5 ขั้นในการไปสู่ SASE – 5 Steps to SASE

คู่มือผู้บริหารของคุณในการไปสู่ SASE – การทำให้เกิดพนักงาน "ทำงานจากทุกที่"

Table of Contents

คำนำ

ในยุคการทำงานระยะไกลในปัจจุบัน การเข้าถึงทรัพยากรทางธุรกิจอย่างปลอดภัยจากทุกสถานที่ด้วยนโยบายการรักษาความปลอดภัยที่บังคับใช้อย่างสม่ำเสมอทุกที่เป็นสิ่งที่ต้องมีสำหรับองค์กรแบบกระจาย

การบรรจบ (ของเทคโนโลยี) ของแนวทางการทำงานที่เป็นคลาวด์ เช่น Secure Access Service Edge (SASE) ช่วยให้คุณใช้งานเว็บคลาวด์ และแอปส่วนตัวได้อย่างมีประสิทธิภาพ โดยได้รับการปกป้องจากภัยคุกคามขั้นสูงและการสูญหายของข้อมูล แต่อะไรเป็นตัวกำหนดรูปแบบของแพลตฟอร์ม SASE ที่สมบูรณ์? ไม่ใช่การเข้าถึง (เครือข่าย) แต่เป็นข้อมูล พูดให้ถูกต้องยิ่งขึ้นคือการควบคุมการใช้ข้อมูล

ซึ่งแตกต่างจากโซลูชั่นที่ให้ความสำคัญกับการเข้าถึง (access-focused solutions) แนวทางที่ให้ความสำคัญกับข้อมูลเป็นหลัก (data-first approach) ในการทำ SASE ช่วยเพิ่มประสิทธิภาพและลดความเสี่ยง ช่วยให้คุณสามารถปรับปรุงให้ดีขึ้นในการเข้าถึงข้อมูล แอป และบริการ และรักษาความปลอดภัยข้อมูลได้ทุกที่ที่มีการใช้งาน คู่มือนี้อธิบายประโยชน์หลักของสถาปัตยกรรม SASE ที่ให้ความสำคัญกับข้อมูลเป็นหลักซึ่งรวมการบังคับใช้นโยบายข้อมูลที่เป็นรูปแบบเดียวกัน (uniform enforcement of data policies) ตัวแทนแบบครบวงจร (unified agents) โมเดลการปรับใช้ที่ยืดหยุ่น และการบังคับใช้นโยบายตามความเสี่ยงเพื่อปกป้องข้อมูลสำคัญและผู้ใช้งานของคุณอย่างต่อเนื่อง

องค์กรที่ใช้เทคโนโลยีในด้านความปลอดภัยบนคลาวด์ ความปลอดภัยเครือข่ายหรือการดำเนินการด้านความปลอดภัยอยู่แล้ว สามารถใช้คู่มือนี้เพื่อทำความเข้าใจขั้นตอนต่อไปในการเปิดใช้งานความสามารถหลัก (in activating key capabilities) ในแพลตฟอร์ม SASE ที่ให้ความสำคัญกับข้อมูลเป็นหลัก

การปกป้องธุรกิจของคุณเริ่มต้นด้วยการปกป้องผู้ใช้และข้อมูล – ในทุกที่

(Protecting your business starts with protecting users and data – everywhere)

นี่คือความเป็นจริงของวันนี้: ข้อมูลของคุณอยู่ในระบบคลาวด์ บุคลากรของคุณกำลังทำงานในทุกสถานที่ ทั้งที่บ้าน ในสำนักงาน และบนท้องถนน และการรักษาความปลอดภัยต้องเข้าไปมีส่วนร่วมด้วย พนักงาน ผู้รับเหมา และผู้ผลิตจำหน่ายสินค้าจำเป็นต้องเข้าถึงข้อมูลทางธุรกิจ เช่น ข้อมูลลูกค้าเข้าถึงบริการคลาวด์ เช่น Office 365 และเข้าถึงแอปพลิเคชั่นส่วนตัวขององค์กร เช่น ERP ไม่ว่าพวกเขาหรือข้อมูลจะอยู่ที่ใดก็ตาม

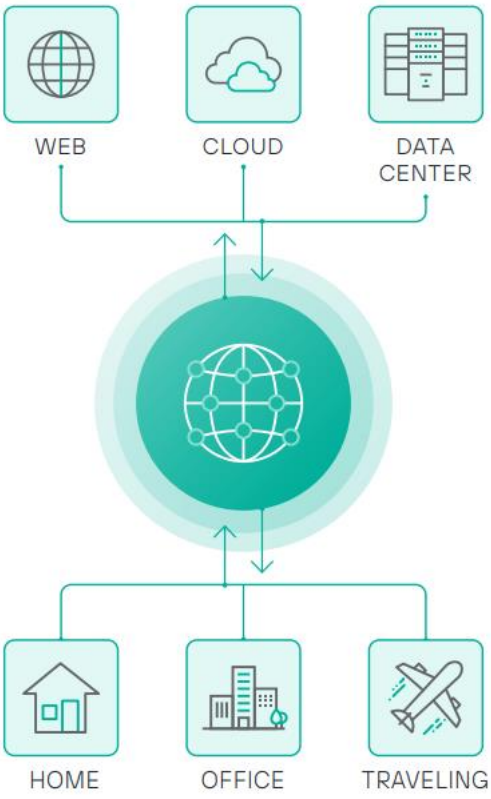
การปฏิสัมพันธ์กันของผู้ใช้งานและข้อมูลสำคัญทำให้บุคลากรและระบบของคุณเปิดเผยต่อการโจมตีรูปแบบใหม่ๆ โดยโจรดิจิทัลหรือรัฐชาติ (nation states) ที่ต้องการขโมยข้อมูลที่ละเอียดอ่อนหรือทรัพย์สินทางปัญญาของคุณ วิธีการแบบเก่าที่ใช้ฮาร์ดแวร์นั้นจะตามไม่ทันและสร้างความซับซ้อนมากขึ้นเมื่อจำนวนชิ้นส่วนที่เคลื่อนไหวมีจำนวนเพิ่มขึ้น

ขอบเขตของระบบรักษาความปลอดภัยได้เปลี่ยนจากการครอบคลุมตามโครงสร้างพื้นฐานขององค์กรของคุณ ขยายตามไปยังทุกที่ที่พนักงานของคุณทำงานและอุปกรณ์ที่พวกเขากำลังทำงานอยู่ แต่ภารกิจของคุณยังคงเหมือนเดิม: คือเพื่อให้บุคลากรของคุณเข้าถึงข้อมูลและบริการที่จำเป็นโดยไม่ขัดขวางประสิทธิภาพการทำงานหรือทำให้ข้อมูลสำคัญตกอยู่ในความเสี่ยง

เมื่อองค์กรมีลักษณะกระจายตัวมากขึ้นกว่าที่เคยเป็น การวางซ้อนกันของอุปกรณ์ต่างๆ ไว้ที่สถานที่ทำงานทุกแห่งหรือใช้ผลิตภัณฑ์ที่แตกย่อยเป็นส่วนย่อยกระจัดกระจายติดไปกับคนทำงานทางไกล ทำให้เกิดช่องโหว่สำหรับผู้โจมตี เสียค่าใช้จ่ายมากเกินไป และเป็นการใช้ทรัพยากรไอทีที่ขาดแคลนให้หมดเปลืองไป

เมื่อเทียบให้เห็นถึงความแตกต่างกับที่กล่าวไปแล้ว Zero Trust เป็นรูปแบบสำหรับการรักษาความปลอดภัยในปัจจุบัน: ทุกคนต้องได้รับการอนุญาตอย่างชัดแจ้งทุกครั้งที่จะเข้าถึงทรัพยากร หรือใช้ข้อมูล วิธีการแบบเบนประจบเข้าหากันบนคลาวด์ เช่น SASE คือวิธีที่คุณสามารถส่งมอบการรักษาความปลอดภัยนั้นได้ SASE ไม่เพียงแค่การย้ายระบบอุปกรณ์เก่าๆ ไปยังระบบคลาวด์ แต่เป็นการสร้างผลิตภัณฑ์ขึ้นใหม่ในรูป

ความสามารถภายในแพลตฟอร์มเพื่อขจัดความซ้ำซ้อนและทำให้การดำเนินงานง่ายขึ้น เมื่อบุคลากรและข้อมูลไปอยู่ทุกหนทุกแห่ง ระบบการรักษาความปลอดภัยจึงต้องตอบคำถาม: ในโลกของการกระจัดกระจายแบบนี้ คุณจะควบคุมการเข้าถึงและการใช้งานอย่างต่อเนื่องได้อย่างไร



ขอบเขตการรักษาความปลอดภัยได้เปลี่ยนจากครอบคลุมโครงสร้างพื้นฐานขององค์กรของคุณขยายตามไปยังทุกที่ที่พนักงานของคุณทำงานและอุปกรณ์ใดก็ตามที่พวกเขากำลังทำงานอยู่

บันได 5 ขั้นสู่ SASE (5 Steps to SASE)

เส้นทางสู่ SASE สามารถเริ่มต้นได้จากจุดใดก็ได้ ขึ้นอยู่กับว่าความต้องการที่สำคัญที่สุดของคุณจะเป็นการให้ความปลอดภัยการเข้าถึงของผู้ใช้งานหรือเป็นการรักษาข้อมูลให้ปลอดภัย ลำดับความสำคัญของคุณอาจมีแตกต่างหลายประการ เช่น การให้สามารถทำงานระยะไกลหรือการปกป้องสาขาเพื่อป้องกันการโจรกรรมทรัพย์สินทางปัญญา (IP theft) หรือการปฏิบัติตามกฎระเบียบ ไม่ว่าในกรณีใดก็ตามคุณสามารถเริ่มต้นการเดินทาง SASE ของคุณได้ห้าวิธีหลัก และดำเนินการตามขั้นตอนอื่นๆ ตามความจำเป็น:

- ปกป้องผู้ปฏิบัติงานระยะไกลในเว็บและคลาวด์: เราเห็นการเริ่มต้นของยุคใหม่ของ “พนักงานทุกแห่งหน” ที่มีอิสระในการทำงานจากทุกที่และทุกเวลา
- ควบคุมการเข้าถึงคลาวด์และแอปส่วนตัวโดยไม่ต้องใช้ VPN: คุณต้องปรับแต่งให้เป็นความปลอดภัยสำหรับบุคคล (personalize security) เพื่อให้ผู้ใช้แต่ละคนสามารถเข้าถึงแอปและทรัพยากรที่ต้องการได้เท่านั้น และภายใต้การมองเห็นและการควบคุมธุรกิจของคุณอย่างสมบูรณ์
- ปกป้องการใช้ข้อมูลในทุกสถานที่: งานของการรักษาความปลอดภัยคือป้องกันไม่ให้มีการใช้ข้อมูลที่สำคัญในทางที่ผิด – ไม่ว่าจะโดยไม่ได้ตั้งใจหรือโดยมุ่งร้าย – จากอุปกรณ์ปลายทางไปถึงระบบคลาวด์
- เชื่อมต่อและปกป้องสำนักงานสาขา: ผู้ใช้ที่ไซต์งานระยะไกลต้องสามารถเข้าถึงเว็บ คลาวด์ และแอปส่วนตัวได้อย่างรวดเร็วและปลอดภัย โดยไม่มีค่าใช้จ่ายหรือความซับซ้อนของลิ้งค์ MPLS ส่วนตัวหรือต้องมีการส่งข้อมูลย้อนกลับไปยัง HQ
- เฝ้าติดตามตรวจสอบความเสี่ยงของผู้ใช้อย่างต่อเนื่อง: การควบคุมการใช้ข้อมูลต้องใช้ทั้งแนวทาง Zero Trust และความเข้าใจในพฤติกรรมของผู้คนเพื่อพิจารณาว่า การกระทำของพวกเขากำลังสร้างความเสี่ยงที่อาจกลายเป็นการละเมิดความปลอดภัย (breaches) หรือไม่

SASE กำลังได้รับความนิยมเพราะมันมาแทนที่การสแต็คของอุปกรณ์เครือข่ายและอุปกรณ์ความปลอดภัยด้วยบริการแบบคลาวด์ที่เป็นการบรรจบกัน (ของเครือข่ายและของความปลอดภัย) ซึ่งจะปรับปรุงเพิ่มให้ดีขึ้นและทำให้ง่ายขึ้นในการปกป้องผู้ใช้และข้อมูลได้อย่างมากมาย เป้าหมายได้เปลี่ยนจากการเปลี่ยนแปลงทางดิจิทัล (digital transformation) ไปสู่การเปลี่ยนแปลงทางธุรกิจ (business transformation) ทว่าวิธีการจัดการแบบเดิมๆ ในการเชื่อมต่อและการรักษาความปลอดภัยไม่สามารถตามทัน

SASE ที่ให้ความสำคัญกับการเข้าถึงสามารถเป็นจุดเริ่มต้น – แต่ยังไม่เพียงพอ (Access-centric SASE is a start – but not enough)

ความยิ่งใหญ่ดังเช่น SASE การนำมาใช้งานในบางครั้ง เพียงแต่เป็นการนำผลิตภัณฑ์หลายชนิดมาใช้งานร่วมกันเท่านั้น ซึ่งเป็นการทรยศต่อคุณสมบัติดั้งเดิมของการเป็นโซลูชั่นโครงสร้างพื้นฐานโซลูชั่นแบบจุด (ทำหน้าที่อย่างใดอย่างหนึ่งไม่เป็นแบบองค์รวม)

- การพึ่งพาอุปกรณ์ปลายทาง (ที่ทำงาน) ชนิดเดียว (single endpoints) หลายๆ ตัวหรือหลายๆ ประเภทของงานในเครือข่ายหรือบนระบบคลาวด์นำไปสู่การแผ่ขยายออกมามากมายของตัวเอเยนต์ของอุปกรณ์ปลายทาง
- การขาดความเป็นหนึ่งเดียว (lack of unification) หมายความถึงนโยบายความปลอดภัยไม่คงที่สม่ำเสมอเปราะบาง ซับซ้อน หรือล้าสมัย
- ในทางกลับกัน บริการที่เป็นบนคลาวด์อย่างเดียวจะละเลย (ไม่สนใจ) ไซต์ที่ต้องการการควบคุมและการบังคับใช้จากในพื้นที่และแบบไฮบริด
- SASE ที่ให้ความสำคัญกับการเข้าถึง (Access-centric SASE) มุ่งเน้นไปที่เนื้อหา (focuses on content) มากเกินไปและละเลยบริบท (context) รอบๆ ผู้ใช้ที่โต้ตอบ (interacting) กับข้อมูลและระบบ

วิธีการของ SASE ที่ให้ความสำคัญกับการเข้าถึงนั้นเปราะบางเกินไปและไม่สามารถปรับขนาดเพื่อตอบสนองต่อความต้องการแบบไดนามิกของพนักงานระยะไกลจำนวนมากในปัจจุบันและต่อการเปลี่ยนแปลงทางธุรกิจ (business transformation)

SASE จะแทนที่การสแต็คของฮาร์ดแวร์เครือข่ายและความปลอดภัยด้วยบริการบนคลาวด์แบบบรรจบรวม (ของเทคโนโลยี)

การรักษาความปลอดภัย SASE ที่ให้ความสำคัญกับข้อมูลเป็นหลัก

(Data – first SASE security)

ท้ายที่สุด เครือข่ายและการรักษาความปลอดภัยล้วนเกี่ยวกับการช่วยให้ผู้คนเข้าถึงและใช้ข้อมูลทางธุรกิจได้อย่างปลอดภัย

SASE แบบอิงการเข้าถึงควรไปไกลกว่าการเข้าถึงโดยต้องสามารถเข้าไปปกป้องวิธีการใช้ ข้อมูลอย่างต่อเนื่อง เราหมายถึงการให้ข้อมูลเป็นศูนย์กลางการทำงานของ SASE

SASE ที่ให้ความสำคัญกับข้อมูลเป็นอันดับแรกจะรวมเอาการเชื่อมต่อที่สมบูรณ์และความสามารถในการรักษาความปลอดภัยจำนวนมากเข้าด้วยกัน และที่สำคัญช่วยให้คุณจัดการกับปัญหาที่แตกต่างกันในแต่ละขั้นตอน คุณสามารถเพิ่มการบริการบนระบบคลาวด์ได้อย่างต่อเนื่อง ไร้รอยต่อเป็นเฟสๆ (phases) ตามความต้องการทางธุรกิจของคุณ

ประโยชน์ของ SASE ที่ให้ความสำคัญกับข้อมูลเป็นหลัก (The benefits of data – first SASE)

การรวมวิธีการที่ให้ความสำคัญกับข้อมูลเป็นอันดับแรกเข้ากับ stack ของ SASE ของคุณจะปกป้องข้อมูลและผู้ใช้อย่างมีรูปแบบ (uniformly) และปรับใช้นโยบายอย่างสม่ำเสมอไม่ เปลี่ยนแปลงในทุกที่:

รวมความปลอดภัยของเว็บ คลาวด์ และข้อมูลไว้ในบริการคลาวด์เดียว (in a single cloud service)

➲ ให้ผู้ใช้ของคุณปลอดภัยและมีประสิทธิภาพไม่ว่าจะทำงานที่ไหน ไม่ว่าจะเป็น ที่บ้าน ในสำนักงาน บนท้องถนน

➲ ลดความเสี่ยงและป้องกันการสูญหายของข้อมูล เนื่องจากพนักงานของคุณใช้เว็บและ แอประบบคลาวด์จากที่ต่างๆ มากกว่าที่เคย

➲ ปกป้องผู้ใช้ที่เคลื่อนที่ (roaming) โดยอัตโนมัติด้วยซอฟต์แวร์จุดสิ้นสุดที่รวมเป็นหนึ่งเดียว

เข้าถึงแอปส่วนตัวจากระยะไกลโดยไม่ต้องเจ็บปวดกับ VPN

➲ นำไซต์ระยะไกลของคุณเข้าสู่ยุคคลาวด์ให้เชื่อมต่อโดยตรงกับอินเทอร์เน็ตและคลาวด์ โดยไม่ต้องใช้ VPN หรือส่งปริมาณการใช้งานกลับไปยังสำนักงานใหญ่ของคุณ

➲ พนักงานและคู่ค้าสามารถเข้าถึงข้อมูล แอป และข้อมูลได้อย่างปลอดภัยโดยไม่กระทบต่อคุณสมบัติหรือความสมบูรณ์ของเครือข่ายระบบและฐานข้อมูลขององค์กร

ความปลอดภัยอัตโนมัติอิงตามความเสี่ยง (Risk-based, automated security)

➲ ขจัดความเสียดทานและทำให้บุคลากรมีประสิทธิผลโดยการปรับความปลอดภัยให้เข้ากับระดับความเสี่ยงที่เกิดจากการกระทำของผู้ใช้แต่ละคนโดยอัตโนมัติ

➲ บังคับให้การใช้นโยบายเป็นไปอย่างราบรื่นทั้งในระบบคลาวด์หรือในเครือข่ายสำนักงานที่ต้องการมีอำนาจอธิปไตยในข้อมูล (ของตนเองโดยไม่ให้ไปอยู่ในการครอบครองของบุคคลอื่น) (with special data sovereignty needs.)

➲ เมื่อคุณพร้อม คุณสามารถมั่นใจได้ว่าข้อมูลที่บุคลากรของคุณกำลังใช้งานอยู่นั้นปลอดภัยบนแล็ปท็อปและในแอปคลาวด์ของพวกเขา และพวกเขาไม่ทำกิจกรรมที่มีความเสี่ยงโดยไม่จำเป็น

ประสิทธิภาพการดำเนินงานโดยจัดการจากคลาวด์ (Operational efficiency, managed from cloud)

➲ ทำให้ทีมไอทีของคุณปลอดจากการต้องไล่ตามการอัปเดตที่ไม่จบสิ้นและต่อสู้กับความไม่คงที่หรือความไม่สอดคล้องกันในอุปกรณ์เฉพาะทางแต่ละชนิด (inconsistencies in point products)

➲ ทำให้นโยบายเข้าใจได้ง่ายขึ้นด้วยการใช้ชื่อของผู้ใช้งานและกลุ่มของคุณเอง เช่นเดียวกับชื่อแอประบบคลาวด์อีกนับพัน

การทำความเข้าใจ (ประเมิน) ความเสี่ยงอย่างต่อเนื่องและการบังคับใช้นโยบายตามความเสี่ยงเป็นวิธีที่มีประสิทธิภาพมากที่สุดในการปกป้องและเปิดใช้การทำงานแบบกระจาย (enable distributed workforces)

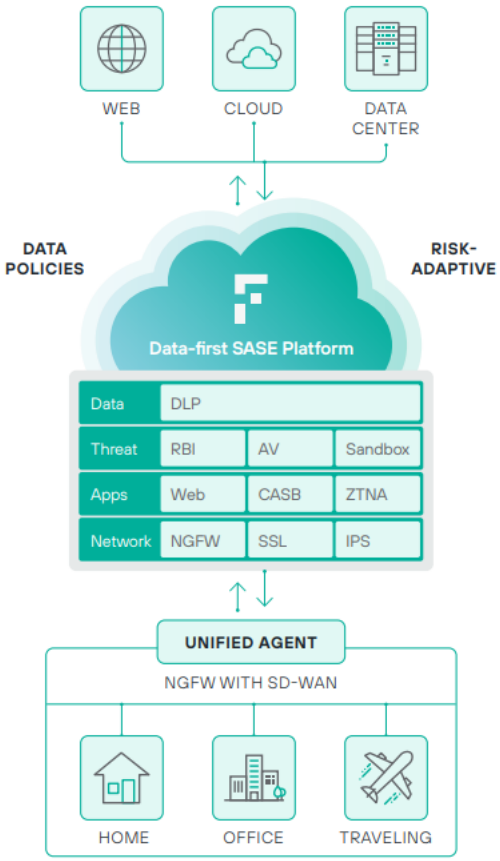
บุคลากรของคุณสามารถทำงานได้อย่างมีประสิทธิภาพไม่ว่าพวกเขาจะอยู่ที่ไหนหรือข้อมูลของพวกเขาอยู่ที่ใดก็ตาม พนักงานและคู่ค้าสามารถเข้าถึงทุกสิ่งที่จำเป็นสำหรับการทำงานได้อย่างปลอดภัยโดยไม่กระทบต่อความสมบูรณ์ของเครือข่ายและข้อมูล

ในท้ายที่สุด แนวทาง SASE ที่ให้ข้อมูลมาเป็นศูนย์กลางยังปิดช่องว่างด้านความปลอดภัยและความซ้ำซ้อน เพื่อควบคุมต้นทุนอีกด้วย ทีมรักษาความปลอดภัยด้านไอทีของคุณสามารถลดค่าใช้จ่ายด้านการลงทุน เช่น ฮาร์ดแวร์ และตัดค่าใช้จ่ายในการดำเนินงานเมื่อกระบวนการและโครงสร้างพื้นฐานเปลี่ยนแปลงและเปลี่ยนไปใช้ระบบคลาวด์

โซลูชั่น SASE ที่อิงตามการเข้าถึงให้ความสำคัญหลักๆ ไปที่การรักษาความปลอดภัยประตูที่ไปสู่ทรัพยากร ส่วนแพลตฟอร์ม SASE ที่ให้ความสำคัญกับข้อมูลเป็นหลักจะไปไกลกว่าคือจะดำเนินการปกป้องวิธีการใช้ข้อมูลอย่างต่อเนื่อง

ความลับในการไปสู่ความสำเร็จของ SASE (Secrets to SASE Success)

แพลตฟอร์ม SASE ที่ให้ความสำคัญกับข้อมูลเป็นอันดับแรกของ Forcepoint เป็นมากกว่าแค่การให้การเข้าถึงที่ปลอดภัยทุกที่ - โดยยังปกป้องการใช้ข้อมูลอย่างสม่ำเสมอทุกที่ เมื่อคุณเขียนนโยบายเกี่ยวกับข้อมูลอย่างมีรูปแบบ (uniform data policies) แล้วก็จะถูกนำไปบังคับใช้ (enforce) กับอุปกรณ์ปลายทางไปจนถึงแอประบบคลาวด์ได้ด้วย SASE ที่ให้ความสำคัญกับข้อมูลเป็นหลัก บุคลากรของคุณสามารถทำงานที่บ้านในสำนักงานสาขา หรือแม้กระทั่งที่ไซต์ของลูกค้า และยังคงได้รับการปกป้องโดยนโยบายความปลอดภัยเดียวกัน โดยถูกออกแบบมา คุณสามารถเปิดใช้งานความสามารถบนคลาวด์ได้ตามที่คุณต้องการเพื่อทำให้การเปลี่ยนแปลงไปสู่ระบบคลาวด์ทำได้ง่ายขึ้น :



การปกป้องข้อมูล (Data Protection) จะให้ความปลอดภัยแก่ข้อมูลซึ่งขณะนี้กำลังไหลระหว่างสำนักงานหลัก ศูนย์ข้อมูล สำนักงานสาขา ผู้ใช้ระยะไกล ซึ่งระบบคลาวด์ SASE ที่ให้ความสำคัญกับข้อมูลเป็นอันดับแรกจะให้ชุดนโยบายการรักษาความปลอดภัยข้อมูลที่ทำงานอย่างสม่ำเสมอ และไร้รอยตะเข็บเป็นชุดเดียวเพื่อบังคับใช้ในการป้องกันข้อมูลสูญหาย (DLP) ทั้งการควบคุมการรับส่งข้อมูลบนคลาวด์และการปกป้องข้อมูลปลายทางแบบบูรณาการทำให้มั่นใจได้ว่าข้อมูลที่มีความอ่อนไหวจะไม่ออกไปสู่คลาวด์หรือปล่อยละเลยอุปกรณ์ของพนักงานไว้ให้อยู่ในสภาพไม่เหมาะสม การปกป้องข้อมูลแบบไฮบริดที่เป็นตัวเลือกจะให้ความสามารถทั้งแบบทำงานบนคลาวด์และแบบติดตั้งภายในองค์กร

การป้องกันภัยคุกคาม (Threat Protection) เป็นสิ่งสำคัญยิ่งสำหรับผู้ปฏิบัติงานที่ทำงานแบบไม่จำกัดสถานที่ (ทำงานทุกแห่งหน) ที่ใช้มาตรการรักษาความปลอดภัยที่อ่อนแอไม่เพียงพอหรือไม่มีอยู่จริงเมื่อทำงานอยู่ที่บ้านหรือบนท้องถนน แพลตฟอร์ม SASE ที่ให้ความสำคัญกับข้อมูลเป็นอันดับแรกของ Forcepoint มอบการป้องกันขอบเครือข่าย (edge protection) ที่แข็งแกร่งและเลเยอร์ในการป้องกันที่ซับซ้อนซ่ำซอง เช่น การตรวจสอบเนื้อหาเชิงลึก การตรวจจับมัลแวร์ขั้นสูง และการแยกเบราว์เซอร์ระยะไกล (remote browser isolation) เพื่อปกป้องจากผู้โจมตีภายนอกที่มีความซับซ้อนมากที่สุด อุปกรณ์แบบที่ติดตั้งในสำนักงาน (on - premise) จะกลายเป็นสิ่งล้าสมัยเนื่องจากระบบคลาวด์จะช่วยให้คุณสามารถทำให้สำนักงานสาขาออนไลน์ได้อย่างรวดเร็วและมีความปลอดภัยด้วยการป้องกันที่ครอบคลุมที่มีพร้อมมาให้ด้วย

ระบบความปลอดภัยสำหรับแอปพลิเคชัน (Application Security) จาก SASE ช่วยให้คุณมองเห็นเข้าไปในและควบคุมศูนย์ข้อมูลและแอปพลิเคชันระบบคลาวด์ อุปกรณ์ และทรัพยากรไอทีที่ซ่อนอยู่ที่เคยมองไม่เห็น (shadow IT resources) คุณควบคุมการใช้งานแอปพลิเคชันและอุปกรณ์ทั้งที่เป็นประเภทถูกจัดการและไม่ถูกจัดการโดยองค์กรผ่านความสามารถต่างๆ (features) เช่น การกรอง URL การตรวจสอบเนื้อหาในเชิงลึก และการมองเห็นและการควบคุมแอปบนคลาวด์ พนักงาน ไม่สามารถหลบเลี่ยงนโยบายความปลอดภัยได้อีกต่อไปเนื่องจากคุณสามารถบล็อกการใช้บริการคลาวด์ที่ไม่ได้รับการอนุมัติได้ นอกจากนี้การตรวจสอบอย่างเต็มรูปแบบและการควบคุมอย่างละเอียดลงไปในส่วนเล็กๆ (granular control over) ของการใช้งานแอปและกิจกรรมต่างๆ ยังช่วยลดความยุ่งยากในการปฏิบัติตามข้อกำหนดในระบบคลาวด์ (simplify compliance in the cloud) และด้วยวิธีการที่ให้ความสำคัญกับข้อมูล คุณสามารถขยายการทำงานของ DLP ไปยังระบบคลาวด์ได้อย่างง่ายดายด้วยการผสานรวมที่ไร้ตะเข็บ

การรักษาความปลอดภัยเครือข่าย (Network Security) มอบการรักษาความปลอดภัยที่มีประสิทธิภาพและเชื่อถือได้โดยใช้บริการไฟร์วอลล์และเว็บพร็อกซีที่เป็นแบบคลาวด์ตั้งแต่ตอนสร้าง (cloud-native) สำหรับการเข้าถึงอินเทอร์เน็ตโดยไม่ต้องติดตั้งอุปกรณ์ในทุกๆ สถานที่ สำนักงานสาขาและพนักงานระยะไกลของคุณสามารถเชื่อมต่อได้โดยอัตโนมัติโดยใช้ SD-WAN ที่มีความปลอดภัยและทำงานประสานแบบองค์รวมและใช้เอเจนท์บนอุปกรณ์ปลายทาง และแทนที่จะบังคับให้ผู้ใช้งานต้องจัดการกับ VPN ที่ยุ่งยากและเจ็บปวดสำหรับการจะเข้าใช้งาน SaaS และแอปส่วนตัว SASE ได้รวมระบบ Cloud Access Security Brokers (CASB) และ Zero Trust Network Access (ZTNA) ที่สามารถป้องกันแรนซัมแวร์ในขณะที่เก็บรักษาข้อมูลที่มีความอ่อนไหวได้ด้วย

ประโยชน์ของแนวทางของ Forcepoint ต่อ SASE (Advantages of Forcepoint's Approach to SASE)

ประโยชน์ #1: นโยบายการรักษาความปลอดภัยของข้อมูลแบบรวมเป็นหนึ่งเดียว (Unified data security policies) ซึ่งการจัดการแพตช์เวิร์ค (patchwork) ของอุปกรณ์เฉพาะทาง (point products) นั้นยุ่งยากและไม่สามารถปรับขนาดได้ (simply doesn't scale) โดยเฉพาะอย่างยิ่งเมื่อผู้ใช้ทำงานมากกว่า (ออกนอก) ขอบเขต (เครือข่าย) ของบริษัท แพลตฟอร์ม SASE ที่ให้ความสำคัญกับข้อมูลเป็นอันดับแรกของ Forcepoint ช่วยให้ทีมสามารถเขียนนโยบายความปลอดภัยเพียงครั้งเดียวและบังคับใช้ทุกที่ตั้งแต่จากอุปกรณ์ปลายทางผ่านครือข่ายไปจนถึงระบบคลาวด์

ประโยชน์ #2: เอเจ้นท์ที่รวมความสามารถหลากหลายเข้าเป็นหนึ่งเดียว (Unified Agents) ซึ่งแพลตฟอร์มของ Forcepoint ผสานรวมซอฟต์แวร์เป็นแบบองค์รวมเพื่อการเข้าถึงทรัพยากรอย่างปลอดภัย บังคับใช้นโยบายความปลอดภัยและตรวจสอบกิจกรรมบนอุปกรณ์ปลายทาง สถาปัตยกรรมนี้ช่วยจำกัดการแพร่กระจายอย่างเกลื่อนกลาดของเอเจนท์และจะให้ซอฟต์แวร์ที่เป็นชิ้นเดียวทำให้ง่ายต่อการติดตั้งใช้งานและการบำรุงรักษา

ประโยชน์ #3: การติดตั้งปรับใช้งานที่ยืดหยุ่น (Flexible deployment) ซึ่ง SASE ที่ให้ความสำคัญกับข้อมูลเป็นหลักควรมอบการเข้าถึงเว็บคลาวด์ และทรัพยากรส่วนตัวที่มีประสิทธิภาพและปลอดภัยและไม่ว่า

บุคลากรของคุณจะทำงานอยู่ที่ใดก็ตาม แพลตฟอร์มนี้ต้องรวมการควบคุมตามบริบทที่สมบูรณ์ (rich context - based controls) การบังคับใช้แบบไฮบริดที่ไซต์โดยมีข้อกำหนดพิเศษ (เช่น การปฏิบัติตามข้อกำหนด) และ SD-WAN ที่ปลอดภัยโดยไม่ต้องใช้ผลิตภัณฑ์เพิ่มเติมโดยทั้งหมดเข้าด้วยกันแบบองค์รวมอย่างประนีประนอม องค์กรคุณ (ปล่อยให้องค์กรของคุณเสี่ยงอยู่ในความไม่ปลอดภัย) (Don't ever compromise your enterprise) เพียงเพราะโมเดลของผู้จำหน่ายที่เป็นระบบคลาวด์อย่างเดียวหรือแบบโมเดลโซลูชั่นของอุปกรณ์เฉพาะทาง (point-solution based model) เพียงอย่างใดอย่างหนึ่ง

ประโยชน์ #4: การบังคับใช้นโยบายที่ปรับเปลี่ยนตามความเสี่ยง (Risk-adaptive policy enforcement)

ลองพิจารณาว่าคุณตรวจสอบความปลอดภัยเว็บหรือนโยบาย DLP บ่อยเพียงใดหรือคุณควรทำบ่อยแค่ไหน โดยตั้งสมมุติฐานถึงการเปลี่ยนแปลงไปอย่างรวดเร็วของสิ่งต่างๆ แทนที่จะใช้โมเดลแบบบล็อกและอนุญาตอย่างตายตัวไม่มีพลวัตรซึ่งต้องการระบบรักษาความปลอดภัยที่ต้องคิดถึงทุกโอกาสของการผสมผสานความเป็นไปได้ที่จะเกิดขึ้นของภัย(การประนีประนอม) และการแก้ไขนั้นๆ Forcepoint ได้แนะนำแนวทางการเปลี่ยนเกมที่ปรับการตอบสนองต่อความปลอดภัยให้เหมาะกับความเสี่ยงโดยอัตโนมัติ เราเรียกสิ่งนี้ว่าการป้องกันแบบปรับเปลี่ยนตามความเสี่ยง (risk-adaptive protection) ความเข้าใจเรื่องความเสี่ยงจะปรับการบังคับใช้ให้เหมาะกับพฤติกรรมนั้นๆ ของผู้ใช้งาน ในขณะที่ใช้ข้อมูล แอป และระบบ

- ✓ ตรวจค้นพบข้อมูลที่อยู่ในทุกที่ (Discover data everywhere)
- ✓ จำแนกข้อมูลโดยใช้ระบบองค์รวม (Classify data with integrations) ซึ่งรวมถึง Microsoft Azure Information Protection, Boldon James, Titus
- ✓ ใช้ประโยชน์จากการตรวจจับและนิติวิทยาศาสตร์ขั้นสูง เช่น การตรวจลายนิ้วมือ (ร่องรอย ของสิ่งที่เกิดขึ้น), OCR และการเรียนรู้เองของเครื่อง (machine learning)
- ✓ สามารถสร้างได้อย่างรวดเร็วจากเทมเพลตนโยบายที่ใหญ่ที่สุดสำหรับการปฏิบัติตามข้อกำหนดและการป้องกัน IP ที่สำคัญ

"บางสิ่งที่ Forcepoint ทำในขณะที่ผู้ผลิตรายอื่นๆ ไม่ได้ทำก็คือการบรรจบกันหรือการรวม DLP แบบคลาวด์และแบบดั้งเดิม เรามองเห็นว่านั่นเป็นเรื่องใหญ่จริงๆ โมเดล DLP ขององค์กรจะไม่สำคัญ (เท่าที่เคยเป็น) เมื่อข้อมูลที่ส่งไปยังคลาวด์มากขึ้นเรื่อยๆ"

About Forcepoint

Forcepoint is the leading user and data protection cybersecurity company, entrusted to safeguard organizations while driving digital transformation and growth. Forcepoint's humanly-attuned solutions adapt in real- time to how people interact with data, providing secure access while enabling employees to create value. Based in Austin, Texas, Forcepoint creates safe, trusted environments for thousands of customers worldwide.