EXECUTIVE VIEWPOINT

How to Defend Endpoints with Hardware-based Security

The shift to remote work, accelerated by COVID-19, has created new endpoint cybersecurity challenges. Yasser Rasheed, Global Director for Enterprise Endpoint & Security Products at Intel, explains the reason why hardware-level protection is needed.

Yasser Rasheed

GLOBAL DIRECTOR FOR ENTERPRISE ENDPOINT & SECURITY PRODUCTS, INTEL

YASSER RASHEED FOCUSES PRIMARILY ON INTEL® VPRO™ PLATFORMS AND INTEL'S COMPETITIVE SALES INITIATIVES. PRIOR TO THIS ROLE, YASSER WAS THE CHIEF TECHNOLOGY OFFICER (CTO) FOR INTEL'S BUSINESS CLIENT PLATFORM DIVISION, RESPONSIBLE FOR TECHNICAL STRATEGY, PRODUCT DEFINITION, ARCHITECTURE AND EXECUTION OF KEY ECOSYSTEM INNOVATION PROGRAMS FOR INTEL'S BUSINESS CLIENT PLATFORMS. YASSER HOLDS A PH.D. IN ELECTRICAL AND COMPUTER ENGINEERING FROM THE UNIVERSITY OF TORONTO, AND AN EXECUTIVE MBA FROM THE UNIVERSITY OF OREGON.

FOR MORE INFORMATION

Learn more about Intel Hardware Shield here.

Q: How have mobility and remote work created new challenges for securing endpoints?

IT leaders have had to rethink remote work so employees as well as IT staff can be productive. Legacy IT management techniques have become useless as traditional connections to wired Ethernet have disappeared. Instead, we all now share resources online or in the cloud. But working remotely, often from home, means sharing network access with teenagers, students, and spouses, sometimes neighbors. Attackers can take advantage of this new paradigm faster than defenders can stop them. The regulatory environment has also changed. Under privacy laws such as GDPR and CCPA, businesses must protect not only data about their business but data about their customers, including metadata for audits.

> "Hardware Shield protects both the operating system and below the OS."

Q: Why is hardware-based security needed to protect endpoint data?

Businesses need to detect threats and prevent them. But businesses also need to protect identities and data, and they need to recover quickly. Hackers are used to attacking software, and even though we're spending more money on software-based defense, attacks are increasing. Hardware-based security can be transformative because it works to disrupt hackers. Intel's silicon-enabled AI threat detection helps stop ransomware and crypto-mining attacks on Windows-based systems.

Q: How does the Intel vPro platform address today's endpoint cybersecurity needs?

The Intel vPro platform comes with Intel Hardware Shield™, which provides threat detection and prevention capabilities, as well as infrastructure for data and application protection. Under Intel Hardware Shield, should a remote system be attacked, Intel Active Management Technology (also part of the Intel vPro platform) can wirelessly and remotely recover the system to a known state.[1] That's important because with the increase in remote work, IT administrators might not have physical access to a machine that has stopped working. Without that capability, a user might have to stop working, ship their computer out, and wait a week for it to be fixed.

Intel Hardware Shield helps protect both the operating system and below the OS. If the OS is compromised, we can identify the attack, track it, and put the OS on hold. Below the OS, Hardware Shield helps keep attackers from hacking into the BIOS to gain powerful supervisor privileges. We detect anomalies at the hardware level. Even if someone gets into the BIOS, they cannot access system memory, and we can detect attempts to insert a layer between the OS and the hardware.

Q: What should IT leaders know about Intel's Zero Day Initiative (ZDI) and Bug Bounty programs?

Through ZDI, we encourage the reporting of zero-day vulnerabilities to affected vendors. ZDI works collaboratively with these vendors to notify the public of vulnerabilities through a joint advisory. Intel's Bug Bounty program invites the security research community to work with us to mitigate and coordinate the disclosure of potential security vulnerabilities.

CIO FROM IDG

[1] Intel AMT requires a network connection; must be a known network for WiFi out-of-band management. Learn more at intel.com/11thgenvpro. Results may vary.