



Adaptive Defense 360

Find the answers, solve the problem



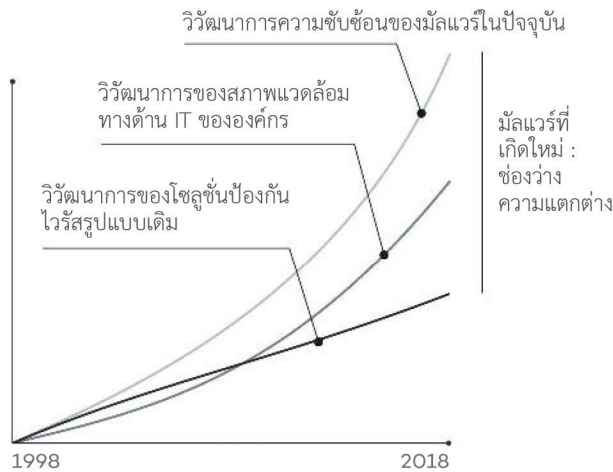
ระบบป้องกันภัยคุกคามสมบูรณ์แบบที่มาพร้อมกับระบบการทำงานรอบด้านทั้งการป้องกัน, การตรวจจับ, การตรวจหาสาเหตุ และการฟื้นฟูทั้งหมดนี้ทำงานร่วมกันในโปรแกรมเดียว

การปกป้องเครื่องลูกข่ายให้ปลอดภัยจากภัยคุกคามและการโจมตีทางด้านต่าง ๆ นั้นถือเป็นเรื่องที่ยากขึ้นทุกขณะ การป้องกันในรูปแบบเก่าๆ ที่ประกอบไปด้วย antivirus/anti-malware, personal firewall, web & email filtering, device control และการใช้เครื่องมือเสริมต่างๆ เพื่ออุดช่องโหว่และป้องกัน zero-day attack ได้ทั้งหมดเป็นเรื่องที่ทำได้ยาก จนกระทั่งเจ้าหน้าที่ IT บางองค์กรเลือกที่จะใช้บริการจาก vendor หลายรายเพื่อที่จะปกป้องเครื่องลูกข่ายให้ดีที่สุด

Adaptive Defense 360 เป็นผลิตภัณฑ์แรกๆ ที่รวมการทำงานระหว่างระบบ antivirus - Endpoint Protection (EPP) และระบบการตรวจจับและค้นหาสาเหตุ - Endpoint Detection & Response (EDR) เข้ามาอยู่ในโปรแกรมเดียว สามารถลดภาระงานทางด้าน IT ได้อย่างมาก, **Adaptive Defense 360** เป็นระบบการป้องกันที่ดีที่สุดของ Panda ซึ่งใช้งานง่าย, บริหารจัดการผ่านศูนย์กลาง, ฟื้นฟูข้อผิดพลาด, ตรวจสอบ และออกรายงานสถานะแบบ real-time, กำหนด policy แบบแบ่งกลุ่ม, ควบคุมการเชื่อมต่ออุปกรณ์ภายนอก และการใช้งานเว็บไซต์ต่างๆ ผ่านศูนย์กลาง

ช่วงระยะเวลาที่เสียไปในการตรวจพบมัลแวร์ตัวใหม่และสร้างฐานข้อมูลในการป้องกันมัลแวร์แต่ละตัวนั้นมีการใช้เวลามากขึ้นตามความซับซ้อน และช่องว่างที่กำลังขยายตัวนี้กลายเป็นช่องโหว่ให้ hacker ทำการปล่อย virus, ransomware, trojan และภัยคุกคามอื่นๆ เข้าไปก่อนวนเครือข่ายขององค์กรต่างๆ โดยภัยคุกคามที่พบบ่อยมากขึ้น เช่น ทำการเข้ารหัสเอกสารสำคัญและทำการเรียกค่าไถ่หรือการขโมยข้อมูลเอกสารสำคัญและใช้ต่อช่องทางต่างๆ

Adaptive Defense เป็นนวัตกรรมใหม่ของ Panda ที่มีการทำงานร่วมกับระบบ EDR โดยทำการตรวจสอบและแบ่งแยกประเภทของโปรแกรมต่างๆ ในทำงานอยู่ในเครื่องได้อย่างแม่นยำ และจะอนุญาตให้โปรแกรมที่มีการจดทะเบียนถูกต้องนำเชื่อถือเท่านั้นที่สามารถใช้งานได้, ระบบ EDR ของ **Panda Adaptive Defense 360** ทำงานอยู่บนหลักการ 3 อย่างคือ ทำการตรวจสอบทุกโปรแกรมที่ทำงานอยู่ในเครื่องลูกข่ายและเซิร์ฟเวอร์, ทำการจัดหมวดหมู่อัตโนมัติโดยใช้ฐานข้อมูลจากระบบ Big Data และสุดท้ายหากมีการตรวจพบโปรแกรมที่ไม่น่าเชื่อถือหรือโปรแกรมที่ไม่มีข้อมูลอยู่ในระบบ Big Data โปรแกรมนั้นจะถูกบล็อกโดยทันที และทำการส่งข้อมูลให้เจ้าหน้าที่ผู้เชี่ยวชาญของ Panda ทำการตรวจสอบการทำงานของโปรแกรมนั้นๆ โดยอัตโนมัติ



อย่างไรก็ตามนี่เป็นเพียงจุดเริ่มต้น ทั้งมัลแวร์และระบบรักษาความปลอดภัยด้าน IT จะมีการเปลี่ยนแปลงที่สำคัญในแง่ของปริมาณและความซับซ้อนอยู่เสมอ มีไวรัสเกิดขึ้นใหม่มากกว่า 200,000 ตัวต่อวัน และมีพัฒนาการความซับซ้อนทางด้านเทคนิคในการหลีกเลี่ยงการตรวจจับ, ความสามารถในการซ่อนตัว, การหาช่องโหว่ของระบบ network เพื่อใช้ในการโจมตี อยู่ตลอดเวลา

ระบบป้องกันไวรัสรูปแบบเดิมมีประสิทธิภาพเพียงแค่การตรวจจับไวรัสที่มีข้อมูลอยู่ในฐานข้อมูล(signature) และการวิเคราะห์พฤติกรรมพื้นฐาน(heuristic) เท่านั้น จึงทำให้ไม่สามารถป้องกันไวรัส, zero-day ได้ทั้งหมด จนเกิดเป็นกราฟ "มัลแวร์ที่เกิดขึ้นใหม่: ช่องว่างความแตกต่าง"



ด้วยการรวมความสามารถต่างๆ เหล่านี้เข้าด้วยกัน ทำให้ Adaptive Defense 360 คือผลิตภัณฑ์ทางด้านความปลอดภัยที่ดีที่สุดของ Panda ถึงเวลาสิ้นสุดวงจรชีวิตที่ต้องคอยวุ่นวายในการปรับตัวให้ก้าวทันภัยคุกคามด้วยนวัตกรรมใหม่นี้ที่รวบรวมการทำงานของระบบต่างๆ เข้าด้วยกันอย่างสมบูรณ์ **Automated prevention, detection, forensic and remediation**

ระบบเดียวที่รับประกันความปลอดภัยของโปรแกรมต่างๆที่กำลังใช้งานอยู่ในเครื่องลูกข่ายและเซิร์ฟเวอร์

COMPLETE AND ROBUST PROTECTION GUARANTEED

Panda Adaptive Defense 360 สามารถปรับโหมดการทำงานได้ 2 รูปแบบ

- **Standard mode** อนุญาตให้โปรแกรมที่น่าเชื่อถือและไม่น่าเชื่อถือสามารถใช้งานได้ โดยโปรแกรมที่น่าเชื่อถือจะสามารถใช้งานได้ดีกว่าที่ทีมงาน Panda Security จะวิเคราะห์ข้อมูลแล้วผลออกมาเป็นภัยคุกคามโปรแกรมที่น่าเชื่อถือนั้นจะถูกบล็อกทันที
- **Extended mode** อนุญาตให้เฉพาะโปรแกรมที่น่าเชื่อถือเท่านั้นที่สามารถใช้งานได้ นี่เป็นรูปแบบที่เหมาะสมสำหรับการใช้งานขององค์กรที่ต้องการปลอดภัยจาก zero risk ต่างๆ

FORENSIC INFORMATION

- **ดูกราฟขั้นตอนการทำงานของมัลแวร์** เพื่อรับรู้และเข้าใจเหตุการณ์ต่างๆที่เกิดขึ้นจากมัลแวร์นั้นๆ
- ตรวจสอบช่องโหว่ของโปรแกรมต่างๆที่ติดตั้งอยู่บนเครื่องข่ายขององค์กร

PROTECTION FOR VULNERABLE OPERATING SYSTEMS AND APPLICATIONS

มีโปรแกรมมากมายหลายชนิดที่ไม่ได้รับการดูแลและพัฒนาต่อจากผู้สร้าง เช่น Windows XP ซึ่งเป็นโปรแกรมที่มีช่องโหว่และนั่นคือช่องทางที่ผู้ใช้งานมักจะถูกผู้ไม่ประสงค์ดีทำการโจมตีผ่านช่องโหว่เหล่านั้น

นอกจากนั้นแล้วก็มีช่องโหว่บนโปรแกรมต่างๆที่ได้รับความนิยมทั่วโลกเช่น Java, Adobe, Microsoft Office และ browser ต่างๆ ซึ่ง 90% ของการแพร่กระจายของมัลแวร์มาจากช่องโหว่ของโปรแกรมต่างๆเหล่านี้

ระบบตรวจสอบและป้องกันช่องโหว่ของ Adaptive Defense 360 จะช่วยให้องค์กรสามารถดำเนินงานต่อไปได้ตามปกติในสภาพแวดล้อมที่ปลอดภัย ถึงแม้ว่าระบบจะไม่เคยได้รับการอัปเดตหรือปรับปรุงใดๆเลยก็ตาม

FULL EPP CAPABILITIES

Adaptive Defense 360 ทำงานร่วมกับระบบป้องกันไวรัส Panda Endpoint Protection Plus ซึ่งจะช่วยให้อาจสามารถตรวจจับภัยคุกคามที่มีความซับซ้อนได้ดียิ่งขึ้น ทำให้ EPP สามารถทำงานได้อย่างเต็มประสิทธิภาพ รวมไปถึง

- ฟันฟูและแก้ไขข้อผิดพลาด

- ควบคุมการเชื่อมต่ออุปกรณ์ภายนอกผ่านศูนย์กลาง : ป้องกันการแพร่กระจายของมัลแวร์และป้องกันการโจรกรรมข้อมูลโดยบล็อกการใช้งานอุปกรณ์ต่างๆ
- ควบคุมการเข้าใช้งานเว็บไซต์ต่างๆตามช่วงเวลาที่เหมาะสม
- ระบบป้องกันไวรัสและสแปมสำหรับ Exchange Server
- Personal Firewall และ อื่นๆ

CONTINUOUS STATUS INFORMATION ON ALL ENDPOINTS IN THE NETWORK

ได้รับการแจ้งเตือนแบบ real-time หากมีการตรวจพบมัลแวร์แพร่กระจายอยู่ในเครื่องข่าย โดยออกรายงานที่มีข้อมูลครบรอบด้าน เช่น ตำแหน่งของไฟล์มัลแวร์, เครื่องที่มีการแพร่กระจายมัลแวร์ และสถานะการป้องกันจากมัลแวร์นั้นๆ สามารถรับรายงานสรุปผลแบบรายวันเกี่ยวกับพฤติกรรมของมัลแวร์ต่างๆที่เกิดขึ้นในเครื่องข่ายผ่านช่องทาง email

100% MANAGED SERVICE

หมดกังวลเกี่ยวกับการลงทุนในบุคลากรทางด้าน IT สำหรับการใช้งานและดูแลความเรียบร้อยต่างๆในการใช้งานผลิตภัณฑ์ Adaptive Defense 360 สามารถทำการตรวจสอบการทำงานของโปรแกรมต่างๆในเครื่องลูกข่ายโดยอัตโนมัติ โดยทำงานเชื่อมต่อกับระบบ Big Data และอยู่ภายใต้การดูแลอย่างต่อเนื่องโดยผู้เชี่ยวชาญจาก PandaLabs

Tech Specs

Internet browser:

All you need is an Internet connection and an up-to-date browser.

- Internet Explorer
- Edge
- Chrome
- Firefox
- Opera

Platforms supported by the products managed through Aether:

Operating system	Supported versions
Windows	XP SP3 or later XP 64-bit SP2 or later
Windows servers	Windows Server 2003 (32/64-bit and R2) SP2 or later
MacOS desktops and servers	macOS 10.10 Yosemite or later
Linux desktops and servers	Ubuntu 14.04 LTS, 14.10, 15.04, 15.10, 16.04 LTS and 16.10 Fedora 23, 24 and 25 * Check with your partner or sales advisor about support for other distributions.
Android	Version 4 or later

