่ได้รับสิทธิ • สามารถนำขึ้นใช้งานด้วยโค้ด	• มีระบบอัตโนมัติที่ยังมีข้อจำกัดในการทำบัญชีและควบคุมการเข้าถึง • เริ่มใช้กลยุทธ์การจัดหมวดหมู่ข้อมูล • เข้ารหัสข้อมูลระหว่างส่ง • เริ่มมีนโยบายจัดการกุญแจการเข้ารหัสแบบรวมศูนย์

ระดับ	ตัวตน	อุปกรณ์	เครือข่าย	แอปพลิเคชันและเวิร์กโหลด	ข้อมูล
			• เข้ารหัสข้อมูลมากขึ้น และกำหนดนโยบายจัดการกุญแจการเข้ารหัสที่เป็นทางการ	ผ่านกระบวนการ CI/CD • มีการทดสอบความมั่นคงปลอดภัยทั้งแบบสแตติกและไดนามิกก่อนนำขึ้นใช้งาน	
พัฒนาแล้ว	• การยืนยันตัวตนแบบหลายปัจจัยที่สามารถต้านทานฟิชชิง • การรวม และบูรณาการแหล่งเก็บข้อมูลตัวตนอย่างมั่นคงปลอดภัย • ประเมินความเสี่ยงตัวตนผู้ใช้แบบอัตโนมัติ • ควบคุมการเข้าถึงตามความจำเป็นหรือตามเซสชัน	• สามารถติดตามสินทรัพย์ส่วนใหญ่ • บังคับใช้การปฏิบัติตามข้อกำหนดพร้อมการป้องกันภัยคุกคามแบบบูรณาการ • การเข้าถึงทรัพยากรเบื้องต้นขึ้นอยู่กับสถานะของอุปกรณ์	• การเพิ่มขยายกลไกการแยกส่วนเครือข่ายและความสามารถในการฟื้นคืนสภาพ • การตั้งค่าสามารถปรับตามการประเมินโปรไฟล์แอปพลิเคชันที่ตระหนักถึงความเสี่ยงอัตโนมัติ • เข้ารหัสการรับส่งข้อมูลที่เกี่ยวข้องและจัดการกุญแจการเข้ารหัส	• แอปพลิเคชันสำคัญส่วนใหญ่สามารถเข้าถึงได้ผ่านเครือข่ายสาธารณะจากผู้ใช้งานที่ได้รับสิทธิ • บูรณาการระบบป้องกันกับทุกแอปพลิเคชันพร้อมการควบคุมการเข้าถึงโดยพิจารณาตามบริบท • ทีมพัฒนา ทีมความมั่นคงปลอดภัย และทีมปฏิบัติการทำงานประสานกัน	• สามารถทำบัญชีข้อมูลแบบอัตโนมัติพร้อมการติดตาม • การจัดหมวดหมู่และติดป้ายกำกับมีความสม่ำเสมอเป็นระดับ และตรงจุด • มีระบบจัดเก็บข้อมูลที่มีความพร้อมใช้งานสูงและมีระบบสำรองข้อมูล • มี DLP แบบสแตติก • การควบคุมการเข้าถึงตามบริบทแบบอัตโนมัติ • เข้ารหัสข้อมูลขณะจัดเก็บ

ระดับ	ตัวตน	อุปกรณ์	เครือข่าย	แอปพลิเคชันและเวิร์กโหลด	ข้อมูล
ปรับปรุงให้เหมาะสม	• การตรวจสอบความถูกต้องและวิเคราะห์ความเสี่ยงอย่างต่อเนื่อง • การบูรณาการระบบยืนยันตัวตนทั่วทั้งองค์กร • การเข้าถึงแบบอัตโนมัติที่ปรับแต่งตามความจำเป็น	• การวิเคราะห์สินทรัพย์ทางกายภาพและเสมือนอย่างต่อเนื่อง รวมถึงการจัดการความเสี่ยงของห่วงโซ่อุปทานแบบอัตโนมัติและการป้องกันภัยคุกคามแบบบูรณาการ • การเข้าถึงทรัพยากรขึ้นอยู่กับการวิเคราะห์ความเสี่ยงของอุปกรณ์แบบเรียลไทม์	• การกำหนดขอบเขตเครือข่ายย่อยแบบกระจายพร้อมการควบคุมการเข้าถึงแบบอนุญาตเมื่อต้องการ และสิทธิเท่าที่จำเป็น • การตั้งค่าสามารถปรับเปลี่ยนตามโปรไฟล์ของแอปพลิเคชัน • บูรณาการแนวทางปฏิบัติที่ดีที่สุดเพื่อความยืดหยุ่นในการเข้ารหัส	• แอปพลิเคชันใช้งานผ่านเครือข่ายสาธารณะได้ด้วยการตรวจสอบสิทธิอย่างต่อเนื่อง • ป้องกันการโจมตีที่ซับซ้อนในทุกขั้นตอนการทำงาน • ใช้เวิร์กโหลดที่ไม่สามารถเปลี่ยนแปลงได้โดยมีการทดสอบความมั่นคงปลอดภัยแบบบูรณาการตลอดวงจรชีวิต	• มีการทำบัญชีข้อมูลอย่างต่อเนื่อง • จัดหมวดหมู่และติดป้ายกำกับข้อมูลแบบอัตโนมัติทั่วทั้งองค์กร • ปรับปรุงการพร้อมใช้ของข้อมูล • ป้องกันการนำข้อมูลออกด้วย DLP • การควบคุมการเข้าถึงแบบไดนามิก • เข้ารหัสข้อมูลขณะใช้งาน

ความสามารถเชิงบูรณาการ

ความสามารถเชิงบูรณาการเป็นปัจจัยสำคัญที่ต้องได้รับการพัฒนา ควบคู่ไปกับเสาหลักทั้ง ๕ เพื่อให้การเปลี่ยนผ่านไปสู่ Zero Trust ประสบความสำเร็จ และเกิดการบูรณาการในระดับองค์กร ความสามารถเหล่านี้ทำหน้าที่ สนับสนุน เชื่อมโยง และยกระดับการทำงานของทุกเสาหลัก ตั้งแต่ระดับการมองเห็น การตัดสินใจเชิงนโยบาย ไปจนถึงการตอบสนองด้านความมั่นคงปลอดภัยแบบอัตโนมัติ มีรายละเอียดดังแสดงในตารางที่ ๓๔ ดังต่อไปนี้

ตารางที่ ๓๔ แสดงความสามารถเชิงบูรณาการ

ความสามารถ	ลักษณะโดยย่อ	การพัฒนาสู่ระดับ ปรับปรุงให้เหมาะสม
การมองเห็นและการวิเคราะห์	การเก็บรวบรวม วิเคราะห์ และเชื่อมโยงข้อมูลที่สังเกตได้ (Observable Artifacts) การมุ่งเน้นที่การวิเคราะห์ข้อมูลที่เกี่ยวข้องกับไซเบอร์สามารถช่วยให้มีข้อมูลสนับสนุนการตัดสินใจด้านนโยบายและอำนวยความสะดวกในการตอบสนองต่อเหตุการณ์ และสร้างโปรไฟล์ความเสี่ยงเพื่อพัฒนามาตรการรักษาความมั่นคงปลอดภัยเชิงรุกก่อนที่จะเกิดเหตุการณ์ขึ้น	การมองเห็นแบบรวมศูนย์ (Centralized Visibility) ร่วมกับการรับรู้สถานการณ์ที่ครอบคลุมทั่วทั้งองค์กร
ระบบอัตโนมัติและการประสานงาน	การใช้เครื่องมือและลำดับขั้นตอนการทำงานแบบอัตโนมัติ เพื่อสนับสนุนการตอบสนองด้านความมั่นคงปลอดภัยและยังกำกับดูแลการใช้นโยบายข้ามระบบผลิตภัณฑ์ และบริการ	มุ่งเน้นการทำงานอัตโนมัติเต็มรูปแบบ เพื่อประสานกิจกรรมการตอบสนองแบบไดนามิกตามสถานการณ์ และเหตุการณ์ที่เกิดขึ้นจริง
การกำกับดูแล	การกำหนดและบังคับใช้นโยบายไซเบอร์ ทั้งภายในและระหว่างเสาหลัก เพื่อบริหารจัดการองค์กร และลดความเสี่ยงตามหลักการ Zero Trust	การประสานงานร่วมกันระหว่างเสาหลัก พร้อมระบบตรวจสอบและเฝ้าระวังภัยคุกคามอย่างต่อเนื่อง

ข้อเสนอแนะสำหรับการนำไปใช้

๑) ประเมินสถานะปัจจุบัน องค์กรควรเริ่มจากการประเมินว่า แต่ละเสาหลัก อยู่ในระดับความสมบูรณ์ใด ก่อนกำหนดแผนการลงทุน และการยกระดับสู่ระดับที่สูงขึ้น

๒) การเปลี่ยนผ่านแบบ ค่อยเป็นค่อยไป การนำ Zero Trust ไปใช้งาน ไม่ใช่โครงการระยะสั้น หากแต่เป็นกระบวนการพัฒนาระยะยาวที่ต้องใช้เวลาหลายปี โดยควรดำเนินการแบบเป็นขั้นตอน เพื่อให้สอดคล้องกับความพร้อมขององค์กรและลดความเสี่ยง

๓) ประสานงานข้ามเสาหลัก แม้แต่ละเสาหลักจะสามารถพัฒนาภายในขอบเขตของตนเองได้ แต่การบรรลุระดับการพัฒนาที่เหมาะสมจำเป็นต้องอาศัยการประสานงาน ความสอดคล้อง และการทำงานร่วมกันของความสามารถระหว่างเสาหลัก เพื่อให้การควบคุมด้านความมั่นคงปลอดภัยมีประสิทธิภาพในระดับองค์กร

ระดับความสมบูรณ์ของเสาหลักของ Zero Trust

หัวข้อนี้อธิบายระดับความสมบูรณ์ของแต่ละเสาหลักของสถาปัตยกรรม Zero Trust โดยแสดงรายละเอียดสิ่งที่ควรทำในแต่ละระดับความสมบูรณ์

ตัวตน (Identity)

รายละเอียดระดับความสมบูรณ์และสิ่งที่องค์กรควรดำเนินการดังแสดงในตารางที่ ๓๕

ตารางที่ ๓๕ แสดงระดับความสมบูรณ์ของเสาหลักตัวตน

ฟังก์ชัน	ดั้งเดิม	เริ่มต้น	พัฒนาแล้ว	ปรับปรุงให้เหมาะสม
การยืนยันตัวตน	ใช้การยืนยันตัวตนโดยใช้รหัสผ่านหรือการยืนยันตัวตนแบบหลายปัจจัย โดยมีการกำหนดสิทธิการเข้าถึงแบบสแตติกสำหรับตัวตนของบุคคล หรืออุปกรณ์	ใช้การยืนยันตัวตนแบบหลายปัจจัย ซึ่งอาจรวมถึงการใช้รหัสผ่านเป็นปัจจัยหนึ่ง และกำหนดให้มีการตรวจสอบความถูกต้องจากคุณลักษณะที่หลากหลาย เช่น สถานที่ตั้ง หรือพฤติกรรมผู้ใช้	ใช้การยืนยันตัวตนแบบหลายปัจจัยที่ป้องกันฟิชชิง และคุณลักษณะต่าง ๆ รวมถึงเริ่มมีการใช้งานการยืนยันตัวตนแบบหลายปัจจัยแบบไร้รหัสผ่านโดยผ่าน FIDO2 หรือ PIV ในระยะเริ่มต้น	ใช้การยืนยันตัวตนอย่างต่อเนื่องด้วยการยืนยันตัวตนแบบหลายปัจจัยที่ป้องกันฟิชชิง โดยไม่ได้ทำเพียงแค่ตอนที่ได้รับอนุญาตให้เข้าถึงในครั้งแรกเท่านั้น
แหล่งเก็บข้อมูลตัวตน	การจัดเก็บข้อมูลตัวตนที่บริหารจัดการเองภายในองค์กรเท่านั้น โดยดำเนินการวางแผนติดตั้ง และบำรุงรักษาเองทั้งหมด	มีการเชื่อมต่อระบบภายในองค์กร กับระบบคลาวด์เข้าด้วยกันในบางจุด เพื่อรองรับการทำ Single Sign-On (SSO) เบื้องต้น	มีการรวมแหล่งเก็บข้อมูลตัวตนทั้งหมดทั้งภายในองค์กรและระบบคลาวด์ให้เป็นหนึ่งเดียวอย่างปลอดภัย เพื่อการจัดการที่รวมศูนย์	มีการเชื่อมต่อข้อมูลตัวตนกับคู่ค้า และทุกสภาพแวดล้อมอย่างมั่นคงปลอดภัย พร้อมปรับเปลี่ยนการควบคุมตามความเหมาะสมแบบไดนามิก
การประเมินความเสี่ยงของตัวตน	การประเมินความเสี่ยงของตัวตนในระดับที่จำกัด เช่น ความน่าจะเป็นที่ตัวตนจะถูกนำไปใช้โดยบุคคลอื่น	มีการประเมินความเสี่ยงของตัวตนโดยใช้วิธีการดำเนินการแมนวล และกฎแบบสแตติก เพื่อการรับรู้ความเสี่ยง	มีการประเมินความเสี่ยงของตัวตนโดยใช้การวิเคราะห์แบบอัตโนมัติบางส่วนและกฎแบบไดนามิก เพื่อใช้เป็นข้อมูล	มีการประเมินความเสี่ยงของตัวตนแบบเรียลไทม์ โดยอาศัยการวิเคราะห์อย่างต่อเนื่อง และกฎแบบไดนามิก เพื่อให้การ

ฟังก์ชัน	ดั้งเดิม	เริ่มต้น	พัฒนาแล้ว	ปรับปรุงให้เหมาะสม
			ประกอบการตัดสินใจในการอนุญาตให้เข้าถึงและการดำเนินการตอบสนอง	ปกป้องที่ครอบคลุมตลอดเวลา
การจัดการสิทธิการเข้าถึง	การอนุญาตการเข้าถึงแบบถาวรโดยมีการทบทวนสิทธิเป็นระยะสำหรับทั้งบัญชีผู้ใช้ที่มีสิทธิสูง และบัญชีผู้ใช้ทั่วไป	มีการอนุญาตการเข้าถึง รวมถึงการร้องขอการเข้าถึงสามารถมีการกำหนดวันหมดอายุและใช้การทบทวนสิทธิแบบอัตโนมัติ	มีการอนุญาตการเข้าถึงตามความจำเป็น และตามรายเซสชัน รวมถึงการอนุญาตการเข้าถึงที่สามารถปรับเปลี่ยนให้เหมาะสมกับกิจกรรม และทรัพยากรที่จำเป็นต้องใช้งาน	มีการอนุญาตการเข้าถึงโดยใช้ระบบอัตโนมัติแบบเฉพาะเมื่อต้องการเข้าถึงและให้สิทธิเท่าที่จำเป็น และสามารถปรับเปลี่ยนให้สอดคล้องกับกิจกรรมและความต้องการในแต่ละทรัพยากร
การมองเห็นและวิเคราะห์	มีการรวบรวมบันทึกเหตุการณ์กิจกรรมของผู้ใช้งาน และเอนทิตีโดยเฉพาะข้อมูลเหตุการณ์ของผู้ที่มีสิทธิสูง และดำเนินการวิเคราะห์แบบแมนวลเป็นประจำ	มีการรวบรวมบันทึกเหตุการณ์กิจกรรมของผู้ใช้งาน และเอนทิตีโดยมีการวิเคราะห์แบบแมนวลเป็นประจำร่วมกับการวิเคราะห์แบบอัตโนมัติบางส่วนแต่ยังมีการเชื่อมโยงความสัมพันธ์ระหว่างประเภทของบันทึก	มีการดำเนินการวิเคราะห์แบบอัตโนมัติครอบคลุมบันทึกเหตุการณ์กิจกรรมของผู้ใช้งาน และเอนทิตีบางประเภท และเพิ่มขอบเขตการรวบรวมข้อมูลเพื่อจัดการกับช่องว่างที่ตรวจพบ	มีการมองเห็นที่ครอบคลุม และการตระหนักรู้ต่อสถานการณ์ (Situational awareness) ทั่วทั้งองค์กร โดยการวิเคราะห์แบบอัตโนมัติทั้งกับบันทึกเหตุการณ์กิจกรรมของผู้ใช้งานประเภทต่าง ๆ และการวิเคราะห์พฤติกรรมของผู้ใช้งาน

ฟังก์ชัน	ดั้งเดิม	เริ่มต้น	พัฒนาแล้ว	ปรับปรุงให้เหมาะสม
		เหตุการณ์อย่างจำกัด		
ระบบอัตโนมัติและการประสานงาน	มีระบบบัญชีตัวตนที่จัดการเอง เช่น การสร้าง การลบ และระงับการใช้งานของผู้ใช้งาน รวมถึงเอนทิตีแบบแมนวล โดยแทบไม่มีการเชื่อมต่อกันระหว่างระบบ และมีการทบทวนสิทธิเป็นประจำ	มีการกำหนดให้ผู้มีสิทธิสูงและผู้ใช้ภายนอกต้องผ่านกระบวนการประสานงานของระบบแบบใช้การดำเนินการด้วยตนเอง ขณะที่ผู้ใช้ทั่วไปและเอนทิตีภายในองค์กรใช้กระบวนการประสานงานของระบบแบบอัตโนมัติ	มีการประสานการทำงานของระบบแบบแมนวลสำหรับผู้มีสิทธิสูง และใช้ระบบอัตโนมัติในการประสานระบบสำหรับทุกผู้ใช้พร้อมทั้งมีการเชื่อมต่อระบบเข้าด้วยกันในทุกสภาพแวดล้อม	มีการใช้ระบบอัตโนมัติในการประสานการทำงานของระบบสำหรับทุกผู้ใช้พร้อมการเชื่อมต่ออย่างสมบูรณ์ในทุกสภาพแวดล้อม โดยสามารถอ้างอิงตามพฤติกรรม การลงทะเบียน และความต้องการในการใช้งาน
การกำกับดูแล	การบังคับใช้นโยบายสำหรับตัวตน (การยืนยันตัวตน ข้อมูลประจำตัว การเข้าถึง วงจรชีวิต ฯลฯ) ผ่านกลไกทางเทคนิคแบบสแตติกและการทบทวนแบบแมนวล	มีการกำหนด และเริ่มบังคับใช้นโยบายสำหรับตัวตนทั่วทั้งองค์กรโดยใช้ระบบอัตโนมัติบางส่วน และเน้นการอัปเดตนโยบายแบบแมนวล	มีการบังคับใช้นโยบายสำหรับตัวตนทั่วทั้งองค์กรด้วยระบบอัตโนมัติ และมีการอัปเดตนโยบายเป็นระยะ	มีการบังคับใช้ และเปลี่ยนนโยบายสำหรับตัวตนทั้งองค์กรให้เป็นแบบอัตโนมัติอย่างสมบูรณ์ สำหรับทุกผู้ใช้งานและเอนทิตีในทุกระบบ โดยมีการบังคับใช้และอัปเดตแบบไดนามิกอย่างต่อเนื่อง

ตารางที่ ๓๖ แสดงภาพรวมของเสาหลักตัวตน

หัวข้อ	สาระสำคัญ
จุดมุ่งหมาย	การยืนยันตัวตน และกำหนดสิทธิให้ตรงกับความจำเป็น โดยมีการประเมินความเสี่ยงและบริบทแบบต่อเนื่อง
แนวทางสำคัญ	ระบบการจัดการตัวตน ใบรับรองดิจิทัล และการเข้าถึง ร่วมกับการยืนยันตัวตนแบบหลายปัจจัยที่ต้านทานฟิชชิง การรวมศูนย์แหล่งจัดเก็บข้อมูลตัวตน และการใช้ระบบอัตโนมัติในการบริหารจัดการ
เป้าหมายสูงสุด	ระบบตัวตนที่สามารถ ตรวจสอบ ประเมิน และปรับสิทธิการเข้าถึงแบบเรียลไทม์โดยอัตโนมัติ พร้อมมีการมองเห็นกิจกรรมของผู้ใช้และระบบอย่างครบถ้วน

อุปกรณ์ (Devices)

องค์กรจำเป็นต้องควบคุมความมั่นคงปลอดภัยของอุปกรณ์ทุกชิ้นที่เข้าถึงระบบ และต้องไม่อนุญาตให้อุปกรณ์ที่ไม่ได้รับการอนุญาตเชื่อมต่อเข้ามาในระบบโดยเด็ดขาด

เพื่อให้บรรลุเป้าหมายนี้ องค์กรควร

๑) รู้จักและมองเห็นอุปกรณ์ทั้งหมดในระบบ

๒) มีบัญชีรายการและข้อมูลเชิงลึกของอุปกรณ์ทุกชิ้น ทั้งอุปกรณ์ทางกายภาพ และอุปกรณ์เสมือนหรือบนคลาวด์

๓) ควบคุมและลดความเสี่ยงจากอุปกรณ์ที่ไม่ได้อยู่ภายใต้การจัดการโดยตรงขององค์กร เช่น อุปกรณ์ส่วนตัวของพนักงาน อุปกรณ์ของคู่สัญญา อุปกรณ์ IoT ฯลฯ

๔) บำรุงรักษาความมั่นคงปลอดภัยของอุปกรณ์อย่างต่อเนื่อง โดยตรวจสอบการตั้งค่าแพตช์ ความเปราะบาง และสถานะของระบบป้องกันภัยคุกคามไซเบอร์

๕) ประเมินสถานะความมั่นคงปลอดภัยของอุปกรณ์ ใช้ประกอบการตัดสินใจอนุญาตหรือปฏิเสธการเข้าถึง

ซึ่งมีรายละเอียดดังแสดงในตารางที่ ๓๗ ดังต่อไปนี้

ตารางที่ ๓๗ แสดงระดับความสมบูรณ์ของเสาหลักอุปกรณ์

ฟังก์ชัน	ดั้งเดิม	เริ่มต้น	พัฒนาแล้ว	ปรับปรุงให้เหมาะสม
การบังคับใช้นโยบายและการติดตามการปฏิบัติตามข้อกำหนด	มีความสามารถในการตรวจสอบการปฏิบัติตามข้อกำหนดของอุปกรณ์ที่จำกัดมากหรือแทบไม่มีเลย เช่น การตรวจสอบพฤติกรรมอุปกรณ์ รวมถึงขาดเครื่องมือที่มีประสิทธิภาพในการบังคับใช้นโยบายหรือการจัดการซอฟต์แวร์ การตั้งค่า และช่องโหว่ต่าง ๆ	มีข้อมูลคุณลักษณะของอุปกรณ์ผ่านการรายงานจากตัวอุปกรณ์เอง เช่น คีย์โทเค็น หรือข้อมูลผู้ใช้งานฯลฯ แต่ยังมีกลไกในการบังคับใช้นโยบายที่จำกัด ทั้งนี้เริ่มมีการกำหนดกระบวนการพื้นฐานในการอนุมัติใช้งานซอฟต์แวร์ รวมถึงการส่งข้อมูลอัปเดตและปรับเปลี่ยนการตั้งค่าไปยังอุปกรณ์	มีข้อมูลเชิงลึกที่ผ่านการตรวจสอบแล้วโดยผู้ดูแลระบบสามารถตรวจสอบและยืนยันข้อมูลบนอุปกรณ์ได้ตั้งแต่การเข้าถึงของอุปกรณ์ในครั้งแรก พร้อมทั้งบังคับใช้นโยบายกับอุปกรณ์และทรัพย์สินเสมือนส่วนใหญ่ผ่านระบบอัตโนมัติ ไม่ว่าจะเป็นการตรวจสอบสถานะการจัดการอุปกรณ์ การอนุมัติซอฟต์แวร์ การระบุช่องโหว่ หรือการติดตั้งแพตช์	มีการตรวจสอบข้อมูลเชิงลึก และบังคับใช้การปฏิบัติตามข้อกำหนดอย่างต่อเนื่องตลอดอายุการใช้งานของอุปกรณ์ และทรัพย์สินเสมือน พร้อมทั้งบูรณาการตรวจสอบสถานะการจัดการอุปกรณ์ ซอฟต์แวร์ การตั้งค่า และช่องโหว่เข้าด้วยกันอย่างสมบูรณ์ในทุกสภาพแวดล้อม
การจัดการความเสี่ยงด้านทรัพย์สินและห่วงโซ่อุปทาน	การขาดการติดตามทรัพย์สินทั้งทางกายภาพ และเสมือนในภาพรวมขององค์กร รวมถึงยังไม่สามารถจัดการข้อมูลข้ามระบบของผู้ผลิตรายต่าง ๆ ได้ ขณะที่	มีการติดตามทรัพย์สินทางกายภาพทั้งหมดและทรัพย์สินเสมือนบางส่วน พร้อมทั้งจัดการความเสี่ยงในห่วงโซ่อุปทาน โดยการกำหนดนโยบาย	เริ่มสร้างมุมมองที่ครอบคลุมทั่วทั้งองค์กรสำหรับทรัพย์สินทางกายภาพและทรัพย์สินเสมือนผ่านกระบวนการอัตโนมัติ ซึ่งสามารถทำงาน	มีความสามารถในการมองเห็นทรัพย์สินทั้งหมดจากทุกผู้ผลิตและผู้ให้บริการได้ครอบคลุมแบบเรียลไทม์พร้อมทั้งใช้ระบบอัตโนมัติสำหรับจัดการความเสี่ยงในห่วงโซ่อุปทาน

ฟังก์ชัน	ดั้งเดิม	เริ่มต้น	พัฒนาแล้ว	ปรับปรุงให้เหมาะสม
	การจัดหาอุปกรณ์และบริการในห่วงโซ่อุปทานยังเป็นแบบเฉพาะกิจ ทำให้มองเห็นความเสี่ยงในระดับองค์กรได้อย่างจำกัด	และเกณฑ์มาตรฐานการควบคุม ตามคำแนะนำของหน่วยงานที่น่าเชื่อถือผ่านกรอบการทำงานที่เข้มแข็ง เช่น สกมช.	ข้ามระบบของผู้ผลิตที่หลากหลาย เพื่อตรวจสอบการจัดหา ติดตามวงจรการพัฒนา และจัดให้มีการประเมินจากหน่วยงานภายนอก	ตามความเหมาะสม โดยเน้นการสร้างการปฏิบัติการที่ยังทำงานต่อได้แม้เกิดความล้มเหลวในห่วงโซ่อุปทาน และนำแนวการปฏิบัติที่เหมาะสมมาปรับใช้
การเข้าถึงทรัพยากร	ไม่ต้องการการมองเห็นอุปกรณ์หรือทรัพย์สินเสมือนที่ใช้ในการเข้าถึงทรัพยากร	มีการกำหนดให้อุปกรณ์ หรือทรัพย์สินเสมือนบางส่วนต้องรายงานคุณลักษณะของตนเอง เพื่อนำข้อมูลดังกล่าวมาใช้ในการอนุมัติการเข้าถึงทรัพยากร	มีการพิจารณาการเข้าถึงทรัพยากรโดยอาศัยข้อมูลเชิงลึกของอุปกรณ์หรือทรัพย์สินเสมือนที่ผ่านการตรวจสอบแล้ว	มีการเข้าถึงทรัพยากร มีการนำผลวิเคราะห์ความเสี่ยงแบบเรียลไทม์ของอุปกรณ์และทรัพย์สินเสมือนมาพิจารณาร่วมด้วย
การป้องกันภัยคุกคามในอุปกรณ์	มีการติดตั้งความสามารถในการป้องกันภัยคุกคามไปยังอุปกรณ์บางส่วนแบบแมนวล	เริ่มมีกระบวนการอัตโนมัติบางส่วนในการติดตั้ง และอัปเดตความสามารถในการป้องกันภัยคุกคามไปยังอุปกรณ์ และทรัพย์สินเสมือน แต่ยังมีการเชื่อมต่อกับส่วนบังคับใช้นโยบาย และส่วนตรวจสอบการปฏิบัติตาม	เริ่มรวบรวมความสามารถในการป้องกันภัยคุกคามเข้าสู่ส่วนกลางสำหรับทั้งอุปกรณ์ และทรัพย์สินเสมือน พร้อมทั้งบูรณาการความสามารถในการป้องกันภัยคุกคามส่วนใหญ่เข้ากับการบังคับใช้นโยบาย และส่วน	มีการติดตั้งโซลูชันการป้องกันภัยคุกคามแบบรวมศูนย์ที่มีขีดความสามารถขั้นสูงสำหรับบนอุปกรณ์ และทรัพย์สินเสมือน โดยใช้แนวทางที่เป็นหนึ่งเดียวกันทั้งในการป้องกันภัยคุกคาม การบังคับใช้นโยบาย และการตรวจสอบ

ฟังก์ชัน	ดั้งเดิม	เริ่มต้น	พัฒนาแล้ว	ปรับปรุงให้เหมาะสม
		ข้อกำหนดอย่างจำกัด	ตรวจสอบการปฏิบัติตามข้อกำหนด	การปฏิบัติตามข้อกำหนด
การมองเห็นและวิเคราะห์	ใช้การทำทะเบียนทรัพย์สินแบบติดป้ายทางกายภาพและใช้ซอฟต์แวร์ตรวจสอบอย่างจำกัดเพื่อทบทวนอุปกรณ์ตามวงรอบปกติ โดยมีการวิเคราะห์แบบแมนวลร่วมด้วยบางส่วน	มีการเริ่มใช้ตัวระบุข้อมูลดิจิทัล เช่น หมายเลขเครื่องแท็กดิจิทัล ควบคู่ไปกับการทำทะเบียนแบบแมนวล และการตรวจสอบเครื่องปลายทาง โดยอุปกรณ์และทรัพย์สินเสมือนบางส่วนอยู่ภายใต้การวิเคราะห์แบบอัตโนมัติ (เช่น การสแกนด้วยซอฟต์แวร์) สำหรับตรวจจับความผิดปกติตามความเสี่ยง	มีการเริ่มใช้ระบบอัตโนมัติทั้งในการรวบรวมข้อมูลทะเบียนทรัพย์สิน รวมถึงการตรวจสอบอุปกรณ์ปลายทางของผู้ใช้ทั้งหมด เช่น เดสก์ท็อป แล็ปท็อป มือถือ แท็บเล็ต และทรัพย์สินเสมือน และการตรวจจับความผิดปกติ เพื่อระบุอุปกรณ์ที่ไม่ได้รับอนุญาต	มีการเริ่มใช้ระบบรวบรวมสถานะของอุปกรณ์ และทรัพย์สินเสมือนทั้งหมดแบบอัตโนมัติ พร้อมทั้งเชื่อมโยงข้อมูลกับผู้ใช้ ทำการตรวจสอบอุปกรณ์ปลายทาง และวิเคราะห์ความผิดปกติ เพื่อใช้เป็นข้อมูลในการตัดสินใจเพื่ออนุญาตให้เข้าถึงทรัพยากร นอกจากนี้ยังมีการติดตามทรัพย์สินเสมือนทั้งรูปแบบของการติดตั้งหรือการถอดถอน เพื่อตรวจหาสิ่งผิดปกติ
ระบบอัตโนมัติและการประสานงาน	มีการดำเนินการจัดเตรียม ตั้งค่า หรือลงทะเบียนอุปกรณ์ภายในองค์กรแบบแมนวล	เริ่มใช้เครื่องมือและสคริปต์เพื่อเปลี่ยนกระบวนการจัดเตรียม ตั้งค่า ลงทะเบียน หรือถอดถอนอุปกรณ์และทรัพย์สิน	เริ่มใช้กลไกการตรวจสอบ และบังคับใช้นโยบายเพื่อระบุอุปกรณ์หรือทรัพย์สินเสมือนที่ไม่ปฏิบัติตามข้อกำหนด เช่น	มีกระบวนการแบบอัตโนมัติอย่างเต็มรูปแบบ ทั้งในการจัดเตรียม ลงทะเบียน ตรวจสอบสถานะแยกอุปกรณ์ที่มีปัญหา แก้ไขช่องโหว่ และ

ฟังก์ชัน	ดั้งเดิม	เริ่มต้น	พัฒนาแล้ว	ปรับปรุงให้เหมาะสม
		เสมือนจากแบบแมนวลให้เป็นอัตโนมัติ	มีช่องโหว่ ใบรับรองดิจิทัลไม่ผ่านการตรวจสอบ หมายเลขเครื่องไม่ได้ลงทะเบียน และดำเนินการตัดการเชื่อมต่อ หรือแยกอุปกรณ์ออกจากระบบ	ถอดถอนอุปกรณ์รวมถึงทรัพย์สินเสมือนออกจากระบบ
การกำกับดูแล	กำหนดนโยบายบางส่วนสำหรับจัดการวงจรชีวิตของอุปกรณ์คอมพิวเตอร์ และอุปกรณ์ต่อพ่วง โดยอาศัยกระบวนการแบบแมนวลในการบำรุงรักษา เช่น การอัปเดต การติดตั้งแพตช์ การล้างข้อมูลอุปกรณ์	มีการกำหนด และบังคับใช้นโยบายสำหรับการจัดซื้ออุปกรณ์ใหม่ และนโยบายวงจรชีวิตของอุปกรณ์ และทรัพย์สินเสมือน รวมถึงกำหนดให้มีการตรวจสอบ และสแกนอุปกรณ์อย่างสม่ำเสมอ	มีการกำหนดนโยบายที่ครอบคลุมทั้งองค์กรสำหรับวงจรชีวิตของอุปกรณ์ และทรัพย์สินเสมือน รวมถึงการทำบัญชีรายชื่อ และการตรวจสอบความรับผิดชอบ โดยมีกลไกการบังคับใช้แบบอัตโนมัติบางส่วน	มีการกำหนดนโยบายสำหรับวงจรชีวิตของอุปกรณ์ และทรัพย์สินเสมือนทั้งหมดที่เชื่อมต่อกับเครือข่ายให้เป็นแบบอัตโนมัติทั่วทั้งองค์กร

ตารางที่ ๓๘ แสดงภาพรวมของเสาหลักอุปกรณ์

หัวข้อ	สาระสำคัญ
เป้าหมายหลัก	รู้จักและควบคุมทุกอุปกรณ์ที่เชื่อมต่อกับระบบทั้งจริงและเสมือน
ประเด็นสำคัญ	บัญชีทรัพย์สินที่ครอบคลุม การป้องกันภัยคุกคามทางไซเบอร์ การตรวจสอบการเป็นไปตามข้อบังคับ และการประเมินความเสี่ยงแบบต่อเนื่อง
ความก้าวหน้าสูงสุด	องค์กรมีระบบอัตโนมัติที่สามารถตรวจจับอุปกรณ์ใหม่ ประเมินความเสี่ยง ปรับสิทธิ และแยกกักกัน (Isolate) อุปกรณ์ที่ไม่ปลอดภัยได้ทันที
ประโยชน์	ลดความเสี่ยงจากอุปกรณ์ที่ไม่ปลอดภัย ปรับปรุงความมั่นคงปลอดภัยในห่วงโซ่อุปทาน และเสริมการทำงานร่วมกับเสาหลักตัวตน และเสาหลักเครือข่าย

เครือข่าย (Networks)

วัตถุประสงค์ของเสานี้คือการลดความเสี่ยงจากการเคลื่อนตัวภายในเครือข่าย การแบ่งเครือข่าย และตรวจสอบทราฟฟิกแบบต่อเนื่อง

เพื่อให้บรรลุเป้าหมายนี้ หน่วยงานควร

๑) การป้องกันและควบคุมการเข้าถึง ทุกการเชื่อมต่อเครือข่ายต้องได้รับอนุญาตตามหลักความมั่นคงปลอดภัย การได้รับสิทธิเท่าที่จำเป็นและมีการตรวจสอบตัวตนของต้นทางและปลายทาง

๒) การแบ่งส่วนเครือข่ายเป็นเครือข่ายย่อย ลดผลกระทบจากการบุกรุก โดยจำกัดขอบเขตของการสื่อสารระหว่างเครือข่ายย่อย

๓) การมองเห็นและการวิเคราะห์ ตรวจสอบทราฟฟิกทั้งหมดทั้งภายในและภายนอก เพื่อหาพฤติกรรมผิดปกติ

๔) การป้องกันเชิงรุกและการตอบสนองแบบอัตโนมัติ ใช้ระบบอัตโนมัติในการยุติหรือจำกัดการเชื่อมต่อที่มีความเสี่ยง

โดยรายละเอียดระดับความสมบูรณ์ของเสาหลักเครือข่ายได้ไว้แสดงดังตารางที่ ๓๙

ตารางที่ ๓๙ แสดงระดับความสมบูรณ์ของเสาหลักเครือข่าย

ฟังก์ชัน	ดั้งเดิม	เริ่มต้น	พัฒนาแล้ว	ปรับปรุงให้เหมาะสม
การแบ่งเครือข่าย	กำหนดสถาปัตยกรรมเครือข่ายโดยใช้การแบ่งส่วนเครือข่ายขนาดใหญ่ หรือการป้องกันแค่ขอบเขตรอบนอก โดยมีการควบคุมในการเข้าถึงระหว่างส่วนต่าง ๆ ของเครือข่ายเพียงเล็กน้อย นอกจากนี้ยังอาจจะต้องมีการเชื่อมต่อกันระหว่างเครือข่าย	เริ่มวางโครงสร้างเครือข่ายที่เน้นการแยกเวิร์กโหลดที่สำคัญออกจากกัน จำกัดการเชื่อมต่อตามหลักการให้สิทธิเท่าที่จำเป็น และเริ่มเปลี่ยนผ่านไปสู่การเชื่อมต่อแบบเฉพาะเจาะจงรายบริการ	มีการขยายกลไกการแยกส่วนการทำงานตามอุปกรณ์ ปลายทาง และแอปพลิเคชันในเครือข่ายย่อยมากขึ้น โดยมีการสร้างขอบเขตย่อย ทั้งขาเข้า และขาออก รวมถึงใช้การเชื่อมต่อแบบเฉพาะเจาะจงรายบริการ	มีสถาปัตยกรรมเครือข่ายประกอบด้วยเครือข่ายย่อยกระจายตัวอย่างสมบูรณ์ และมีการแบ่งส่วนเครือข่ายแบบย่อย อย่างกว้างขวางตาม โพรไฟล์แอปพลิเคชันโดยใช้การเชื่อมต่อแบบ ไดนามิกที่ให้สิทธิการเข้าถึงเฉพาะเวลาที่จำเป็นและเท่าที่จำเป็นสำหรับแต่ละบริการ
การบริหารจัดการทราฟฟิกเครือข่าย	ใช้การกำหนดค่าและข้อกำหนดเครือข่ายแบบสแตติกด้วยวิธีแบบแมนวล โดยมีความสามารถในการตรวจสอบที่จำกัด เช่น การตรวจสอบประสิทธิภาพแอปพลิเคชัน หรือการตรวจจับความผิดปกติ และใช้วิธี	เริ่มใช้การกำหนดโพรไฟล์แอปพลิเคชันตามลักษณะของทราฟฟิกที่แตกต่างกัน และเริ่มจัดหมวดหมู่แอปพลิเคชันทั้งหมดเข้ากับโพรไฟล์เหล่านี้ พร้อมทั้งขยายการใช้กฎแบบสแตติกให้ครอบคลุมทุก	เริ่มใช้การกำหนดค่าและข้อกำหนดเครือข่ายแบบไดนามิก เพื่อเพิ่มประสิทธิภาพการใช้ทรัพยากร ซึ่งกฎเหล่านี้จะถูกปรับเปลี่ยนเป็นระยะ ตามผลการตรวจสอบ และการประเมินโพรไฟล์ของแอปพลิเคชันแบบอัตโนมัติที่	เริ่มใช้การกำหนดค่าและข้อกำหนดเครือข่ายแบบไดนามิกที่มีการพัฒนาอย่างต่อเนื่องเพื่อให้สอดคล้องกับโพรไฟล์ของแอปพลิเคชัน และจัดลำดับความสำคัญของแอปพลิเคชันใหม่ตามความสำคัญของภารกิจ และความเสี่ยงฯลฯ

ฟังก์ชัน	ดั้งเดิม	เริ่มต้น	พัฒนาแล้ว	ปรับปรุงให้เหมาะสม
	แบบแมนวลในการตรวจสอบและทบทวนการเปลี่ยนแปลงโพรไฟล์ของแอปพลิเคชันที่มีความสำคัญ	แอปพลิเคชัน และทำการประเมินโพรไฟล์ของแอปพลิเคชันแบบแมนวลเป็นระยะ	ตระหนัก และตอบสนองต่อความเสี่ยง	
การเข้ารหัสและปกป้องทราฟฟิก	มีการเข้ารหัสทราฟฟิกเพียงเล็กน้อย และพึ่งพากระบวนการแบบแมนวล หรือแบบเฉพาะกิจในการจัดการ และดูแลความมั่นคงปลอดภัยของคีย์ที่ใช้ในการเข้ารหัส	มีการเริ่มเข้ารหัสทราฟฟิกทั้งหมดที่ไปยังแอปพลิเคชัน และให้ความสำคัญกับการเข้ารหัสทราฟฟิกที่ไปยังแอปพลิเคชันภายนอกเป็นอันดับต้น รวมถึงเริ่มจัดทำนโยบายการจัดการคีย์อย่างเป็นทางการ และดูแลความมั่นคงปลอดภัยของคีย์เข้ารหัสสำหรับเซิร์ฟเวอร์ หรือบริการ	มีการรับประกันการเข้ารหัสสำหรับโปรโตคอลที่ใช้ในการรับส่งข้อมูลทั้งภายใน และภายนอกที่เกี่ยวข้องทั้งหมด มีการจัดการการออกและหมุนเวียนคีย์และใบรับรองดิจิทัล รวมถึงเริ่มนำแนวการปฏิบัติที่ดีที่สุดด้านความยืดหยุ่นทางการเข้ารหัสมาปรับใช้	มีการดำเนินการเข้ารหัสทราฟฟิกทั้งหมดอย่างต่อเนื่อง บังคับใช้หลักการให้สิทธิเท่าที่จำเป็นในการจัดการคีย์ที่ปลอดภัยทั่วถึงทั้งองค์กร และนำแนวปฏิบัติที่ดีที่สุดด้านความยืดหยุ่นทางการเข้ารหัสมาปรับใช้ให้กว้างขวางที่สุดเท่าที่จะเป็นไปได้
ความยืดหยุ่นของเครือข่าย	มีการตั้งค่าความสามารถของเครือข่ายเป็นรายกรณี (Case-by-case) เพื่อให้สอดคล้องกับความ	มีการเริ่มตั้งค่าความสามารถของเครือข่ายเพื่อจัดการความต้องการด้านความพร้อมใช้งานสำหรับ	มีการตั้งค่าความสามารถของเครือข่ายให้สามารถจัดการความต้องการด้านความพร้อมใช้งาน และ	มีการบูรณาการในทุกด้านเพื่อให้สามารถปรับตัวตามการเปลี่ยนแปลงของความต้องการด้านความพร้อมใช้งาน

ฟังก์ชัน	ดั้งเดิม	เริ่มต้น	พัฒนาแล้ว	ปรับปรุงให้เหมาะสม
	ต้องการด้านความพร้อมใช้งานของแต่ละแอปพลิเคชันเท่านั้น โดยมีกลไกความยืดหยุ่นที่จำกัดสำหรับเวิร์กโหลดที่ไม่สำคัญต่อภารกิจ	แอปพลิเคชันเพิ่มเติม และขยายกลไกความยืดหยุ่นไปยังเวิร์กโหลดที่ไม่สำคัญต่อภารกิจให้มากขึ้น	กลไกความยืดหยุ่นแบบไดนามิกสำหรับแอปพลิเคชันส่วนใหญ่ขององค์กร	สำหรับทุกแอปพลิเคชันและเวิร์กโหลด พร้อมทั้งจัดให้มีความยืดหยุ่นที่เหมาะสมกับความสำคัญของแต่ละระบบ
ความสามารถการมองเห็น และวิเคราะห์	มีความสามารถในการเฝ้าระวังเครือข่ายที่เน้นเฉพาะขอบเขตรอบนอกอย่างจำกัด และมีการวิเคราะห์เพียงเล็กน้อยเพื่อเริ่มสร้างความตระหนักรู้สถานการณ์ จากส่วนกลาง	มีความสามารถในการเฝ้าระวังเครือข่ายตามดัชนีบ่งชี้แสดงการบุกรุก (IOC) เพื่อสร้างความตระหนักรู้สถานการณ์ในแต่ละสภาพแวดล้อม และเริ่มเชื่อมโยงข้อมูลข้ามประเภทของทราฟฟิก และสภาพแวดล้อมเพื่อการวิเคราะห์ และการค้นหาภัยคุกคาม	มีความสามารถในการตรวจจับสิ่งผิดปกติบนเครือข่าย เพื่อสร้างความตระหนักรู้สถานการณ์ในทุกสภาพแวดล้อม เริ่มเชื่อมโยงข้อมูลจากหลายแหล่งเพื่อการวิเคราะห์ และรวมกระบวนการอัตโนมัติเข้ากับการค้นหาภัยคุกคามที่เข้มแข็ง	มีความสามารถในการมองเห็นการสื่อสารในทุกเครือข่าย และสภาพแวดล้อมขององค์กร พร้อมทั้งสร้างความตระหนักรู้สถานการณ์ทั่วทั้งองค์กร และมีขีดความสามารถในการเฝ้าระวังขั้นสูงที่เชื่อมโยงข้อมูลจากทุกแหล่งตรวจจับโดยอัตโนมัติ
ระบบอัตโนมัติและการประสานงาน	ใช้กระบวนการแบบแมนวลในการจัดการการตั้งค่าและจัดการวงจรชีวิตของทรัพยากรบนเครือข่าย และจัดการสภาพแวดล้อมของ	เริ่มใช้วิธีการอัตโนมัติในการจัดการการตั้งค่าและจัดการวงจรชีวิตของทรัพยากรบนบางเครือข่ายหรือบางสภาพแวดล้อม และ	ใช้วิธีจัดการการเปลี่ยนแปลงแบบอัตโนมัติ เช่น CI/CD เพื่อจัดการการตั้งค่า และจัดการวงจรชีวิตของทรัพยากรบนทุกเครือข่าย และ	เครือข่าย และสภาพแวดล้อมถูกกำหนดขึ้นจากการสร้างโครงสร้างพื้นฐานด้วยโค้ด ซึ่งจัดการผ่านการจัดการการเปลี่ยนแปลงแบบ

ฟังก์ชัน	ดั้งเดิม	เริ่มต้น	พัฒนาแล้ว	ปรับปรุงให้เหมาะสม
	องค์กร โดยมีการบูรณาการข้อกำหนดด้านนโยบาย และการตระหนักรู้สถานการณ์เป็นระยะ	รับประกันว่าทรัพยากรทั้งหมดมีการกำหนดระยะเวลาการใช้งานไว้ชัดเจนตามนโยบาย	สภาพแวดล้อม และมีการตอบสนองและบังคับใช้นโยบาย และการป้องกันความเสี่ยง	อัตโนมัติ รวมถึงมีการเริ่มใช้งาน และยกเลิกการใช้งานโดยอัตโนมัติที่สอดคล้องกับความต้องการที่เปลี่ยนแปลงไป
การกำกับดูแล	มีการบังคับใช้นโยบายเครือข่ายแบบสแตติกการเข้าถึง โปรโตคอล การแบ่งส่วน การแจ้งเตือน และการแก้ไข โดยใช้แนวทางที่มุ่งเน้นการป้องกันเฉพาะขอบเขตรอบนอกเป็นหลัก	มีการกำหนด และเริ่มบังคับใช้นโยบายที่ปรับแต่งให้เหมาะสมกับแต่ละส่วนของเครือข่าย และทรัพยากร พร้อมทั้งรับเอาเกณฑ์การปฏิบัติขององค์กรมาปรับใช้ตามความเหมาะสม	มีการนำระบบอัตโนมัติมาใช้ในการบังคับใช้นโยบายที่ปรับแต่งอย่างเหมาะสม และสนับสนุนการเปลี่ยนผ่านจากการป้องกันที่มุ่งเน้นเพียงขอบเขตรอบนอกให้ครอบคลุมเครือข่ายภายในมากขึ้น	มีการบังคับใช้นโยบายเครือข่ายทั่วทั้งองค์กร มีการควบคุมในระดับย่อยที่เหมาะสม มีการอัปเดตแบบไดนามิก และมีการเชื่อมต่อกับภายนอกที่ปลอดภัย โดยอิงกับแอปพลิเคชัน และผู้ใช้งาน

ตารางที่ ๔๐ แสดงภาพรวมของเสาหลักเครือข่าย

หัวข้อ	สาระสำคัญ
เป้าหมายหลัก	ตรวจสอบ ควบคุม และจำกัดการรับส่งข้อมูลทราฟฟิก ทุกเส้นทาง โดยพิจารณาตามบริบทและระดับความเสี่ยง
หลักการสำคัญ	ไม่มีโซนที่ถือว่า “ปลอดภัยโดยปริยาย” ใช้การแบ่งเครือข่ายระดับย่อย การเข้ารหัสในทุกระดับ และการควบคุมการเข้าถึงเครือข่ายแบบอิงตัวตน
การพัฒนา	บังคับใช้นโยบายเครือข่ายแบบอัตโนมัติที่ขับเคลื่อนด้วยข้อมูล การวิเคราะห์ และปัญญาประดิษฐ์
ผลลัพธ์สูงสุด	เครือข่ายที่สามารถตรวจจับภัยคุกคามแบบเรียลไทม์ ตอบสนองโดยอัตโนมัติ และบังคับใช้นโยบายตามบริบทของผู้ใช้และอุปกรณ์ได้ทันที

แอปพลิเคชันและเวิร์กโหลด (Applications and Workloads)

วัตถุประสงค์ของเสาหลักแอปพลิเคชันและเวิร์กโหลด

๑) ป้องกันการเข้าถึงแอปพลิเคชันโดยไม่ได้รับอนุญาต

๒) เพิ่มความมั่นคงปลอดภัยตลอดวงจรชีวิตของแอปพลิเคชัน ตั้งแต่การพัฒนา การทดสอบ ไปจนถึงการนำขึ้นใช้งานจริง

๓) ผสานระบบป้องกันภัยคุกคามเข้ากับแต่ล่ะลำดับขั้นตอนการทำงานของแอปพลิเคชันโดยตรง

๔) ทำให้แอปพลิเคชันสามารถเข้าถึงผ่านเครือข่ายสาธารณะได้อย่างปลอดภัย

๕) เพิ่มความสามารถในการตรวจจับความผิดปกติแบบต่อเนื่องในระดับแอปพลิเคชัน

เพื่อให้บรรลุเป้าหมายนี้ หน่วยงานควรเตรียม

๑) การควบคุมการเข้าถึงแอปพลิเคชัน

๑.๑) จำกัดสิทธิการเข้าถึงตามหลักให้สิทธิเท่าที่จำเป็น

๑.๒) ใช้บริบทประกอบการอนุมัติสิทธิในแต่ละคำขอ

๒) การป้องกันภัยคุกคามภายในแอปพลิเคชัน ผสานกลไกป้องกันภัยคุกคามเข้ากับตัวแอปพลิเคชันโดยตรง เช่น การตรวจสอบข้อมูลนำเข้า การป้องกัน API การตรวจจับภัยคุกคามขณะทำงานฯลฯ

๓) การเข้าถึงแอปพลิเคชันผ่านอินเทอร์เน็ตอย่างปลอดภัย อนุญาตให้ผู้ใช้เข้าถึงแอปพลิเคชันผ่านเครือข่ายสาธารณะได้อย่างปลอดภัย โดยผ่านตัวกลางสื่อสารที่เชื่อถือได้และเข้ารหัส และมีการควบคุมตามหลัก Zero Trust

๔) กระบวนการพัฒนา ทดสอบ และเปิดใช้งานอย่างปลอดภัย

๔.๑) มาตรการด้านความมั่นคงปลอดภัยในทุกขั้นตอนของการพัฒนาแอปพลิเคชัน

๔.๒) ใช้ CI/CD Pipeline ที่มีการควบคุม การตรวจสอบ และการทดสอบความมั่นคงปลอดภัยแบบอัตโนมัติ

๕) การมองเห็นและการวิเคราะห์ในระดับแอปพลิเคชัน ตรวจสอบสถานะ ประสิทธิภาพ ความผิดปกติ และเหตุการณ์ด้านความมั่นคงปลอดภัยของแอปพลิเคชันอย่างต่อเนื่อง

๖) ระบบอัตโนมัติและการประสานงานในการกำหนดค่าแอปพลิเคชัน ปรับแต่งการตั้งค่าของแอปพลิเคชันโดยอัตโนมัติ ตามระดับความเสี่ยง สภาพการใช้งาน และนโยบายขององค์กร

โดยรายละเอียดระดับความสมบูรณ์ของเสาหลักแอปพลิเคชันและเวิร์กโหลดได้ไว้แสดงดังตารางที่ ๔๑

ตารางที่ ๔๑ แสดงระดับความสมบูรณ์ของเสาหลักแอปพลิเคชันและเวิร์กโหลด

ฟังก์ชัน	ดั้งเดิม	เริ่มต้น	พัฒนาแล้ว	ปรับปรุงให้เหมาะสม
การเข้าถึงแอปพลิเคชัน	การอนุมัติการเข้าถึงแอปพลิเคชันโดยอาศัยการอนุญาตสิทธิเฉพาะส่วน และการกำหนดแอตทริบิวต์แบบสแตติกเป็นหลัก	เริ่มใช้ความสามารถในการอนุมัติการเข้าถึงแอปพลิเคชันที่นำข้อมูลบริบทมาพิจารณา เช่น ตัวตน การปฏิบัติตามข้อกำหนดของอุปกรณ์ หรือแอตทริบิวต์อื่น ๆ ต่อการร้องขอแต่ละครั้ง และมีการกำหนด เวลาหมดอายุ	มีการใช้ระบบอัตโนมัติในการอนุมัติการเข้าถึงแอปพลิเคชันโดยใช้ข้อมูลบริบทที่ครอบคลุมมากขึ้น และบังคับใช้เงื่อนไขการเข้าถึงที่ยึดตามหลักการให้สิทธิเท่าที่จำเป็น	มีการตรวจสอบการอนุญาตการเข้าถึงแอปพลิเคชันอย่างต่อเนื่อง โดยรวมการวิเคราะห์ความเสี่ยงแบบเรียลไทม์และปัจจัยต่าง ๆ เช่น พฤติกรรม หรือรูปแบบการใช้งานมาพิจารณาร่วมด้วย
ป้องกันภัยคุกคามแอปพลิเคชัน	มีระบบป้องกันภัยคุกคามที่มีการเชื่อมโยงกับขั้นตอนการทำงานของแอปพลิเคชันน้อยมาก โดยเน้นการป้องกันทั่วไปสำหรับภัยคุกคามที่รู้จัก	มีการบูรณาการการป้องกันภัยคุกคามเข้ากับขั้นตอนการทำงานของแอปพลิเคชันที่มีความสำคัญ โดยมีการป้องกันทั้งภัยคุกคามที่รู้จักทั่วไปและภัยคุกคามเฉพาะเจาะจงที่พุ่งเป้ามายังแอปพลิเคชัน	มีการบูรณาการการป้องกันภัยคุกคามเข้ากับขั้นตอนการทำงานของแอปพลิเคชันทั้งหมด เพื่อป้องกันภัยคุกคามเฉพาะทาง และภัยคุกคามที่มีเป้าหมายเฉพาะเจาะจง	มีการบูรณาการการป้องกันภัยคุกคามขั้นสูงเข้ากับขั้นตอนการทำงานของทุกแอปพลิเคชัน โดยให้การมองเห็นแบบเรียลไทม์ และการป้องกันที่ตระหนักถึงเนื้อหารายละเอียด เพื่อรับมือกับการโจมตีที่มีความซับซ้อนที่ถูกออกแบบมาเพื่อโจมตีแต่ละ

ฟังก์ชัน	ดั้งเดิม	เริ่มต้น	พัฒนาแล้ว	ปรับปรุงให้เหมาะสม
				แอปพลิเคชันโดยเฉพาะ
การเข้าถึงแอปพลิเคชัน	เปิดให้เข้าถึงแอปพลิเคชันที่มีความสำคัญบางส่วนผ่านเครือข่ายสาธารณะที่ได้มีการเข้ารหัสพร้อมกับมีการเฝ้าระวัง	เปิดให้เข้าถึงแอปพลิเคชันที่มีความสำคัญบางส่วนผ่านเครือข่ายสาธารณะที่มีการเข้ารหัสให้แก่ผู้ใช้งานที่ได้รับอนุญาต และตามความจำเป็น	เปิดให้เข้าถึงแอปพลิเคชันที่มีความสำคัญส่วนใหญ่ผ่านการเชื่อมต่อเครือข่ายสาธารณะที่มีการเข้ารหัส ให้แก่ผู้ใช้งานที่ได้รับอนุญาตและตามความจำเป็น	เปิดให้เข้าถึงแอปพลิเคชันทั้งหมดผ่านเครือข่ายสาธารณะที่มีการเข้ารหัสให้แก่ผู้ใช้งาน และอุปกรณ์ที่ได้รับอนุญาตและตามความจำเป็น
การพัฒนาที่ปลอดภัยและลำดับขั้นตอนในการนำไปใช้	มีสภาพแวดล้อมสำหรับการพัฒนา ทดสอบ และปฏิบัติงานแบบเฉพาะกิจ โดยมีกลไกในการนำโค้ดขึ้นใช้ ที่ขาดความเข้มแข็ง	มีการจัดเตรียมโครงสร้างพื้นฐานสำหรับสภาพแวดล้อมการพัฒนา ทดสอบ และปฏิบัติงาน รวมถึงมีระบบอัตโนมัติที่มีกลไกในการนำโค้ดขึ้นใช้ผ่านกระบวนการ CI/CD และมีการควบคุมการเข้าถึงที่จำเป็นเพื่อสนับสนุนหลักการให้สิทธิเท่าที่จำเป็น	มีการใช้ทีมงานที่แยกส่วน และประสานงานกันระหว่างฝ่ายพัฒนา ฝ่ายความมั่นคงปลอดภัย และฝ่ายปฏิบัติงาน พร้อมทั้งยกเลิกสิทธิการเข้าถึงระบบงานหลักโดยนักพัฒนาเพื่อการนำโค้ดขึ้นใช้งาน	มีการใช้เวิร์กโหลดแบบไม่เปลี่ยนแปลง โดยอนุญาตให้มีการเปลี่ยนแปลงผ่านกรณีการนำขึ้นใช้ใหม่เท่านั้น และยกเลิกสิทธิการเข้าถึงสภาพแวดล้อมการติดตั้งของผู้ดูแลระบบ เพื่อเปลี่ยนไปใช้กระบวนการอัตโนมัติในการนำโค้ดขึ้นใช้งานแทน

ฟังก์ชัน	ดั้งเดิม	เริ่มต้น	พัฒนาแล้ว	ปรับปรุงให้เหมาะสม
การทดสอบความมั่นคงปลอดภัยแอปพลิเคชัน	มีการทดสอบความมั่นคงปลอดภัยของแอปพลิเคชันก่อนการนำขึ้นใช้งาน โดยเน้นใช้วิธีการทดสอบแบบแมนวลเป็นหลัก	เริ่มใช้วิธีการทดสอบทั้งแบบสแตติก และแบบไดนามิกขณะแอปพลิเคชันกำลังทำงาน เพื่อตรวจสอบความมั่นคงปลอดภัย รวมถึงมีการวิเคราะห์โดยผู้เชี่ยวชาญแบบแมนวลก่อนการนำแอปพลิเคชันขึ้นใช้งาน	มีการบูรณาการการทดสอบความมั่นคงปลอดภัยเข้ากับกระบวนการพัฒนาและการนำแอปพลิเคชันขึ้นใช้งานรวมถึงมีการใช้วิธีการทดสอบแบบไดนามิกเป็นระยะ	มีการบูรณาการการทดสอบความมั่นคงปลอดภัยของแอปพลิเคชันทั้งองค์กรเข้ากับวงจรชีวิตการพัฒนาซอฟต์แวร์ พร้อมทั้งมีการทดสอบแอปพลิเคชันที่นำขึ้นใช้งานแล้วแบบอัตโนมัติเป็นประจำ
การมองเห็นและการวิเคราะห์	ดำเนินการตรวจสอบประสิทธิภาพ และความมั่นคงปลอดภัยของแอปพลิเคชันในระบบงานหลักเพียงบางส่วน โดยมีการรวบรวมข้อมูล และการวิเคราะห์ที่จำกัด	เริ่มใช้ระบบอัตโนมัติในการตรวจสอบโพรไฟล์ของแอปพลิเคชัน เช่น สถานะ ความสมบูรณ์ของระบบ และประสิทธิภาพ และความมั่นคงปลอดภัย มีการปรับปรุงการจัดเก็บการรวบรวม และการวิเคราะห์บันทึกเหตุการณ์ให้ดียิ่งขึ้น	เริ่มใช้ระบบอัตโนมัติในการตรวจสอบ โพรไฟล์ และความมั่นคงปลอดภัยของแอปพลิเคชันส่วนใหญ่ โดยใช้หลักการวิเคราะห์เชิงพฤติกรรม เพื่อระบุแนวโน้มทั้งในระดับแอปพลิเคชัน และระดับองค์กร พร้อมทั้งปรับปรุงกระบวนการอย่างต่อเนื่อง เพื่อเพิ่ม	เริ่มดำเนินการตรวจสอบแอปพลิเคชันทั้งหมดอย่างต่อเนื่อง และเป็นแบบไดนามิก เพื่อรักษาความสามารถในการมองเห็นและวิเคราะห์ที่ครอบคลุมทั่วทั้งองค์กร

ฟังก์ชัน	ดั้งเดิม	เริ่มต้น	พัฒนาแล้ว	ปรับปรุงให้เหมาะสม
			ประสิทธิภาพในการรวบรวมข้อมูล	
ระบบอัตโนมัติและการประสานงาน	มีการกำหนดสถานที่จัดเก็บแอปพลิเคชัน และการเข้าถึงแบบสแตติกด้วยกระบวนการแบบแมนวลในขั้นตอนการจัดเตรียมทรัพยากร โดยมีการบำรุงรักษาและการตรวจสอบที่จำกัด	มีการปรับปรุงการตั้งค่าแอปพลิเคชันเป็นระยะ รวมถึงสถานที่จัดเก็บ และการเข้าถึง เพื่อให้บรรลุเป้าหมายด้านความมั่นคง ปลอดภัย และประสิทธิภาพ	มีการใช้ระบบอัตโนมัติในการตั้งค่าแอปพลิเคชันเพื่อตอบสนองต่อการเปลี่ยนแปลงด้านการปฏิบัติงานและสภาพแวดล้อม	มีการใช้ระบบอัตโนมัติในการตั้งค่าแอปพลิเคชันเพื่อเพิ่มประสิทธิภาพ ด้านความมั่นคง ปลอดภัย และประสิทธิภาพของระบบอย่างต่อเนื่อง
การกำกับดูแล	มีการพึ่งพาการบังคับใช้นโยบายแบบแมนวลเป็นหลัก สำหรับการเข้าถึงแอปพลิเคชัน การพัฒนา การนำขึ้นใช้งาน การจัดการซอฟต์แวร์ การทดสอบ และการประเมินความมั่นคงปลอดภัยเมื่อมีการนำเทคโนโลยีใหม่มาใช้	เริ่มใช้ระบบอัตโนมัติในการบังคับใช้นโยบายสำหรับการพัฒนาแอปพลิเคชัน รวมถึงการเข้าถึงโครงสร้างพื้นฐานของแอปพลิเคชันเพื่อการพัฒนา การนำขึ้นใช้งาน การจัดการซอฟต์แวร์ การทดสอบ การอัปเดตแพตช์ และการติดตามตรวจสอบ	มีการบังคับใช้นโยบายแบบแบ่งระดับ และปรับแต่งให้เหมาะสมทั่วทั้งองค์กร ทั้งในส่วนของแอปพลิเคชัน และทุกแง่มุมของวงจรชีวิตของการพัฒนา และการนำแอปพลิเคชันขึ้นใช้งาน พร้อมทั้งนำระบบอัตโนมัติมาใช้ในส่วนที่ทำได้เพื่อสนับสนุน	มีการใช้ระบบอัตโนมัติอย่างเต็มรูปแบบกับนโยบายที่กำกับการพัฒนาและการนำขึ้นใช้งานแอปพลิเคชัน รวมถึงการรวมการอัปเดตแบบไดนามิกสำหรับแอปพลิเคชันผ่านกระบวนการ CI/CD

ฟังก์ชัน	ดั้งเดิม	เริ่มต้น	พัฒนาแล้ว	ปรับปรุงให้เหมาะสม
	มีการอัปเดตแพตช์และมีการติดตามตรวจสอบองค์ประกอบของซอฟต์แวร์	องค์ประกอบของซอฟต์แวร์ โดยอิงตามความจำเป็น (เช่น การใช้บัญชีรายการองค์ประกอบของซอฟต์แวร์)	การบังคับใช้นโยบาย	

ตารางที่ ๔๒ แสดงภาพรวมของเสาหลักแอปพลิเคชันและเวิร์กโหลด

หัวข้อ	สาระสำคัญ
เป้าหมายหลัก	ทำให้แอปพลิเคชันทั้งหมดมีความมั่นคงปลอดภัยตลอดวงจรชีวิต ตั้งแต่การพัฒนา การทดสอบ การนำขึ้นใช้งาน จนถึงการเปิดให้เข้าถึงผ่านเครือข่ายสาธารณะอย่างปลอดภัย ตามหลัก Zero Trust
หลักการสำคัญ	ใช้การควบคุมการเข้าถึงแบบละเอียด ผสานการป้องกันภัยคุกคามเข้ากับแอปพลิเคชันโดยตรง ใช้กระบวนการการพัฒนาแอปพลิเคชัน CI/CD ที่ปลอดภัย และไม่ถือว่าแอปพลิเคชันทั้งหมด “น่าเชื่อถือโดยปริยาย”
การพัฒนา	พัฒนาจากกระบวนการทำงานแบบแมนวล ไปสู่การควบคุมและบังคับใช้นโยบายแบบอัตโนมัติ โดยอิงบริบทและระดับความเสี่ยง
ผลลัพธ์สูงสุด	แอปพลิเคชันทุกตัวถูกตรวจสอบ ป้องกันภัยคุกคาม และปรับใช้นโยบายได้แบบเรียลไทม์ พร้อมการทดสอบและการนำขึ้นใช้งานแบบอัตโนมัติครบถ้วนตลอดทั้งกระบวนการ

ข้อมูล (Data)

วัตถุประสงค์ของเสาหลักข้อมูล

๑) ป้องกันไม่ให้ข้อมูลถูกเข้าถึง ใช้งาน หรือถูกนำออกไปโดยไม่ได้รับอนุญาต

๒) ทำให้ข้อมูลสามารถถูกเข้าถึงได้เฉพาะ ในกรณีที่ตัวตนและบริบทมีความถูกต้องและปลอดภัย

๓) ปรับระดับการปกป้องให้เหมาะสมกับความอ่อนไหวของข้อมูล

๔) มีการเก็บสถานะของข้อมูล และการวิเคราะห์สถานะ เพื่อทำให้มองเห็นว่าข้อมูลถูกใช้อย่างไร

๕) ใช้มาตรการการเข้ารหัส เครื่องมือป้องกันข้อมูล เช่น DLP ครอบคลุมทั้งองค์กร

เพื่อให้บรรลุเป้าหมายนี้ หน่วยงานควรทำ

๑) การจำแนกและติดป้ายข้อมูล

๑.๑) จัดประเภทข้อมูลตามระดับความสำคัญและความอ่อนไหว

๑.๒) ติดป้ายกำกับข้อมูลเพื่อให้ระบบอื่นสามารถบังคับใช้นโยบายได้อย่างถูกต้องและต่อเนื่อง

๒) การควบคุมการเข้าถึงข้อมูล

๒.๑) บังคับใช้นโยบายการเข้าถึงตามหลักการเข้าถึงข้อมูลเท่าที่จำเป็น

๒.๒) อ้างอิงตัวตน อุปกรณ์ เวิร์กโหลด และระดับความอ่อนไหวของข้อมูล

๓) การป้องกันข้อมูล

๓.๑) ใช้มาตรการ เช่น การเข้ารหัส การแปลงข้อมูล การปิดบังข้อมูล (Masking) และ DLP

๓.๒) รวมถึงการป้องกันการนำข้อมูลออกจากระบบโดยไม่ได้รับอนุญาต (Exfiltration Protection)

๔) การมองเห็นและการวิเคราะห์การใช้ข้อมูล

๔.๑) ตรวจสอบว่า ใครเข้าถึงข้อมูลอะไร ถูกใช้งานที่ไหน เมื่อใด และอย่างไร

๔.๒) รองรับการตรวจจับพฤติกรรมผิดปกติที่เกี่ยวข้องกับข้อมูล

๕) การจัดการวงจรชีวิตของข้อมูล (Data Lifecycle Management)

๕.๑) ควบคุมข้อมูลตั้งแต่การสร้าง การใช้งาน การแบ่งปัน การเก็บ ไปจนถึงการทำลาย

๕.๒) ให้มั่นใจว่าทุกขั้นตอนมีความมั่นคงปลอดภัย และเป็นไปตามนโยบาย

๖) ระบบอัตโนมัติและการบังคับใช้นโยบายด้านข้อมูล (Data Automation & Enforcement) บังคับใช้นโยบายด้านข้อมูลแบบอัตโนมัติ เช่น การปิดกั้นการดาวน์โหลดข้อมูลลับเมื่ออุปกรณ์ไม่อยู่ในสถานะที่ปลอดภัย

โดยรายละเอียดระดับความสมบูรณ์ของเสาหลักข้อมูลได้ไว้แสดงดังตารางที่ ๔๓

ตารางที่ ๔๓ แสดงระดับความสมบูรณ์ของเสาหลักข้อมูล

ฟังก์ชัน	ดั้งเดิม	เริ่มต้น	พัฒนาแล้ว	ปรับปรุงให้เหมาะสม
การบริหารจัดการรายการทรัพย์สินของข้อมูล	มีการระบุ และทำบัญชีข้อมูลขององค์กรเพียงบางส่วน เช่น ข้อมูลที่สำคัญ ด้วยกระบวนการแบบแมนวล	มีการเริ่มใช้กระบวนการอัตโนมัติในการทำบัญชีข้อมูลสำหรับทั้งภายในองค์กรและบนคลาวด์ ซึ่งครอบคลุมข้อมูลส่วนใหญ่ขององค์กร และเริ่มนำมาตรการป้องกันข้อมูลรั่วไหล (DLP) มาใช้	มีการใช้ระบบอัตโนมัติในการทำบัญชีข้อมูล และติดตามข้อมูลทั่วทั้งองค์กร ครอบคลุมข้อมูลที่เกี่ยวข้องทั้งหมด และมีกลยุทธ์ในการป้องกันข้อมูลรั่วไหล ที่อิงตามคุณลักษณะของข้อมูลแบบสแตติก หรือมีการติดป้ายกำกับข้อมูล หรือทั้งสองอย่าง	มีการทำบัญชีข้อมูลที่เกี่ยวข้องทั้งหมดอย่างต่อเนื่อง และใช้กลยุทธ์การป้องกันข้อมูลรั่วไหลที่เข้มแข็ง ซึ่งสามารถระงับการพยายามนำข้อมูลออกไปภายนอกที่น่าสงสัยได้แบบไดนามิก
การจัดหมวดหมู่ของข้อมูล	มีการใช้ความสามารถในการจัดหมวดหมู่ข้อมูลอย่างจำกัด และเป็นแบบเฉพาะกิจ	เริ่มนำกลยุทธ์การจัดหมวดหมู่ข้อมูลมาใช้ โดยมีการติดป้ายกำกับข้อมูลที่ชัดเจน และใช้กลไกการบังคับใช้แบบสแตติก	มีการใช้ระบบอัตโนมัติในบางกระบวนการในการจัดหมวดหมู่ และมีการติดป้ายกำกับข้อมูล อย่างเป็นระบบ สอดคล้องกัน และมีเป้าหมายในการจัดรูปแบบของข้อมูลเป็นโครงสร้างอย่างง่าย และมีการทบทวนอย่างสม่ำเสมอ	มีการใช้ระบบอัตโนมัติในการจัดหมวดหมู่ และติดป้ายกำกับข้อมูลทั่วทั้งองค์กรด้วยเทคนิคที่เข้มแข็ง มีรูปแบบโครงสร้างข้อมูลที่ละเอียดและชัดเจน และมีกลไกที่สามารถจัดการข้อมูลได้ทุกประเภท

ฟังก์ชัน	ดั้งเดิม	เริ่มต้น	พัฒนาแล้ว	ปรับปรุงให้เหมาะสม
ความพร้อมใช้งานของข้อมูล	การให้บริการข้อมูลจากแหล่งจัดเก็บข้อมูลภายในองค์กรเป็นหลัก และมีการสำรองข้อมูลไว้นอกสถานที่เพียงบางส่วน	เริ่มให้สามารถเข้าถึงข้อมูลจากแหล่งจัดเก็บข้อมูลสำรอง ที่มีความพร้อมใช้งานสูง เช่น ระบบคลาวด์ และมีการสำรองข้อมูลไว้นอกสถานที่	มีความสามารถให้บริการข้อมูลจากแหล่งจัดเก็บข้อมูลสำรองได้สมบูรณ์ มีความพร้อมใช้งานสูง และรับประกันความสามารถในการเข้าถึงข้อมูลย้อนหลัง	มีการใช้วิธีการแบบไดนามิกเพื่อเพิ่มประสิทธิภาพของความพร้อมใช้งานของข้อมูล รวมถึงการเข้าถึงข้อมูลย้อนหลัง ตามความต้องการของผู้ใช้งาน
การเข้าถึงข้อมูล	การเข้าถึงข้อมูลของผู้ใช้งาน เช่น การอ่าน เขียนคัดลอก การมอบสิทธิให้ผู้อื่น ฯลฯ มีการควบคุมแบบสแตติก	เริ่มใช้การควบคุมการเข้าถึงข้อมูลแบบอัตโนมัติที่นำหลักการให้สิทธิเท่าที่จำเป็นมาปรับใช้ทั่วทั้งองค์กร	มีการใช้ระบบอัตโนมัติในการควบคุมการเข้าถึงข้อมูล โดยพิจารณาจากแอตทริบิวต์ต่างๆ เช่น ตัวตน ความเสี่ยงของอุปกรณ์ แอปพลิเคชัน หมวดหมู่ของข้อมูล และอื่น ๆ พร้อมทั้งมีการจำกัดเวลาการเข้าถึงให้เหมาะสม	มีการใช้ระบบอัตโนมัติในการควบคุมการเข้าถึงข้อมูลแบบไดนามิกทั้งเวลาที่ต้องใช้และสิทธิเท่าที่จำเป็นทั่วทั้งองค์กร พร้อมทั้งมีการตรวจสอบสิทธิการเข้าถึงอย่างต่อเนื่อง
การเข้ารหัสข้อมูล	มีการเข้ารหัสข้อมูลขององค์กรเพียงส่วนน้อยทั้งในขณะจัดเก็บข้อมูล และระหว่างการส่งข้อมูล โดยพึ่งพาคนหรือกระบวนการ	มีการเข้ารหัสข้อมูลทั้งหมดทั้งในขณะจัดเก็บและระหว่างการส่งข้อมูล เช่น ข้อมูลที่สำคัญ และข้อมูลที่ต้องจัดเก็บภายนอก พร้อมเริ่ม	มีการเข้ารหัสข้อมูลทั้งหมด ทั้งในขณะจัดเก็บข้อมูล และระหว่างการส่งข้อมูลทั่วทั้งองค์กรให้มากที่สุดเท่าที่จะทำได้ เริ่มมีความ	มีการเข้ารหัสข้อมูลในขณะใช้งานที่เหมาะสม บังคับใช้หลักการให้สิทธิเท่าที่จำเป็นสำหรับการจัดการกุญแจเข้ารหัสที่ปลอดภัย

ฟังก์ชัน	ดั้งเดิม	เริ่มต้น	พัฒนาแล้ว	ปรับปรุงให้เหมาะสม
	แบบแมนวลในการจัดการ และปกป้องกุญแจเข้ารหัส	กำหนดนโยบายการจัดการกุญแจเข้ารหัสให้เป็นทางการ และมั่นคงปลอดภัย	ยืดหยุ่นในการเข้ารหัส และการปกป้องกุญแจเข้ารหัส เช่น ไม่ฝังรหัสไว้ในโค้ด และมีการเปลี่ยนกุญแจรหัสเป็นประจำ	ทั่วทั้งองค์กร และใช้การเข้ารหัสที่มีมาตรฐานและทันสมัยรวมทั้งมีความยืดหยุ่นในการเข้ารหัสอย่างเต็มประสิทธิภาพ
การมองเห็นและการวิเคราะห์	มีความสามารถในการมองเห็นข้อมูลอย่างจำกัด ทั้งในเรื่องสถานที่จัดเก็บ การเข้าถึง และการใช้งาน โดยการวิเคราะห์ส่วนใหญ่ใช้กระบวนการแบบแมนวล	มีความสามารถในการมองเห็นข้อมูลในคลังข้อมูล การจัดหมวดหมู่ การเข้ารหัส และความพยายามในการเข้าถึงข้อมูล พร้อมทั้งมีการวิเคราะห์และการหาความสัมพันธ์ของข้อมูลแบบอัตโนมัติบางส่วน	มีความสามารถมองเห็นข้อมูลที่ครอบคลุมมากขึ้นทั่วทั้งองค์กร ใช้การวิเคราะห์ และการหาความสัมพันธ์ของข้อมูลแบบอัตโนมัติ และเริ่มนำการวิเคราะห์เชิงพยากรณ์มาใช้	มีความสามารถมองเห็นข้อมูลครอบคลุมตลอดวงจรชีวิตของข้อมูล พร้อมการวิเคราะห์ที่เข้มแข็ง รวมถึงการวิเคราะห์เชิงพยากรณ์ที่ครอบคลุมข้อมูลขององค์กรอย่างครบถ้วน และมีการประเมินสถานะความมั่นคงปลอดภัยอย่างต่อเนื่อง
ระบบอัตโนมัติและการประสานงาน	มีการบังคับใช้นโยบายความมั่นคงปลอดภัย และกำหนดวงจรชีวิตของข้อมูล เช่น การเข้าถึง	มีการใช้กระบวนการอัตโนมัติในบางส่วนเพื่อบังคับใช้นโยบายความมั่นคง	มีการบังคับใช้นโยบายความมั่นคงปลอดภัย และวงจรชีวิตของข้อมูลผ่านวิธีการอัตโนมัติเป็นหลัก สำหรับข้อมูล	มีการใช้ระบบอัตโนมัติอย่างเต็มประสิทธิภาพเท่าที่ทำได้ ในการจัดการวงจรชีวิตของข้อมูล และนโยบายความ

ฟังก์ชัน	ดั้งเดิม	เริ่มต้น	พัฒนาแล้ว	ปรับปรุงให้เหมาะสม
	การใช้งาน การจัดเก็บ การเข้ารหัส การตั้งค่า การป้องกัน การสำรองข้อมูล การจัดหมวดหมู่ การทำลายข้อมูลผ่านกระบวน การแบบแมนวล และเป็นแบบเฉพาะกิจ	ปลอดภัย และวงจรชีวิตของข้อมูล	ส่วนใหญ่ขององค์กรอย่างเป็นระบบสอดคล้องกัน และมีการแบ่งชั้นข้อมูลอย่างเหมาะสมทั่วทั้งองค์กร	มั่นคงปลอดภัยสำหรับข้อมูลทั้งหมดขององค์กร
การกำกับดูแล	มีการกำหนดนโยบายการกำกับดูแลข้อมูลแบบเฉพาะกิจ เช่น นโยบายการป้องกัน การจัดหมวดหมู่ การเข้าถึง การทำบัญชี การจัดเก็บ การกู้คืน การลบข้อมูล ฯลฯ โดยมีการบังคับใช้แบบแมนวล	มีการกำหนดนโยบายการกำกับดูแลข้อมูลในระดับสูง ด้วยกระบวนการแบบแมนวลเป็นหลัก และนำไปใช้แบบแบ่งเป็นส่วน	เริ่มมีการบูรณาการการบังคับใช้นโยบายวงจรชีวิตของข้อมูลทั่วทั้งองค์กร ซึ่งช่วยให้การกำหนดนโยบายในการกำกับดูแลข้อมูลมีความเป็นมาตรฐานเดียวกันมากขึ้น	วงจรชีวิตข้อมูลมีความเป็นมาตรฐานเดียวกันอย่างสูงสุดเท่าที่จะเป็นไปได้ มีการบังคับใช้นโยบายทั่วทั้งองค์กรแบบไดนามิก และมีการกำกับดูแลข้อมูลที่เป็นมาตรฐานเดียวกันทั่วทั้งองค์กร

ตารางที่ ๔๔ แสดงภาพรวมของเสาหลักข้อมูล

หัวข้อ	สาระสำคัญ
เป้าหมายหลัก	ปกป้องข้อมูลทุกประเภทในทุกสภาพแวดล้อม และควบคุมการเข้าถึงข้อมูลโดยอิงบริบทและระดับความอ่อนไหวของข้อมูล
หลักการสำคัญ	จัดประเภทข้อมูลอย่างเป็นระบบ ใช้หลักการให้สิทธิเท่าที่จำเป็น ร่วมกับการเข้ารหัสข้อมูล ระบบป้องกันข้อมูลรั่วไหล (DLP) การควบคุมการเข้าถึงตามคุณลักษณะ และการตรวจสอบอย่างต่อเนื่อง
การพัฒนา	พัฒนาจากการปกป้องข้อมูลด้วยกระบวนการแบบแมนนวล ไปสู่การจัดการและบังคับใช้นโยบายด้านข้อมูลแบบอัตโนมัติ ครอบคลุมตลอดวงจรชีวิตของข้อมูล
ผลลัพธ์สูงสุด	องค์กรสามารถตรวจจับ ป้องกัน และบังคับใช้นโยบายด้านข้อมูลได้แบบเรียลไทม์ ด้วยระบบอัตโนมัติที่ทำงานครบวงจร

ความสามารถเชิงบูรณาการ

ความสามารถเชิงบูรณาการ เป็นกลไกสำคัญที่ช่วยบูรณาการการทำงานของ ๕ เสาหลักประสานร่วมกันเพื่อยกระดับศักยภาพโดยรวมขององค์กร ทุกเสาหลักควรถูกนำมาบูรณาการร่วมกัน ดังต่อไปนี้

๑) การมองเห็นและการวิเคราะห์ ช่วยให้หน่วยงานสามารถมองเห็นข้อมูลและสถานการณ์ได้อย่างครอบคลุม สนับสนุนการกำหนดนโยบาย การตัดสินใจ และการดำเนินการตอบสนองต่อเหตุการณ์ต่าง ๆ ได้อย่างมีประสิทธิภาพ

๒) ระบบอัตโนมัติและการประสานงาน นำข้อมูลเชิงลึกจากการวิเคราะห์มาใช้เพื่อสนับสนุนการปฏิบัติงานด้านความมั่นคงปลอดภัยให้มีความเป็นระบบ คล่องตัว ประสานการทำงานร่วมกัน ให้มีประสิทธิภาพสูงขึ้น โดยสามารถรองรับการจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยและการตอบสนองต่อเหตุการณ์ที่เกิดขึ้นได้อย่างทันท่วงที

๓) การกำกับดูแล ช่วยให้หน่วยงานสามารถบริหารจัดการและติดตามข้อกำหนดด้านกฎหมาย กฎระเบียบ สิ่งแวดล้อม มาตรฐานภาครัฐ และข้อกำหนดทางปฏิบัติการ เพื่อสนับสนุนการตัดสินใจบนพื้นฐานความเสี่ยง นอกจากนี้ความสามารถด้านการกำกับดูแล ยังช่วยให้มั่นใจได้ว่ามีบุคลากร กระบวนการและเทคโนโลยีที่เหมาะสมรองรับพันธกิจ การบริหารความเสี่ยง และเป้าหมายด้านการปฏิบัติตามข้อกำหนดอย่างครบถ้วน โดยรายละเอียดระดับความสมบูรณ์ของความสามารถเชิงบูรณาการได้ไว้แสดงดังตารางที่ ๔๕

ตารางที่ ๔๕ แสดงระดับความสมบูรณ์ของความสามารถเชิงบูรณาการ

ฟังก์ชัน	ดั้งเดิม	เริ่มต้น	พัฒนาแล้ว	ปรับปรุงให้เหมาะสม
การมองเห็นและการวิเคราะห์	มีการเก็บรวบรวมบันทึกเหตุการณ์จำนวนจำกัด โดยข้อมูลไม่มีความชัดเจน และมีการวิเคราะห์เพียงเล็กน้อย	เริ่มใช้ระบบอัตโนมัติในการดำเนินการรวบรวมและวิเคราะห์บันทึกเหตุการณ์และเหตุการณ์ต่างๆ ที่มีฟังก์ชันที่สำคัญต่อภารกิจ และมีการประเมินกระบวนการเป็นประจำเพื่อหาข้อผิดพลาดในการมองเห็นข้อมูล	มีการขยายการรวบรวมบันทึกเหตุการณ์ และเหตุการณ์ต่าง ๆ แบบอัตโนมัติให้ครอบคลุมสภาพแวดล้อมทั่วทั้งองค์กร เพื่อการวิเคราะห์แบบรวมศูนย์ที่เชื่อมโยงกันระหว่างหลายแหล่งที่มาของข้อมูล เช่น คลาวด์ อุปกรณ์ปลายทาง ฯลฯ	มีการรักษาความสามารถในการมองเห็นภาพรวมขององค์กรได้อย่างครอบคลุม ผ่านการตรวจสอบแบบไดนามิกจากส่วนกลาง และการวิเคราะห์ข้อมูลบันทึกเหตุการณ์ขั้นสูงของเหตุการณ์ทั่วทั้งองค์กร
ระบบอัตโนมัติและการประสานงาน	ใช้กระบวนการแบบสแตติกเป็นหลักในการประสานการดำเนินงาน และการตอบสนองต่อเหตุการณ์ เช่น ภัยคุกคาม ฯลฯ โดยมีการนำระบบอัตโนมัติมาใช้ในวงจำกัด	มีการเริ่มดำเนินการแบบอัตโนมัติกับการประสานงานและการตอบสนองภัยคุกคาม เพื่อสนับสนุนภารกิจที่สำคัญ	มีการเริ่มดำเนินการประสานงาน และตอบสนองต่อเหตุการณ์ ทั่วทั้งองค์กรโดยอัตโนมัติ โดยใช้ประโยชน์จากข้อมูลเชิงบริบทจากหลายแหล่งในการประกอบการตัดสินใจ	การประสานงานและตอบสนองต่อเหตุการณ์ทั่วทั้งองค์กรแบบไดนามิก ตามการเปลี่ยนแปลงของสิ่งแวดล้อมในองค์กร
การกำกับดูแล	มีนโยบายสำหรับการบังคับใช้การกำกับดูแลแบบ	มีการกำหนด และเริ่มดำเนินการนโยบายสำหรับการ	มีการกำหนด และบังคับใช้นโยบายแบบแบ่งระดับ และ	มีการกำหนดนโยบายระดับองค์กรแบบ

ฟังก์ชัน	ดั้งเดิม	เริ่มต้น	พัฒนาแล้ว	ปรับปรุงให้เหมาะสม
	เฉพาะกิจทั่วทั้งองค์กร โดยบังคับใช้ผ่านกระบวนการแบบแมนวล หรือกลไกทางเทคนิคแบบสแตติก	บังคับใช้การกำกับดูแลด้วยระบบอัตโนมัติอย่างจำกัด และยังคงมีการอัปเดตแบบแมนวลเป็นหลัก	ปรับให้เหมาะสมกับส่วนต่าง ๆ ทั่วทั้งองค์กร พร้อมทั้งนำระบบอัตโนมัติมาใช้เพื่อสนับสนุนการกำกับดูแลเท่าที่สามารถดำเนินการได้ โดยการพิจารณานโยบายด้านการเข้าถึงระบบจะอาศัยข้อมูลเชิงบริบทจากหลายแหล่งที่มาประกอบการตัดสินใจ	อัตโนมัติอย่างสมบูรณ์ ซึ่งช่วยให้สามารถควบคุมภาพรวมทั้งระบบได้อย่างเหมาะสม พร้อมการบังคับใช้อย่างต่อเนื่อง และมีการอัปเดตแบบไดนามิก

เอกสารอ้างอิง

Cybersecurity and Infrastructure Security Agency (CISA), Zero Trust Maturity Model, Version 2.0, 2023

ผนวก ง อภิธานศัพท์

ผู้จัดทำได้รวบรวบคำศัพท์ภาษาอังกฤษ คำแปลภาษาไทย และคำอธิบายดังแสดงในตารางที่ ๔๖ เพื่อเป็นข้อมูลให้กับผู้อ่านประกอบการอ่านเนื้อหาในแนวปฏิบัติฉบับนี้ได้โดยสะดวกและมีความเข้าใจตรงตามที่ผู้จัดทำต้องการสื่อสาร ทั้งนี้อภิธานศัพท์นี้ไม่สามารถนำไปใช้ทดแทนอภิธานศัพท์ที่ปรากฏในเอกสารอื่น ๆ หรือใช้อ้างอิงเป็นคำศัพท์และคำอธิบายทางการได้

ตารางที่ ๔๖ แสดงอภิธานศัพท์คำศัพท์และความหมาย

คำศัพท์ภาษาอังกฤษ	ตัวย่อ	คำศัพท์ภาษาไทย	คำอธิบาย
Authentication	-	การยืนยันตัวตน	กระบวนการตรวจสอบว่าผู้ใช้หรืออุปกรณ์เป็นตัวตนที่อ้างจริงก่อนให้เข้าถึงระบบหรือทรัพยากร
Authorization	-	การกำหนดสิทธิ	กระบวนการกำหนดสิทธิการเข้าถึงทรัพยากรหลังจากผ่านการยืนยันตัวตนแล้ว
Bring Your Own Device	BYOD	การนำอุปกรณ์ส่วนตัวมาใช้ในที่ทำงาน	นโยบายที่อนุญาตให้พนักงานนำอุปกรณ์ส่วนตัวมาใช้ในการทำงานและเข้าถึงทรัพยากรขององค์กร
Cloud Access Security Broker	CASB	ระบบบริการตัวกลางควบคุมความมั่นคงปลอดภัยการเข้าถึงบริการคลาวด์	โซลูชันด้านการรักษาความมั่นคงปลอดภัย สำหรับควบคุมและตรวจสอบการใช้งานแอปพลิเคชันแบบ SaaS
Continuous Diagnostics and Mitigations	CDM	ระบบจัดการความมั่นคงปลอดภัยเชิงต่อเนื่อง	แนวทางติดตาม ประเมิน และลดความเสี่ยงด้านความมั่นคงปลอดภัยของอุปกรณ์อย่างต่อเนื่อง เพื่อตรวจสอบสถานะด้านความมั่นคงปลอดภัยของอุปกรณ์อยู่เสมอ

คำศัพท์ภาษาอังกฤษ	ตัวย่อ	คำศัพท์ภาษาไทย	คำอธิบาย
Continuous Verification	-	การตรวจสอบอย่างต่อเนื่อง	กระบวนการตรวจสอบสิทธิและสถานะความปลอดภัยของผู้ใช้และอุปกรณ์ตลอดระยะเวลาการเชื่อมต่อ
Distributed Denial of Service	DDoS	การโจมตีเพื่อขัดขวางการให้บริการแบบกระจาย	การโจมตีจากหลายจุดเพื่อทำให้ระบบหรือบริการทำงานช้าลงหรือไม่สามารถให้บริการได้
Endpoint Security Posture Management	ESPM	ระบบจัดการสถานะความปลอดภัยของอุปกรณ์ปลายทาง	ระบบที่ ควบคุม ประเมิน และตรวจสอบความมั่นคงปลอดภัยของอุปกรณ์ปลายทางอย่างต่อเนื่องเพื่อให้สอดคล้องกับนโยบายขององค์กร
Enhanced Identity Governance	-	แนวทางการกำกับดูแลตัวตนขั้นสูง	แนวทางกำกับดูแลการเข้าถึงในสถาปัตยกรรม Zero Trust ที่ใช้ตัวตนและบริบทแวดล้อมเป็นฐานในการประเมินความน่าเชื่อถือและกำหนดสิทธิอย่างเหมาะสม
Infrastructure-as-a-Service	IaaS	โครงสร้างพื้นฐานในรูปแบบบริการ	รูปแบบการให้บริการบนคลาวด์ที่จัดเตรียมทรัพยากรโครงสร้างพื้นฐานด้านไอที เช่น เครื่องแม่ข่ายเสมือน หน่วยเก็บข้อมูลบนคลาวด์ และระบบเครือข่ายเสมือน ที่ผู้ใช้สามารถกำหนดค่าและบริหารจัดการได้ด้วยตนเองผ่านอินเทอร์เน็ต
Identity	-	ตัวตน	ข้อมูลที่ใช้ระบุตัวตนของผู้ใช้หรืออุปกรณ์ เพื่อใช้ในการตัดสินใจ

คำศัพท์ภาษาอังกฤษ	ตัวย่อ	คำศัพท์ภาษาไทย	คำอธิบาย
			เพื่ออนุญาตและกำกับสิทธิการเข้าถึง
Identity Provider	IdP	ผู้ให้บริการยืนยันตัวตน	ผู้ให้บริการยืนยันตัวตนและออกใบรับรองดิจิทัล เพื่อใช้ในการเข้าถึงระบบหรือบริการ
Intrusion Prevention System	IPS	ระบบป้องกันการบุกรุก	ระบบความปลอดภัยที่ทำหน้าที่เฝ้าระวัง ตรวจสอบ และป้องกันการโจมตีหรือกิจกรรมที่ผิดปกติบนเครือข่ายโดยอัตโนมัติ
Least Privilege	-	การกำหนดสิทธิเท่าที่จำเป็น	หลักการความปลอดภัยที่จำกัดสิทธิการเข้าถึงของผู้ใช้หรืออุปกรณ์ให้มีเพียงเท่าที่จำเป็นต่อการปฏิบัติงานเท่านั้น
Lateral Movement	-	การโจมตีแบบการเคลื่อนตัวในเครือข่าย	เทคนิคการโจมตีที่ผู้โจมตีขยายขอบเขตการเข้าถึงจากระบบหนึ่งไปยังอีกระบบหนึ่งเพื่อเพิ่มสิทธิหรือเข้าถึงทรัพยากรที่มีความสำคัญ
Micro-Perimeter	-	ไมโครเพอริมิเตอร์	การแบ่งขอบเขตความปลอดภัยให้มีขนาดเล็กและเฉพาะเจาะจงรอบ ๆ ทรัพยากรหรือแอปพลิเคชันที่มีลักษณะคล้ายคลึงกัน
Micro-Segmentation	-	การแบ่งส่วนเครือข่ายแบบย่อย	การแบ่งเครือข่ายออกเป็นส่วนย่อยตามลักษณะงานหรือทรัพยากรเพื่อควบคุมการเข้าถึงระหว่างเครือข่ายย่อย และลดความเสี่ยงจากการเข้าถึงที่ไม่จำเป็นหรือเกินขอบเขตที่กำหนด

คำศัพท์ภาษาอังกฤษ	ตัวย่อ	คำศัพท์ภาษาไทย	คำอธิบาย
Multi-Factor Authentication	MFA	การยืนยันตัวตนแบบหลายปัจจัย	การยืนยันตัวตนที่ต้องใช้ปัจจัยมากกว่าหนึ่งประเภท เพื่อเพิ่มความมั่นใจและความปลอดภัยในการเข้าถึงระบบ
mutual Transport Layer Security	mTLS	การเข้ารหัสแบบการยืนยันตัวตนแบบสองทางด้วย TLS	การเข้ารหัสการสื่อสารพร้อมการยืนยันตัวตนแบบสองทางระหว่างเครื่องลูกข่ายและเครื่องแม่ข่ายโดยใช้ใบรับรองดิจิทัลผ่านโปรโตคอล TLS
Operational Technology	OT	เทคโนโลยีเชิงปฏิบัติการ	เทคโนโลยีที่ใช้ควบคุม ตรวจวัด หรือปฏิบัติการกับกระบวนการทางกายภาพในอุตสาหกรรมหรือโครงสร้างพื้นฐาน
Policy Administrator	PA	ส่วนบริหารนโยบาย	ส่วนบริหารนโยบายที่ควบคุมสั่งการจุดบังคับใช้นโยบายให้ดำเนินการตามข้อกำหนดการเข้าถึงขององค์กร เช่น การอนุญาตหรือปฏิเสธการเข้าถึง
Policy Decision Point	PDP	จุดตัดสินใจตามนโยบาย	ส่วนที่ทำหน้าที่ประเมินข้อมูลและบริบทของผู้ร้องขอและตัดสินใจอนุญาตหรือปฏิเสธตามนโยบายการเข้าถึง
Policy Enforcement Point	PEP	จุดบังคับใช้นโยบาย	ส่วนที่บังคับใช้นโยบายโดยเปิดใช้งาน ตรวจสอบ หรือยุติการเข้าถึงตามคำสั่งของจุดตัดสินใจตามนโยบาย ซึ่งอาศัยผลการตัดสินใจจากจุดตัดสินใจตามนโยบาย
Policy Engine	PE	ส่วนขับเคลื่อนนโยบาย	ส่วนที่ทำหน้าที่ประเมินนโยบายและข้อมูลประกอบเพื่อกำหนดว่า

คำศัพท์ภาษาอังกฤษ	ตัวย่อ	คำศัพท์ภาษาไทย	คำอธิบาย
			ผู้ร้องขอจะได้รับอนุญาตให้เข้าถึงทรัพยากรขององค์กรหรือไม่ โดยจะสั่งการไปยังจุดบังคับใช้นโยบายต่อไป
Pre-vetting	-	กระบวนการตรวจสอบล่วงหน้า	กระบวนการตรวจสอบล่วงหน้าที่ใช้ยืนยันความถูกต้องและความน่าเชื่อถือของผู้ร้องขอก่อนอนุญาตให้สร้างการเชื่อมต่อกับเครื่องปลายทางหรือบริการในระบบ SDP
SDP Controller	-	ศูนย์ควบคุมการเชื่อมต่อ SDP	ศูนย์ควบคุมการเชื่อมต่อที่ทำหน้าที่ตรวจสอบและยืนยันตัวตน ยืนยันอุปกรณ์ และดำเนินกระบวนการตรวจสอบล่วงหน้าก่อนอนุญาตให้เริ่มต้นเซสชันหรือเปิดเผยบริการ
SDP Gateway	-	เกตเวย์ SDP	จุดบังคับใช้นโยบายที่ควบคุมการเชื่อมต่อไปยังบริการที่ไม่ปรากฏต่อสาธารณะ โดยอนุญาตเฉพาะผู้ใช้และอุปกรณ์ที่ผ่านการตรวจสอบแล้ว พร้อมรองรับการตรวจสอบด้านความมั่นคงปลอดภัยและการบันทึกการเชื่อมต่อ
Security Information and Event Management	SIEM	ระบบจัดการข้อมูลและเหตุการณ์ด้านความมั่นคงปลอดภัย	ระบบรวบรวม จัดเก็บ และวิเคราะห์เหตุการณ์ด้านความมั่นคงปลอดภัยจากหลายแหล่งเพื่อช่วยตรวจจับความผิดปกติ

คำศัพท์ภาษาอังกฤษ	ตัวย่อ	คำศัพท์ภาษาไทย	คำอธิบาย
			และแจ้งเตือนเหตุการณ์ที่อาจเป็นภัยคุกคาม
Secure Web Gateway	SWG	เกตเวย์ควบคุมความมั่นคงปลอดภัยการใช้งานเว็บไซต์	โซลูชันด้านความมั่นคงปลอดภัยที่กรองการรับส่งข้อมูลเว็บ เพื่อป้องกันภัยคุกคามและบังคับใช้นโยบายการใช้งานอินเทอร์เน็ต
Single Sign-On	SSO	การยืนยันตัวตนครั้งเดียว	บริการที่ช่วยให้ผู้ใช้งานทำการยืนยันตัวตนเพียงครั้งเดียว แต่สามารถเข้าถึงแอปพลิเคชันหลายแอปพลิเคชันที่เกี่ยวข้องได้โดยไม่ต้องยืนยันตัวตนซ้ำ
Single Packet Authorization	SPA	กระบวนการอนุญาตสิทธิด้วยแพ็กเก็ตเดียว	กระบวนการตรวจสอบสิทธิก่อนเริ่มต้นการสื่อสารที่มีการเข้ารหัสและสามารถตรวจสอบ และยืนยันแหล่งที่มา ตัวตน และสิทธิของผู้ร้องขอก่อนเปิดเผยบริการที่ไม่ปรากฏต่อสาธารณะ
Software-as-a-Service	SaaS	ซอฟต์แวร์ในรูปแบบบริการ	รูปแบบการให้บริการซอฟต์แวร์บนระบบคลาวด์ ที่ผู้ใช้สามารถเข้าถึงและใช้งานได้โดยไม่ต้องติดตั้ง ดูแล หรือจัดการโครงสร้างพื้นฐานด้วยตนเอง
Software-Defined Perimeter	SDP	แนวทางการแบ่งขอบเขตเครือข่ายที่กำหนดด้วยซอฟต์แวร์	สถาปัตยกรรมควบคุมการเข้าถึงเครือข่ายตามแนวคิดของ CSA ที่บังคับใช้หลัก Zero Trust โดยทำให้บริการไม่ปรากฏต่อสาธารณะเป็นค่าเริ่มต้น และอนุญาตให้เข้าถึงได้เมื่อผ่านการยืนยันตัวตนและมีสิทธิในการเข้าถึง

คำศัพท์ภาษาอังกฤษ	ตัวย่อ	คำศัพท์ภาษาไทย	คำอธิบาย
Threat Intelligence	TI	ข้อมูลข่าวกรองด้านภัยคุกคาม	ข้อมูลข่าวกรองด้านภัยคุกคามที่ช่วยให้เข้าใจรูปแบบ แหล่งที่มา และความเสี่ยงของการโจมตีเพื่อใช้ในการเตรียมการป้องกันอย่างเหมาะสม และรู้ถึงภัยคุกคามรูปแบบใหม่
Trust Zone	-	พื้นที่ที่เชื่อถือได้	พื้นที่หรือขอบเขตของระบบที่ได้รับการกำหนดให้เชื่อถือได้ตามระดับความเสี่ยงและนโยบายการเข้าถึงขององค์กร
Untrust Zone	-	พื้นที่ที่ไม่น่าเชื่อถือ	พื้นที่หรือขอบเขตของระบบที่ยังไม่ได้รับความเชื่อถือหรือไม่เป็นที่ไว้วางใจตามระดับความเสี่ยง นโยบายการเข้าถึงขององค์กร
User and Entity Behavior Analytics	UEBA	การวิเคราะห์พฤติกรรมผู้ใช้และเอนทิตี	การใช้เทคโนโลยีวิเคราะห์ข้อมูลเพื่อวิเคราะห์ความผิดปกติของพฤติกรรมของผู้ใช้งานหรืออุปกรณ์ที่อาจบ่งบอกถึงการเป็นภัยคุกคาม
Virtual Private Network	VPN	ระบบเครือข่ายส่วนตัวเสมือน	เทคโนโลยีที่สร้างช่องทางการสื่อสารที่เข้ารหัสผ่านเครือข่ายสาธารณะ เพื่อเชื่อมต่อเข้ากับเครือข่ายภายในองค์กร