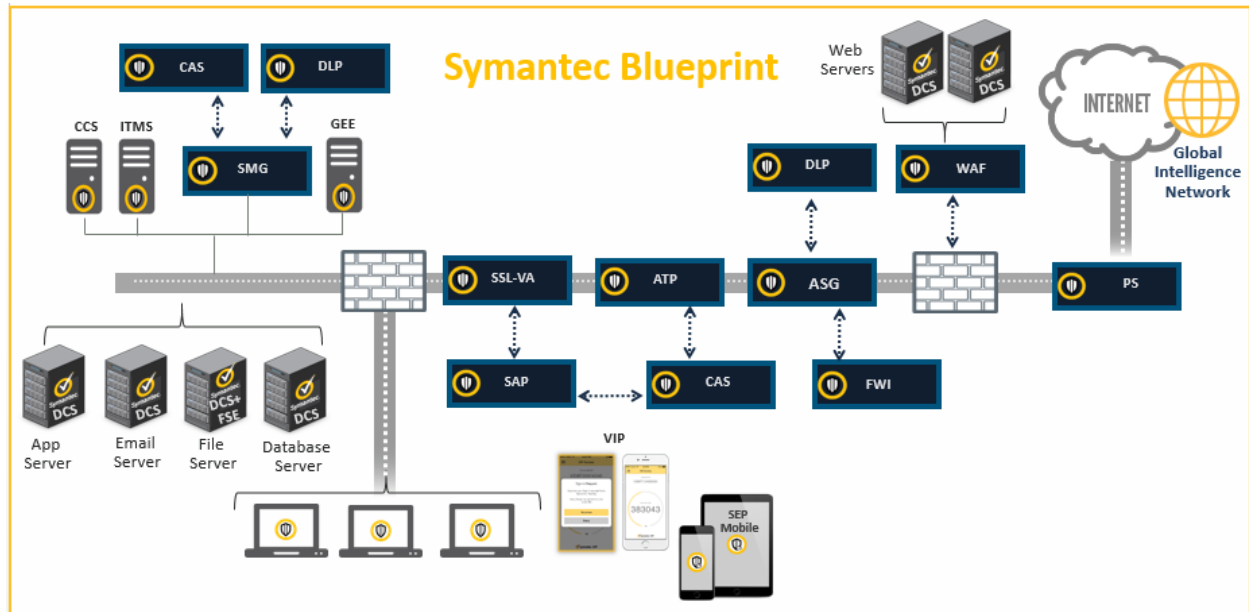


Symantec นำเสนอระบบรักษาความปลอดภัยแบบครบวงจรและเชื่อมโยงการทำงาน



ไซแมนเทคผู้นำทางด้าน Cyber Security นำเสนอโซลูชันทางด้านความปลอดภัยแบบครบวงจร เพื่อปกป้องระบบเครือข่าย (Network security), เซิร์ฟเวอร์ (Server security) และเครื่องของผู้ใช้ (Endpoint security) จากภัยคุกคามทั้งรูปแบบเก่า (Known malwares) และแบบใหม่ (Unknown malwares/Zero-Day malwares)

โซลูชันสำหรับปกป้องระบบเครือข่าย (Network security) ของไซแมนเทคเป็นโซลูชันแบบเกตเวย์สำหรับป้องกัน malware ที่มากับเว็บและอีเมล สามารถป้องกัน malwares ได้ทั้งแบบเก่าและแบบใหม่ก่อนที่จะไปถึงเครื่องของผู้ใช้ สามารถทำงานร่วมกับ Endpoint Protection เพื่อทำการค้นหาและกำจัด Zero-Day malwares จากเครื่องของผู้ใช้ได้แบบอัตโนมัติ นอกจากนี้ระบบวิเคราะห์ข้อมูล (Analytics) และอุปกรณ์ถอดรหัสกราฟฟิคประเภท SSL ของไซแมนเทคยังช่วยให้องค์กรสามารถวิเคราะห์หาสิ่งผิดปกติและ malwares ที่แพร่กระจายผ่านระบบเครือข่ายได้เองทั้งแบบที่เข้ารหัส SSL และไม่เข้ารหัส โซลูชันที่เกตเวย์ของไซแมนเทคยังทำหน้าที่ป้องกันไม่ให้ข้อมูลสำคัญขององค์กรรั่วไหลออกไปภายนอกผ่านทางเว็บและอีเมลอีกด้วย

โซลูชันสำหรับปกป้องเครื่องเซิร์ฟเวอร์ (Server security) ทำหน้าที่ป้องกันเครื่องเซิร์ฟเวอร์จากการโจมตีและการโจรกรรมข้อมูลสำคัญขององค์กรทุกรูปแบบ ช่วยค้นหาช่องโหว่และปิดช่องโหว่ให้กับเซิร์ฟเวอร์ เชนรหัสไฟล์สำคัญที่เก็บบนเซิร์ฟเวอร์ เป็นต้น

โซลูชันสำหรับปกป้องเครื่องผู้ใช้ (Endpoint security) นำเสนอการป้องกันที่ทันสมัย และครอบคลุมทุก platform ทั้ง Windows, MAC, Android และ iOS รวมทั้งอุปกรณ์ IOT ช่วยป้องกัน malwares ประเภทต่าง ๆ รวมถึง Advanced

malwares และ Zero-day malwares ทำการปิดช่องโหว่ให้กับเครื่องของผู้ใช้ และป้องกันข้อมูลรั่วไหลจากเครื่องของผู้ใช้ โดยไม่มีผลกระทบต่อประสิทธิภาพและการทำงานของเครื่อง

นอกจากนำเสนอโซลูชันแบบ On-Premise โซลูชันเหล่านี้ยังนำเสนอโซลูชันในรูปแบบ On-Cloud เช่น บริการ Cloud สำหรับปกป้องผู้ใช้นอกสำนักงานให้สามารถใช้เว็บอย่างปลอดภัยเหมือนกับทำงานอยู่ในสำนักงาน บริการ Cloud สำหรับกรองอีเมล spams ป้องกัน malwares ที่มาด้วยอีเมล และป้องกันข้อมูลรั่วไหลผ่านทางอีเมล บริการสำหรับปกป้อง services และแอปพลิเคชันขององค์กรที่อยู่บน Cloud เช่น o365, Salesforce, และ services บน AWS และ Azure จากการโจมตีรูปแบบต่างๆ ป้องกันข้อมูลสำคัญจากการถูกโจรกรรมและรั่วไหล และบริการพิสูจน์ตัวตนผู้ใช้ (authentication) แบบ 2 factors ก่อนที่จะอนุญาตให้ผู้ใช้สามารถใช้ services ของตนบน Cloud ได้ เป็นต้น

สำหรับองค์กรที่มีทรัพยากรบุคคลทางด้านความปลอดภัยที่จำกัดหรือขาดผู้เชี่ยวชาญ โซลูชันเหล่านี้ยังมีบริการที่ช่วยแบ่งเบาภาระให้กับองค์กร โดยนำเสนอบริการดังต่อไปนี้ บริการข้อมูล malwares ใหม่ (Threat Intelligence) บริการระบบ SOC บน Cloud บริการแก้ไขปัญหาเมื่อเกิดภัยคุกคาม (Incident Response) และบริการฝึกอบรมทางด้านความปลอดภัย เป็นต้น ให้กับองค์กร

สามารถอ่านข้อมูลเพิ่มเติมได้ที่ www.symantec.com

Network Security

ASG – Advanced Secure Gateway (Web Gateway)

อุปกรณ์เว็บ security ขั้นสูง, กรองเว็บ และป้องกันอันตราย เช่น malware, adv. malware จากเว็บ

PS - PacketShaper (Bandwidth Management)

อุปกรณ์บริหารจัดการทราฟฟิก ทำ QoS และ monitor การทำงานของแอปพลิเคชัน

DLP – Data Loss Prevention

ระบบตรวจสอบและป้องกันข้อมูลสำคัญรั่วไหล

ATP – Advanced Threat Protection

ระบบตรวจหาและป้องกัน known และ unknown malwares ที่ network และสามารถค้นหาและกำจัด unknown malwares ที่หลุดรอดไปยังเครื่องของผู้ใช้ได้

SSL-VA – SSL Visibility Appliance

อุปกรณ์ถอดรหัสทราฟฟิกประเภท SSL

SAP – Security Analytic Platform

อุปกรณ์เก็บ packets และช่วยวิเคราะห์ข้อมูล พร้อมแสดงรายงานทาง security สามารถวิเคราะห์ข้อมูลย้อนหลังได้

WAF – Web Application Firewall

อุปกรณ์ไฟร์วอลล์สำหรับเว็บ

SMG – Symantec Messaging Gateway (Mail Gateway)

อุปกรณ์รักษาความปลอดภัยสำหรับอีเมล และป้องกัน spam

CAS - Content Analysis System (Anti-Virus and Sandboxing)

อุปกรณ์ช่วยตรวจจับ known และ unknown malwares สามารถ run และตรวจสอบพฤติกรรมของไฟล์ได้ (Sandboxing)

FWI – Full Web Isolation

อุปกรณ์เปลี่ยนหน้าเว็บให้เป็นภาพ โดยทำการเปลี่ยนหน้าเว็บให้เป็นสตรีมของภาพ สามารถตรวจจับ input ทาง mouse และ keyboard เช่น การ click หรือ การพิมพ์ข้อความ บนส่วนต่างๆ ของภาพ ผู้ใช้จะได้รับความรู้สึกเหมือนกับใช้เว็บจริง ๆ สามารถป้องกัน Malware จากการท่องเว็บได้ 100%

Server Security

DCS – Data Center Security

โซลูชันรักษาความปลอดภัยสำหรับเครื่องเซิร์ฟเวอร์

CCS – Control Compliance Suite

โซลูชันสำหรับตรวจหาช่องโหว่บนเครื่องเซิร์ฟเวอร์ เทียบกับมาตรฐานหรือข้อบังคับ

ITMS – IT Management Suite

โซลูชันสำหรับบริหารจัดการเครื่องผู้ใช้ และเครื่องเซิร์ฟเวอร์ เช่น ลง patch และ software, เปลี่ยน configuration และทำ Inventory เป็นต้น

FSE – File Share Encryption

โซลูชันสำหรับเข้ารหัสไฟล์ข้อมูลสำคัญที่เก็บบนไฟล์เซิร์ฟเวอร์

GEE – Gateway Email Encryption

เกตเวย์สำหรับเข้ารหัสอีเมลสำคัญ

Endpoint Security

SEP – Symantec Endpoint Protection

ซอฟต์แวร์สำหรับป้องกัน malware เช่น virus บนเครื่องของผู้ใช้

EDR - Endpoint Detection & Response

ความสามารถในการทำงานร่วมกับระบบ ATP เพื่อกำจัด unknown malwares

SEE - Symantec Endpoint Encryption

ซอฟต์แวร์สำหรับเข้ารหัสไฟล์ และ Harddisk

DLP Endpoint

ซอฟต์แวร์สำหรับป้องกันข้อมูลสำคัญรั่วไหลจากเครื่องของผู้ใช้

VIP – Validation and ID Protection

บริการสำหรับช่วยพิสูจน์ตัวตน แบบ 2 Factor Authentication หรือ

One time password

SEP Mobile

ซอฟต์แวร์สำหรับทำ security ให้กับเครื่อง Mobile (Android และ iOS)