Securing the Anywhere Organization

Any location. Any device. Any resource.

Remote working is here to stay: according to Gartner, 74% of organizations expect some employees to work remotely once the pandemic is over1. At the same time, the resources people need to do their jobs are also in multiple locations: on servers in the office; in cloud based applications like Office 365 or Salesforce; and in private or public cloud environments on Amazon Web Services (AWS) and Microsoft Azure.
การทำงานจากระยะไกล (Remote working) จะยังคงอยู่ต่อไป การ์ทเนอร์ระบุว่า 74% ขององค์กรยังคงคาดว่าพนักงานหลายคนจะทำงานจากระยะไกลต่อไปแม้ว่าโรคระบาดนี้จะหมดไปแล้วก็ตาม พร้อมกันนั้นทรัพยากรทั้งหลายที่พนักงานจำเป็นต้องใช้ในการทำงานจะมีการกระจายไปอยู่หลายสถานที่เป็นต้นว่า อยู่ที่เซิร์พเวอร์ในที่ทำงาน อยู่ในแอพพลิเคชั่นที่เป็นคลาวด์เช่น Office 365 หรือ Salesforce หรืออยู่ที่ไพรเวทคลาวด์หรือพับบลิคคลาววด์บน Amazon Web Services (AWS) หรือ Microsoft Azure

IT teams are tasked with protecting every user and every resource, no matter where they are. Meanwhile, bad actors continue to find better and more subversive ways to penetrate increasingly virtual organizations at every intersection.
คณะทำงานด้านไอทีมีหน้าที่ปกป้องผู้ใช้งานทุกคนและทรัพยากรทุกชนิด ไม่ว่าจะอยู่ที่ไหนก็ตาม ในขณะที่ผู้ร้ายก็ยังคงพยายามหาวิธีที่ดีกว่าและทำลายล้างได้มากกว่าเดิมเพื่อจะเจาะเข้าไปในองค์กรซึ่งมีความเสมือนมากขึ้น (มีลักษณะภายนอกที่ปรากฏไม่ชัดเจน) ในทุกจุดที่เป็นจุดตัดขวาง (เชื่อม) การจราจรของเครือข่าย

Securing organizations where people and resources can be anywhere requires:

- Secure connectivity, so users can access resources from any location: home, on-site, or in the office
- Protection for the devices used to make those connections — desktops, laptops, mobile phones, and tablets
- Protection for the data and workloads that users need to access, whether they're in the cloud or on your local network
- Simple management, so IT teams can manage their distributed organizations from anywhere, without adding to their workload

การให้ความปลอดภัยแก่องค์กรที่มีพนักงานหรือผู้ใช้งานและทรัพยากรซึ่งสามารถจะอยู่ที่ไหนก็ได้นั้นต้องการความสามารถและการกระทำต่างๆ ดังนี้

- รักษาความปลอดภัยการเชื่อมต่อเครือข่าย เพื่อให้ผู้ใช้งานสามารถเข้าถึงทรัพยากรจากสถานที่ไหนก็ได้ ไม่ว่าจะเป็นจากที่บ้าน จากที่ไซต์งาน หรือจากในที่ทำงานก็ตาม
- ปกป้องอุปกรณ์ที่เป็นตัวเชื่อมต่อเครือข่าย ไม่ว่าจะเป็น เดสค์ท็อป แล็ปท็อป โทรศัพท์มือถือ หรือแท็ปเล็ท
- ปกป้องข้อมูลและเวิร์คโหลด (โปรแกรม หรือ แอพพลิเคชั่น และรวมถึงทรัพยากรในการประมวลผล จัดเก็บ เคลื่อนย้าย ที่เกี่ยวข้องกับการทำงานกับข้อมูล) ที่ผู้ใช้งานต้องการเข้าถึง ไม่ว่าสิ่งเหล่านี้จะอยู่บนคลาวด์หรืออยู่ในเครือข่ายท้องถิ่นของคุณ
- มีการบริหารจัดการที่ง่ายไม่ซับซ้อน เพื่อที่ทีมงานไอทีจะสามารถบริหารจัดการองค์กร ที่เป็นแบบกระจายไม่รวมศูนย์จากที่ไหนก็ได้โดยไม่ต้องมีภาระงานที่ต้องทำมากขึ้น

Fortunately, Sophos supports all these areas. We offer a complete portfolio of next-gen security products packed with advanced protection capabilities. Everything is controlled via a single, web-based security platform which slashes day-to-day admin overheads while enabling IT teams to manage their organization's security from anywhere

โชคดีที่ Sophos สามารถสนับสนุนทุกการทำงานในลักษณะดังกล่าว เราสามารถเสนอชุดสินค้าระบบรักษาความปลอดภัยที่เป็นรุ่นถัดไปมัดรวมกับความสามารถในการปกป้องแบบก้าวหน้า การควบคุมสั่งการการทำงานของทุกอุปกรณ์ สามารถทำผ่านแพลทฟอร์มระบบรักษาความปลอดภัยเดียวที่เป็นแบบเว็บเบส ซึ่งจะช่วยลดงานประจำวันของงานแอ็ดมินในขณะที่ยังทำให้ทีมไอทีสามารถบริหารจัดการระบบรักษาความปลอดภัยขององค์กรจากที่ใดก็ได้

This solution brief walks you through how Sophos addresses each of these requirements. It also explores the productivity and protection benefits customers see when employing a Sophos cybersecurity system to secure their organization

ภาพการทำงานของโซลูชั่นนี้จะแสดงให้คุณเห็นการทำงานอย่างเป็นขั้นตอน ว่า Sophos จะสามารถตอบโจทย์ความต้องการเหล่านี้อย่างไร และยังช่วยเปิดให้เห็นผลของการทำงานและประโยชน์ในการปกป้องเมื่อได้นำระบบรักษาความปลอดภัยไซเบอร์ของ Sophos มาใช้งานเพื่อรักษาความปลอดภัยให้กับองค์กรของท่าน

Connect securely การเชื่อมเครือข่ายอย่างปลอดภัย

There's no argument that the COVID pandemic has driven a massive increase in remote working. During May 2020, 62% of employed Americans were working from home (WFH). However, remote working was already a trend even before COVID hit, and many in-office employees were already transitioning to working from home a few days a week. In the UK, remote working climbed at a rate of 74% in the last decade, while in Australia about a third of the workforce was regularly WFH.

อย่างที่เห็นโดยชัดแจ้งแล้วว่าการระบาดขนานใหญ่ของโควิดนั้นเป็นตัวผลักดันให้มีการทำงานจากทางไกลเพิ่มขึ้นอย่างใหญ่หลวง ในช่วงเดือนพฤษภาคม 2020 นั้น 62% ของพนักงานลูกจ้างในอเมริกามีการทำงานจากบ้าน อย่างไรก็ตามการทำงานจากทางไกลได้กลายเป็นที่นิยมไปเรียบร้อยแล้วก่อนที่จะเกิดโควิดด้วยซ้ำ พนักงานที่ทำงานในออฟฟิศหลายๆ คน

ได้ปรับเปลี่ยนไปเป็นทำงานจากบ้าน 2-3 วันต่อสัปดาห์ ในประเทศอังกฤษอัตราการทำงานจากทางไกลได้เติบโตถึง 74% ในขณะที่ในประเทศออสเตรเลียนั้นประมาณ 1 ใน 3 ของคนทำงานนั้นทำงานจากบ้านเป็นปกติประจำไปแล้ว

Remote working is a win-win for companies and staff: employees save commuting time and costs while enjoying added flexibility and greater productivity. Meanwhile, organizations reduce costs and turnover rates. But for IT teams, long-term remote working creates additional security challenges. Whether employees are logging in from their living rooms, visiting a customer location, or sipping coffee at a Wi-Fi hotspot thousands of miles across the globe, your network and data must remain protected at all times. With Sophos, your employees can quickly, efficiently, and securely connect and work from anywhere, and we offer both traditional VPN-based and Zero Trust Network Access (ZTNA) options

การทำงานจากทางไกลเป็นการได้ประโยชน์ของทั้ง 2 ฝ่ายระหว่างบริษัทและพนักงาน โดยพนักงานสามารถประหยัดเวลาและค่าใช้จ่ายในการเดินทางในขณะเดียวกันยังได้รับความพอใจที่เกิดความยืดหยุ่นในการทำงานเพิ่มขึ้นและได้ผลงานที่มากขึ้น ในขณะที่องค์กรก็สามารถลดค่าใช้จ่ายและลดอัตราการลาออกของพนักงานลง แต่สำหรับทีมไอทีแล้วการทำงานจากทางไกลในระยะยาว จะเป็นความท้าทายที่เพิ่มขึ้นหลายประการ เกี่ยวกับเรื่องการดูแลระบบความปลอดภัย ไม่ว่าพนักงานจะล็อคอินจากห้องนั่งเล่นที่บ้านเข้าไปยังเครือข่าย หรือจากที่ทำงานของลูกค้าที่พนักงานไปเยี่ยม หรือจากฮ็อตสป็อตของร้านกาแฟที่ตนเองไปนั่งจิบซึ่งห่างออกไปเป็นหลายพันไมล์ข้ามโลกก็ตาม เครือข่ายและข้อมูลของคุณต้องได้รับการปกป้องตลอดเวลา ด้วยการใช้ระบบของ Sophos พนักงานของคุณสามารถเชื่อมต่อเข้ามายังเครือข่ายได้อย่างรวดเร็วมีประสิทธิภาพและปลอดภัย โดยสามารถทำงานจากที่ใดๆ ก็ได้และระบบของ Sophos มีทางเลือกให้ใช้ในการทำงาน โดยให้เลือกว่าจะใช้งานลักษณะเป็น VPN-based ซึ่งเป็นแบบที่ใช้กันอยู่โดยทั่วไปหรือจะเป็นแบบ Zero Trust Network Access (ระบบที่ไม่เชื่อใครหรืออะไรทั้งสิ้นต้องทำการตรวจสอบสิทธิอย่างเข้มข้นเสมอ) ก็ได้

VPN (Virtual Private Network)

Use our free, easy-to-deploy Sophos Connect VPN client together with Sophos Firewall to connect remote workers to the main office and your cloud-based resources. With over 1.4 million users worldwide, Sophos Connect gives your remote users secure access to resources on the corporate network or public cloud from Windows and macOS devices

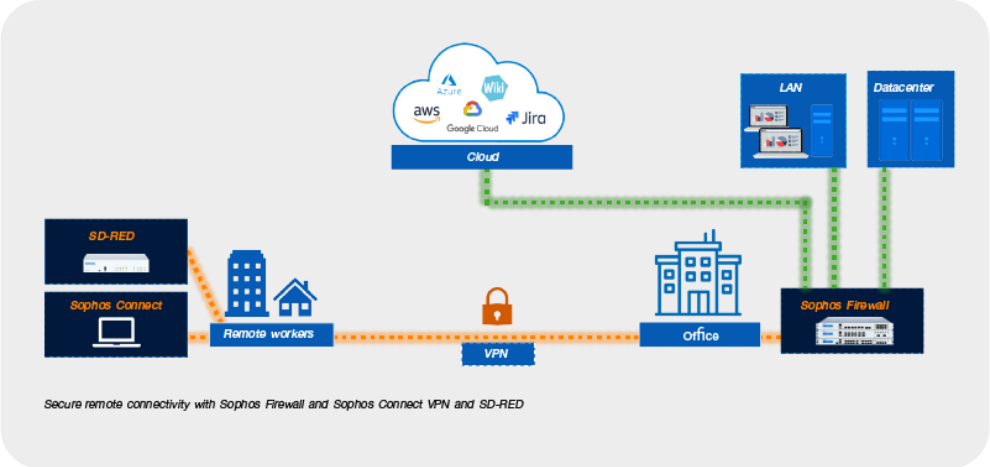
ด้วยการใช้ระบบ Sophos Connect VPN ที่ติดตั้งง่ายและไม่คิดเงินที่จะติดตั้งลงในอุปกรณ์ของผู้ใช้งาน ซึ่งจะทำงานร่วมกับระบบอุปกรณ์ไฟร์วอลของ Sophos เพื่อเชื่อมต่อผู้ใช้งานจากทางไกลเข้ามายังสำนักงานใหญ่และหรือมายังทรัพยากรต่างๆ ของคุณที่อยู่บนคลาวด์ ยืนยันด้วยจำนวนผู้ใช้งานที่มีมากกว่า 1.4 ล้านคนทั่วโลกที่ใช้ระบบนี้ Sophos Connect จะให้การเชื่อมต่อจากทางไกลอย่างปลอดภัยแก่ผู้ใช้งานของท่านเชื่อมไปยังทรัพยากรต่างๆ ที่อยู่บนเครือข่ายขององค์กร หรือที่อยู่บนคลาวด์สาธารณะจากอุปกรณ์ของผู้ใช้งานที่เป็นวินโดว์หรือเป็น macOS

For the ultimate in remote connectivity, Sophos SD-RED (Remote Ethernet Device) is a simple plug-and-play device that works with the Sophos Firewall to connect branch offices, remote sites, and individuals to your main network (whether physical or in the cloud).

It provides an always-on dedicated or split-tunnel VPN that's easy to deploy and manage with flexible options. It's also very small and portable, making it ideal for senior managers and other individuals who need to access a secure connection at any time, and from anywhere.

โดยสรุปที่เกี่ยวกับเรื่องการเชื่อมต่อจากทางไกลแล้ว Sophos SD-RED (Remote Ethernet Device อุปกรณ์เครือข่ายตามมาตรฐานอีเทอร์เน็ตประเภทหนึ่ง) เป็นอุปกรณ์เชื่อมต่อทางไกลที่ใช้งานง่ายแบบเสียบปลั๊กแล้วใช้งานได้เลยซึ่งจะทำงานร่วมกับระบบไฟร์วอลของ Sophos ในการเชื่อมต่อสำนักงานสาขา หรือไซต์งานที่อยู่ห่างไกล และหรือผู้ใช้งานคนใดๆ เชื่อมเข้ามายังเครือข่ายหลักของท่าน (ไม่ว่าจะเป็นเครือข่ายจริงหรือที่อยู่บนคลาวด์ก็ตาม)

ระบบนี้จะสร้างท่อ VPN เพื่อใช้เฉพาะงานนี้หรือแบ่งท่อย่อย VPN มาให้ ซึ่งทั้ง 2 ประเภทจะเป็นท่อที่ใช้งานได้ตลอดเวลา ซึ่งง่ายต่อการติดตั้งใช้งานและบริหารจัดการและมีทางเลือกใช้ที่มีความยืดหยุ่นหลายทางเลือก เป็นอุปกรณ์ขนาดเล็กแบบพกพาเหมาะสำหรับผู้จัดการระดับสูงหรือพนักงานทั่วไปที่ต้องการการเชื่อมต่อที่ปลอดภัยที่จะเชื่อมต่อในเวลาใดๆ หรือจากสถานที่ใดๆ ก็ได้ (ทุกเวลา ทุกสถานที่)



Secure remote connectivity with Sophos Firewall and Sophos Connect VPN and SD-RED

ZTNA

For years, VPN technology has successfully enabled workers to connect remotely. And it was a savior at the beginning of the pandemic, allowing organizations to quickly pivot to secure remote working in just days. However, many organizations are starting to want more than VPN was ever designed to deliver.

หลายปีที่ผ่านมา เทคโนโลยี VPN มีความสำเร็จในการช่วยให้ผู้ใช้งานสามารถเชื่อมต่อเครือข่ายจากทางไกลเป็นอย่างดี และก็เป็นตัวช่วยในช่วงต้นของการระบาดขนาดใหญ่ของโรคที่ทำให้องค์กรสามารถกลับตัวมาใช้แก้ปัญหาในการทำงาน โดยช่วยให้สามารถทำงานจากทางไกลได้อย่างปลอดภัยได้ภายในไม่กี่วัน อย่างไรก็ตามก็มีหลายองค์กรเริ่มมีความต้องการที่จะใช้งานในลักษณะที่มากกว่าหรือเกินกว่าสิ่งที่ VPN ได้รับการออกแบบมาอีก

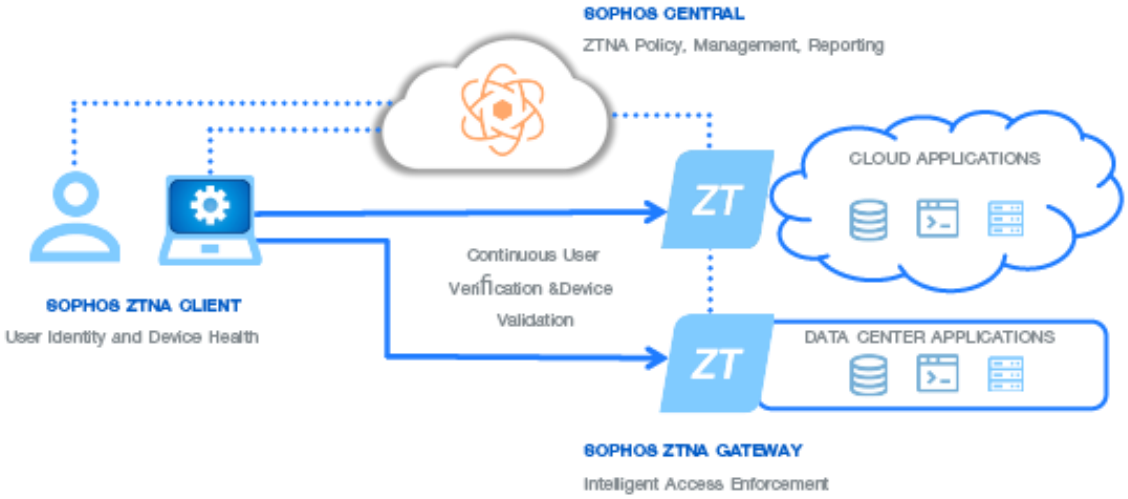
Sophos Zero Trust Network Access (ZTNA) is a great alternative to remote access VPN, enabling users to connect to corporate resources from any location in a straightforward and transparent way. At the same time, it also enhances your security by constantly verifying the user — typically with multi-factor authentication and an identity provider — and validating the health and compliance of the device.

Sophos Zero Trust Network Access (ZTNA) เป็นทางเลือกที่ยอดเยี่ยมสำหรับการใช้งานในการเชื่อมต่อเครือข่าย จากทางไกลแทนแบบ VPN เพื่อทำให้ผู้ใช้งานเชื่อมต่อกับทรัพยากรขององค์กรจากที่ใดๆ ก็ได้อย่างตรงไปตรงมาไม่ซับซ้อน ในขณะเดียวกันก็ช่วยให้ระบบความปลอดภัยของคุณสามารถที่จะตรวจสอบยืนยันตัวตนผู้ใช้งานได้อย่างสม่ำเสมอเที่ยงตรง – โดยทั่วไปโดยการทำงานร่วมกับระบบพิสูจน์ตัวตนแบบพหุ (multi-facture authentication) และผู้ให้บริการกำหนดเอกลักษณ์ (identity provider) – และตรวจสอบสุขภาพและความมีคุณสมบัติพร้องกับมาตรฐานของอุปกรณ์ว่ามีหรือไม่

Sophos ZTNA makes sure the device is enrolled, up-to-date, properly protected, and has encryption enabled. It then uses that information to make decisions based on customizable policies to determine user access and privilege to your critical networked applications.

Sophos ZTNA จะทำให้มั่นใจได้ว่าอุปกรณ์ (ที่จะเชื่อมต่อเข้าเครือข่าย) ต้องได้รับการลงทะเบียนจากระบบเรียบร้อยแล้ว ได้รับการทำให้ทันสมัย ได้รับการปกป้อง และเปิดใช้งานการเข้ารหัสแล้ว และ Sophos ZTNA จะใช้ข้อมูลเหล่านี้ในการ

ตัดสินใจบนฐานของนโยบายที่ปรับให้เหมาะสมได้เพื่อการอนุญาตเข้าเครือข่ายแก่ผู้ใช้งาน และสิทธิ์ในการเข้าถึงแอพพลิเคชั่นเครือข่ายที่สำคัญทั้งหลายของท่าน



Sophos ZTNA approach - วิธีการของ Sophos ZTNA

With Sophos ZTNA, you can:

- Enhance your cyber defenses. Sophos ZTNA gives you very granular controls: any user, any device, any application can all be individually controlled based on individual corporate policy and the risk level you're comfortable with. It also eliminates the concept of implicit trust in an individual based on their presence on the network alone. Instead, it elevates protection and minimizes the risk of lateral movement within the network by continually assessing identity and device health before allowing access.
- Increase efficiency. Because Sophos ZTNA is managed through the Sophos Central platform, it's easy to enroll new users or support a changing work environment. Plus, it's more transparent for end-users and provides them with a friction free "it just works" type of connection experience when compared to VPN.

เมื่อใช้ Sophos ZTNA คุณสามารถทำ :

- เพิ่มความสามารถในการป้องกันด้านไซเบอร์ของท่าน Sophos ZTNA จะให้ความสามารถในการควบคุมลงไปในแต่ละส่วนเล็กๆ เป็นต้นว่า ผู้ใช้งานแต่ละคน อุปกรณ์แต่ละตัว แอพพลิเคชั่นแต่ละตัว สิ่งเหล่านี้สามารถถูกกควบคุมจัดการแยกเป็นรายๆ บนฐานของนโยบายขององค์กรแต่ละนโยบาย และตามระดับความเสี่ยงที่ท่านพอใจยอมรับได้ Sophos ZTNA จะกำจัดแนวคิดของการเชื่อถือผู้ใช้งานหรืออุปกรณ์ใดๆ โดยไม่มีความระแวงใดๆ เพียงเฉพาะได้เห็นการปรากฏตัวอยู่ในเครือข่ายเท่านั้นออกไป ในทางตรงข้ามนั้น Sophos ZTNA ยกระดับการปกป้องและลดความเสี่ยงของการจะมีเคลื่อนที่แบบ Lateral Movement ในเครือข่าย (ดูคำอธิบายต่อไป) โดยการประเมินตรวจสอบอย่างต่อเนื่องสำหรับเอกลักษณ์ตัวตนและสุขภาพของอุปกรณ์ก่อนที่จะอนุญาตให้เข้าเครือข่าย

- เพิ่มประสิทธิภาพ เนื่องจากว่าการบริหารจัดการ Sophos ZTNA จะกระทำผ่านแพลทฟอร์มกลางของ Sophos ทำให้สะดวกที่จะลงทะเบียนผู้ใช้งานคนใหม่หรือจะเปลี่ยนแปลงสภาพแวดล้อมของการทำงาน นอกเหนือจากนั้น ความโปร่งใส ไม่ยุ่งยากซับซ้อนของ Sophos ZTNA ต่อผู้ใช้งาน ทำให้สามารถเข้าหรือเชื่อมต่อเครือข่ายได้ง่ายเมื่อเปรียบเทียบกับ VPN

Whichever method you choose, Sophos award-winning security products will help you secure your employees in any location and on any device.
ไม่ว่าคุณจะเลือกใช้วิธีใดก็ตาม (VPN หรือ ZTNA) Sophos จะช่วยคุณให้ความปลอดภัยแก่พนักงาน (เชื่อมต่อเครือข่าย) ไม่ว่าจะอยู่ที่ใดหรือใช้อุปกรณ์ใดก็ตาม

(คำอธิบายเพิ่มเติม Lateral Movement - เป็นลักษณะการทำงานของ Hacker เมื่อ Hacker สามารถเข้าถึง Network ของเราได้แล้ว แต่อุปกรณ์ ตัวที่ Hacker สามารถเข้าถึงและควบคุมได้เป็นเครื่องแรก อาจจะไม่ใช่ตัวที่สำคัญหรืออาจจะไม่ใช่ตัวเป้าหมายที่ต้องการ ดังนั้นวิธีการขั้นต่อไป คือ ก็ต้อง "เคลื่อนที่" ไปยังอุปกรณ์ตัวอื่นๆ ในเครือข่ายเพื่อเข้าควบคุมและหาข้อมูลจากอุปกรณ์ตัวนั้นๆ ไปเรื่อยๆ จนกระทั่งสามารถเข้าถึงและควบคุมเครื่องเป้าหมายที่ต้องการได้)

Protect devices ให้การปกป้องอุปกรณ์

51% of organizations were hit by ransomware in the last year, with attackers succeeding in encrypting data in 73% of attacks2.
Couple those alarming statistics with the need to secure all sorts of equipment — desktops, laptops, corporate and personal devices — and a slew of operating systems, from Windows, macOS, Linux, Android, Chromebook, and iOS, and you have an intense cybersecurity headache brewing.
51% ของจำนวนองค์กรได้ถูกโจมตีโดย Ransomware ในปีที่ผ่านมาโดยที่ผู้โจมตีได้ทำการเข้ารหัสข้อมูลไป 73% ของการโจมตี
สถิติของคำเตือนดังกล่าวแสดงให้เห็นถึงความจำเป็นในการที่จะต้องรักษาความปลอดภัยให้กับอุปกรณ์ทุกชนิดไม่ว่าจะเป็น เด็สท็อป แล็ปท็อป อุปกรณ์ต่างๆ ทั้งขององค์กรและของส่วนบุคคล และให้ความปลอดภัยแก่ Operating System (OS) ทั้งหลายไม่ว่าจะเป็น Windows, macOS, Linux, Andriod, Chromebook และ IOS และยังบอกว่าคุณจะมีเรื่องปวดหัวเกี่ยวกับงานด้านความปลอดภัยไซเบอร์อย่างยิ่งอีกด้วย

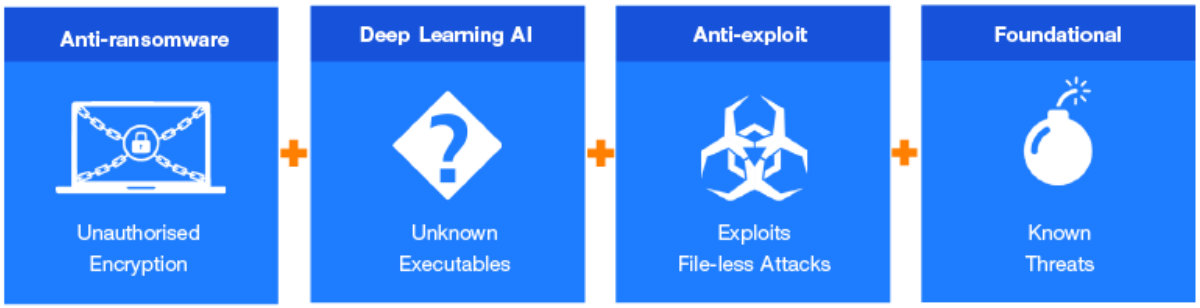
Sophos Intercept X gives you the world's best protection across all these devices and platforms. You benefit from multiple layers of technology that stop attackers at numerous points in the kill chain, including:

- Anti-ransomware protection, which blocks the unauthorized encryption of files, hard disks, and boot records, restoring them to their safe state
- Deep Learning AI, which uses millions of file attributes to analyze threats and prevent both known and never-seen-before malware, stops them before they can execute

- Anti-exploit technology, to block exploits, active adversary techniques, and fileless and script-based attacks
- Foundational signature-based protection, which stops known threats

Sophos Intercept X จะให้การปกป้องที่ดีที่สุดสำหรับอุปกรณ์และแพลทฟอร์มทั้งหลายที่กล่าวไปข้างต้น คุณจะได้ประโยชน์จากเทคโนโลยี่ที่มีลักษณะการทำงานเป็นชั้นๆ เพื่อที่จะหยุดยั้งนักโจมตีทั้งหลาย ณ หลายจุดของห่วงโซ่ของการทำลาย ซึ่งความสามารถต่างๆ รวมถึง

- Anti-Ransomware protection การป้องกันการโจมตีของ Ransomware ซึ่งจะบล็อคการเข้าระหัสไฟล์ หรือฮาร์ดดิสค์ หรือบูธเร็คคอร์ดที่ไม่ได้รับสิทธิ์ แล้วจะกู้คืนข้อมูลดังกล่าวกลับคืนไปสู่จุด หรือสถานะเดิมที่เคยปลอดภัย
- Deep Learning AI – ใช้ปัญญาประดิษฐ์การเรียนรู้เชิงลึก ซึ่งจะใช้คุณลักษณะของไฟล์จำนวนหลายล้านลักษณะ เพื่อจะวิเคราะห์การโจมตีหรือเทร็ตที่เข้ามาและจะป้องกันมัลแวร์ทั้งหลายทั้งที่เคยรู้จักและไม่เคยเห็นมาก่อนหยุดยั้งพวกมันก่อนที่จะเริ่มทำงาน
- Anti-exploit technology ใช้เทคโนโลยี่ในการป้องกันการโจมตีประเภทเจาะจุดอ่อนหรือเจาะช่องโหว่ของระบบ (exploit) บล็อคชุดคำสั่งที่จะถูกทิ้งไว้ในระบบของเราเพื่อคอยโจมตีในภายหลัง (Active adversary techniques) และบล็อคชุดการโจมตีแบบที่ไม่ใช่ไฟล์และหรือที่เป็นแบบ Script-based
- Foundational signature-based protection การป้องกันหรือหยุดยั้งการโจมตีของเทร็ตที่เคยรู้จัก หรือเคยพบเห็นมาแล้ว



Plus, **Sophos Intercept X** secures any device on any platform – so your employees can work securely on any device they choose:

- Desktops and laptops running Windows and macOS
- Windows and Linux servers
- Virtual desktop environments hosted with cloud providers
- Mobile devices running Android, iOS, or Chromebook

นอกเหนือจากนั้น Sophos Intercept X จะปกป้องอุปกรณ์ใดๆ ของแพลทฟอร์มใดๆ ก็ตาม เพื่อทำให้พนักงานของท่านสามารถเลือกใช้อุปกรณ์ใดๆ ในการทำงานก็ได้ ไม่ว่าจะเป็น :

- เดสท็อป หรือแล็บท็อป ที่เป็น วินโดว์ หรือ macOS

- เซิร์พเวอร์ที่เป็นวินโดว์หรือลินุกซ์
- เวอร์ชวลเดสท็อปที่โฮสท์อยู่กับผู้ให้บริการคลาวด์
- อุปกรณ์หอบหิ้วหรือพกพาที่เป็นแอนดรอยด์ iOS หรือ Chromebook

Endpoint Detection and Response (EDR)

The most devastating cyber threats involve human-led attacks, often exploiting legitimate tools and processes such as PowerShell. Hands-on, live hacking enables attackers to bypass security products and protocols by modifying their tactics, techniques, and procedures (TTPs). When inside your network, attackers can move laterally to exfiltrate data, deploy ransomware, and install malware and backdoors for future attacks.

การโจมตีไซเบอร์ที่สร้างความหายนะอย่างร้ายแรงนั้นจะเป็นการโจมตีที่มีมนุษย์เป็นตัวนำพา ซึ่งมักจะใช้หรือเจาะผ่านช่องโหว่ของชุดเครื่องมือหรือกระบวนการทำงานที่ถูกต้องใช้งานจริงเช่น PowerShell เป็นต้น การสาธิตแสดงสดการ Hack โชว์ทำให้พวกนักโจมตีนำไปใช้เพื่อหลีกเลี่ยงการตรวจจับของอุปกรณ์ และโปรโตคอลของระบบรักษาความปลอดภัย โดยการแก้ไขปรับปรุงเปลี่ยนแปลงวิธีการ (แท็คติก เทคนิค) และขั้นตอนการทำงานของพวกเขา และเมื่อเข้าไปในเครือข่ายได้แล้วนักโจมตีจะใช้วิธีการเคลื่อนที่จากอุปกรณ์ตัวหนึ่งไปยังอีกตัวหนึ่ง เพื่อสอดแนมหาข้อมูลและจัดวาง ransomware และติดตั้งมัลแวร์และแบล็คดอร์เพื่อใช้ในการโจมตีในภายหน้า

Stopping these human-led attacks requires human-led threat hunting. Intercept X with EDR (Endpoint Detection and Response) gives you the tools you need to perform threat hunts from the same console used to manage your Intercept X endpoint protection.
It's the first EDR designed for security analysts and IT administrators. While other EDR tools often require dedicated headcount or their own internal security operations center (SOC), Sophos EDR is simple to use without sacrificing the ability to perform robust analysis.
การจะหยุดยั้งการโจมตีที่มีมนุษย์เป็นผู้นำพานั้น ต้องการความสามารถในการล่าสิ่งอันตรายหรือเทร็ตประเภทมนุษย์เป็นผู้นำพาเช่นกัน Intercept X with EDR (Endpoint Detection and Response ระบบตรวจจับและตอบโต้ของอุปกรณ์ปลายทาง) จะให้เครื่องมือที่คุณต้องการในการล่าเทร็ตผ่านการทำงานจากคอนโซลตัวเดียวกันกับที่คุณใช้บริหารจัดการ Intercept X endpoint protection ของคุณ

Intercept X with EDR เป็น ตัวแรกที่ถูกออกแบบมาสำหรับนักวิเคราะห์ด้านระบบความปลอดภัยและผู้ดูแลจัดการ EDR ระบบไอที ในขณะที่EDR ตัวอื่นๆ ต้องการผู้ดูแลใช้งานเป็นการเฉพาะหรือต้องมีศูนย์ปฏิบัติการด้านความปลอดภัยภายในส่วนตัวสำหรับระบบนี้ ส่วน EDR ของ Sophos นั้นใช้งานง่ายไม่ซับซ้อนไม่ต้องใช้ความสามารถด้านการวิเคราะห์ที่เลอเลิศมาจัดการเลย

With Intercept X with EDR, you can investigate suspicious signals and threats—and improve your IT hygiene—with powerful out-of-the-box customizable SQL queries. Common use cases include:

- Chrome running slowly. Identify which unauthorized Chrome extensions have been installed
- Network activity check. Look for failed login attempts and active communication from PowerShell
- Software queries. Check that sensitive files have been removed from devices and/or that you haven't exceeded software license usage
- Phishing investigation. Identify users that clicked on a suspect link and if they downloaded files

โดยการใช้งาน Intercept X with EDR คุณสามารถสอบสวนหาสัญญาณหรือเทร็ตที่น่าสงสัย และเพิ่มภูมิต้านทาน/สุขอนามัยของไอทีของคุณให้สูงขึ้น ด้วยการใช้คำสั่ง SQL querires สมรรถนะสูงที่ปรับแต่งให้เหมาะสมตามความต้องการได้ การใช้งานในการแก้ปัญหาที่ผ่านมาที่พบบ่อยๆ ได้แก่

- การที่ Chrome ทำงานช้าลง Intercept X with EDR จะช่วยชี้ให้เห็นว่ามีการติดตั้ง Chrome Extensions ที่ไม่ได้รับอนุญาตมาใช้งานหรือไม่
- Network Activity Check ใช้ตรวจหาความพยายามของการล็อกอินที่ล้มเหลวและกิจกรรมการสื่อสาร ที่กำลังส่งออกมาจาก PowerShell
- Software Queries ใช้ตรวจสอบว่ามีการนำไฟล์ที่สำคัญออกไปจากอุปกรณ์หรือไม่ และหรือคุณได้ใช้ซอฟท์แวร์ไลเซนส์เกินที่กำหนดหรือไม่
- Phishing investigation ใช้ตรวจหาว่าผู้ใช้งานรายใดที่ได้คลิ๊กหรือเข้าไปในลิ้งค์น่าสงสัยและหรือได้มีการดาวน์โหลดไฟล์ลงมาด้วยหรือไม่

Plus, you can remotely access devices using a command-line tool to remediate issues, such as rebooting devices, terminating active processes, running scripts or programs, editing configuration files, running forensic tools, and installing/uninstalling software.

นอกเหนือจากนั้น คุณสามารถเข้าหาอุปกรณ์จากทางไกลโดยการใช้ Command-line tool เพื่อแก้ปัญหาต่างๆ เช่นการรีบูตอุปกรณ์ต่างๆ สั่งหยุดการทำงานของโปรเซสต่างๆ สั่งรันสคริปต์ หรือรันโปรแกรมต่างๆ ให้ทำงาน แก้ไฟล์คอนฟิกกูเรชั่น สั่งเครื่องมือในการวิเคราะห์หาสาเหตุที่เกิดขึ้น และสั่งติดตั้งหรือล้างซอฟท์แวร์ต่างๆ ออกได้

Managed Detection and Response (MDR) บริการตรวจจับและตอบโต้การโจมตี

If you don't have the time, capacity, or expertise to run your own threat hunting and investigations, the Sophos Managed Threat Response (MTR) service is here to help.

Sophos MTR is a team of threat hunters and response experts who provide 24/7 monitoring, detection, and response capabilities delivered as a fully-managed service. They proactively hunt for and validate potential threats and incidents—and stop them before they can cause harm.

They also correlate data feeds from your Sophos protection solutions to identify indicators of compromise. Unlike other managed detection and response services, Sophos doesn't just notify you of issues; we also determine and apply the most appropriate actions to neutralize the threat.

ถ้าคุณไม่มีเวลา ไม่มีสมรรถนะ Intercept X with EDR ไม่มีความรู้ความเชี่ยวชาญที่จะทำการล่าและตรวจสอบเทร็ตเอง Sophos มีบริการ Sophos Managed Threat Response (MTR) service ให้คุณ

Sophos MTR เป็นทีมนักล่าและผู้เชี่ยวชาญในการตอบโต้เทร็ตซึ่งจะให้บริการตลอด 24 ชั่วโมง x 7 วัน เพื่อเฝ้ามอง ติดตาม ตรวจจับ และตอบโต้ ในแบบ managed services อย่างเต็มรูปแบบ ทีมนี้จะทำงานเชิงรุกเพื่อล่า ค้นหา ตรวจสอบยืนยัน หาเทร็ตและอินซิเด้นท์ที่มีโอกาสที่จะเป็น และหยุดยั้งพวกมันก่อนที่จะเริ่มทำความเสียหาย ทีมนี้จะทำการหาความเกี่ยวเนื่องเชื่อมโยงของข้อมูลต่างๆ ที่ได้จากระบบโซลูชั่นป้องกันของ Sophos เพื่อระบุหาตัวชี้วัดของการโจมตีที่จะเกิดขึ้น จะต่างจากระบบบริการ managed detection and response อื่นๆ ตรงที่ Sophos ไม่เพียงแต่จะส่งสัญญานเตือนภัยต่อคุณเท่านั้น ยังทำการแก้ไขหรือตอบโต้ที่เหมาะสมเพื่อหยุดยั้งเทร็ตที่เกิดขึ้นด้วย

Mobile Devices

When employees use personal devices for work, IT teams face the challenge of protecting company data without compromising user privacy. Our unified endpoint management solution, Sophos Mobile, secures iOS, Android, Chrome OS, Windows 10, and macOS devices. It lets you protect any combination of personal and corporate-owned devices with minimal effort and is ideal for BYOD (Bring Your Own Device) scenarios. Sophos Mobile enables you to:

- Stop mobile threats. Get industry-leading defense against mobile malware, phishing, man-in-the-middle attacks, and more, all powered by Intercept X
- Secure corporate data. Choose full-device or container-only management, depending on your needs
- Reduce admin. The flexible self-service portal lets users enroll their personal macOS, Windows 10, or mobile devices, reset passwords, and get help – with no IT involvement

เมื่อพนักงานนำอุปกรณ์ส่วนตัวมาใช้ทำงาน ทีมไอทีจะเจอปัญหาท้าทายเกี่ยวกับการปกป้องข้อมูลของบริษัท โดยที่ไม่ต้องเสียสละเรื่องนโยบายความเป็นส่วนตัวของผู้ใช้งาน โซลูชั่นจัดการอุปกรณ์ปลายทางแบบรวมเป็นหนึ่งของโซฟอส Sophos Mobile จะให้ความปลอดภัยกับอุปกรณ์ที่เป็น iOS, Android, Chrome OS, Windows 10 และ macOS มันจะช่วยปกป้องการใช้งานแบบผสมอุปกรณ์ที่เป็นของส่วนตัวและขององค์กรโดยลงแรงไปเพียงเล็กน้อยเท่านั้น และมันดีเยี่ยมเหมาะสมสำหรับการทำงานแบบใช้อุปกรณ์ประเภท BYOD และ Sophos Mobile จะช่วยให้คุณ

- หยุดยั้งเทร็ตของอุปกรณ์พกพา ด้วยการป้องกันระดับชั้นนำของอุตสาหกรรมในการป้องกันมัลแวร์ Phishing การโจมตีแบบ man-in-the-middle สำหรับอุปกรณ์พกพา ซึ่งทั้งหมดขับเคลื่อนด้วยพลังของ Intercept X
- ปกป้องให้ความปลอดภัยแก่ข้อมูลขององค์กร โดยเลือกการจัดการแบบ Full-device หรือ Container-only (Container ลักษณะคล้ายกับ Virtual Machine-VM แต่เป็นการสร้างคอมพิวเตอร์จำลองระดับ OS ไม่ใช้แบบจำลองทั้งตัวเหมือน VM ใช้ทรัพยากรน้อยกว่าแต่ยืดหยุ่นน้อยกว่า VM) ขึ้นอยู่กับความต้องการของคุณ
- ลดภาระงานแอดมิน โดยให้ทำงานผ่านพอร์ทอลแบบให้บริการตนเอง (self-service) ผู้ใช้งานสามารถลงทะเบียนอุปกรณ์ได้ด้วยตนเองไม่ว่า macOS, Windows 10 หรืออุปกรณ์พกพาอื่นๆ หรือแม้แต่ รีเซ็ทพาสเวิร์ดได้เอง หรือขอความช่วยเหลือหรือคำแนะนำจากระบบด้วยตัวเองโดยไม่ต้องขอความช่วยเหลือจากทีมไอที

Secure resources ปกป้องให้ความปลอดภัยทรัพยากรต่างๆ

Depending on your organization's needs, you may be running servers on-premises, consuming cloud-based applications, or hosting resources in private and public cloud environments on AWS, Azure, or GCP. More likely, you're doing all of the above.

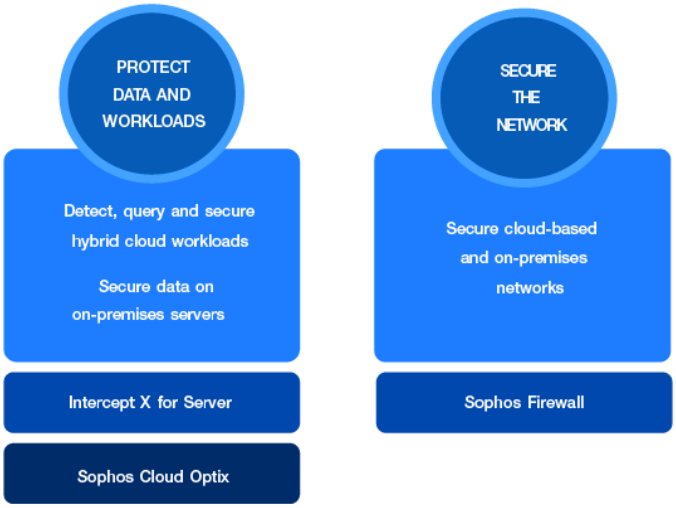
The cloud is rapidly becoming more and more central to most organizations' day-to-day operations. Because of this, cybercriminals are alert to opportunities provided by the cloud—so much so that 70% of companies using the public cloud suffered a cloud security incident in the last 12 months3.

ขึ้นอยู่กับความต้องการขององค์กรของคุณ คุณสามารถทำงานแบบ ติดตั้งใช้งานเซิร์พเวอร์ในองค์กร หรือใช้งานแอพพลิเคชั่นบนคราวด์ ฝากติดตั้งทรัพยากรไว้บนคลาวด์ทั้งที่เป็นไพรเวทคลาวด์หรือพับบลิคคลาวด์ เช่น บน AWS, Azure หรือ GCP ซึ่งคุณอาจทำทั้งหมดแบบข้างบน

คลาวด์กำลังจะกลายเป็นศูนย์กลางของการทำงานประจำวันขององค์กรมากยิ่งขึ้นเรื่อยๆ เพราะเหตุนี้ อาชญากรรมไซเบอร์กำลังตื่นตัวในโอกาสที่คลาวด์นำมาให้ มากขนาดที่ 70% ขององค์กรที่ใช้พับบลิคคลาวด์ ได้รับความเดือดร้อนจากการโจมตีความปลอดภัยจากคลาวด์ในช่วง 12 เดือนที่ผ่านมา

When it comes to securing your resources—wherever they are located—you need to do two things:

1. Protect the data and workloads themselves
2. Secure the network they're on to keep intruders out



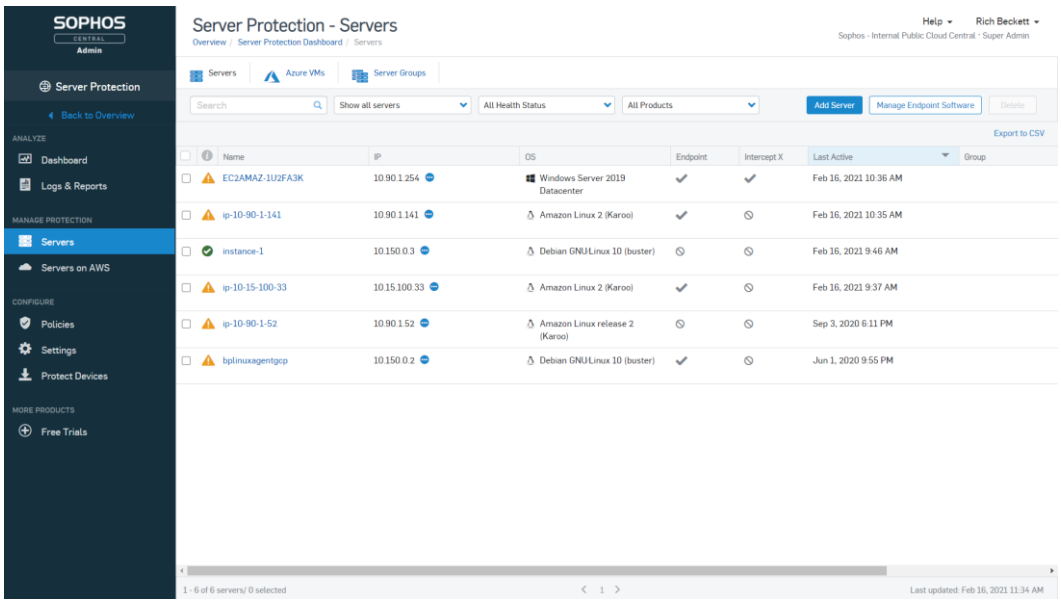
เมื่อพูดถึงการปกป้องให้ความปลอดภัยทรัพยากรของคุณ ไม่ว่ามันจะอยู่ที่ไหนก็ตาม คุณต้องทำ 2 สิ่งนี้

1. ปกป้องข้อมูลและเวิร์คโหลด
2. ปกป้องให้ความปลอดภัยเครือข่ายที่ทรัพยากรของคุณอยู่ เพื่อกีดกันผู้บุกรุกให้ห่างออกไป

Protecting your data and workloads ปกป้องข้อมูลและเวิร์คโหลดของคุณ

Your data and workloads are your most important assets. Sophos Intercept X for Server secures cloud, on-premises, or hybrid workload environments. It protects Windows and Linux virtual machines and virtual desktops from the latest threats.

- Stop advanced attacks. Including ransomware, exploit-based attacks, and malware that has never been seen before
- Lockdown your server workloads. Control what can and can't run and get notifications for any unauthorized change attempts
- Manage everything centrally. Deploy and maintain everything from a single console, including mixed scenarios that include cloud workloads and on-premises servers

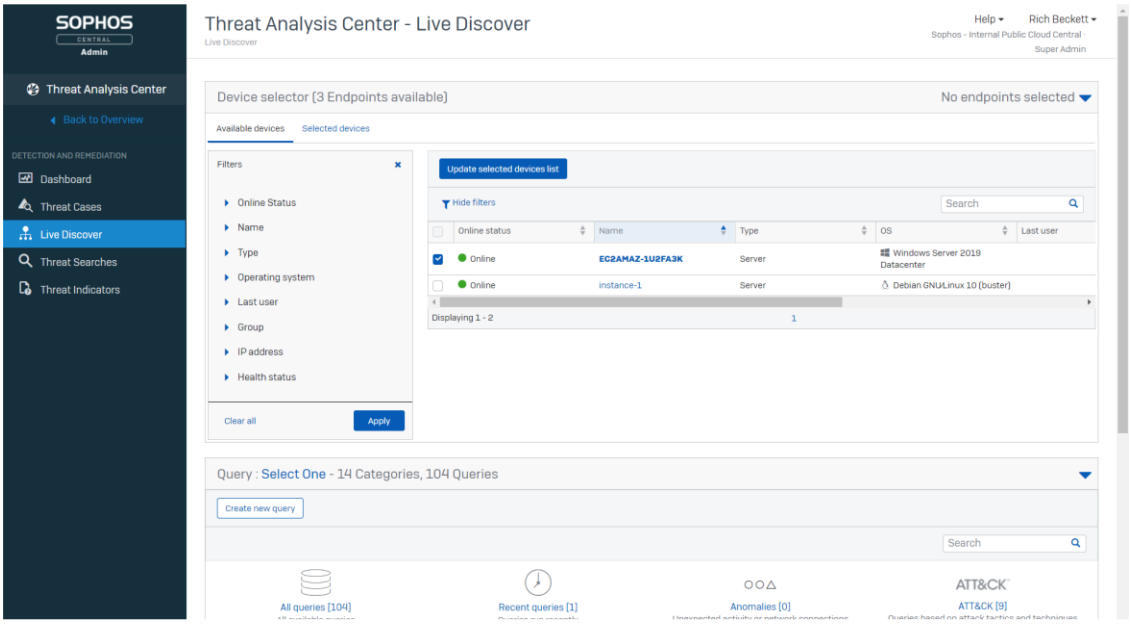


ข้อมูลและเวิร์คโหลดเป็นทรัพย์สินที่สำคัญมากของคุณ Sophos Intercept X for Server จะปกป้องข้อมูลและเวิร์คโหลดในเซิร์พเวอร์ที่อยู่บนคลาวด์ หรือที่สำนักงาน หรือเวิร์คโหลดที่อยู่บนทั้งคู่ จะปกป้องวินโดว์และลินุกซ์และเวอร์ชวลเดสท็อปจากเทร็ตล่าสุด

- หยุดยั้งการโจมตีที่ก้าวหน้าล้ำสมัยซึ่งรวมถึง Ransomware, exploit-based และมัลแวร์ที่ไม่เคยพบเห็นมาก่อน
- ปกป้องเวิร์คโหลดของเซิร์พเวอร์ ควบคุมว่าอะไรบ้างที่จะอนุญาตให้ทำงานได้ (Run) และไม่ให้ทำงาน และแจ้งเตือนเมื่อมีความพยายามที่จะทำการแก้ไขที่ไม่อนุญาตหรือไม่มีสิทธิ์จะแก้ไข
- บริหารจัดการทุกอย่างจากศูนย์กลาง ทั้งการติดตั้งปรับใช้ เคลื่อนพล หรือดูแลทำนุบำรุงทุกอย่างซึ่งรวมถึงลักษณะสภาพแวดล้อมแบบผสมซึ่งหมายถึงเวิร์คโหลดบนคลาวด์และเซิร์พเวอร์ในสำนักงาน โดยสั่ง/ทำงานผ่านคอนโซลเดียวกัน

You can also extend your EDR investigations to your servers, whether on-premises or in the cloud, with Intercept X for Server with EDR. This enables you to:

- Perform critical IT operations and threat hunting tasks. Identify performance issues, see what's installed where, and hunt down suspicious activity
- Automatically detect cloud workloads. Keep eyes on critical cloud services, including S3 buckets, databases, and server less functions
- Detect insecure deployments. Rely on constant AI monitoring of your cloud environments and notification of irregularities



คุณสามารถขยายการสอบสวนของ EDR ไปยังเซิร์พเวอร์ของคุณไม่ว่าเซิร์พเวอร์จะอยู่ที่สำนักงานในเครือข่ายของคุณหรืออยู่บนคลาวด์ก็ตามได้โดยใช้ Intercept X for Server with EDR ซึ่งจะช่วยให้คุณมีความสามารถทำ :

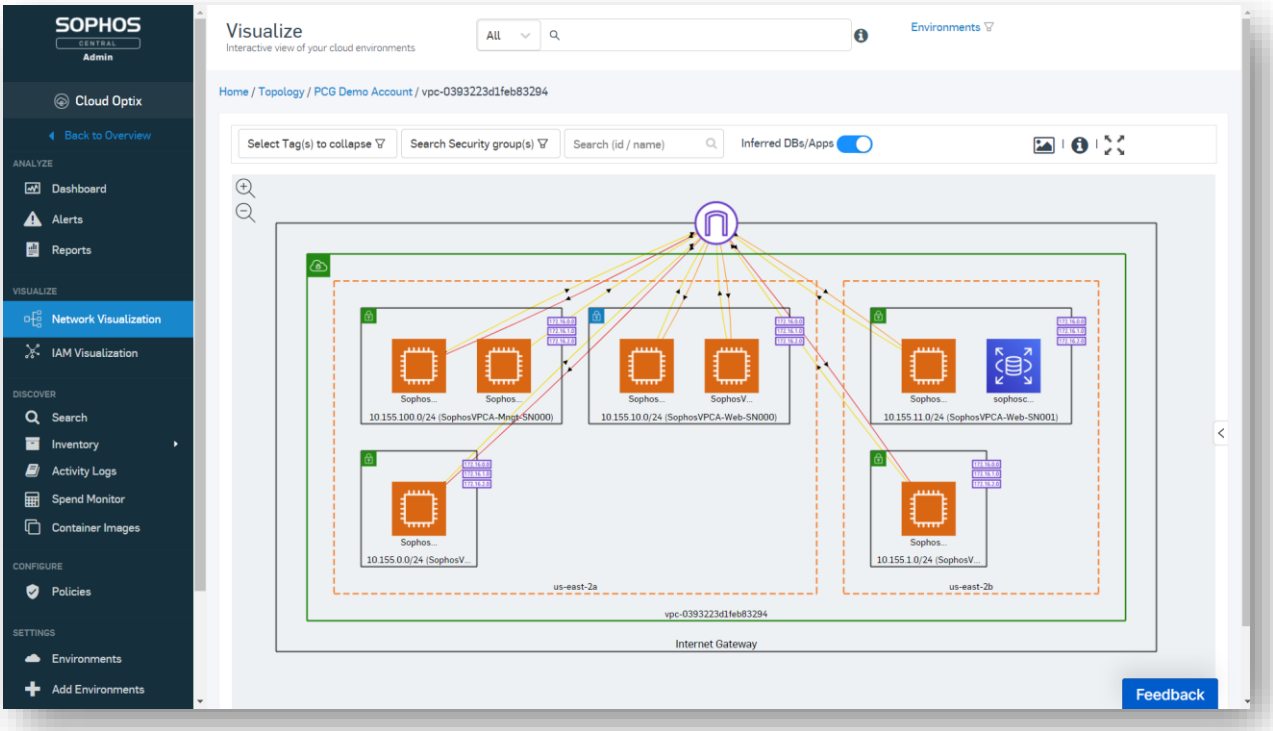
- ปฏิบัติการด้านไอทีที่สำคัญและทำการตามล่าหาเทร็ต ระบุหาการเกิดปัญหาของสมรรถนะของระบบ มองหาว่ามีอะไรถูกติดตั้งไว้ที่ไหนบ้าง และตามล่าหากิจกรรมที่น่าสงสัยที่เกิดขึ้น
- ตรวจพบเวิร์คโหลดของคลาวด์โดยอัตโนมัติ จับตาเฝ้ามองติดตามบริการบนคลาวด์ที่สำคัญสุดยอด ซึ่งรวมถึงทรัพยากรที่ใช้เป็นที่จัดเก็บข้อมูลที่อยู่บนคลาวด์ ของ Amazon Web Services (S3 Buckets) ฐานข้อมูลบนคลาวด์ (Databases) ดาต้าเบส และบริการให้ใช้โปรแกรมหรือฟังชั่นในการประมวลผลที่ไม่ต้องใช้เซิร์ฟเวอร์
- ตรวจพบการทำงานหรือการเคลื่อนพลที่ไม่ปลอดภัย โดยการใช้การเฝ้ามองติดตามสภาพแวดล้อมของคลาวด์และการแจ้งเตือนความผิดปกติโดยใช้ปัญญาประดิษฐ์อย่างสม่ำเสมอ (AI)

Protection is one side of the data and workload protection coin. Visibility is the other. You need a continuous and clear line of sight into what you have running and the ability to configure cloud provider services to prevent security breaches. Sophos Cloud Optix, our Cloud Security Posture Management solution, gives you the visibility you need to secure your organization, including:

- Multi-cloud visibility. Detailed cloud resource inventory, including servers, containers, storage, network and IAM for AWS, Azure, and GCP
- Risk-based prioritization. Continually analyze configurations for security risks and over-privileged IAM access
- Compliance management. Continuously monitor compliance with out-of-the-box templates, custom policies, and collaboration tools
- Integrated security. Identify Sophos Firewalls and workload protection on AWS
- Cloud cost optimization. Manage AWS and Azure spending on a single screen

การปกป้องเป็นด้านหนึ่งของเหรียญ การปกป้องข้อมูลและเวิร์คโหลด ทัศนวิสัย/การมองเห็นได้ก็เป็นอีกด้านหนึ่ง ของเหรียญ คุณต้องสามารถมองเห็นสิ่งที่คุณกำลังสั่งให้ทำงานอย่างชัดเจนและต่อเนื่องและมีความสามารถในการตั้งค่า (configure) การบริการของผู้ให้บริการคลาวด์เพื่อป้องกันการละเมิดความปลอดภัยที่จะเกิดขึ้น Sophos Cloud Optix ซึ่งเป็นโซลูชั่น Cloud Security Posture Management จะให้ความสามารถในการเห็นเพื่อให้คุณรักษาความปลอดภัยองค์กรของคุณ ประกอบด้วย

- Multi-cloud visibility การมองเห็นคลาวด์หลายกลุ่ม ให้รายละเอียดรายการทรัพยากรของคลาวด์ เป็นต้นว่า เซิร์ฟเวอร์ต่างๆ Container ส่วนเก็บข้อมูล (Storage) เครือข่าย และระบบจัดการตัวตนและการเข้าถึงทรัพยากร และบริการของ Amazon Web Service-AWS และ Azure (แพล็ทฟอร์มคลาวด์ของไมโครซอฟท์ GCP (Google Cloud Platform) เป็นฟังชั่นสำหรับให้บริการประมวลผลทำ Big Data และ Machine Learning)
- Risk-based prioritization การจัดลำดับตามความเสี่ยง จะทำการวิเคราะห์การตั้งค่าความเสี่ยงของระบบรักษาความปลอดภัยและการเข้าถึงที่เกินสิทธิ์ที่ควรได้รับของระบบ IAM อย่างต่อเนื่อง (โดยน่าจะใช้หลักการได้รับสิทธิ์ขั้นต่ำในการทำงาน - The principle of least privilege)
- Compliance Management (การบริหารจัดการการปฏิบัติตามกฎหมาย ระเบียบ มาตรฐาน) คอยเฝ้ามองติดตามว่ามีการปฏิบัติตามแม่แบบที่กำหนดไว้ หรือตามนโยบายที่องค์กรกำหนดไว้เอง และตามเครื่องมือการประสานงานต่างๆ อย่างต่อเนื่อง
- Integrated Security (ความปลอดภับแบบบูรณาการ) ระบุหา Sophos Firewalls และการป้องกันเวิร์คโหลดบน AWS
- Cloud Cost Optimization (ช่วยให้เกิดค่าใช้จ่ายการใช้งานของคลาวด์ที่เหมาะสมที่สุด) บริหารจัดการการใช้ AWS และ Azure ผ่านหน้าจอเดียวกัน



Sophos Cloud Optix

While security alerts for your cloud environments are helpful, with services such as Amazon GuardDuty providing great value, it's all too easy to get overwhelmed by the sheer volume of notifications. That can make it virtually impossible to recognize which notifications you actually need to deal with.

ขณะที่การแจ้งเตือนเกี่ยวกับความปลอดภัยสำหรับสภาพแวดล้อมของคลาวด์ของคุณมีประโยชน์ เช่น บริการแจ้งคำเตือนที่ได้จาก Amazon GuardDuty แต่ข้อมูล/ข้อความแจ้งเตือนเหล่านี้ก็จะประเดประดังเข้ามา จนท่วมท้นจนคุณไม่สามารถที่จะแยกตระหนักให้ชัดว่าข้อความใดที่คุณต้องจัดการกับมัน

At Sophos, we use Sophos Cloud Optix to protect the Amazon Web Services environments used to host Sophos Central, our cybersecurity platform. One of the main benefits that our own security team has gained from Cloud Optix is the ability to focus on what's important.

แต่ที่ Sophos พวกเราใช้ Sophos Cloud Optix ในการปกป้องสภาพแวดล้อมของ AWS ที่ใช้เป็นที่ติดตั้ง Sophos Central ซึ่งเป็นแพลทฟอร์มความปลอดภัยไซเบอร์ของเรา หนึ่งในประโยชน์หลักที่ทีมงานความปลอดภัยของเราเองได้รับจาก Cloud Optix ก็คือความสามารถในการทำให้รู้ว่าข้อความหรือเรื่องใดที่สำคัญที่เราต้องให้ความสนใจนั่นเอง

"With Sophos Cloud Optix, we significantly minimize alert fatigue. The powerful artificial intelligence built into Sophos Cloud Optix correlates the data and shows us what is truly meaningful and actionable." Ross McKerchar, VP and CISO, Sophos

Ross McKerchar รองประธานบริษัทและประธานเจ้าหน้าที่ด้านระบบความปลอดภัยข้อมูลสารสนเทศของบริษัท Sophos กล่าวว่า "ด้วยการใช้ Sophos Cloud Optix พวกเราลดความเหนื่อยล้าที่เกิดจากการรับข้อความแจ้งเตือน ลงเหลือน้อยมาก ปัญญาประดิษฐ์ที่ทรงพลังที่มากับ Sophos Cloud Optix จะช่วยสร้างความสัมพันธ์ของข้อมูล (ที่เกี่ยวข้องกับการแจ้งเตือน) เพื่อหาประเด็นที่ชัดเจนและจะแจ้งมาเฉพาะที่มีความหมายจริงๆ และต้องการให้จัดการจริงๆ เท่านั้น"

Secure the network ให้ความปลอดภัยแก่เครือข่าย

To guard your resources, you also need to secure the networks that they run on. Sophos Firewall delivers unmatched protection and visibility for both on-premises, AWS, and Azure environments.

- Integrated, multi-layered protection to stop even the most advanced threats
- Powerful all-in-one solution for WAF, IPS, ATP, URL filtering, path-based routing, and country-level blocking, with extensive reporting, including full insight into user and network activity
- Cloud application visibility, shadow IT discovery, and automated threat response
- Ability to harden your cloud workloads against hacking attempts like SQL injection and cross-site scripting while providing secure access to users with reverse proxy authentication
- Flexibility to run as a standalone and high-availability solution

And to make cloud-based deployment easy, everything is available in a single, preconfigured virtual-machine image.

ในการคุ้มครองทรัพยากรของคุณ คุณยังต้องให้ความปลอดภัยแก่เครือข่ายที่ทรัพยากรเหล่านั้นทำงานอยู่บนนั้นด้วย Sophos Firewall จะให้การปกป้องและให้ความสามารถในการเห็นสำหรับอุปกรณ์และเครือข่ายทั้งที่ติดตั้ง ในออฟฟิศของคุณและที่อยู่บนสภาพแวดล้อมคลาวด์ของ AWS และ Azure อย่างที่ไม่มีใครเทียบได้

- ให้การป้องกันหลายชั้นและแบบบูรณาการเพื่อหยุดยั้งแม้แต่เทร็ตที่ก้าวหน้าล้ำสมัยก็ตาม
- เป็นโซลูชั่นแบบรวมความสามารถทั้งหมดอยู่ในหนึ่งนี้ที่ทรงพลังสำหรับ WAF-Web Access Firewall, IPS-Intrusion Prevention System, ATP-Advanced Threat Protection, URL filtering, Path based routing และ country-level blocking และมาพร้อมด้วยการทำรายงานที่ครอบคลุมหลากหลายรวมถึงการให้ข้อมูลเชิงลึกของผู้ใช้งานและกิจกรรมที่เกิดขึ้นในเครือข่าย
- การให้เห็นข้อมูลของแอพพลิเคชั่นที่อยู่บนคลาวด์ และ Shadow IT Discovery ซึ่งหมายถึงการค้นหาและพบ Cloud Application ที่ไม่ได้อนุญาตจากองค์กรหรือไม่ได้แจ้งให้องค์กรรับทราบ (ซึ่งอาจก่อให้เกิดความเสี่ยงต่อองค์กร เช่น ถูกใช้เป็นที่ผ่านเข้ามาของ hacker หรือทำให้ข้อมูลรั่วไหลสู่ภายนอก หรืออาจทำให้เกิดค่าใช้จ่ายซ่อนเร้นของการใช้ทรัพยากรขององค์กรเพื่อประโยชน์ส่วนตัว เป็นต้น) และความสามารถในการตอบโต้เทร็ตโดยอัตโนมัติ
- ความสามารถในการเสริมความแข็งแรงด้านความปลอดภัยให้กับ Cloud workloads ของคุณเพื่อต้านทานความพยายามของ hacker ที่จะเจาะเข้ามาไม่ว่าจะเป็นการการที่ hackerใช้ SQL injection ซึ่งเป็นเทคนิคหรือรูปแบบการโจมตีของ hacker โดยอาศัยช่องโหว่ของโปรแกรม ทำให้สามารถแอบใส่คำสั่ง SQL เข้าไปทาง Input ทั้งหลายบน User Interface เพื่อที่จะสามารถดึงข้อมูลออกมาจากฐานข้อมูลได้ หรือแม้กระทั่งใช้คำสั่ง INSERT, UPDATE, DELETE, DROP อะไรก็แล้วแต่ที่กระทำกับฐานข้อมูลได้ หรือใช้ cross-site scripting (XSS) ซึ่งเป็นเทคนิคการฝังโค้ดเข้าไปกับหน้าเวปเพจที่มีช่องโหว่ และเมื่อผู้ใช้โหลดหน้าเวปเพจนี้ไป ข้อมูลที่สำคัญบางอย่าง เช่น ค่าของ cookie, username, password และอื่นๆ ก็อาจจะถูกขโมยไปได้ ในขณะเดียวกัน Sophos Firewall ก็ยังให้ความปลอดภัยในการเชื่อมต่อเข้ามาของผู้ใช้งานด้วยการทำตรวจสอบตัวตน/สิทธิด้วยการทำ reverse proxy authentication

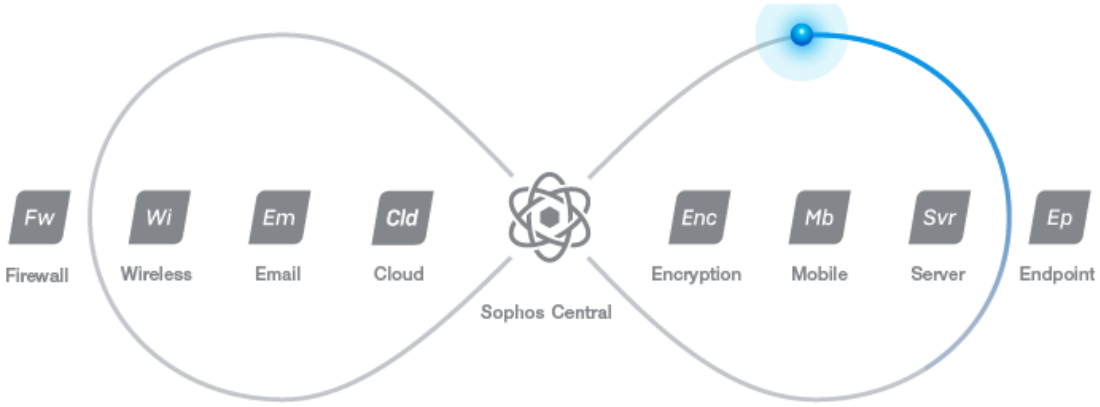
- ให้ความยืดหยุ่นในการทำงานไม่ว่าจะเป็นการทำงานแบบอุปกรณ์ตัวเดียวหรือจะทำงานแบบ High Availability หรือ 2 ตัวทำงานด้วยกัน

และเพื่อให้การติดตั้งควบคุมการใช้งานผ่านคลาวด์ทำได้ง่ายขึ้น เครื่องมือทุกอย่างจะถูกทำให้อยู่ในรูปของอิมเมจของ Virtual Machine ที่ได้ตั้งค่าไว้ล่วงหน้าแล้วเพียงอิมเมจเดียวเท่านั้น

Simplify Management - การบริหารจัดการที่ง่ายไม่ซับซ้อน

With Sophos, you can manage all of your security through a single web-based platform: Sophos Central. No more jumping from console to console to secure your organization; everything is in one place. It also enables you to conduct cross-product investigations with ease, correlating data from multiple services easily. And because Sophos Central is hosted in the cloud, it's ideal for dispersed IT teams. With over 400,000 users worldwide, you can relax knowing you're using the world's most trusted cybersecurity platform

ในการใช้งาน Sophos คุณสามารถจัดการระบบและอุปกรณ์รักษาความปลอดภัยทั้งหมดของคุณผ่านแพลทฟอร์มที่เป็นเว็บที่เรียกว่า Sophos Central เพียงแพลทฟอร์มเดียวเท่านั้น ไม่ต้องข้ามกลับไปกลับมา จากคอนโซลตัวหนึ่งไปอีกตัวหนึ่ง ทุกสิ่งทุกอย่างอยู่ในที่เดียวกันหมด มันยังให้คุณสามารถทำการสอบสวนตรวจสอบข้ามระบบอุปกณ์กันได้ง่ายมาก การสร้างความสัมพันธ์ของข้อมูลที่ได้จากบริการต่างๆ ก็ทำได้ง่ายเช่นกัน และเพราะว่า Sophos Central นั้นถูกโฮสท์อยู่บนคลาวด์มันก็ยิ่งทำให้ง่ายที่คุณจะส่งทีมงานไอที กระจายออกไปทำงานในหลายสถานที่ได้ Sophos มีจำนวนผู้ใช้งานมากกว่า 400,000 คนทั่วโลก นั่นจะทำให้คุณรู้สึกสบายใจขึ้นที่ทราบว่าคุณได้ใช้แพลทฟอร์มความปลอดภัยไซเบอร์ที่ได้รับความเชื่อถือที่สุดในโลก



Sophos Central also enables Sophos products to share real-time threat health and security information and work together to automatically respond to threats—what we call Synchronized Security. Benefits include:

- Automated incident response. If a Sophos product detects something suspicious—such as a malware infection or a device out of compliance—it shares this information with the rest of the cybersecurity system. The other products then respond automatically to the incident, in seconds. For example:
  - Sophos Firewall instantly isolates infected devices, preventing the threat from spreading and blocking lateral movement.
  - Intercept X automatically scans an endpoint when compromised mailboxes are detected, limiting the impact of email-borne threats.
  - Sophos Wi-Fi restricts network access for non-compliant devices, keeping rogue and insecure devices off your wireless network.
- Unique insights. IT teams enjoy increased visibility and control of their network, including the ability to:
  - Identify infected by name rather than IP address, speeding up security investigations.
  - Identify all apps on the network. On average, 43% of network traffic passes through as 'unclassified,' so the IT team has no idea if it's good, bad, or malicious. With Synchronized Security, Sophos Firewall and Intercept X work together to automatically identify and classify ALL apps on the network.

Sophos Central จะช่วยให้ระบบอุปกรณ์ของ Sophos ทั้งหลายแบ่งปันข้อมูลด้านความปลอดภัย และสุขภาพของเทร็ตต่างๆ ซึ่งกันและกันในลักษณะเรียลไทม์ และทำงานร่วมกันในการตอบโต้กับเทร็ตโดยอัตโนมัติ ซึ่งเราเรียกลักษณะการทำงานแบบนี้ว่า Synchronized Security (การทำงานที่พร้อมเพียงกัน ประสานงานกัน ช่วยกัน และแลกเปลี่ยนข้อมูลซึ่งกันและกัน) ซึ่งให้ประโยชน์ดังนี้

- สามารถตอบโต้เหตุการณ์ที่เกิดขึ้นโดยอัตโนมัติ หากว่าอุปกรณ์ตัวใดตัวหนึ่งของ Sophos ตรวจพบบางสิ่งที่น่าสงสัย เช่น มีการติดมัลแวร์ หรืออุปกรณ์ไม่สอดคล้องกับระเบียบกฎเกณฑ์ที่วางไว้ มันก็จะแบ่งปันข้อมูลเหล่านี้ไปยังอุปกรณ์ตัวอื่นๆ ที่เหลือของระบบความปลอดภัยไซเบอร์ และอุปกรณ์ตัวอื่นๆ นั้นก็จะตอบโต้เหตุกาณ์นั้นทันทีโดยอัตโนมัติภายในไม่กี่วินาที ตัวอย่างเช่น
  - Sophos Firewall จะแยกอุปกรณ์ตัวที่ติดมัลแวร์นั้นกันออกมาเพื่อป้องกันไม่ให้เทร็ตแพร่ออกไปและยังบล็อคป้องกันไม่ให้มีการทำ Lateral movement เกิดขึ้นด้วย
  - Intercept X จะทำการสแกนอุปกรณ์ปลายทางโดยอัตโนมัติเมื่อมีการตรวจพบเมลบ็อกถูกบุกรุกหรือถูกโจมตีเพื่อจำกัดผลกระทบที่จะเกิดขึ้นจากการแพร่เชื้อจากเมลที่ติดเชื้อนั้นๆ
  - Sophos Wi-Fi จะจำกัดหรือห้ามการเข้าเครือข่ายจากอุปกรณ์ที่ไม่ปฏิบัติสอดคล้องกับกฎระเบียบเพื่อกีดกันอุปกรณ์แปลกปลอมและไม่ปลอดภัยให้ออกไปจากเครือข่ายไร้สายของคุณ
- ข้อมูลเชิงลึกที่เป็นเอกลักษณ์ไม่เหมือนใคร ทีมไอทีจะยินดีที่จะมีความสามารถเพิ่มขึ้นในการเห็นข้อมูล และสามารถควบคุมเครือข่ายของพวกเขาซึ่งรวมถึงความสามารถ
  - ระบุพบ (Identify) อุปกรณ์ที่ติดเชื้อจากชื่ออุปกรณ์แทนที่จะเป็นหมายเลขไอพี ซึ่งจะช่วยให้การสืบสวนด้านความปลอดภัยเร็วขึ้น

- ระบุพบ (Identify) แอพพลิเคชั่นทั้งหมดบนเครือข่าย โดยเฉลี่ยแล้ว 43% ของจราจรเครือข่ายเดินทางไปในลักษณะไม่จัดกลุ่ม/ประเภท (unclassified) ซึ่งทีมไอทีไม่สามารถรู้ได้เลยว่ามันเป็นข้อมูล/จราจรที่ดีหรือไม่ดี หรือจะเป็นมัลแวร์ ด้วยวิธีการทำงานแบบ Synchronized Security ที่ Sophos Firewall และ Intercept X ทำงานร่วมกันเพื่อระบุพบ จัดชั้นแอพพลิเคชั่นทุกตัวที่อยู่บนเครือข่าย

Unmatched Protection. Unmatched Efficiency การป้องกันที่ไม่มีใครเทียบได้ ประสิทธิภาพที่ไม่มีใครเทียบได้

Running a Sophos cybersecurity system gives you next-gen protection, a single management platform, the sharing of threat intelligence across products, and automated incident response. Together, these capabilities deliver tremendous efficiency and productivity gains for IT teams. In fact, customers running Sophos Intercept X and Sophos Firewall, managed through Sophos Central, consistently say that they are able to double the efficiency of the IT team while also enjoying an 85% drop in security incidents.

"Having tools that automatically detect and correct most security events enables our small IT team to manage the company's security and prevent it being compromised." Chief Technology Officer, Software Services Provider

การใช้งานระบบความปลอดภัยไซเบอร์ของ Sophos จะให้การป้องกันของยุคสมัยหน้าแก่คุณโดยใช้แพลทฟอร์มจัดการเพียงตัวเดียวเท่านั้นซึ่งหมายรวมถึง การแบ่งปันข้อมูล การแบ่งปันคุณลักษณะเชิงลึกของเทร็ต ระหว่างอุปกรณ์ต่างๆ และการตอบโต้เหตุการณ์โดยอัตโนมัติ ด้วยความสามารถทั้งหลายนี้รวมกันจะยังมาซึ่งประสิทธิภาพและประสิทธิผลที่ยิ่งใหญ่เป็นประโยชน์ที่จะให้กับทีมไอทีของคุณ ในความเป็นจริงแล้วลูกค้าที่ใช้งาน Sophos Intercept X และ Sophos Firewall ให้ทำงานร่วมกันโดยบริหารจัดการผ่าน Sophos Central จะกล่าวเสมอๆ ว่า ประสิทธิภาพของทีมงานไอทีเพิ่มเป็น 2 เท่า ในขณะที่การเกิดเหตุการณ์ด้านความปลอดภัยลดลงไปถึง 85% เลยที่เดียว

ประธานเจ้าหน้าที่ด้านเทคโนโลยีของบริษัทผู้ให้บริการด้านซอฟท์แวร์ รายหนึ่ง กล่าวว่า "การมีเครื่องมือที่สามารถตรวจพบและแก้ไขเหตุกาณ์ด้านความปลอดภัยโดยอัตโนมัติช่วยให้ทีมงานไอทีของเราที่มีขนาดเล็กๆ สามารถจัดการกับความปลอดภัยของบริษัทและป้องกันไม่ให้ถูกบุกรุกโจมตีได้เป็นอย่างดี"

Securing Any location. Any device. Any resource. ให้ความปลอดภัยกับทุกสถานที่ ทุกอุปกรณ์ ทุกทรัพยากร

There's no turning back from the move to flexible, remote working and the growing use of the cloud. They make lives easier, but they also pose new challenges for IT teams and new opportunities for bad actors. Securing this new environment requires secure connections, secure resources, and secure devices, wherever they are—without adding to IT overheads. Sophos can help you address these modern challenges with powerful, trusted

solutions. Contact your Sophos representative to discuss your requirements, or activate a noobligation free trial to take any of our products for a test drive

จะไม่มีการหันกลับจากการเดินไปสู่การทำงานจากทางไกลที่มีความยืดหยุ่น และจากการเพิ่มขึ้นในการใช้งานคลาวด์อย่างแน่นอน ซึ่งแน่นอนว่าสิ่งเหล่านี้ทำให้ชีวิตง่ายขึ้น แต่ก็สร้างความท้าทายใหม่ๆ ให้กับทีมไอทีและสร้างโอกาสใหม่ๆ ให้กับผู้ร้ายเช่นกัน การจะให้ความปลอดภัยกับสภาวะใหม่เช่นนี้ต้องให้ความปลอดกับกับการเชื่อมต่อทรัพยากรทั้งหลายและอุปกรณ์ต่างๆ ไม่ว่าสิ่งเหล่านี้จะอยู่ที่ใด โดยที่ต้องไม่เพิ่มภาระด้านไอที Sophos ช่วยพาคุณไปพบกับความท้าทายสมัยใหม่นี้ด้วยโซลูชั่นที่เชื่อถือได้และทรงพลัง โปรดติดต่อตัวแทนของ Sophos เพื่อปรึกษาถึงความต้องการของคุณหรือขอการทดสอบใช้งานอุปกรณ์ของเราโดยไม่มีข้อผูกมัดและไม่มีค่าใช้จ่ายใดๆ ทั้งสิ้น