SOLUTION BRIEF

Intel vPro® Platform
Information Security

The Intel vPro® Platform: Proactive Device Protection against Modern Threats

As threats evolve and escape detection, organizations need an end-to-end approach to security that begins in hardware.

intel vPro® Platform

The cybersecurity landscape is shifting at an accelerating rate. As organizations witness a rise in sophisticated attacks, the Intel vPro® platform—built to give businesses a broad and solid base for performance, security, stability, and manageability—is offering a strong response to these new threats through a proactive, hardware-based defense.

Attacks against organizations are rising sharply in both number and variety,[1,2] with an increase in firmware exploits targeting the surface below the operating system.[3] It's becoming clear to those responsible for defending corporate networks—such as chief information security officers (CISOs), chief information officers (CIOs), and others—that a new approach to enterprise security is needed. The traditional perimeter-based model of defense is giving way to a tighter, "zero-trust" model, a strategy in which no single entity is assumed to be secure. In a zero-trust approach to security, the entire software stack must be monitored and protected top to bottom, and communication must be secured from cloud to endpoint.

Zero-Trust Approach to Security Must Be Rooted in Hardware

This new, holistic view requires a rock-solid security foundation based in hardware. It's only at the hardware layer that the root of trust can be established and passed upwards transitively through the entire stack, as illustrated in Figure 1. Not rooting a chain of trust in hardware is like leaving the ground floor of your building unlocked and unmonitored. This lack of protection allows all manner of malicious code (such as rootkits and bootkits) to secretly hijack systems as devices are starting, while remaining hidden to traditional antivirus applications, which typically cannot see beyond the scope of the operating system.

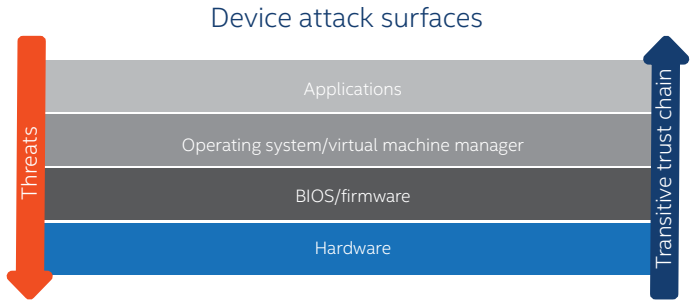

Figure 1. Security must be rooted in hardware to offer a better end-to-end defense

Intel vPro® Platform: A More Secure IT Environment

Intel is committed to helping organizations and IT professionals meet today's security challenges. To this end, Intel vPro® technology helps enable a security strategy built on hardware. As shown in Figure 2, Intel® Hardware Shield acts as the foundation for the Intel vPro® platform, with features built on top of this foundation that help CISO/CIO teams meet their four highest-priority security goals:

- Improving the efficacy of threat detection
- Improving data protection against theft and tampering
- Improving identity and access protection
- Improving recovery time after a breach

To help improve the efficacy of threat detection, the Intel vPro® platform offers Intel® Threat Detection Technology (a feature described later in this document). To help improve data protection against theft and tampering, the platform provides data encryption capabilities such as encryption acceleration and Intel® Secure Key, which generates high-entropy keys. The Intel vPro® platform infrastructure also supports a variety of multi-factor authentication solutions to enable improved identity and access protection. Finally, the platform helps ensure faster recovery times through Intel® Active Management Technology (also described later in this document).

Intel® Hardware Shield, Available Exclusively on the Intel vPro® Platform

Modern cyber threats often target devices on levels below the operating system (OS), where they can do damage and cover their tracks beyond the visibility and supervision of anti-malware applications. The Intel vPro® platform helps address these threats through a new security technology called Intel® Hardware Shield, which helps extend security to the BIOS and firmware layer. This hardware-based technology helps reduce the risk that a bug or vulnerability in firmware (or device drivers) could be used to inject malicious code into the platform at runtime and hide that code from traditional antivirus solutions.

Intel® Hardware Shield provides built-in security features to help protect against firmware attacks. It achieves this improved protection against firmware attacks by:

- Helping to prevent malicious code injection by restricting memory access in the BIOS at runtime.
- Dynamically launching the OS and hypervisor in a secured code environment inaccessible from firmware. This technique also helps verify that the operating system and its virtual environment are running directly on Intel hardware, as opposed to malware that is spoofing the hardware.
- Providing operating system visibility into the BIOS- and firmware-protection methods used at boot time.

A strong security foundation is required to keep the rest of the stack more secure. Intel® Hardware Shield helps provide a more solid security base for an organization's fleet of PCs, whether they are found inside or outside the corporate firewall, by helping protect machines from start-up to the launch of the operating system and during runtime.

Intel® Active Management Technology (Intel® AMT)

Preventing and responding to attacks has grown more complicated in today's distributed workforce, with so many company devices found in remote locations outside the corporate firewall. Addressing firmware vulnerabilities remotely is a case in point. A remote administrator typically needs to connect to a device's OS to interact with that device and apply a software patch. However, some firmware patches are applied through applications that run even before the OS boots, and others might require IT technicians to interact

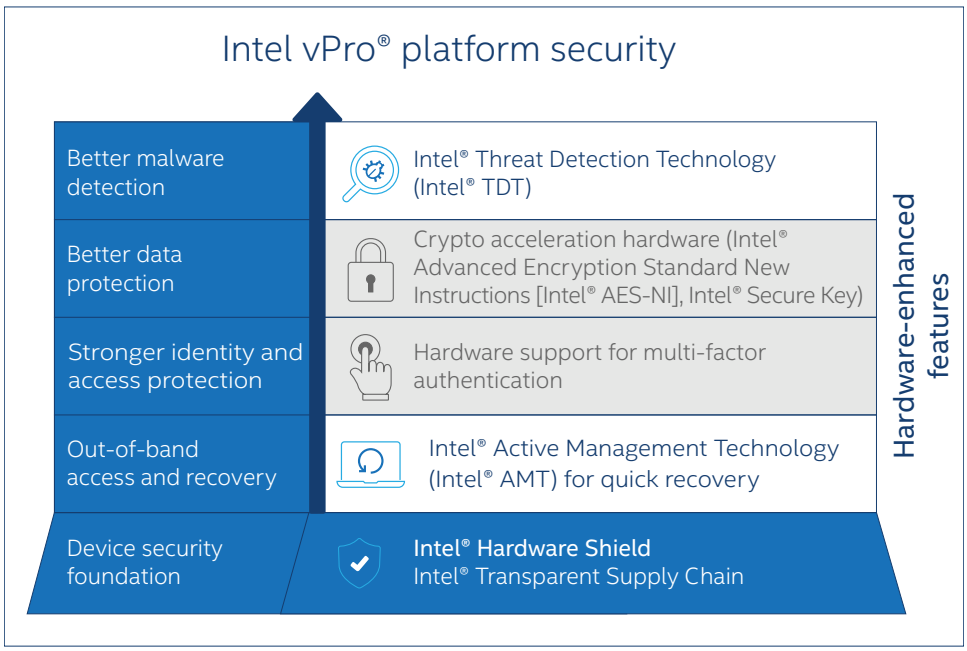

Figure 2. The Intel vPro® platform provides a hardware foundation for an end-to-end security strategy

physically with the device firmware below the OS. And if a device is eventually compromised, your organization might cede control of that device to a malicious actor, who can then steal or delete valuable data, or even demand a ransom to return the device. From a remote location, it's not always feasible to physically access the device quickly to power it off before damage is done.

The Intel vPro® platform provides a way both to remotely patch low-level software and to gain back control of devices from hackers through a feature called Intel® Active Management Technology (Intel® AMT). Intel® AMT, together with the Intel® Endpoint Management Assistant (Intel® EMA) software-management tool, provides a persistent out-of-band connection to devices below the operating system, delivering full keyboard, video, and mouse (KVM) functionality, along with the ability to boot more securely to a safe environment stored on a remote server. Intel® AMT provides CISOs the peace of mind that they can better keep their devices safe, in addition to helping ensure that, whether in-band or out-of-band via the cloud, they can more safely regain control of systems that are compromised or frozen.

Intel® Threat Detection Technology (Intel® TDT)

Modern exploits use many techniques to escape detection, a fact that creates an enormous headache for CISOs and other security officers who need to protect their organizations' assets. One such technique is for malware to reside in (and change) system memory, thus evading signature-based disk scanning techniques. The Intel vPro® platform helps address gaps in traditional anti-malware protection through Intel® Threat Detection Technology (Intel® TDT).

Intel® TDT is a suite of hardware-assisted technologies that security providers can use to augment their existing anti-malware solutions for detecting advanced cyber threats. It is offered as a software development kit (SDK) and as a reference solution to partner security providers.

Intel® TDT offers the following classes of capabilities:

- **Silicon acceleration** for specific security workloads. Accelerated Memory Scanning (AMS) enables memory scanning for malware to be offloaded to the onboard Intel graphics engine. This method helps improve memory-scanning efficiency while lowering performance overhead, and it also ultimately helps expand detection coverage of malware hiding in system memory. To build upon its existing benefits, the feature set of Intel® TDT will be expanded in the near future to enable this offloading capability for several other security-related functions.
- **Exploit detection** with targeted detection is another powerful feature of Intel® TDT that combines artificial intelligence (AI) with hardware telemetry unique to Intel as a way to help profile exploits and detect their behavior. This capability adds a highly effective, low-overhead tool to the arsenal of security providers without requiring intrusive scanning techniques or signature databases, leading to improved malware detection. This feature is especially useful against threats that do not have a signature to detect, such as malware hiding from disk scanners and zero-day attacks.

Built for Business: Intel vPro® Platform Gives PCs a More Secure Foundation

Intel is aware of the threats your organization faces every day, and it will continue to develop new technologies to help keep your devices secure. Endpoint security begins in the hardware, and the Intel vPro® platform helps create a solid foundation that can deliver end-to-end security now and in the future.

For more information about the security features of the Intel vPro® platform, contact an Intel sales representative or visit the following links:

- intel.com/vpro
- intel.com/hardwareshield
- intel.com/amt

[1] WatchGuard. "WatchGuard's Threat Lab Analyzes the Latest Malware and Internet Attacks." watchguard.com/wgrd-resource-center/security-report-q1-2019.

[2] Dark Reading. "Malware Variety Grew by 13.7% in 2019." December 2019. darkreading.com/threat-intelligence/malware-variety-grew-by-137--in-2019/d/d-id/1336611.

[3] National Institute of Standards and Technology (NIST). National Vulnerability Database. https://nvd.nist.gov/vuln/search/results?form_type=Basic&results_type=overview&query=firmware+&search_type=all.

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software, or service activation. Performance varies depending on system configuration. **No product or component can be absolutely secure.** Check with your system manufacturer or retailer or learn more at intel.com.

Intel does not control or audit third-party data. You should review this content, consult other sources, and confirm whether referenced data are accurate.

Intel technologies may require enabled hardware, specific software, or services activation. Check with your system manufacturer or retailer.

Printed in USA 0120/MM/PRW/PDF Please Recycle 342345-001US