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.

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] Working with chief information security officers (CISOs) and others responsible for defending corporate and government networks, Intel demonstrates the limits of perimeter security to introduce the "zero-trust" security concept.

For example, public-private partnerships use public clouds to drive API-enabled efficiencies and improved effectiveness across government agencies around the world. But these reforms cannot use the traditional perimeter-based model of defense. Instead, a tighter, zero-trust strategy assumes no single entity is secure indefinitely. In this approach to security, the entire stack must be monitored continuously, protected from top to bottom and from cloud to endpoint.

As organizations witness a rise in sophisticated attacks, the Intel vPro® platform offers a zero-trust response to emerging threats through a proactive, hardware-based security strategy that helps protect, detect and recover your systems.

Enhanced protection comes through Intel® Hardware Shield, with features for below the operating system security, app and data protection, and advanced threat detection. If a system is compromised, Intel® Active Management Technology (Intel® AMT) allows your IT department to recover it remotely, and for greater supply-chain visibility, Intel® Transparent Supply Chain provides the ability to trace the authenticity of system components.

The Intel vPro platform is built for business, with business-class performance and experiences, a built-in, more secure foundation, modern manageability for IT, and reliable, stable platforms.

A Zero-trust Approach to Security Must be Rooted in Hardware

This new, holistic view of enterprise security 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. 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 to secretly hijack systems as devices are starting, while remaining hidden to traditional software-based anti-malware applications, which typically cannot see beyond the scope of the operating system.

Intel vPro Platform: Endpoints for a More Secure IT Environment

The Intel vPro platform helps enable an enterprise security strategy built on hardware, designed to protect before an attack occurs, detect attacks with minimal impact to the user experience and recover quickly in the event of a breach. As shown in Figure 1, the Intel vPro platform with Intel Hardware Shield, Intel AMT and Intel Transparent Supply Chain helps CISO teams meet their highest-priority security goals:

- Improving data protection against theft and tampering
- Improving the efficacy of threat detection

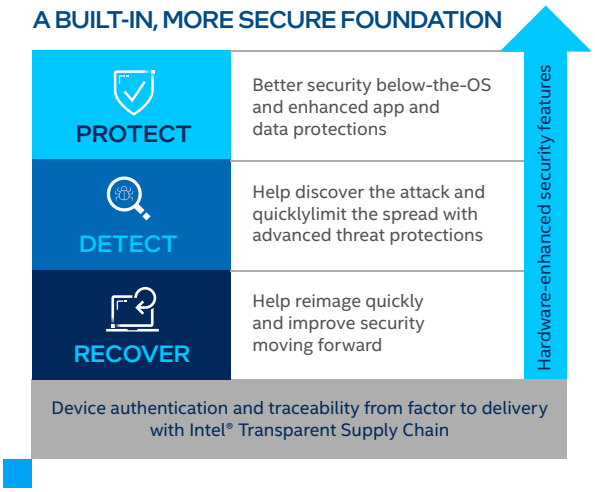

Figure 1. The Intel vPro platform provides a hardware foundation for an end-to-end security strategy

Below-the-OS Security with Intel Hardware Shield

Modern cyber threats often target devices at levels below-the-OS, where they can do damage and cover their tracks beyond the visibility and supervision of anti-malware applications. The Intel vPro platform addresses these threats through the below-the-OS security features of Intel Hardware Shield, extending 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 anti-malware solutions.

Intel Hardware Shield provides built-in security features to help protect against firmware attacks by:

- Providing OS visibility into the BIOS and firmware-protection methods used at boot time
- Locking down system-critical resources to help prevent malicious software injection
- Helping to identify unauthorized changes to hardware and firmware
- Reducing the negative consequence of firmware-based attacks
- Helping to prevent malicious code injection with Unified Extensible Firmware Interface (UEFI) protection and visibility

Help Protect Endpoint Applications and Data with Intel Hardware Shield

Another set of Intel Hardware Shield features uses hardware accelerated virtualization and encryption to help protect applications and data without adversely impacting user productivity. For example, virtual machines (VMs) can provide complete isolation from the PC OS and other VMs for strong security boundaries. Virtualization also can help computers recover faster—for virtualized workloads that are compromised, independently isolated workspaces can help reduce the time and cost to resolve matters without impacting other workloads.

Intel Hardware Shield complements accelerated virtualization with accelerated encryption—protecting data requires hardware-based security capabilities at every layer, including data and system memory encryption.

Better Detection of Advanced Cyber Threats with Intel Hardware Shield

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. Intel Hardware Shield helps address gaps in traditional anti-malware protection with features for advanced threat detection.

The advanced threat detection capabilities of Intel Hardware Shield consist of a suite of hardware-assisted technologies that security providers can use to augment their existing anti-malware solutions for detecting advanced cyber threats. This capability is offered as a software development kit (SDK) and as a reference solution to partner security providers.

Advanced threat detection is achieved with minimal impact to user experience and productivity through:

- **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 improves memory-scanning efficiency while lowering performance overhead, and it also ultimately expands detection coverage for malware hiding in system memory. To build upon its existing benefits, the threat-detection feature set will be expanded in the near future to enable this offloading capability for several other security-related functions.
- **Targeted exploit detection** with targeted detection, which combines artificial intelligence (AI) with hardware telemetry unique to Intel as a way to 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.

- **Memory malware protections** against jump/call-oriented programming (JOP/COP) and return-oriented programming (ROP) attack methods which comprise over half of ZDI-disclosed vulnerabilities. Now with 11th Gen Intel Core vPro processors, our Intel engineers invented ground-breaking technology to help shut down an entire class of attacks that long evaded software only solutions.[4]

Help Protect Against Control-flow Hijacking Attacks

Control-flow hijacking is a rapidly growing class of malware that attacks system memory, targeting operating systems, browsers, readers and many other applications. These code re-use attacks can be particularly hard to detect or prevent because the attacker hijacks existing code running from executable memory to change program behavior.

Intel developed Intel® Control-flow Enforcement Technology (Intel® CET), included in Intel Hardware Shield, to deliver effective, hardware-integrated protection with minimal impact on the user-experience.

Software developers like Microsoft use Intel CET to help stop code re-use threats such as Return Oriented Programming and Jump/Call Oriented Programming. Intel worked closely with Microsoft to enable Windows 10 Enterprise and developer tools, so applications and the industry at large can offer better protection against control-flow hijacking threats.

Intel CET offers software developers two key capabilities to help defend against control-flow hijacking malware: indirect branch tracking and shadow stack. Indirect branch tracking delivers indirect branch protection to defend against jump/call-oriented programming (JOP/COP) attack methods. Shadow stack delivers return address protection to help defend against ROP attack methods where attackers use the RET (return) instruction to stitch together a malicious code flow that was not programmer-intended.

Remote Recovery in the Event of a Breach with Intel AMT

Preventing and responding to attacks has grown more complicated with today's distributed workforce that has so many company devices 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 can be corrupted by bad actors to steal or delete valuable data, or even demand a ransom to return the device to operation. From a remote location, it's not always feasible to physically access the device quickly and power it off before damage is done.

The Intel vPro platform provides a remote way to keep devices patched and up-to-date, to patch low-level software, and to regain control of devices from hackers through 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-OS, 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 safely regain control of systems that are compromised or frozen.

Provide Component Traceability with Intel® Transparent Supply Chain

The cyber landscape extends beyond just network attacks. There is a growing concern about supply-chain and channel security. Supply chain practices start with trusted sources, but today's processes provide limited transparency and traceability into where, with what, and how PC systems are manufactured.

Intel Transparent Supply Chain is a set of policies and procedures meant to trace the authenticity of system components. It includes a certificate-based tool designed to trace system components from the point of manufacture to help identify counterfeit PC components with output that is compliant with the Trusted Computing Group Platform Certificate 1.1 Specification.

For example, before a PC leaves the factory, an OEM can take a digital fingerprint of the PC and store it in the cloud. When the PC arrives at the customer, the customer takes another digital fingerprint and compares that against the original, which is protected by digital certificates. If these fingerprints don't match, the customer can immediately quarantine the PC and begin an investigation with the OEM.

Intel Transparent Supply Chain also provides increased transparency for customers. It enables component-level traceability for select Intel commercial and Intel vPro platform–based systems that helps to mitigate the risk of counterfeit electronic parts. Customers have access to data reports that contain information on various PC components, in addition to a verification tool that identifies certain system changes from the time of manufacturing to the time of first boot. This helps to boost customer confidence in the authenticity of their PC purchases.

In summary, Intel Transparent Supply Chain allows customers to:

- **Obtain visibility** into the details of their business PC fleets
- **Trace and verify the provenance** of systems and components
- **Improve quality assurance (QA)** for business PCs and servers

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

Intel continues to develop new technologies to help keep your devices secure and aligned with modern IT strategies. Choosing the right device, keeping it patched, up-to-date and layering services are critical to helping protect organizations from cyber-attacks. 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.

Learn More

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.

[4] Intel® Control-flow Enforcement Technology (Intel® CET) is designed to help protect against jump/call-oriented programming (JOP/COP) attack methods and return-oriented programming (ROP) attack methods, malware known as memory safety issues and which comprise over half of ZDI-disclosed vulnerabilities. Visit www.intel.com/11thgenvpro for details. No product or component can be absolutely secure. Results may vary.

All information provided here is subject to change without notice. Contact your Intel representative to obtain the latest Intel product specifications and roadmaps.
Performance varies by use, configuration and other factors. Learn more at www.Intel.com/PerformanceIndex.
Performance results are based on testing as of dates shown in configurations and may not reflect all publicly available updates. See Performance Index for configuration details.
Intel provides these materials as-is, with no express or implied warranties.
No product or component can be absolutely secure.
Your costs and results may vary.

0521/MZ/DCC/PDF