



สถาปัตยกรรมแบบ Zero Trust คืออะไร และจะนำมาใช้อย่างไร



สารบัญ

สถาปัตยกรรมแบบ zero trust คืออะไร?	3
การแบ่งเซกเมนต์ระดับมาโครและไมโคร	5
เหตุที่ต้องใช้ทั้งสองระดับ	6
การนำมาใช้	7
วิธีการ	7
ท้ายสุด	12
ทำไมต้อง ALE?	12
สิ่งที่ได้เรียนรู้	13



สถาปัตยกรรมแบบ zero trust คืออะไร?

ก่อนอื่น เราต้องทำความเข้าใจเสียก่อนว่าสถาปัตยกรรมแบบ zero trust (ZTA) นั้นคืออะไร ความหมายของ ZTA นั้นหมายความว่าผู้ใช้ทุกคนและอุปกรณ์ทุกเครื่องจะต้องผ่านการยืนยันตัวตนก่อนที่จะได้รับอนุญาตให้เข้าถึงข้อมูลได้ หรือถ้าอธิบายในอีกแง่หนึ่ง ZTA นั้นจะไม่ไว้วางใจใครทั้งสิ้นและจะตรวจสอบทุก ๆ อย่าง

เปรียบเปรยให้เข้าใจง่ายขึ้น

ถ้าเราเปรียบระบบรักษาความปลอดภัยแบบดั้งเดิมเป็นป้อมปราการที่ปกป้องหมู่บ้านแห่งหนึ่ง เราจะต้องสร้างกำแพงของป้อม (Firewall) ล้อมรอบหมู่บ้าน (องค์กร) เอาไว้ สิ่งแปลกปลอมจากภายนอกนั้นไม่น่าไว้วางใจและจะต้องถูกตรวจสอบอย่างถี่ถ้วน ส่วนอะไรก็แล้วแต่ที่อยู่ภายในป้อมปราการนั้นถือว่าเป็นสิ่งที่เชื่อถือได้และได้รับการอนุญาตไปโดยปริยาย ความไว้วางใจนี้เป็นที่เข้าใจตรงกันระหว่างคนที่ถูกแบ่งกันอยู่คนละฝั่งของกำแพง トラバดที่คุณอยู่ภายใน เราก็ไม่จำเป็นต้องตรวจสอบหรือสอบสวนคุณแต่ประการใด หากเรามองเครือข่ายภายในองค์กรด้วยมุมมองแบบนี้ กำแพงที่ทำหน้าที่แบ่งกันในระดับเบื้องต้นก็คือ VLAN, SSID, subnet หรืออินเทอร์เน็ตเฟสต่าง ๆ ที่ผูกอยู่กับ Firewall แต่กำแพงกันเหล่านี้มันไม่มีความยืดหยุ่น และถูกออกแบบมาเพื่อให้ยากก็การขยายขนาดของเครือข่ายและการบริหารจัดการเสียมากกว่า โดยมีได้คำนึงความปลอดภัยเป็นจุดประสงค์หลัก

แต่ในปัจจุบันนี้ การรักษาความปลอดภัยด้วย Firewall (ป้อมปราการ) นั้นเริ่มมีประสิทธิภาพน้อยลงทุกวัน ด้วยสาเหตุหลายประการ ประการแรกคือความคล่องตัว การที่ผู้ใช้เชื่อมต่อเข้ากับเครือข่ายอื่น ๆ ภายนอกองค์กรนั้นอาจจะนำภัยมาให้ได้ ประการที่สอง บุคคลภายนอกนั้นใช้ว่าจะไว้วางใจได้เสมอไป บางคนบอกว่าแม้แต่กับพนักงานเอง (คนในป้อมปราการ) เราก็ควรจะต้องระวังเอาไว้เสียบ้าง ประการที่สาม อุปกรณ์ IoT (Internet of Things) เริ่มถูกนำมาเชื่อมต่อเข้ากับเครือข่ายกันมากขึ้น อุปกรณ์ประเภทดังกล่าวมีความเสี่ยงด้านความปลอดภัยสูง เพราะฝ่าย IT อาจจะไม่ได้อนุญาตหรือบริหารจัดการอุปกรณ์เหล่านี้ นอกจากนี้พวกมันก็มักจะไม่มีระบบรักษาความปลอดภัยในตัวด้วย หากเรายังใช้วิธีการรักษาความปลอดภัยแบบ 'ป้อมปราการ' หรือ 'Firewall ปกป้ององค์กร' อย่างที่ใช้กันมาตลอดนั้น หากมีผู้ใดคนใดหรืออุปกรณ์เครื่องใดถูกโจมตี ก็แทบจะไม่มีอะไรเลยที่สามารถป้องกันไม่ให้ความเสียหายลุกลามไปยังผู้ใช้อื่นหรืออุปกรณ์เครื่องอื่น เมื่อภัยนั้นเจาะระบบเข้ามาได้ มันก็มีอิสระจะทำอะไรก็ได้ตามใจชอบ

หากคุณป้องกันหมู่บ้านด้วยป้อมปราการ สักวันข้าศึกก็จะเรียนรู้วิธีปีนกำแพงป้อม และเมื่อวันนั้นมาถึง ความเสียหายอย่างใหญ่หลวงจะมาเยือน





แล้วเราจะแก้ไขปัญหานี้ได้อย่างไร? ลองมาวิเคราะห์ปัญหานี้ด้วยหลักการแบบที่ 'ไม่ไว้ใจใคร' หรือ 'zero trust' กันดู

ตามหลักการแบบ zero trust ทั้งคนในและคนนอกจะต้องผ่านขั้นตอนการตรวจสอบแบบเดียวกันเราจะไม่ไว้ใจใครทั้งนั้น แม้ว่าจะเป็นคนในก็ตาม การเข้าสู่ระบบในทุกๆ ครั้งจะต้องผ่านการตรวจสอบและได้รับการอนุญาตเสียก่อน

ถ้าเทียบกับป้อมปราการ ก็หมายความว่านอกจากจะมีกำแพงไว้กันภัยจากนอกป้อมแล้ว บ้านทุก ๆ หลังภายในป้อมก็ยังมีกำแพงอีกชั้นหนึ่งไว้ป้องกันภัยจากภายในป้อมเองด้วย สำหรับในองค์กรนั้น สิ่งที่เราเรียกกันว่า การแบ่งระบบเครือข่ายระดับไมโครด้วยซอฟต์แวร์ (software-defined micro-segmentation) จะเพิ่มความปลอดภัยเข้าไปอีกชั้นหนึ่ง มีกำแพงป้อมอยู่รอบนอก บ้านแต่ละหลังมีการรักษาความปลอดภัย และชาวบ้านแต่ละคนก็ยังมีเจ้าหน้าที่รักษาความปลอดภัยส่วนตัวคอยเดินติดตามไปทุกที่ หากต้องการจะไปที่ใดภายในป้อม เราจะต้องยื่นพาสปอร์ตให้ตรวจสอบในทุกๆ ครั้ง

สำหรับเครือข่ายขององค์กรแล้ว นั้นแปลว่าความไว้วางใจนั้นไม่ได้เป็นสิ่งที่ชัดเจนเหมือนกับกำแพงป้อม แต่เป็นสิ่งที่ถูกแจกจ่ายกระจายไปทั่วเครือข่าย และเป็นสิ่งที่เคลื่อนไหวได้ ไม่ได้ถูกกักบริเวณไว้ที่ Switch Port หรือ VLAN มันเป็นสิ่งที่ขึ้นอยู่กับตัวบุคคล อุปกรณ์ สถานการณ์ เวลาในแต่ละวัน และอื่น ๆ มันเป็นสิ่งที่ถูกกำหนดโดยซอฟต์แวร์ (software-defined) และสามารถถูกปรับเปลี่ยนได้ในระหว่างการทำงาน

ด้วยวิธีการนี้ องค์กรประกอบต่าง ๆ จะต้องได้รับการควบคุมให้สามารถปรับตัวเพื่อตอบสนองต่อภัยหรือการเปลี่ยนแปลงของกระบวนการในการทำงานได้ (workflow)



การแบ่งเซกเมนต์ระดับมาโครและไมโคร

สถาปัตยกรรมแบบ zero trust มีการแบ่งระบบเครือข่ายอยู่ 2 ประเภท คือแบบมาโครและไมโคร ถ้าเทียบกับป้อมปราการแล้ว กำแพงรอบนอกเปรียบว่าเป็นการแบ่งระดับมาโคร ส่วนระบบรักษาความปลอดภัยส่วนตัวนั้นคือการการแบ่งระดับไมโคร

ในการแบ่งเซกเมนต์ระดับมาโครนั้น เครือข่ายทางกายภาพถูกแบ่งออกเป็นเซกเมนต์ (ส่วนต่างๆ) ซึ่งเซกเมนต์เหล่านี้จะเป็น VLAN และ VRF หรืออาจจะเป็น VPN หากเรากำลังพูดถึงการส่งข้อมูลผ่านเส้นทางที่สั้นที่สุด หรือ Shortest Path Bridging (SPB), MPLS, หรือแม้แต่ VXLAN หรืออุโมงค์ GRE Tunnel การส่งผ่านข้อมูลระหว่างผู้ใช้หรืออุปกรณ์ที่อยู่คนละเซกเมนต์กันล้วนถูกควบคุมโดย Firewall ทั้งสิ้น องค์กรทุกองค์กรนั้นต่างก็ใช้การแบ่งเซกเมนต์ประเภทนี้ในรูปแบบใดก็รูปแบบหนึ่ง แต่มักจะไม่ใช้เพราะเหตุผลทางด้านความปลอดภัย องค์กรมักจะใช้การแบ่งประเภทเพราะว่ามันง่ายกับการขยายเครือข่าย การบริหาร และการจัดระเบียบเสียมากกว่า ถ้าอุปกรณ์สองเครื่องมี VLAN ที่แตกต่างกัน แต่สามารถติดต่อกันได้โดยไม่ต้องผ่าน Firewall แปลว่าสองอุปกรณ์นี้อยู่ในมาโครเซกเมนต์เดียวกัน ตัวอย่างที่มักจะมีให้เห็นกันของการแบ่งเซกเมนต์ประเภทนี้ คือการใช้ IP Phone บน VLAN และ VRF ที่แตกต่างกัน ซึ่งไม่ได้เชื่อมต่อในทางตรรกะกับ PC แต่ละเครื่อง

คำถามคือ เราจะรู้ได้อย่างไรว่าผู้ใช้แต่ละคนนั้นหรืออุปกรณ์แต่ละเครื่องนั้นอยู่ในเซกเมนต์ไหน? เราอาจจะใช้สวิตช์, Switch Port, หรือ SSID ก็ได้ แต่วิธีเหล่านี้มันล้าสมัยไปแล้ว พวกมันเป็นวิธีที่ไม่ ยืดหยุ่น และไม่เหมาะสมสำหรับผู้ใช้หรืออุปกรณ์พกพา หากเป็นไปได้ คุณควรใช้ระบบการยืนยันตัวตนที่เป็นซอฟต์แวร์ กันที่ผู้ใช้หรืออุปกรณ์เข้าเชื่อมต่อกับเครือข่ายและยืนยันตัวตนแล้ว พวกเขาจะได้รับโปรไฟล์เฉพาะตัว และโปรไฟล์ดังกล่าวจะจัดหาเซกเมนต์ที่เหมาะสมให้ไม่ว่าผู้ใช้หรืออุปกรณ์นั้นจะอยู่ที่ใด หรือมี Switch Port หรือ SSID ใดก็ตาม

แม้ว่าการแบ่งเซกเมนต์ระดับมาโครนี้จะมีประโยชน์ทางด้านความปลอดภัย แต่องค์กรมักจะนำมันมาใช้สำหรับการบริหารจัดการหรือการจัดระเบียบเสียมากกว่า ตัวอย่างเช่น กล้องและลิฟต์ประตูอยู่ภายใต้การดูแลของแผนกความปลอดภัยควบคุมคนเข้าคนออก ส่วนเครื่องควบคุมอุณหภูมิห้องนั้นมีแผนกซ่อมบำรุงเป็นผู้ดูแล

ส่วนการแบ่งเซกเมนต์ระดับไมโครนั้นเก็บรายละเอียดมากกว่านั้นเสียอีก ผู้ใช้ทุกคนใช้ว่าจะเท่าเทียมกัน ดังนั้นแต่ละคนจึงไม่จำเป็นต้องสามารถเข้าถึงทรัพยากรต่าง ๆ ได้เหมือนกันหมด โปรไฟล์ที่จัดหาเซกเมนต์ให้กับผู้ใช้นั้นมีกฎเกณฑ์ที่กำหนดที่ควบคุมสิทธิ์การเข้าถึงของผู้ใช้หรืออุปกรณ์โดยขึ้นอยู่กับตำแหน่งหน้าที่ต่าง ๆ ในองค์กร เช่น ทรัพยากรมนุษย์ หรือการเงิน ระบบแบบนี้เรียกว่า สิทธิ์การเข้าใช้งาน (role-based access) และเกี่ยวข้องกันโดยตรงกับหลักการให้สิทธิ์เท่าที่จำเป็น (principle of least privilege) ด้วยเหตุนี้เอง กล้องและลิฟต์ประตูจึงไม่จำเป็นต้องใช้ทรัพยากรร่วมกันถึงแม้ว่าพวกมันทั้งสองจะอยู่ในเซกเมนต์ เดียวกันก็ตาม กล้องต้องสื่อสารกับเครื่องบันทึกวิดีโอ ลิฟต์ต้องสื่อสารกับเซิร์ฟเวอร์ของมัน กล้องไม่จำเป็นต้องไปสื่อสารกับลิฟต์ เช่นเดียวกับที่ลิฟต์ไม่จำเป็นต้องไปสื่อสารกับลิฟต์ตัวอื่น การให้สิทธิ์การเข้าถึงเหล่านี้เป็นไปตามนโยบายที่มาพร้อมกับโปรไฟล์ และถูกบังคับใช้กันที่อุปกรณ์ผ่านการยืนยัน

เหตุผลที่การแบ่งเซกเมนต์ระดับไมโครจะต้องดำเนินการผ่านซอฟต์แวร์นั้นมีหลายประการ ผู้ใช้หรืออุปกรณ์ IoT นั้นไม่มีความคงที่ พวกเขาสลัดไหว่ เชื่อมต่อและตัดการเชื่อมต่ออยู่ตลอดเวลา นโยบายสิทธิ์การเข้าถึงไม่อาจจะไปผูกติดอยู่กับสถานที่หรือพอร์ตใดพอร์ตหนึ่งได้ การตั้งค่าของการแบ่งเซกเมนต์ระดับไมโครนี้ต้องมีความ ยืดหยุ่น โดยต้องคำนึงถึงปัจจัยหลาย ๆ อย่าง รวมไปถึงแต่ไม่จำกัดเพียง สถานที่ ผู้ใช้คือใคร อุปกรณ์ใดต้องการจะเชื่อมต่อ และตอนนี้เวลาที่มองแล้ว เป็นต้น

สรุป เมื่อ Firewall เป็นตัวควบคุมการสื่อสารระหว่างเซกเมนต์ต่าง ๆ นั่นคือการแบ่งเซกเมนต์ แบบมาโคร เมื่อนโยบายควบคุมสิทธิ์ในการเข้าถึงเครือข่าย (Network Access Control, NAC) ของอุปกรณ์หรือบทบาทของผู้ใช้เป็นสิ่งที่ควบคุมการสื่อสารภายในเซกเมนต์ เดียวกัน นั่นคือการแบ่งเซกเมนต์ระดับไมโคร.



เหตุที่ต้องใช้ทั้งสองระดับ

จะเกิดอะไรขึ้นหากคุณใช้การแบ่งเพียงระดับเดียวเท่านั้น?

มาดูระดับมาโครกันก่อนเป็นอันดับแรก เมื่อมีข้อมูลจำนวนมากไหลผ่าน Firewall เข้ามา เพื่อเข้ารับการยืนยันตัวตนและการอนุญาต Firewall จะกลายเป็นคอขวด ซึ่งสามารถลดประสิทธิภาพในการทำงานของเครือข่ายลงได้ คุณจะเพิ่มจำนวน Firewall ให้มากขึ้นก็ได้ที่ชั้นกลางของเครือข่าย (Distribution Layer) แต่ก็มียึดที่สูงและอาจจะไม่เพิ่มประสิทธิภาพการทำงานเลยก็เป็นได้เพราะ Firewall นั้นไม่ได้ทำงานด้วยความเร็ว Wire Speed นอกจากนี้ หากเราใช้วิธีนี้ จุดที่ต้องบังคับใช้นโยบายก็จะมีมากขึ้น ทำให้การแก้ไขนโยบายและการบริหารจัดการนั้นเป็นสิ่งที่ยุ่งยาก

อีกทางเลือกหนึ่งคือการใช้แบ่งระดับไมโคร เท่านั้น ถ้าเป็นเช่นนั้น การบังคับใช้นโยบายการเข้าถึงทั้งหมดจะถูกควบคุมโดย NAC เท่านั้น รายการนโยบายต่าง ๆ จะยาวและซับซ้อนมากจนเกินกว่าที่ศักยภาพของอุปกรณ์จะรับได้

โดยสรุปแล้ว เราควรนำการแบ่งเซกเมนต์ทั้งสองระดับนี้มาใช้ให้สมดุลกันจะดีกว่า โดยให้ Firewall ควบคุมการเดินทางของข้อมูลระหว่างเซกเมนต์ (แนวดิ่ง) ส่วนภายในเซกเมนต์นั้นปล่อยให้ทำหน้าที่ของ NAC (แนวนอน)

เมื่อผสมผสานสองวิธีนี้ คุณจะสามารถจัดการกับภัยที่แพร่กระจายจากเซกเมนต์หนึ่งสู่อีกเซกเมนต์ หนึ่ง และภัยที่เคลื่อนที่ในแนวนอนภายในเซกเมนต์ ถ้าจะอธิบายให้เห็นภาพ เมื่อผู้ประสงค์ร้ายสามารถเข้าถึงกล่องได้แล้ว การแบ่งเซกเมนต์ระดับไมโครจะป้องกันไม่ให้ผู้ประสงค์ร้ายใช้ช่องโหว่นี้เป็นฐานปฏิบัติการเพื่อเข้าโจมตีทรัพยากรอื่น ๆ ต่อไป เช่น ลีคประตุ

เป้าหมาย คือ เราจะต้องตรวจสอบการเชื่อมต่อในทุก ๆ ครั้งและให้การอนุมัติแก่ผู้ใช้แต่ละคนและอุปกรณ์แต่ละเครื่อง หรือก็คือ การใช้การแบ่งเซกเมนต์เพื่อป้องกันการแพร่กระจายของภัยในแนวนอน การเฝ้าสังเกตอยู่ตลอด และแยกตัวผู้ใช้หรืออุปกรณ์ที่ถูกจับออกมา.





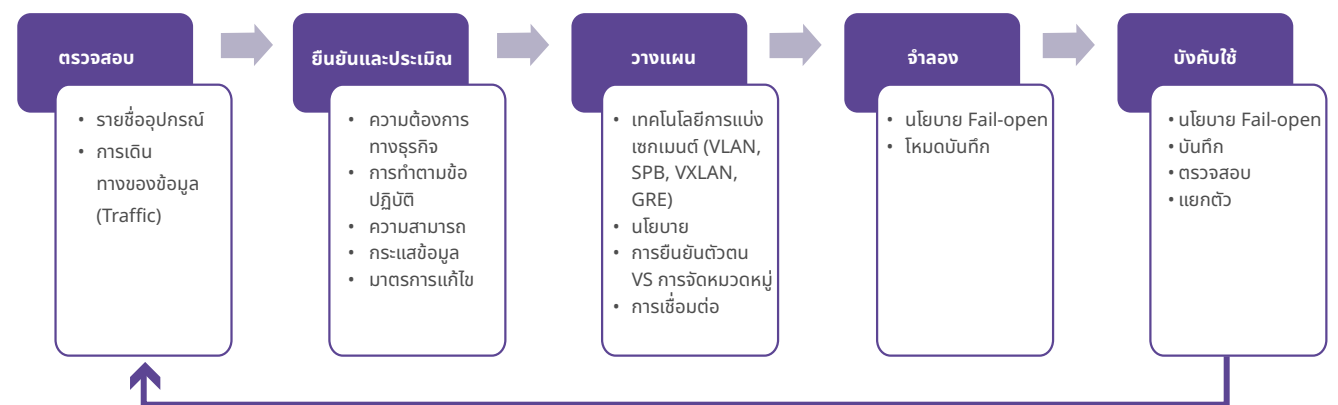
การนำมาใช้

ถ้าเป็นสร้างเครือข่ายขึ้นมาใหม่จากศูนย์ (Greenfield) การสร้างสถาปัตยกรรมแบบ zero trust ที่ใช้การแบ่งระดับโมโครนั้นเป็นเรื่องง่าย แต่เมื่อเป็นการพัฒนาต่อยอดจากซอฟต์แวร์เดิม (Brownfield) หากเรานำการแบ่งระดับโมโครมาใช้ ผู้ใช้ อุปกรณ์ และแอปพลิเคชันอาจถูกกีดกันออกจากเครือข่ายได้เนื่องจาก การตรวจสอบตัวตนล้มเหลวหรือนโยบายสิทธิ์การเข้าถึงที่ยังไม่เสร็จสมบูรณ์ การที่องค์กรหนึ่งจะสามารถเปลี่ยนมาใช้ระบบนี้ได้ในรวดเร็ว ด้วยการรีเฟรชเพียงครั้งเดียวนั้น เป็นสิ่งที่เป็นไปได้ยาก

ในการต่อยอดซอฟต์แวร์เดิม จะมีบางช่วงที่เครือข่ายจะต้องใช้สถาปัตยกรรมทั้งแบบ non-zero trust และแบบ zero trust ไปพร้อม ๆ กัน การเปลี่ยนแปลงจะค่อย ๆ เกิดขึ้นในทีละระดับชั้นหรือทีละตำแหน่ง สิ่งที่สำคัญคือ คุณจะต้องมั่นใจว่าองค์ประกอบโครงสร้างที่คุณเพิ่มเข้ามาและวิธีการที่คุณใช้ในการเพิ่มองค์ประกอบดังกล่าวเข้ามานั้น สามารถปฏิบัติการในโหมด zero trust หรือโมโครเชกเมนต์ได้เมื่อองค์ประกอบอื่น ๆ ของโครงสร้างนั้นพร้อมใช้งาน นี่หมายความว่าโครงสร้างที่เพิ่มเข้ามานั้นจะต้องสามารถทำงานร่วมกับองค์ประกอบที่มีอยู่แล้วและองค์ประกอบที่จะเพิ่มเข้ามาในอนาคตได้

วิธีการ

การนำสถาปัตยกรรม zero trust มาใช้มีอยู่ 5 ขั้นตอน ดังนี้ เฟ้าสังเกต, ยืนยันและประเมิน, วางแผน, จำลอง, และบังคับใช้.



ภาพที่ 1 - วิธีการ



ขั้นตอนที่ 1 ตรวจสอบ

ขั้นตอนแรก คุณจะต้องตรวจสอบ สร้างผัง และสร้างรายชื่อสิ่งที่อยู่ในเครือข่ายของคุณ

ในการเปลี่ยนไปใช้ ZTA นั้น คุณต้องมีความรู้มากพอเกี่ยวกับทรัพย์สิน (ทั้งที่เป็นกายภาพและซอฟต์แวร์), เจ้าของข้อมูล (รวมถึงสิทธิ์การเข้าถึงของผู้ใช้ด้วย), และกระบวนการทางธุรกิจที่เกี่ยวข้องหรือใช้งานเครือข่ายนี้อยู่ หากมีความรู้ไม่เพียงพอ อาจทำให้ไม่สามารถเข้าถึงบางส่วนของเครือข่ายได้เนื่องจากมีข้อมูลไม่เพียงพอ เหตุการณ์นี้จะเป็นปัญหาอย่างมากหากมีการใช้อุปกรณ์หรือซอฟต์แวร์ที่ฝ่าย IT ไม่ทราบ (Shadow IT หรือ Shadow IoT) อยู่ในองค์กร

เริ่มตรวจสอบอุปกรณ์และกระแสข้อมูล สร้างรายชื่ออุปกรณ์ทั้งหมดที่อยู่ในเครือข่ายจัดหมวดหมู่ตามประเภทอุปกรณ์, ผู้ผลิต, โมเดล, ระบบปฏิบัติการ, และอื่นๆ รายชื่อนี้ควรแสดงด้วยว่าอุปกรณ์แต่ละเครื่องถูกพบล่าสุดที่ Switch Port หรือ SSID ใด ข้อมูลดังกล่าวหาได้จาก MAC Address, DHCP Signature, และ HTTP user agent

อุปกรณ์จากบุคคลที่สามมักจะแสดงที่อยู่ IP เท่านั้น และไม่แสดงประเภทของอุปกรณ์ ดังนั้น คุณควรจะมีโปรแกรมสร้างรายชื่อ IoT หรืออุปกรณ์เพื่อให้การสร้างโปรไฟล์ NAC สำหรับอุปกรณ์แต่ละประเภทได้อย่างง่ายและรวดเร็ว

อีกสิ่งหนึ่งที่เรารู้ในการสร้างนโยบายคือการเดินทางของข้อมูล คุณสามารถเก็บข้อมูลตัวนี้ได้ด้วยโปรแกรมตรวจสอบกระแสข้อมูล เช่น sFlow, Netflow, หรือ Deep Packet Inspection (DPI) ขึ้นอยู่กับประเภทของอุปกรณ์ที่คุณมี

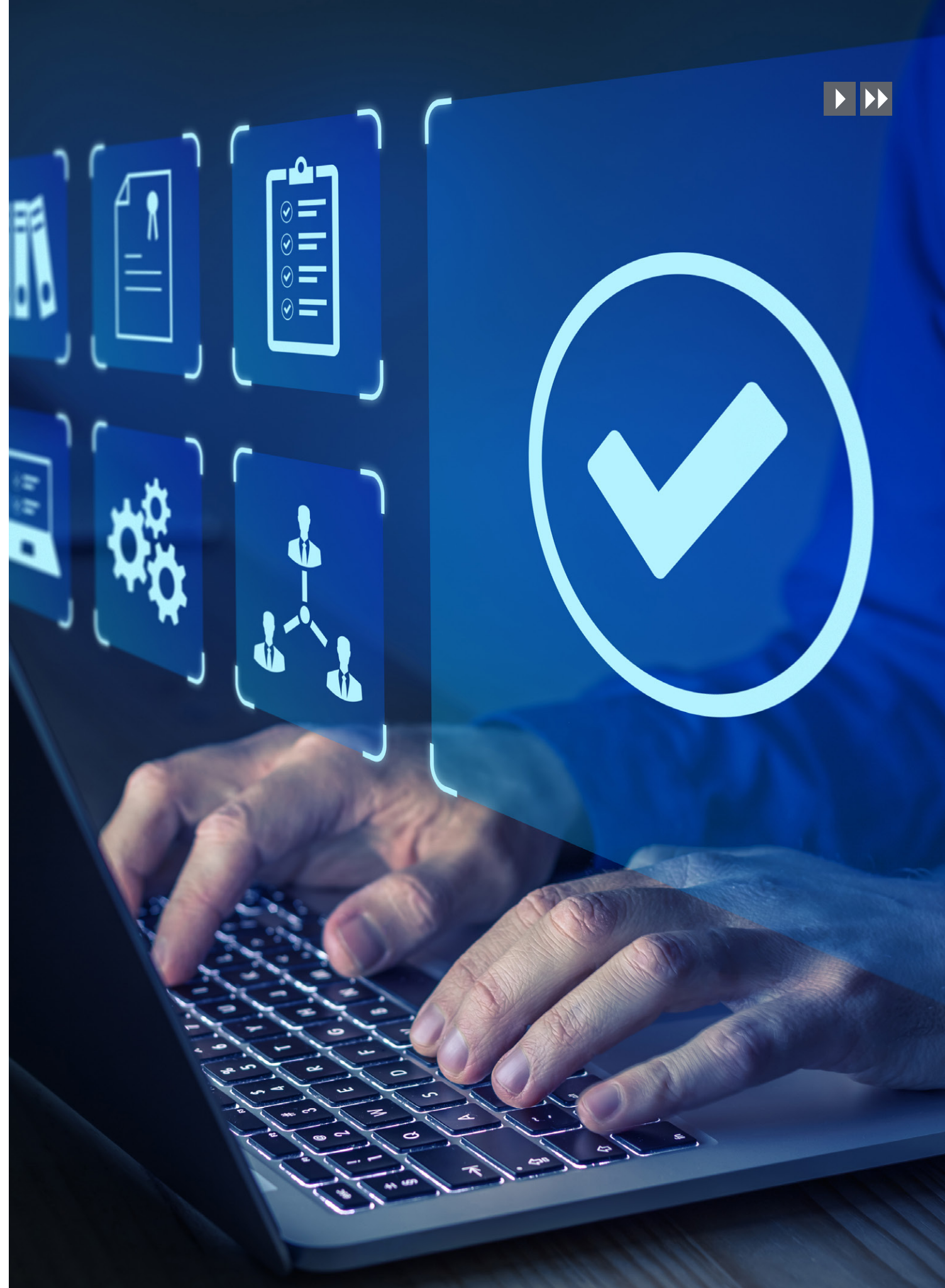
กระบวนการนี้จะต้องทำ ซ้ำ หลายครั้ง ในครั้งแรกที่คุณเริ่มการตรวจสอบ ข้อมูลที่ได้อาจจะไม่มีประโยชน์มากนัก แต่เมื่อคุณเริ่มดำเนินการตามขั้นตอนต่อ ๆ ไป มันจะเริ่มมีความเฉพาะเจาะจงและมีประโยชน์มากยิ่งขึ้น ข้อมูลที่คุณเก็บในขั้นตอนนี้จะมีความสำคัญในขั้นตอนถัด ๆ ไป



ขั้นตอนที่ 2 ยืนยันและประเมิน

ขั้นตอนต่อไป คือการยืนยันความถูกต้องของข้อมูลเหล่านี้และประเมินความต้องการทางธุรกิจ Shadow IoT ที่พบควรถูกกำจัดออกไปเพราะจะเป็นการเพิ่มช่องโหว่ให้เกิดการโจรกรรมได้ง่ายขึ้น สำหรับอุปกรณ์และซอฟต์แวร์อื่น ๆ ให้คุณระบุเจ้าของข้อมูล (ผู้ใช้และอุปกรณ์), กระแสข้อมูล, และกระบวนการปฏิบัติงาน เพราะข้อมูลเหล่านี้มีความสำคัญในการกำหนดนโยบายสิทธิ์การเข้าถึง ตัวอย่างเช่น ผู้ใช้คนใดสามารถเข้าถึงทรัพยากรใดได้ และพวกเขามีสิทธิ์ทำอะไรได้บ้างต่อทรัพยากรเหล่านั้น ใช้หลักการให้สิทธิ์เท่าที่จำเป็น

เมื่อใช้การแบ่งเซกเมนต์ระดับโมโครแล้ว ไม่ได้หมายความว่าเราควรจะ ลด ปล่อยมาตรการความปลอดภัยอื่น ๆ เช่น รหัสผ่านหรือการอัปเดตเฟิร์มแวร์ความสามารถแต่ละอย่างของอุปกรณ์ต้องได้รับการประเมิน เช่น อุปกรณ์เหล่านี้สามารถใช้การยืนยันด้วยใบรับรองแบบดิจิทัลได้หรือไม่ (Certificate-based authentication) มีซอฟต์แวร์ด้านบริหารจัดการใดหรือไม่ที่ช่วยในการออกและบังคับใช้ใบรับรองเหล่านี้ จะต้องมีการแส ข้อมูลปริมาณเท่าใด เป็นต้น คุณสามารถหาข้อมูลเหล่านี้ได้จากผู้ผลิต แต่คุณก็ควรเปรียบเทียบข้อมูลจากผู้ผลิตกับรายงานเคราะห์กระแสข้อมูล ของคุณเองเช่นกัน ถ้าคุณพบทรัพยากรชิ้นใดที่ขัดต่อนโยบายองค์กร คุณ จะต้องมีการเตรียมเอาไว้เพื่อแก้ไขให้ทรัพยากรดังกล่าวเป็นไปตาม นโยบาย หรือคุณจะต้องเพิ่มมาตรการควบคุมให้มากขึ้น





ขั้นตอนที่ 3 วางแผน

ในขั้นตอนนี้ คุณได้รู้เกี่ยวกับทรัพย์สิน, เจ้าของข้อมูล (ผู้ใช้), กระแสข้อมูล, และกระบวนการปฏิบัติงานเป็นที่เรียบร้อยแล้ว ต่อไป ก่อนที่จะเริ่มสร้างสถาปัตยกรรมที่ใช้การแบ่งระดับไมโครได้ คุณจะต้องกลับกรองข้อมูลที่มีนี้ออกมาเป็นนโยบายการยืนยันตัวตนและการรักษาความปลอดภัยเสียก่อน ตามที่ได้กล่าวไว้ ณ ข้างต้น ผลลัพธ์ที่ดีที่สุดนั้นเกิดจากการผสมผสานการแบ่งระดับไมโครและไมโครเข้าด้วยกัน จำไว้ว่าในการพัฒนาแบบ Brownfield ส่วนมาก คุณจะต้องคำนึงถึงสถาปัตยกรรมที่มีอยู่ก่อนแล้วด้วย

การแบ่งเซกเมนต์ระดับไมโครนั้นมีหลากหลายวิธีให้เลือกได้ เช่น VLAN, VRF, SPB VPN, VXLAN, หรือ GRE Tunnel และวิธีพิเศษอย่างเช่น VLAN ส่วนตัว แต่ละอย่างต่างก็มีทั้งข้อดีและข้อเสียในสถานการณ์ที่แตกต่างกันออกไป ส่วนสำหรับการแบ่งเซกเมนต์แบบไมโครนั้น คุณจะต้องรู้ว่าแต่ละโปรไฟล์สำหรับผู้ใช้และอุปกรณ์แต่ละประเภทนั้นต้องมีสิทธิ์การเข้าถึงใดบ้าง สุดท้าย คุณจะต้องสร้างกฎเกณฑ์ในการกำหนดเซกเมนต์และนโยบายสิทธิ์การเข้าถึงของผู้ใช้และอุปกรณ์ โดยทำได้ด้วยการยืนยันตัวตนหรือการจัดหมวดหมู่ ซึ่งอาจจะเป็นลายนิ้วมือของอุปกรณ์ (Device Fingerprinting)

หากเป็นไปได้ คุณควรลงทุนซื้อเทคโนโลยี (software-defined segmentation) ที่จะช่วยให้คุณสร้างนโยบายการยืนยันตัวตนที่มีความยืดหยุ่นได้ เพื่อให้การอัปเดตโปรไฟล์ในเครือข่ายเป็นไปได้ง่าย

เราขอแนะนำให้คุณออกแบบขั้นตอนการยืนยันตัวตนดังนี้

1. การยืนยันตัวตนผ่านใบรับรอง 802.1x โดยการใช้เซิร์ฟเวอร์ RADIUS ระบบจะสร้างบันทึกการยืนยันตัวขึ้นมา ซึ่งข้อมูลนี้สามารถแชร์ไปยัง Firewall ได้
2. ถ้าคุณไม่สามารถยืนยันตัวตนผ่านใบรับรอง 802.1x ได้ คุณควรลองใช้การยืนยันตัวตนด้วย MAC Address เป็นอันดับต่อไป (MAC Authentication) ถึงแม้ว่าวิธีการนี้จะไม่ปลอดภัยเท่ากับ 802.1x แต่มันก็ยังดีกว่าการที่ไม่มีการยืนยันตัวตนเลย ให้ใช้วิธีนี้จนกว่าจะสามารถใช้ 802.1x ได้

3. ถ้ายังไม่มีโปรไฟล์ใดปรากฏขึ้นมา คุณอาจจะลองใช้วิธีการตรวจลายนิ้วมือ (Fingerprinting) ซึ่งเป็นวิธีที่ใช้จัดหาเซกเมนต์และตั้งกฎเกณฑ์ให้กับโปรไฟล์ได้เช่นเดียวกัน วิธีนี้จะไม่ทำการบันทึกการยืนยันตัวตนหรือบัญชี แต่จะถูกลงทะเบียนไว้ในฐานข้อมูลรายชื่อ IoT
4. สุดท้าย คุณสามารถตั้งค่าเริ่มต้นให้ทุก ๆ โปรไฟล์ไปก่อนถ้าวิธีการอื่น ๆ ไม่สามารถยืนยันตัวตนของโปรไฟล์ได้ เพราะในขั้นตอนต้น ๆ เรายังคงต้องหาเซกเมนต์และกฎเกณฑ์ให้กับโปรไฟล์อยู่และต้องบันทึกโปรไฟล์เข้าสู่ฐานข้อมูลรายชื่อบัญชี

ขั้นตอนปฏิบัติการเหล่านี้ควรมีความยืดหยุ่นเพื่อให้คุณสามารถปรับเปลี่ยนได้ในภายหลัง เช่น คุณอาจจะต้องการเลือกใช้ MAC Authentication ไปก่อน แล้วนำกลับมาใช้ในภายหลังเมื่อคุณได้รับรายงานรายชื่อที่อยู่ MAC แล้ว และระหว่างที่คุณทำการพัฒนากระบวนการนี้ต่อไป คุณก็สามารถเปลี่ยนเซกเมนต์และกฎเกณฑ์ของโปรไฟล์ที่กำลังใช้ค่าเริ่มต้นดังกล่าวให้เป็นกฎที่เข้มงวดมากยิ่งขึ้น โดยอนุญาตให้ Bastion Host มีสิทธิ์ในการเข้าถึงแต่เพียงผู้เดียว

คุณควรแชร์บทบาทของอุปกรณ์กับ Firewall ด้วยเช่นกัน เพื่อให้กฎเกณฑ์ของ Firewall นั้นขึ้นอยู่กับบทบาท ไม่ใช่แค่ Subnet หรือที่อยู่ IP เท่านั้น การกระทำเช่นนี้มีประโยชน์อยู่ 2 ประการ ประการแรก Firewall จะสามารถบังคับใช้นโยบายที่มีความละเอียดอ่อนกับอุปกรณ์ IoT เหล่านั้นได้ ประการที่สอง นโยบายของ Firewall จะขึ้นอยู่กับตัวผู้ใช้หรือบทบาท และไม่เกี่ยวเนื่องกับ Subnet หรือที่อยู่ IP อีกต่อไป นี่จะทำให้คุณสามารถออกแบบเครือข่ายและแบ่งเซกเมนต์ของเครือข่ายได้อีกครั้งในอนาคต

กระบวนการนี้จะต้องทำ ซ้ำ หลายครั้ง คุณจะต้องเปลี่ยนแปลง ปรับปรุง และปรับแต่งคุณมีประสบการณ์กับระบบการยืนยันตัวตนและการแบ่งเซกเมนต์มากขึ้นในอนาคตเมื่อ



ขั้นตอนที่ 4 จำลอง

ไม่ว่าคุณจะวางแผนมาอย่างดีขนาดไหนก็ตาม มันคงจะเป็นไม่ได้ที่คุณจะทำทุกอย่างได้อย่างถูกต้องและครบถ้วนในครั้งแรก ข้อผิดพลาดใด ๆ ก็ตามในระบบการยืนยันตัวตน หรือหากเกิดการ เพี้ยนพลาด หลงลืมสิ่งใดระหว่างที่คุณสร้างรายชื่อผู้มีสิทธิ์ในนโยบายความปลอดภัย จะทำให้เกิดข้อบกพร่องในกระบวนการทางธุรกิจได้ ดังนั้น ระบบการยืนยันตัวตนและสิทธิ์การเข้าถึงจะต้องปฏิบัติการด้วยโหมดที่เรียกว่า “fail-open” อุปกรณ์หรือผู้ใช้ใดที่ยืนยันตัวตนไม่ได้จะยังคงได้รับอนุญาตให้เข้าใช้เครือข่ายอยู่ และกระแสข้อมูลที่ไม่รู้จักก็จะได้รับอนุญาตด้วยเช่นกัน แต่เมื่อได้รับอนุญาตให้เข้ามาแล้ว จะต้องถูกบันทึกเอาไว้เพื่อใช้ในการปรับปรุงระบบการยืนยันตัวตนและนโยบายต่อไป

ขั้นตอนที่ 5 บังคับใช้

หลังจากที่ปรับปรุงระบบเป็นที่เรียบร้อยแล้ว และไม่พบความผิดพลาดในการยืนยันตัวตนหรือการปฏิเสธกระแสข้อมูลที่น่าเชื่อถืออีกต่อไป ให้คุณเปลี่ยนโหมดของนโยบายเหล่านี้จาก “fail-open” ไปเป็น “fail-close” ซึ่งจะบล็อกอุปกรณ์ที่ไม่รู้จักและปฏิเสธกระแสข้อมูลที่ไม่รู้จัก

แน่ออยู่แล้ว คุณยังจำเป็นต้องเฝ้าระวังอุปกรณ์และกระแสข้อมูลที่ไม่รู้จักต่อไป และอาจจะต้องทำตามกระบวนการเดิมทั้งหมดถ้าหากจำเป็น



ท้ายสุด

ในการเฝ้าระวัง เก็บบันทึก และการแยกตัวอุปกรณ์หรือผู้ใช้ที่มีปัญหานั้น เราขอแนะนำให้คุณลงทุนติดตั้งระบบตรวจจับการรุกราน, ภายนอก (Intrusion Detection System, IDS) ถึงแม้ว่าการโจมตีในรูปแบบ Distributed Denial of Service (DDoS) นั้นจะมีหลายประเภทที่ Switch สามารถตรวจจับได้ ระบบ DDoS สามารถเฝ้าระวังภัยได้มากกว่านั้นเสียอีก เช่น โไวรัส หรือความผิดปกติต่าง ๆ คุณอาจจะจำเหตุการณ์เมื่อไม่กี่ปีก่อนได้กล้องวงจรปิดหลายตัวโดนไวรัสมาแวร์ที่ชื่อว่า Mirai หรือเหตุการณ์ที่เซิร์ฟเวอร์ DNS ทั่วทั้งโลกถูกโจมตี ส่งผลผลกระทบถึงเว็บไซต์อย่างเช่น Twitter, Spotify, หรือ Paypal Switch ของคุณอาจจะไม่สามารถตรวจจับการโจมตีเหล่านี้ได้ แต่ IDS ที่ถูกออกแบบเพื่อหน้าที่นี้โดยเฉพาะนั้นทำได้

เมื่อการโจมตีถูกตรวจพบแล้ว IDS จะรายงานระบบบริหารจัดการเครือข่าย (NMS) ของที่อยู่ IP ของอุปกรณ์ที่ได้รับผลกระทบ NMS สามารถระบุตำแหน่งอุปกรณ์เหล่านี้ได้ในฐานข้อมูลของมัน และจะเปลี่ยนโปรไฟล์ของอุปกรณ์เหล่านี้ไปเป็นโปรไฟล์ที่มี “บทบาทการแยกตัว” (quarantine role)

“บทบาทการแยกตัว” นั้นเป็นบทบาทที่มีข้อจำกัดเยอะมาก โดยทั่วไปแล้ว โดยบทบาทนี้จะได้รับอนุญาตให้ติดต่อกับ Bastion Host เท่านั้นเพื่อดำเนินการแก้ไขปัญหา ตัวอย่างเช่น เปลี่ยนรหัสผ่านให้ซับซ้อนมากยิ่งขึ้น อัปเดตเฟิร์มแวร์ หรืออื่น ๆ

ทำไมต้อง ALE?

อัลคาเทล-ลูเซน เอนเตอร์ไพรส์ (ALE) [ดิิจัล เจ เน็ตเวิร์คกิ้ง](#) โซลูชัน ใช้การแบ่งเซกเมนต์ด้วยซอฟต์แวร์ (software-defined segmentation) ที่มีความแข็งแกร่ง และยังมีนโยบาย DPI NAC ที่มีความยืดหยุ่น ซึ่งจะช่วยให้คุณเปลี่ยนไปใช้สถาปัตยกรรมแบบ zero trust ได้อย่างค่อยเป็นค่อยไป

ดิิจัล เจ เน็ตเวิร์คกิ้ง คือพิมพ์เขียวของ ALE ที่ช่วยให้ธุรกิจและองค์กรต่าง ๆ เข้าสู่ยุคดิจิทัล และขยายกิจการแบบดิจิทัลได้ โดยยึดถือหลักการหลัก 3 ประการ

- [เครือข่ายอัตโนมัติ](#) ที่สามารถเชื่อมต่อผู้คน, กระบวนการ, แอปพลิเคชัน, และจุดประสงค์หลักต่าง ๆ เข้ากันได้โดยอัตโนมัติ อย่างง่ายดาย และปลอดภัย เน็ตเวิร์คอัตโนมัติของ ALE ถูกออกแบบโดยมีพื้นฐานมาจากพอร์ตโฟลิโอที่มีประสิทธิภาพ ซึ่งมีแพลตฟอร์มการจัดการแบบครบครัน บังคับใช้นโยบายความปลอดภัยไปทั่วทั้ง LAN และ WLAN ของเรา เน็ตเวิร์คอัตโนมัติสามารถใช้ได้ทั้งภายในอาคาร ภายนอกอาคาร และในสภาพแวดล้อมทางอุตสาหกรรม สามารถบริหารจัดการเน็ตเวิร์คได้ในสถานที่ทำงาน ในระบบคลาวด์ หรือผสมผสานทั้งสองแบบ แล้วแต่ความต้องการของลูกค้า
- [เชื่อมต่ออุปกรณ์ IoT ได้อย่างปลอดภัยและมีประสิทธิภาพ](#): การแบ่งเครือข่ายนั้นจะกักอุปกรณ์ไว้ภายในเซกเมนต์ของมันและลดความเสี่ยงที่อุปกรณ์และเครือข่ายจะถูกโจมตี การแบ่งเซกเมนต์ IoT ช่วยให้องค์กรรู้ได้ในทันทีว่าอุปกรณ์กำลังทำงานอย่างเป็นปกติหรือไม่เพื่อการปกป้องเครือข่ายให้ปลอดภัย
- [สร้างนวัตกรรมทางธุรกิจ](#) ผ่านกระบวนการดำเนินงานอัตโนมัติ เชื่อมต่อผู้ใช้, แอปพลิเคชัน, และเมตริก IoT ในแบบเรียลไทม์เข้าสู่แพลตฟอร์มการทำงาน (Collaboration Platform) ด้วยข้อมูลระบุตำแหน่ง ทำให้การสร้างและการเปิดตัวกระบวนการธุรกิจและการให้บริการแบบดิจิทัลเป็นเรื่องที่เรียบง่าย อีกทั้งยังแจ้งให้ฝ่ายรักษาความปลอดภัยและฝ่ายบริหารจัดการเครือข่ายได้ทราบในทันทีหากตรวจพบการละเมิดกฎใด ๆ

คุณมีซอฟต์แวร์สำหรับสร้างรายชื่อ IoT หรืออุปกรณ์หรือไม่? คุณมีซอฟต์แวร์สำหรับตรวจสอบกระแสข้อมูลของแอปพลิเคชันหรือไม่? Current Switch และ Access Point แบบไร้สายของคุณได้รับการแบ่งเซกเมนต์ด้วยซอฟต์แวร์แล้วหรือไม่? ถ้าคุณยังไม่มีซอฟต์แวร์เหล่านี้ [กรุณาดูต่อเรา](#) และเราจะช่วยเอง



สิ่งที่ได้เรียนรู้

มาตรฐานสำคัญกัน:

- ZTA จะมีประสิทธิภาพได้ก็เมื่อคุณผสานการแบ่งเซกเมนต์ทั้งในระบบมาโครและระดับไมโคร
- การติดตั้ง ZTA นั้นมีอยู่ 5 ขั้นตอน ตรวจสอบ, ยืนยัน, วางแผน, จำลอง, และบังคับใช้
- ZTA ใช้การแบ่งเซกเมนต์ระดับไมโคร ซึ่งมีหลักการหลักอยู่ 3 ประการ การยืนยันตัวตน โดยมี 802.1x EAP-TLS เป็นวิธีการที่สำคัญที่สุด, นโยบายการเข้าถึงที่ขึ้นอยู่กับบทบาทของผู้ใช้หรืออุปกรณ์ตามหลักการให้สิทธิ์เท่าที่จำเป็น, และการตรวจตราและกักตัวโปรไฟล์ที่มีปัญหา
- ในสภาพแวดล้อมแบบผสมผสานและแบบที่มีอุปกรณ์พกพา นั้น จะต้องทำการแบ่งเซกเมนต์ ระดับไมโครด้วยซอฟต์แวร์ นั้นหมายความว่า การแบ่งเซกเมนต์แบบนี้จำเป็นต้องมีความ ยืดหยุ่นและขึ้นอยู่กับนโยบายการเข้าถึงเพื่อความสะดวกในการใช้งาน จะต้องไม่ถูกจำกัดไว้ในตำแหน่งใดตำแหน่งหนึ่ง

การเปลี่ยนมาใช้ ZTA ผ่านการแบ่งเซกเมนต์ระดับไมโครนั้นเป็นกระบวนการที่ต้องใช้เวลา การจะให้องค์กรไม่ว่าจะขนาดใดก็ตามเปลี่ยนมาใช้ได้ด้วยการกดรีเฟรชเพียงครั้งเดียวนั้นคงจะเป็นไปไม่ได้ แต่ทุกๆ ครั้ง ที่มีการรีเฟรช หรือออกแบบระบบใหม่ หรือปรับปรุงระบบนั้น คุณจะต้องเข้าใจเป้าหมายเข้าไปทุกทีถ้าคุณวางโครงสร้างและออกแบบได้อย่างถูกต้อง

อัลคาเทล-ลูเชน เอนเตอร์ไพรส์ มุ่งมั่นในการพัฒนาเทคโนโลยีด้านเครือข่ายและวิธีแก้ไขปัญหาคือจะช่วยให้คุณพร้อมเข้าสู่ยุคดิจิทัลเพื่อความสำเร็จทางธุรกิจ

