PROWESS

Advanced Threats Require Advanced Defenses

Hardware-based security helps detect and protect against advanced and below-the-operating-system attacks, including ransomware.

Today's cyber threats pose a serious challenge to traditional client-security software, which runs above the operating system (OS) and has limited ability to protect system hardware and firmware from below-the-OS attacks.

Software-based protection alone is not enough. A thorough security solution for PCs and laptops should include hardware-based security capabilities, in addition to traditional malware scanning software. Hardware-enabled security can help detect and protect against new types of threats, including memory safety–based threats, ransomware, and cryptomining attacks.

Ransomware, Cryptomining, and Below-the-OS Attacks Are Rising

Ransomware and cryptomining are rising in popularity among hacking groups.

26%
increase in new coin-miner malware in the first half of 2020[1]

7x
growth in ransomware attacks in 2020, compared to 2019[2]

77%
of organizations hit by ransomware in 2018 were running up-to-date endpoint-protection software[5]

51%
of businesses were affected by ransomware in 2019[3]

$20 billion
projected damage caused by ransomware in 2021[4]

Introducing Intel® Hardware Shield: Hardware-Enhanced Detection and Protection

To defend against modern attacks, a top-to-bottom model of security is needed, one that begins in the hardware. Intel® Hardware Shield offers an imposing defensive wall of this type. Available exclusively on the Intel vPro® platform, Intel Hardware Shield grounds security below the OS, constructing a hardware-anchored barrier to strengthen organizations' security in the face of sophisticated incursion attempts. It also offers its own direct, secondary line of defense against application and OS attacks by relying upon unique hardware features to detect threats such as ransomware and cryptomining.

Table 1 shows a selection of Intel Hardware Shield capabilities. For a more thorough discussion, **see the full paper**.

Table 1. Intel® Hardware Shield hardens business clients against today's evolving threats through silicon-based capabilities that work out of the box, some of which are shown here

Capability	What It Does
Below-the-OS Protection	Intel® Hardware Shield locks down memory in the BIOS against firmware attacks and enforces a secure boot at the hardware level. These below-the-OS security features are set up by the PC manufacturer, so IT departments and users can take advantage of them right out of the box.
Data and App Protection	Helps protect endpoint applications, operating systems, and data without impacting the user experience.
Advanced Threat Detection	Enhances detection of advanced threats including ransomware and cryptomining without impeding the user experience. Through Intel® Control-flow Enforcement Technology, Intel Hardware Shield has the potential to eliminate an entire class of attacks: control-flow hijacking.

In today's security landscape, with ever-evolving attacks and increasing numbers of threats, software-only solutions are no longer adequate. That's why a hardened client fleet is critical to businesses that want to strengthen their protection against advanced threats such as ransomware and control-flow programming attacks.

Learn More

Download the full paper: www.prowesscorp.com/areyoufighting/

Learn more about Intel Hardware Shield: www.intel.com/hardwareshield

The analysis in this document was done by Prowess Consulting and commissioned by Intel.

[1] McAfee. "McAfee Labs COVID-19 Threats Report." July 2020. **www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-july-2020.pdf**.

[2] Bitdefender. "Mid-Year Threat Landscape Report." 2020. **www.bitdefender.com/files/News/CaseStudies/study/366/Bitdefender-Mid-Year-Threat-Landscape-Report-2020.pdf**.

[3] Comodo. "Ransomware Attacks 2020." November 2020. **https://enterprise.comodo.com/blog/recent-ransomware-attacks/**.

[4] Cybercrime Magazine. "Global Ransomware Damage Costs Predicted To Reach $20 Billion (USD) By 2021." October 2019. **https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/**.

[5] Sophos. "Businesses Impacted by Repeated Ransomware Attacks and Failing to Close the Gap on Exploits, According to Sophos Global Survey." January 2018. **www.sophos.com/en-us/press-office/press-releases/2018/01/businesses-impacted-by-repeated-ransomware-attacks-according-to-sophos-global-survey.aspx**.