CSO

Microsoft Security

เนื้อหาที่ได้รับการสนับสนุน

Zero Trust security: ถอดบทเรียน จากผู้ใช้กลุ่มแรก

CSO Microsoft Security

สารบัญ

- บทนำ
- Zero Trust อยู่ที่นี่และมอบคุณค่า
- สิ่งขับเคลื่อนการปรับใช้ Zero Trust
- ภัยคุกคามไม่เคยลดน้อยลง
- อุปสรรคในการปรับใช้ Zero Trust
- ความท้าทายในการปรับใช้
- แนวทางปฏิบัติที่ดีที่สุดในการนำ Zero Trust มาใช้
- คุณอยู่จุดใดบนเส้นทางสู่ Zero Trust

CSO Microsoft Security

ข้อมูลเบื้องต้น

การหยุดชะงักในช่วงสองปีที่ผ่านมาได้สร้างความสั่นสะเทือนให้กับโมเดลด้านไอทีและการรักษาความปลอดภัยแบบเดิมๆ ด้วยเหตุนี้ การรักษาความปลอดภัยแบบ Zero Trust จึงได้รับการพัฒนาอย่างรวดเร็วจากการเป็นแนวคิดที่น่าสนใจไปสู่รากฐานของการรักษาความปลอดภัยองค์กรสมัยใหม่

งานวิจัยใหม่จาก Foundry พบว่า 52% ขององค์กรกำลังนำร่องหรือได้ปรับใช้สถาปัตยกรรม Zero Trust แล้ว และอีก 15% กำลังศึกษาค้นคว้าเกี่ยวกับโมเดล Zero Trust ผู้ที่ปรับใช้เหล่านี้รายงานประโยชน์มากมายจากการปรับใช้ รวมถึงการปกป้องข้อมูลลูกค้าที่ได้รับการปรับปรุง ความซับซ้อนที่ลดลง และการส่งมอบการเข้าถึงทรัพยากรขององค์กรที่ปลอดภัยและเชื่อถือได้

e-book เล่มนี้จะสำรวจผลลัพธ์ของการวิจัยของ Foundry ซึ่งเน้นย้ำถึงความสำคัญของกลยุทธ์ Zero Trust ในการช่วยให้ CISO ปกป้ององค์กรของตนจากความเสี่ยงที่มากมายจากเวกเตอร์การโจมตีจำนวนมาก นอกจากนี้ยังมีคำแนะนำเกี่ยวกับวิธีการใช้งาน Zero Trust สำหรับผู้ที่เริ่มต้นเส้นทาง

เกี่ยวกับแบบสำรวจ

Foundry ได้สำรวจธุรกิจในสหรัฐอเมริกาในเดือนกุมภาพันธ์และมีนาคม 2022 เพื่อสำรวจสถานะปัจจุบันของการปรับใช้ Zero Trust ผู้ตอบแบบสอบถามจะต้องเป็นผู้จัดการฝ่ายไอทีขึ้นไปในบริษัทที่มีพนักงานมากกว่า 500 คน และมีบทบาทในการซื้อผลิตภัณฑ์และบริการด้านการรักษาความปลอดภัยทางไซเบอร์

มีผู้ตอบแบบสอบถามทั้งหมด 250 คน สำหรับแบบสำรวจ 23 คำถาม

CSO Microsoft Security

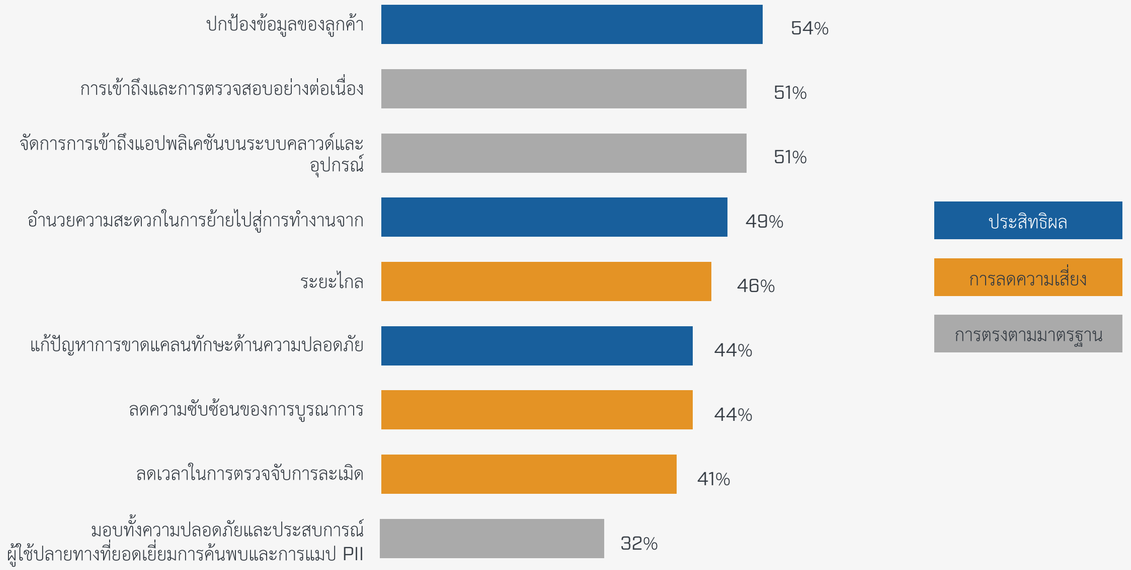
Zero Trust อยู่ที่นี่และมอบคุณค่า

จากผลการสำรวจ ควบคู่ไปกับการสัมภาษณ์เชิงลึกกับผู้บริหารด้านไอทีและความปลอดภัย จะเห็นได้ชัดว่าองค์กรส่วนใหญ่ให้ความสำคัญกับ Zero Trust และผู้ที่ปรับใช้คอมโพเนนต์ของ Zero Trust ต่างกันก็เห็นประโยชน์อยู่แล้ว

ผู้ตอบแบบสอบถามส่วนใหญ่ที่ใช้ Zero Trust (87%) กล่าวว่าสถาปัตยกรรมนี้ช่วยให้บรรลุวัตถุประสงค์เดิมหรือยิ่งกว่านั้นในการนำไปปฏิบัติ การปรับใช้ และการบูรณาการ

“[Zero Trust] ได้กลายเป็นขั้นตอนการปฏิบัติงานมาตรฐานสำหรับเรา ฉันไม่เห็นทางที่เราจะกลับไปเป็นเหมือนเดิม” ผู้อำนวยการฝ่ายไอทีของบริษัทค้าปลีกระดับโลกกล่าว (ผู้ตอบแบบสำรวจได้รับอนุญาตให้ปกปิดตัวตนเพื่อแลกกับการพูดคุยเกี่ยวกับแผนการรักษาความปลอดภัยของพวกเขาอย่างอิสระ)

ประโยชน์ที่ได้รับตั้งแต่เริ่มนำ Zero Trust มาใช้



12% ของผู้ตอบแบบสอบถามกล่าวว่าพวกเขาบรรลุผลประโยชน์เหล่านี้ *ทั้งหมด*

Source: Zero Trust Adoption Survey, มีนาคม 2022, Foundry Base: 250

CSO Microsoft Security

ผู้ตอบแบบสอบถาม 44% รายงานว่า Zero Trust ช่วยลดความซับซ้อนในการใช้งานสถาปัตยกรรมความปลอดภัยแบบบูรณาการ “เนื่องจากคุณกำลังจัดการและทำเฟรมเวิร์กซึ่งลดความซับซ้อนของทุกอย่างลง” CISO ของบริษัทคอลเซ็นเตอร์ที่มีพนักงาน 3,500 คนกล่าว

รองประธานและ CISO ของบริษัทผู้ให้บริการทางการเงินที่มีพนักงาน 17,000 คนกล่าวว่าการพิสูจน์ตัวตนแบบหลายปัจจัย (MFA) ที่บริษัทของเขานำไปใช้โดยเป็นส่วนหนึ่งของ Zero Trust ได้รับความนิยมอย่างมากในหมู่พนักงาน “ทำให้พนักงานมีความพึงพอใจมากขึ้น เพราะตอนนี้พวกเขาไม่ต้องใช้เครื่องที่บริษัทจัดหาให้และใช้ไคลเอนต์ VPN แต่พนักงานสามารถเข้าถึงทรัพยากรได้จากทุกที่” เขากล่าว

แนวคิดของการเข้าถึงที่มีสิทธิ์น้อยที่สุดก็ให้ผลตอบแทนเช่นเดียวกัน CISO กล่าว “เรามีข้อผิดพลาดร้ายแรงที่เกิดจากผู้ดูแลระบบน้อยลง เนื่องจากการปรับใช้ระบบการเข้าถึงสิทธิ์นั้น” เขากล่าว “พวกเขาได้รับสิทธิ N สำหรับบางสิ่งและกรอบเวลาที่เฉพาะเจาะจง ซึ่งหมายความว่าพวกเขามีโอกาสน้อยที่สร้างความผิดพลาด”

ด้วยความแพร่หลายของฟิชชิ่งและการโจมตีทางไซเบอร์อื่นๆ ที่เพิ่มขึ้น ผู้อำนวยการฝ่ายไอทีของบริษัทค้าปลีกจึงสรุปประโยชน์ของ Zero Trust ไว้ดังนี้: “หากเราไม่มีเครื่องมือประเภทนี้ เราอาจอยู่ในสถานการณ์ที่ย่ำแย่และต้องจ่ายเงินให้ใครบางคนเป็น bitcoin แล้วตอนนี้”

CSO Microsoft Security

สิ่งขับเคลื่อนการปรับใช้ Zero Trust

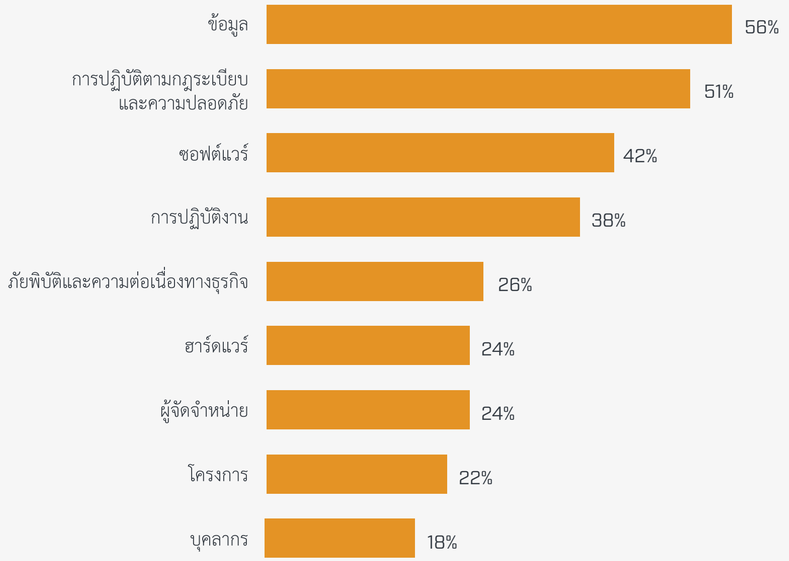
การบรรจบกันของเหตุการณ์มากมายกำลังผลักดันให้อย่างน้อยบริษัทต่างๆ พิจารณาสถาปัตยกรรม Zero Trust สิ่งสำคัญอันดับต้นๆ คือ ความจำเป็นในการจัดการความเสี่ยงต่อทรัพยากรที่มีอยู่มากมายจากภัยคุกคามจำนวนมาก ผู้ตอบแบบสำรวจระบุว่าเหตุการณ์ด้านความปลอดภัยที่ต้องใช้เวลาหลายปีมีสาเหตุหลายประการ ซึ่งเกิดขึ้นจากช่องโหว่ด้านความปลอดภัยจากบุคคลหรือองค์กรภายนอก สาเหตุอื่นๆ ได้แก่:

- ความเสี่ยงทางธุรกิจที่ไม่ได้คาดการณ์ไว้
- การกำหนดค่าบริการหรือระบบผิดพลาด
- การโจมตีจากภายในโดยเจตนาที่มุ่งร้าย
- ข้อผิดพลาดของผู้ใช้ที่ไม่รุนแรง รวมถึงเหยื่อฟิชชิ่ง
- ข้อมูลส่วนบุคคลอยู่ในอันตราย
- ซอฟต์แวร์ที่ไม่ได้แพตช์
- ข้อมูลประจำตัวถูกขโมย

เหตุการณ์เหล่านี้ก่อให้เกิดความเสี่ยงมากมายที่เกิดจากข้อมูล

สำหรับหลายๆ องค์กร การเปลี่ยนไปใช้การทำงานจากระยะไกลอย่างกะทันหันจากการระบาดครั้งใหญ่ได้เร่งแผนการปรับใช้ Zero Trust เนื่องจากรูปแบบการรักษาความปลอดภัยตามขอบเขตแบบเดิมนั้นล้าสมัย หลายองค์กรได้มุ่งหน้าไปในทิศทางนั้นแล้ว จากการที่พวกเขาได้ย้ายแอปพลิเคชันและโครงสร้างพื้นฐานด้านไอทีจำนวนมากขึ้นไปยังระบบคลาวด์ แต่การระบาดครั้งใหญ่ทำให้เกิดแรงกระเพื่อมมากขึ้น

หมวดหมู่อันดับต้นๆ ที่มีความเสี่ยงจากภัยคุกคามด้านความปลอดภัยทางไซเบอร์



Source: Zero Trust Adoption Survey, มีนาคม 2022, Foundry Base: 250

CSO Microsoft Security

ตัวอย่างเช่น CISO ของบริษัทเทคโนโลยีทางการแพทย์ที่มีพนักงาน 1,700 คนกล่าวว่าระบบคลาวด์และการระบาดครั้งใหญ่เป็นแรงผลักดันให้หันมาใช้ Zero Trust ซึ่งขณะนี้เป็นรากฐานที่ปลอดภัยสำหรับโมเดลการทำงานจากทุกที่ที่รออยู่ข้างหน้า

“ตัวขับเคลื่อนธุรกิจคือความจริงที่ว่าเราเป็นบริษัทบนระบบคลาวด์ และจำเป็นต้องรักษาความปลอดภัยให้กับสภาพแวดล้อมของเราได้” เขากล่าว “เรายังต้องจัดหาบุคลากรระยะไกลที่มีความสามารถในช่วงการระบาดครั้งใหญ่ [Zero Trust] ช่วยให้เราลดฟุตพรินต์ด้านอสังหาริมทรัพย์ลงได้อย่างมาก และมีแนวโน้มว่าเราจะยังคงเป็นบริษัทเสมือนจริงจากระยะไกลอย่างน้อย 60%”

CSO Microsoft Security

ภัยคุกคามไม่เคยลดน้อยลง

ความจำเป็นในการปฏิบัติตามกฎระเบียบยังเป็นแรงผลักดันให้โมเดลความปลอดภัยที่แข็งแกร่งขึ้นอีกด้วย “หน่วยงานกำกับดูแลกำลังจับตาดูเราอยู่ และพวกเขาคาดหวังให้เราปรับปรุงเฟรมเวิร์กการรักษาความปลอดภัยของเราต่อไป” รองประธานอาวุโสฝ่ายความปลอดภัยของข้อมูลทั่วโลกของบริษัทผู้ให้บริการทางการเงินที่มีพนักงาน 290,000 คน กล่าว

บางองค์กรได้ดำเนินการในเชิงรุกเพื่อมุ่งสู่ Zero Trust เพื่อหลีกเลี่ยงการละเมิดขนาดใหญ่ที่ทำให้พวกเขาตกเป็นเป้าด้วยเหตุผลที่ไม่ถูกต้อง “ทุกสิ่งล้วนเกี่ยวกับการทำให้เป็นเชิงรุกและพยายามไม่ให้เป็นข่าว” CIO ของสถาบันอุดมศึกษาที่มีพนักงาน 3,500 คนกล่าว “ซึ่งเป็นเรื่องสยองขวัญที่เกิดขึ้นจริงกับสถาบันอื่นๆ ในท้องที่ที่มีขนาดพอๆ กับเรา ซึ่งประสบปัญหามาเป็นเวลานาน”

คนอื่นๆ ได้ประสบกับเหตุการณ์ความปลอดภัยทางไซเบอร์ที่ร้ายแรงมาแล้ว ซึ่งทำให้พวกเขาทบทวนกลยุทธ์การรักษาความปลอดภัยอย่างรวดเร็ว หลังจากที่บริษัทประกันภัยที่มีพนักงาน 6,000 คนประสบกับการโจมตีด้วยแรนซัมแวร์ที่ปิดเครือข่ายองค์กรเป็นเวลาสองสัปดาห์ คำสั่งในการนำ Zero Trust มาปรับใช้นั้นมาจาก CEO โดยตรง “เราเร่งการนำไปใช้งาน” รองประธานฝ่ายพัฒนาด้านไอทีของบริษัทกล่าว “ในตอนแรก แน่นอนว่านั่นเป็นแนวทางปฏิบัติที่ดีที่สุดและจากนั้นก็ถูกเร่งความเร็วอย่างมากหลังจากที่เราถูกแรนซัมแวร์โจมตี”

ตัวเร่งปฏิกิริยาบนระบบคลาวด์

รองประธานและ CISO ของบริษัทผู้ให้บริการทางการเงินรายใหญ่กล่าวว่าทีมของเขาตระหนักดีถึงความต้องการสถาปัตยกรรมการรักษาความปลอดภัยใหม่เมื่อหลายปีก่อน เนื่องจากบริษัทเริ่มใช้ทรัพยากรบนระบบคลาวด์มากขึ้น และผู้ใช้มีอุปกรณ์พกพามากขึ้น

“เราตระหนักดีว่าสถาปัตยกรรมการรักษาความปลอดภัยเชิงรับแบบดั้งเดิมที่เราเคยใช้ในอดีตไม่อาจปกป้องเราจากผู้โจมตีในอนาคตได้” เขากล่าว

ความเป็นจริงนั้นชัดเจนขึ้นอย่างมากในต้นปี 2020 เมื่อบริษัทค้นพบว่าในปีก่อนหน้านั้นผู้โจมตีได้เจาะขอบเขตและขยายตัวไปในแนวนอนภายในสภาพแวดล้อมโดยไม่ถูกตรวจจับ “เราต้องการสถาปัตยกรรมใหม่ที่เราสามารถปกป้องและตรวจสอบการใช้ทรัพยากรเหล่านั้นได้ทุกที่ และ Zero Trust เป็นสถาปัตยกรรมที่ออกแบบมาเพื่อสิ่งนั้น”

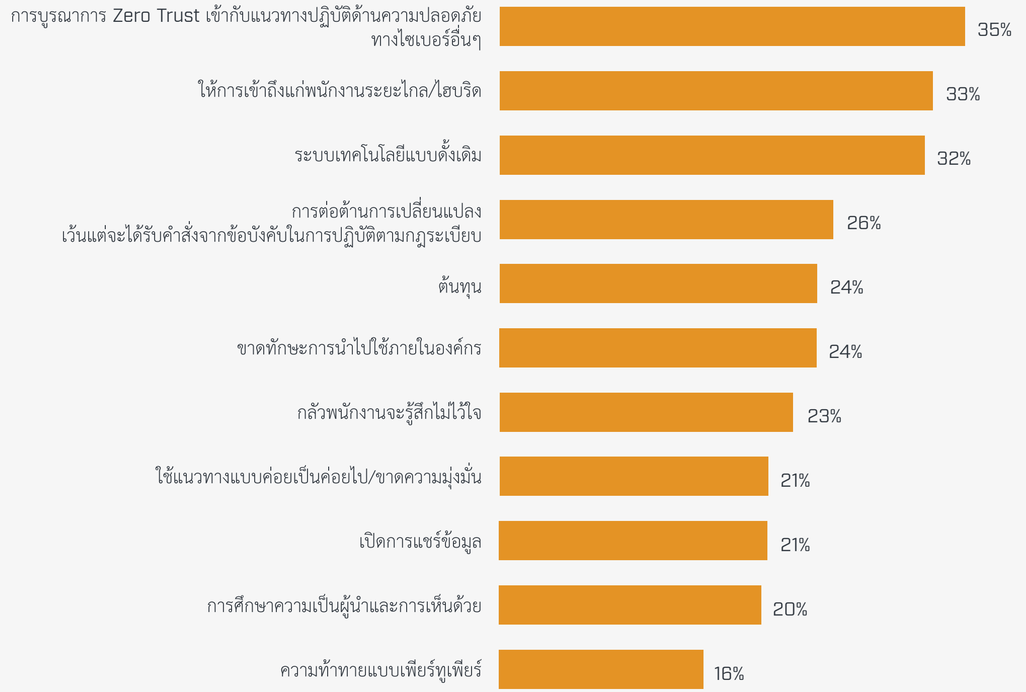
CSO Microsoft Security

อุปสรรคในการปรับใช้ Zero Trust

สำหรับองค์กรหลายแห่ง Zero Trust แสดงถึงการเปลี่ยนแปลงที่พื้นฐานของโครงสร้างการรักษาความปลอดภัย กระบวนการ และกรอบความคิด ซึ่งอธิบายถึงอุปสรรคบางอย่างที่พวกเขาต้องเอาชนะก่อนที่จะปรับใช้

“มีไซโลที่แตกต่างกันมากมายที่เราเริ่มต้นภายในองค์กร” CISO ของบริษัทคอลเซ็นเตอร์ระบุ โดยอธิบายว่าทีมเซิร์ฟเวอร์ เครือข่าย และฐานข้อมูลแต่ละทีมมีเว็บเซิร์ฟเวอร์และเครื่องมือที่ต่างกันออกไป “นั่นทำให้เราอึดอัดเพราะทุกคนมีความคิดที่แตกต่างกันเกี่ยวกับว่าจะไปที่ไหนและทำอย่างไร”

อะไรคือสิ่งที่เหนี่ยวรั้งไม่ให้ปรับใช้ Zero Trust



Source: Zero Trust Adoption Survey, มีนาคม 2022, Foundry Base: 250

CSO Microsoft Security

Anthony Mocny ผู้จัดการฝ่ายการตลาดผลิตภัณฑ์อาวุโสของ Zero Trust ที่ Microsoft เปิดเผยว่าการค้นพบปัญหาดังกล่าวอาจเป็นผลข้างเคียงเชิงบวกของ Zero Trust “ในฐานะที่สถาปัตยกรรม Zero Trust ได้รับการออกแบบมาเพื่อทำลายไซโลของทีมรักษาความปลอดภัยที่อยู่ภายในเสาหลักของเทคโนโลยี และช่วยให้ทีมทำงานร่วมกันได้อย่างเหนียวแน่น” เขากล่าว “ซึ่งอาจจะหมายถึงการเปลี่ยนแปลงทางวัฒนธรรมเช่นกันในแง่ของวิธีการที่ทีมทำงานร่วมกัน”

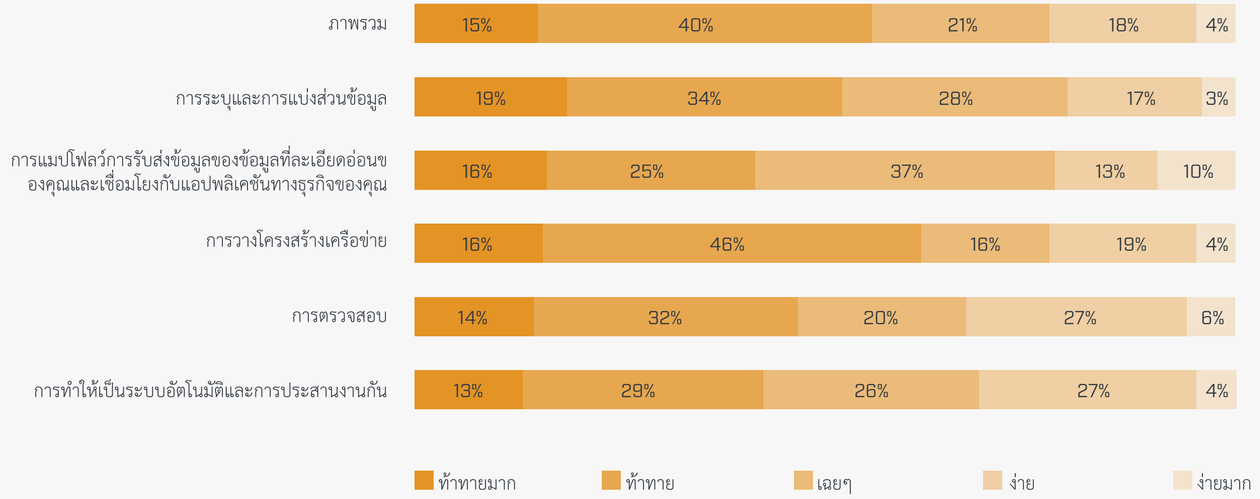
สำหรับรองประธาน/CISO ของบริษัทให้บริการทางการเงิน แอปพลิเคชันรุ่นเก่าเป็นอุปสรรคต่อการก้าวไปสู่ Zero Trust “แอปพิลเคชันต้องได้รับการปรับปรุงใหม่ด้วยเทคโนโลยีการยืนยันตัวตนที่ทันสมัย” เขากล่าว “ขึ้นอยู่กับว่าแอปพลิเคชันเก่าแค่ไหน ซึ่งอาจไม่ใช่เรื่องง่ายเลยที่จะทำ”

CSO Microsoft Security

ความท้าทาย ในการปรับใช้

เมื่อบริษัทต่างๆ เริ่มต้นเส้นทาง Zero Trust ความท้าทายในการนำไปใช้งานต่างๆ ก็อาจเกิดขึ้นได้เช่นกัน กว่าครึ่งของผู้ตอบแบบสำรวจ (56%) ยอมรับว่าการนำ Zero Trust ไปใช้นั้นท้าทายหรือท้าทายมาก โดยเฉพาะอย่างยิ่ง:

การใช้งาน **Zero Trust** ท้าทายมากเพียงใด



Source: Zero Trust Adoption Survey, มีนาคม 2022, Foundry Base: 168

CSO Microsoft Security

ความท้าทายเกี่ยวกับการแบ่งส่วนและการแบ่งส่วนย่อยเกิดขึ้นบ่อยครั้งในการสัมภาษณ์เชิงลึก

“คุณกำลังแบ่งส่วนเครือข่ายของคุณออกเป็นแต่ละโฮสต์” รองประธาน/CISO ของบริษัทผู้ให้บริการทางการเงินกล่าว “ก็เหมือนกับการวางไฟร์วอลล์เล็กๆ ไว้ระหว่างทุกโฮสต์บนเครือข่ายภายใน คุณจึงสามารถดูการรับส่งข้อมูลทั้งหมดและควบคุมได้โดยตรงที่เครื่องแต่ละเครื่อง มีประโยชน์ด้านความปลอดภัยมหาศาล แต่กลับเป็นสิ่งที่ยากมากที่จะนำไปใช้ เพราะตอนนี้คุณต้องจัดการไฟร์วอลล์นับหมื่น”

การแมปโฟลว์การรับส่งข้อมูลอาจเป็นอีกกระบวนการหนึ่งที่มีระยะเวลาหลายเดือน สำหรับ CTO ของบริษัทสำนักพิมพ์และสื่อที่มีพนักงาน 5,000 คน หลังจากกำหนดข้อมูลสำคัญ แอปพลิเคชัน และบริการเครือข่ายที่จำเป็นต้องปกป้อง “เราจับคู่ขั้นตอนธุรกรรมในเครือข่ายและพยายามทำความเข้าใจให้เป็นกลุ่มของข้อมูล” เขากล่าว “[จากนั้นเรา] แบ่งส่วนของข้อมูลนั้นและวิธีที่พาดยาวไปตามแนวเครือข่าย แม้กระทั่งลงไปที่แพ็กเก็ตข้อมูลเดียว” ณ จุดนั้น บริษัทได้ใช้นโยบาย Zero Trust กับโฟลว์การรับส่งข้อมูลแต่ละประเภท “เรายังสร้างความสามารถใหม่ๆ ในการตรวจสอบและบำรุงรักษาเครือข่ายของเราอีกด้วย”

แม้จะมีความท้าทายอยู่บ้าง แต่ผู้ตอบแบบสอบถามจำนวนมากเชื่อว่าในที่สุด Zero Trust จะทำให้การดำเนินงานในแต่ละวันง่ายขึ้น ด้วยเทคโนโลยีแบบเดิมๆ “ต้องใช้เวลาหลายวันในการเปลี่ยนแปลง คุณต้องผลักดันทั่วทั้งคอมโพเนนต์ฮาร์ดแวร์และซอฟต์แวร์ทั้งหมด และเรากำลังใช้ทรัพยากรจำนวนมากสำหรับสิ่งนั้น” รองประธานอาวุโสฝ่ายรักษาความปลอดภัยของข้อมูลทั่วโลกของบริษัทที่ให้บริการทางการเงินกล่าว “เมื่อเราดูที่ Zero Trust สิ่งนี้ช่วยลดความซับซ้อนทางสถาปัตยกรรมในระยะยาว และลดจำนวนพนักงานที่เราจำเป็นต้องมีเพื่อทำงานประเภทเดียวกัน”

แนวทางปฏิบัติที่ดีที่สุดในการนำ **Zero Trust** มาใช้

จากการที่บริษัทจำนวนมากขึ้นใช้สถาปัตยกรรม Zero Trust ซึ่งพวกเขากำลังพัฒนาแผนงานและแนวทางปฏิบัติที่ดีที่สุดเพื่อให้ผู้อื่นได้ปฏิบัติตาม นี่คือ 5 ข้อควรพิจารณาเมื่อวางแผนปรับใช้

อย่าใช้เวลามากเกินไปในการเริ่มต้น

การแมปกลยุทธ์ Zero Trust อาจเป็นเรื่องที่น่ากลัว หากคุณดูเฉพาะในบริบทกว้างๆ ว่าต้องแก้ไขนโยบายและการป้องกันทั่วทั้งเครือข่าย ข้อมูล แอปพลิเคชัน ข้อมูลประจำตัว อุปกรณ์ปลายทาง และโครงสร้างพื้นฐาน “ในตอนแรก เราแค่มองไปที่ภูเขาขนาดใหญ่เพื่อปีนขึ้นไป และเราสงสัยว่าเราจะทำกันจริงๆ ใช่ไหม” CIO ระดับสูงกล่าว “คุณแค่ต้องก้าวไปทีละขั้น”

ในที่สุด CIO และทีมของพวกเขาก็ใช้วิธี “ทำตามเงิน” โดยให้ความสำคัญกับการแบ่งส่วนแอปพลิเคชันการเงินและบัญชีเงินเดือนในเครือข่ายที่แยกจากกัน

การระบุสินทรัพย์ที่สำคัญที่สุดในการปกป้องคือแนวทางที่ดี ตามที่ Mocny กล่าว “คำนึงถึงเหตุผลที่คุณใช้ Zero Trust ตั้งแต่แรก“ เขากล่าว

เมื่อสงสัย ให้เริ่มด้วยหลายปัจจัย หรือ **multifactor**

เมื่อจัดลำดับความสำคัญของสแตกความปลอดภัย CISO และผู้จัดจำหน่ายด้านการรักษาความปลอดภัยจำนวนมากแนะนำว่าในขั้นต้นให้เน้นที่การรับรองความถูกต้องและการปกป้องข้อมูลประจำตัวอื่นๆ “หากคุณไม่มีจุดเริ่มต้นในใจ การพิสูจน์ตัวตนแบบหลายปัจจัย (MFA) เป็นจุดเริ่มต้นที่ดีที่ควรพิจารณา” Mocny กล่าว

Microsoft ประมาณการว่าการรับรองความถูกต้องแบบหลายปัจจัยสามารถป้องกันการโจมตีโดยอาศัยข้อมูลประจำตัวได้มากกว่า 90%

รองประธาน/CISO ของบริษัทที่ให้บริการทางการเงินเห็นด้วย “การรับรองความถูกต้องเป็นองค์ประกอบพื้นฐานของการนำสถาปัตยกรรม Zero Trust ไปใช้ ไม่มีองค์ประกอบอื่นใดจะได้ผล หากคุณไม่สามารถตรวจสอบตัวตนของผู้ใช้ปลายทางได้ ดังนั้นเราจึงเริ่มต้นที่นั่น”

ถัดมารองประธาน/CISO ของบริษัทที่ให้บริการทางการเงินเห็นได้จัดการกับองค์ประกอบของเครือข่าย ซึ่งให้ประโยชน์ในการสนับสนุนพนักงานที่ทำงานจากระยะไกลทันที ทีมได้แยกส่วนย่อยออกไปจนกว่าจะถึงช่วงท้ายของเส้นทาง เนื่องจากธุรกิจส่วนใหญ่ไม่สามารถมองเห็นได้ชัดเจน “เมื่อคุณทำเสร็จแล้ว คุณจะปลอดภัยมากขึ้นอย่างเห็นได้ชัด แต่ไม่มีใครรู้ถึงความแตกต่าง” เขากล่าว

CSO Microsoft Security

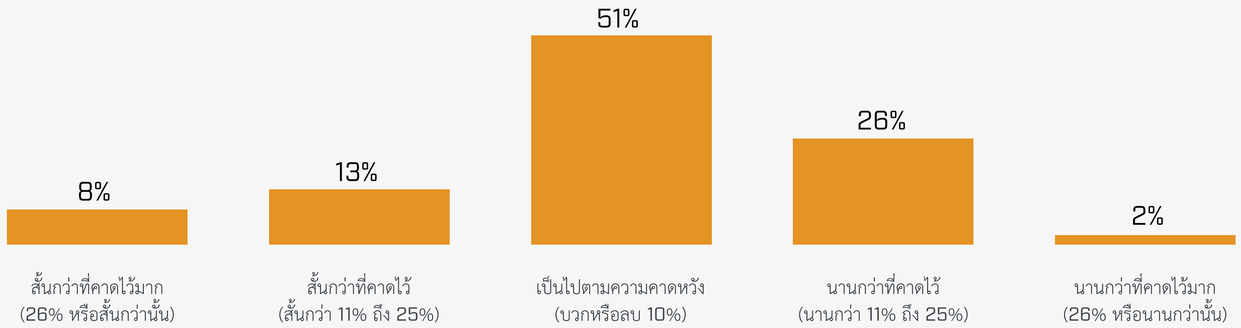
อยู่กับความเป็นจริงเกี่ยวกับไทม์ไลน์

สิ่งสำคัญคือ CISO จะต้องกำหนดความคาดหวังที่เป็นจริงได้เกี่ยวกับการปรับใช้ Zero Trust “การนำสถาปัตยกรรม Zero Trust ไปใช้นั้นเป็นแค่โปรแกรม ไม่ใช่โครงการ” รองประธาน/CISO ของบริษัทที่ให้บริการทางการเงินกล่าว “นี่เป็นการเปลี่ยนแปลงครั้งใหญ่ ไม่มีการปรับใช้สถาปัตยกรรม Zero Trust ที่ง่ายและรวดเร็ว ให้ทำสิ่งที่เกี่ยวข้องกับโครงการมากมายอย่างถูกต้องซึ่งน่าจะใช้เวลานานหลายปี”

รองประธานอาวุโสฝ่ายการเงินของเขาเห็นด้วย “ผมไม่คิดว่าเราจะทำสำเร็จเพราะมีเทคโนโลยีใหม่ๆ ออกมาเสมอ มีมัลแวร์ใหม่ๆ ออกมาอยู่เสมอ มีภัยคุกคามใหม่ๆ ออกมาเสมอ” เขากล่าว

ผู้ตอบแบบสำรวจส่วนใหญ่ (72%) กล่าวว่าไทม์ไลน์การปรับใช้เป็นไปตามแผนหรือเร็วกว่า โดยที่เหลือระบุว่าการนำไปใช้งานนั้นใช้เวลานานกว่าที่คาดไว้

Zero Trust จะบรรลุวัตถุประสงค์ตามไทม์ไลน์ของคุณหรือไม่



Source: Zero Trust Adoption Survey, มีนาคม 2022, Foundry Base: 168

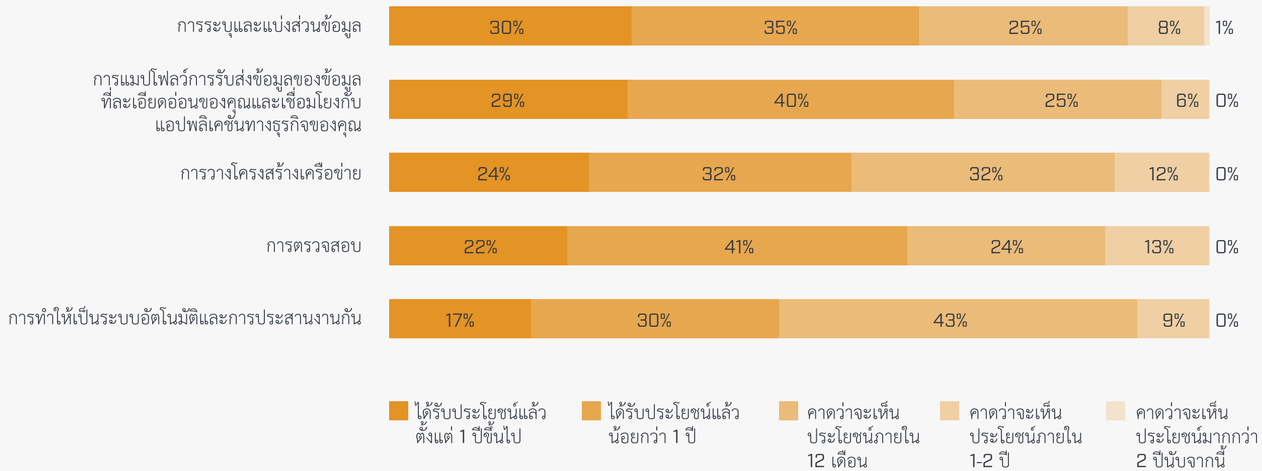
CSO Microsoft Security

วัดผลไปพร้อมๆ กับการปรับใช้

ในขณะที่การปรับใช้ Zero Trust กำลังดำเนินอยู่ CISO สามารถและควรสร้างไมล์สโตนไปพร้อมๆ กันเพื่อวัดความคืบหน้า เป็นสัญญาณที่ดีว่าประมาณ 2 ใน 3 ของผู้ตอบแบบสำรวจกล่าวว่าพวกเขาได้รับประโยชน์จากด้านต่างๆ โครงการเป็นส่วนใหญ่ภายในหนึ่งปี และอีกประมาณ 1 ไตรมาสหรือมากกว่านั้นไม่เกิน12 เดือน จากกิจกรรมหลักต่างๆ ได้แก่ การระบุและแบ่งส่วนข้อมูล การแมปโฟลว์การรับส่งข้อมูล และการวางโครงสร้างเครือข่าย

“Zero Trust เปรียบดังเส้นทางเนื่องจากการประเมินผลอย่างต่อเนื่องที่คุณต้องใช้ในการป้องกันรูปแบบของการโจมตีที่เปลี่ยนแปลงไป” Mocny กล่าว “คอยมองหาการปรับปรุงอยู่เสมอ”

ไทม์ไลน์ในการรับประโยชน์จาก **Zero Trust**



Source: Zero Trust Adoption Survey, มีนาคม 2022, Foundry Base: 103

CSO Microsoft Security

โฟกัสที่คน ไม่ใช่แค่เทคโนโลยี

การเข้าถึงโมเดลความปลอดภัย Zero Trust ในวงกว้างส่งผลต่อพนักงานทุกคน รวมถึงทีมไอทีและความปลอดภัยที่ได้รับมอบหมายให้ปรับใช้ ด้วยเหตุนี้ เช่นเดียวกับโครงการเทคโนโลยีขนาดใหญ่ สิ่งสำคัญคือต้องตรวจสอบให้แน่ใจว่าการปรับใช้สอดคล้องกับกระบวนการใหม่และแนวทางการจัดการการเปลี่ยนแปลงเพื่อให้แน่ใจว่าการเปิดตัวจะราบรื่นและประสบความสำเร็จ

“นอกจากการเปลี่ยนแปลงทางเทคโนโลยีแล้ว ยังมีการเปลี่ยนแปลงทางวัฒนธรรมอีกด้วย” Mocny กล่าว “หากคุณมีทีมหลายทีมที่จัดการกับความปลอดภัย รวมถึงสถาปนิกเครือข่ายหรือผู้เชี่ยวชาญด้านข้อมูลประจำตัว คุณต้องเปลี่ยนวิธีที่ทีมเหล่านั้นทำงานร่วมกัน คุณต้องทำลายไซโลเพื่อให้แน่ใจว่าเทคโนโลยีทั้งหมดทำงานร่วมกันอย่างกลมกลืน”

การกำจัดระบบไซโลเกี่ยวข้องกับการจัดหาทีมจากทุกฝ่ายที่เกี่ยวข้องอย่างใกล้ชิดในโครงการนำร่องและพิสูจน์แนวคิด (POC) ผู้อำนวยการระบบไอทีกับบริษัทโทรคมนาคมซึ่งมีพนักงานประมาณ 2,000 คนได้เรียนรู้บทเรียนดังกล่าวหลังจากประสบปัญหาความล้มเหลวเพียงจุดเดียวในระหว่างการปรับใช้ ซึ่งรวมถึงบริการที่ไม่สามารถรับรองความถูกต้องและ "ไม่น่าเชื่อถือ" ในทันที ซึ่งแสดงผลเหมือนกับว่าบางระบบไม่พร้อมใช้งาน

“การปรับใช้บริการหนึ่งอาจส่งผลเป็นโดมิโนและทำให้บริการอื่นๆ แย่ลง” เขากล่าว นับจากนี้ไป “เราจะระมัดระวังมากขึ้น ให้เวลา POC มากขึ้น ทบทวนให้มากขึ้นและตรวจสอบทางสถาปัตยกรรมกับผู้เชี่ยวชาญเฉพาะด้านเพิ่มเติมก่อนที่จะปรับใช้”

ROI ของ Zero Trust

งานวิจัยที่ดำเนินการโดย **Forrester Consulting Total Economic Impact™** ในปี 2021 ระบุปริมาณการประหยัดต้นทุนและผลประโยชน์ทางธุรกิจของโซลูชัน Microsoft Zero Trust จาก 5 องค์กรที่ Forrester สัมภาษณ์ องค์กรแบบผสมได้รับผลตอบแทนจากการลงทุน 92% ในระยะเวลาสามปีโดยการใช้สถาปัตยกรรม Zero Trustกับ Microsoft

องค์กรแบบผสมนี้ยังประหยัดเงินได้โดยเฉลี่ย 20 ดอลลาร์ต่อพนักงานหนึ่งคนต่อเดือนโดยไม่จำเป็นต้องใช้เครื่องมือรักษาความปลอดภัยที่กลายเป็นสิ่งซ้ำซ้อนภายใต้ Zero Trust รวมถึงโซลูชันการจัดการอุปกรณ์ปลายทาง แอนตี้ไวรัส และป้องกันมัลแวร์

CSO Microsoft Security

คุณอยู่จุดใดบนเส้นทางสู่ Zero Trust

จากการสำรวจระบุว่าประโยชน์ของโมเดลการรักษาความปลอดภัยแบบ Zero Trust นั้น
มีความสำคัญมากกว่าความท้าทายในการปรับใช้ที่ CISO และทีมรักษาความปลอดภัยที่กำลังเผชิญอยู่
การรับมือกับความท้าทายเหล่านี้ด้วยแผนงานที่รอบคอบสามารถช่วยให้องค์กรของคุณปรับปรุง
การป้องกัน ลดความเสี่ยง และเริ่มสร้างมูลค่าให้กับธุรกิจได้อย่างรวดเร็ว

หากต้องการประเมินระดับการเติบโตของ Zero Trust ขององค์กร
และดูทรัพยากรการปรับใช้ที่ใช้งานได้จริง ลองทำ**แบบประเมินรูปแบบ**
การเติบโตของ Zero Trust ของ Microsoft