Securing the 21st century workspace

Strengthen your data, systems, and business with the enhanced security features of Windows® 10 and Intel® Core™ vPro® processor platform with Intel® Hardware Shield

September 2020

"In an era of cyber intrusions, security is an essential priority for every business. Strengthen your security posture by investing and implementing the security features of Windows 10 and the Intel vPro® platform with Intel® Hardware Shield."

Sumera Baker,
MPS—Strategic Cybersecurity and Information Management.
Adjunct Professor
Georgetown University—Cyber Risk Management

Introduction

You own Windows 10, you implement the updates as they are released and you refresh your devices every three to four years. However, are you ensuring you have taken the necessary steps to secure your workplace systems? What is the added advantage of using Windows 10 with the latest Intel vPro® platform-based devices?

The simple answer is an enhanced security posture. We all know that security is not absolute—even with an unlimited budget there is no guarantee that an organization won't suffer a breach. Hackers are getting smarter, and advanced persistent threat (APT) hackers with state affiliations have the resources and time to breach any network or organization.

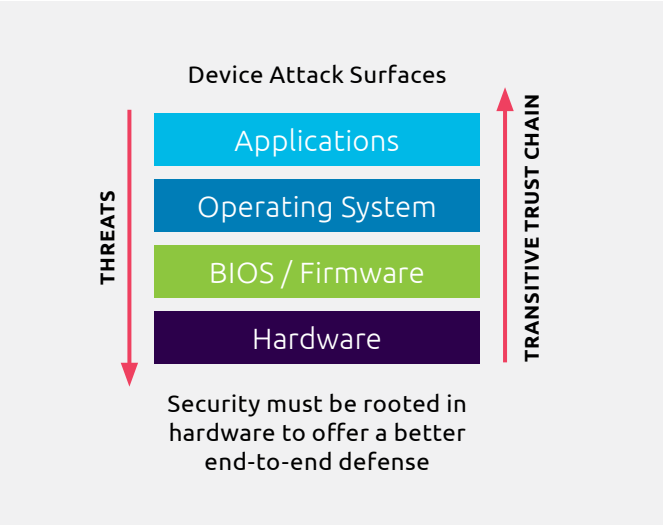

Figure 1: Why hardware-based security?

The nature of security needs to evolve as today's hackers continue looking for ways to take advantage of attack surfaces to create zero-day exploits. Current tools can help protect against attacks that happen at the software application, operating system (OS), and virtual machine (VM) level. Today we are beginning to see threats increasing in sophistication as hackers continue to evolve their techniques and move towards the hardware infrastructure, making the compromised components more difficult to detect. A compromised

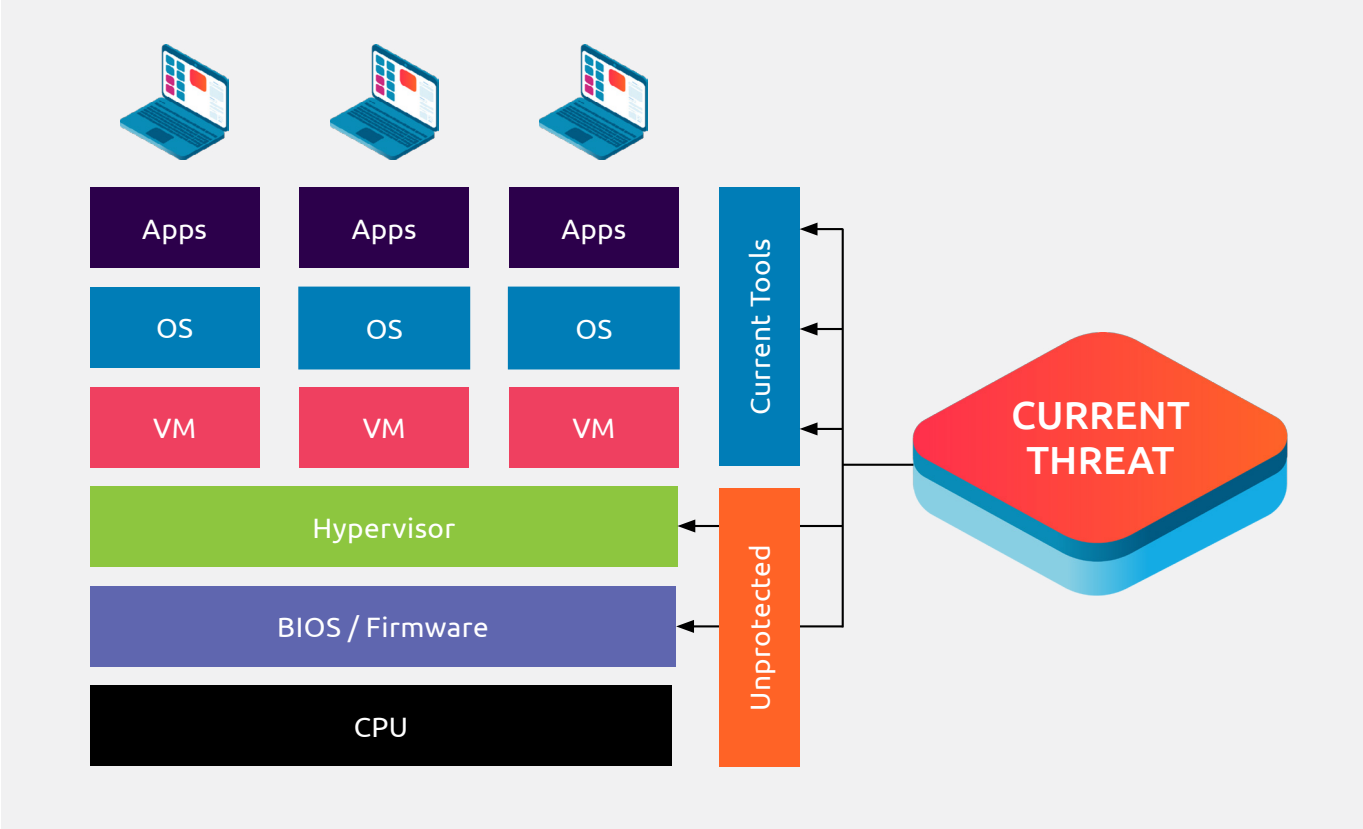

Figure 2: Security is needed at all layers.

PC can offer up access identity, encryption keys, and passwords, in addition to sensitive data.

These types of attacks have unfortunately become part of our daily reality and our technology, and our strategies must get smarter as well. Therefore, businesses need to invest in better technology with the hardware capabilities that help ensure security from the core to the application layer. This way security is present not only in applications, security tools, and perimeter firewalls, but embedded in the hardware and OS.

What we will cover?

We must acknowledge that no security feature or set of features provide absolute security. It is essential that you implement security features to minimize the risk to your business.

Microsoft Windows 10 continues to evolve as threats are detected and mitigated in the OS updates. Since the Windows 10 initial release, Microsoft has consistently worked with security professionals around the world to detect, remediate, and enhance the Windows 10 security profile.

We will also cover the components of the security features of the Intel vPro platform with Intel® Hardware Shield. Intel Hardware Shield comprises Intel's out-of-the-box hardware security features, built into 10th Gen and future Intel Core vPro-based business-class systems to help protect the PC against attacks at the foundational level. Intel Hardware Shield provides features for below-the-OS security, app and data protection, and advanced threat protection.

Security technologies: Microsoft

Windows 10 has introduced, improved, and enhanced essential security features, and with each semi-annual channel of Windows 10, security remains on the forefront of its design. Identity and credential protection, application protection, and storage protection all protect against existing and emerging threats. Many of these technologies rely on hardware, such as Trusted Platform Module (TPM) 2.0, Unified Extensible Firmware interface (UEFI) BIOS, Secure Boot, and the CPU, like Intel Core vPro processors.

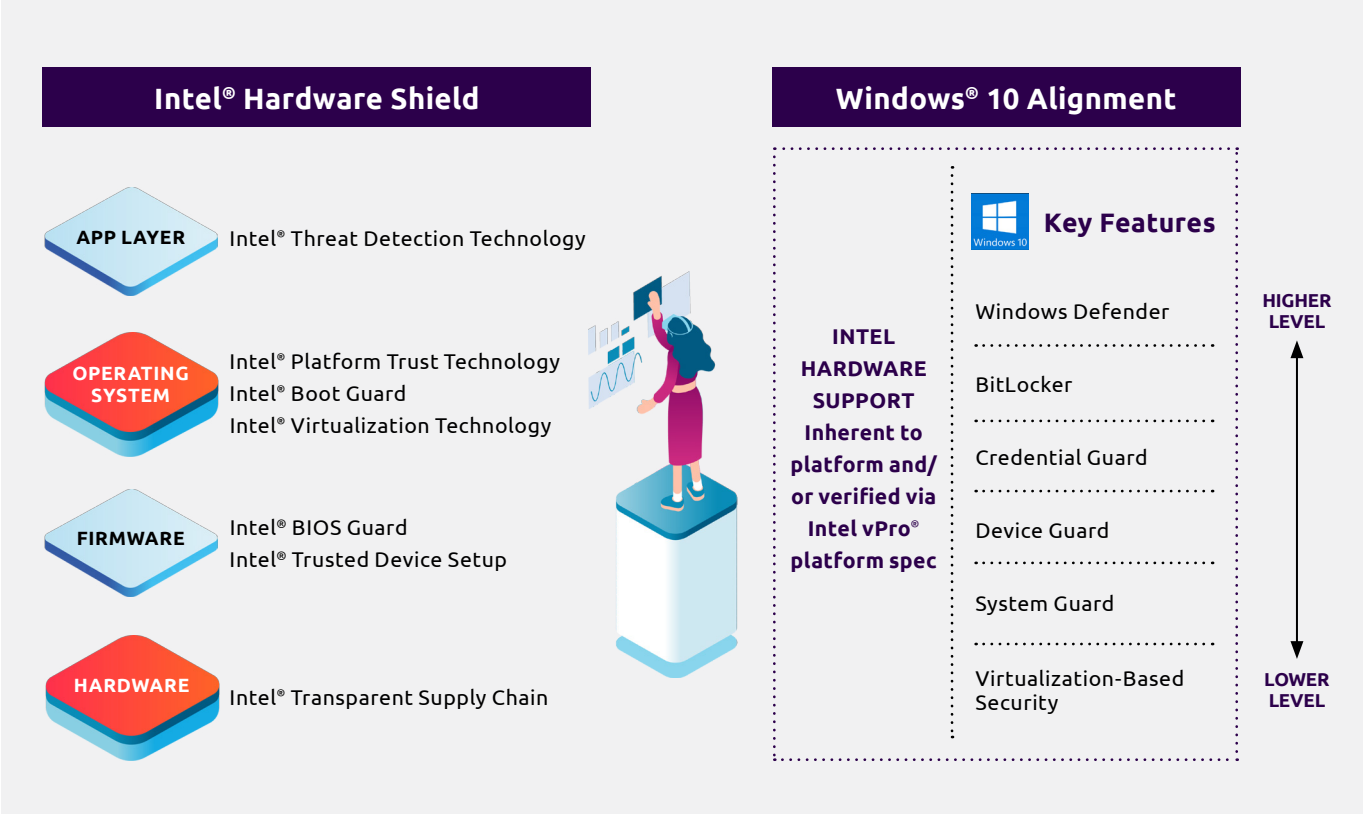

Figure 3: Windows 10 security on Intel.

Microsoft 365 Defender

Microsoft 365 Defender delivers a comprehensive, ongoing, and real-time protection against software threats like viruses, malware, and spyware, across email, apps, the cloud, and the web. Microsoft 365 Defender is always on and eliminates the need for any third-party antivirus solutions.

Microsoft 365 Defender provides accelerated memory scanning with minimal impact to user experience by utilizing Intel® Threat Detection Technology (Intel® TDT), part of Intel Hardware Shield.

Microsoft Defender for Endpoint

Microsoft Defender for Endpoint (Formerly Microsoft Defender Advanced Threat Protection) uses a combination of technologies built into Windows 10 and Microsoft's robust cloud service. These technologies include:

- **Endpoint behavioral sensors:** Embedded in Windows 10, these sensors collect and process behavioral signals from the OS and send this data to your private, isolated cloud instance of Microsoft Defender for Endpoint
- **Cloud security analytics:** Leveraging big data, machine learning, and unique Microsoft optics across the Windows ecosystem, enterprise cloud products (such as Office 365), online assets, and behavioral signals are translated into insights, detections, and recommended responses to advanced threats
- **Threat intelligence:** Generated by Microsoft hunters, security teams, and augmented by threat intelligence provided by partners, threat intelligence enables Microsoft Defender for Endpoint to identify attacker tools, techniques, and procedures, and generate alerts when these are observed in collected sensor data

Microsoft Defender for Endpoint includes threat and vulnerability management, attack surface reduction, next- generation protection, endpoint detection and response, and automated investigation and remediation. Additional licenses may be required for Microsoft Defender for Endpoint. Learn more here.

Figure 4: Microsoft Defender for Endpoint.

Windows Defender Credential Guard

Windows Defender Credential Guard was introduced with Windows 10, version 1607 and Windows Server 2016 to isolate secrets so that only privileged system software can access them, preventing credential theft attacks. Credential Guard, which utilizes Intel Hardware Shield, can be enabled via Intune, Group Policy, editing the Windows Registry, or using the Device Guard and Credential Guard hardware readiness tool.

Windows Defender Device Guard

Windows 10 includes a set of hardware and OS technologies that, when configured together, allow enterprises to "lock down" Windows 10 systems so they operate with many of the properties of mobile devices. In this configuration, specific technologies work together to restrict devices to only run authorized apps by using a feature called configurable code integrity, while simultaneously hardening the OS against kernel memory attacks through virtualization-based protection of code integrity (more specifically, HVCI). Windows Defender Device Guard is enabled on devices with Intel Hardware Shield.

Windows Defender Application Guard

Windows Defender Application Guard is designed to help prevent old and newly emerging attacks to keep employees productive. Using a unique hardware isolation approach, the goal is to destroy the playbook that attackers use by making current attack methods obsolete. Designed for Windows 10 and Microsoft Edge, Application Guard helps to isolate enterprise-defined untrusted sites, protecting your company while your employees browse the Internet. In Windows 10, version 2004, Application Guard also protects Microsoft 365 Apps (Office 365 ProPlus).

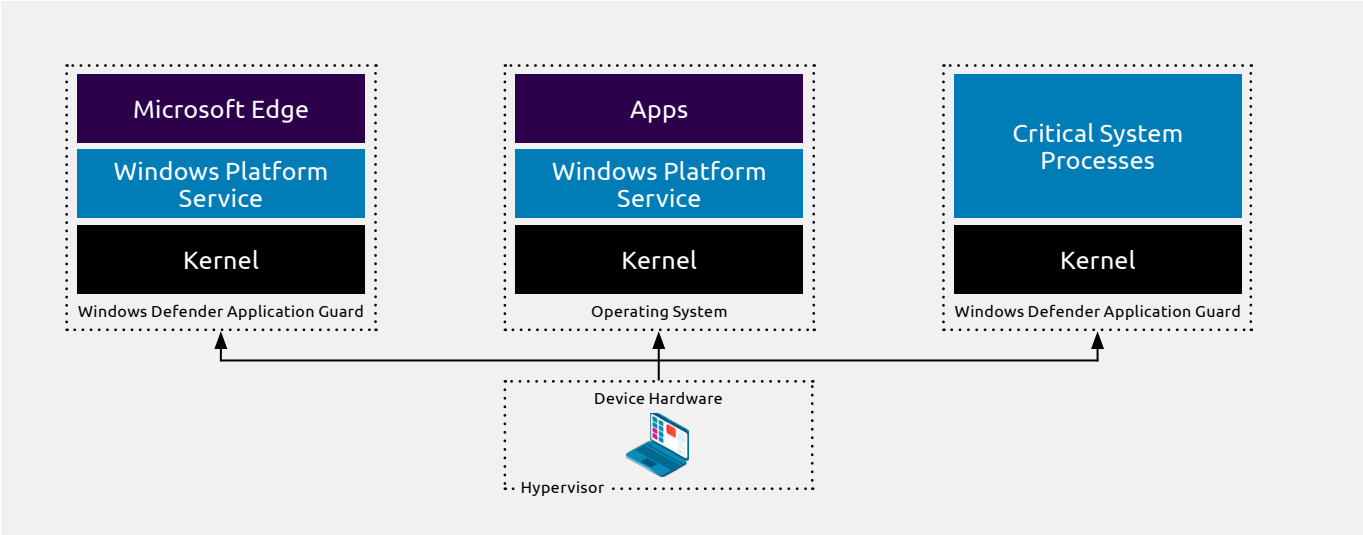

Figure 5: Windows Defender Application Guard.

Passwordless login to Windows

You can adopt modern authentication technologies to provide ease of use without the risk of using passwords. Some of the built-in passwordless technologies include Windows Hello, Windows Hello for Business, Microsoft Authenticator, FIDO2 security keys, and the broad set of passwordless authenticators that work with the new Microsoft Edge browser. Windows Hello and Windows Hello for Business require devices with biometric sensors, such as those built on Intel® processors and technologies.

Microsoft BitLocker

Introduced with Windows Vista, and improved upon in Windows 7 and Windows 10, Microsoft BitLocker is a full disk encryption technology. With Microsoft Bitlocker, you can ensure a disk is encrypted from preboot through login, and beyond. A data disk removed from one computer cannot be placed into another computer without a PIN or key to unlock the drive. And now, with Microsoft Endpoint Manager, you can fully manage Microsoft BitLocker, from requiring encryption, to pausing encryption, to removing encryption, and allowing users to retrieve their own recovery keys, if they happen to be locked out of their device.

Azure Information Protection

Azure Information Protection allows you to control secure email, documents, and sensitive data that you share outside of your organization. From easy classification to embedded labels and permissions, Azure Information Protection always offers data protection, no matter where the data is stored.

Windows Update for Business

Windows Update for Business enables IT administrators to keep all the Windows devices in their organization always up to date with the latest security defenses and Windows features. Devices can receive these updates whether they are connected to the corporate network or not, by connecting directly to the Windows Update service. Use Group Policy or Microsoft Intune to configure settings that control how and when Windows 10 devices are updated.

Microsoft Edge browser

Windows 10 has a built-in Edge browser, for securely browsing of the Internet, and the secure use of web apps. In recent versions of Windows 10, Microsoft also introduced the Edge browser built on Chromium. The Edge browser provides security features ranging from Application Guard, to InPrivate browsing, to tightening the reins on website certificate handling.

Windows UEFI Secure Boot

Another important security feature for Windows 10 is UEFI Secure Boot. It was created to enhance security in the preboot environment and allows only apps that are signed and trusted by administrators. This helps thwart efforts by some of the most dangerous hackers who attack computers by injecting low-level malware like rootkits during the PC boot process. The UEFI specification is an interface framework that provides firmware, OS, and hardware providers a defense against potential malware attacks. Without UEFI Secure Boot, malware developers can easily take advantage of several preboot attack points, including the system-embedded firmware itself, and the interval between firmware initiation and loading the OS. Windows UEFI Secure Boot is enabled by the Intel Boot Guard component of Intel Hardware Shield on Intel vPro-based platforms.

Windows Virtual Secure Mode (VSM)

Windows 10 Enterprise and Professional editions offer a capability called VSM that uses a PC's CPU virtualization to protect key aspects, including data and credentials (aka tokens) on the system's hard drive. The VSM prevents the hacker from obtaining

credentials and infiltrating the enterprise infrastructure. For virtualization to be enabled, the CPU must have hardware virtualization capability, such as that inside Intel Core vPro processor.

Microsoft Secured-core PC

Microsoft has partnered with leading PC manufacturers, like Intel, to create an industry standard Root of Trust, coupled with the security capabilities built into modern Intel Core vPro processors.

A Secured-core PC with Intel Hardware Shield is a modern Windows device that comes with the highest level of hardware, software, and identity protection features. The below-the-OS protection features of Intel Hardware Shield help minimize the risk of malicious code injection by locking down firmware when software is running to help prevent planted malware from compromising the OS.

Secured-core PCs with Intel Hardware Shield require a specific configuration to fully enable the highest level of protection against attack. Secured-core PCs with Intel Hardware Shield provide a hardware-isolated operating environment to help prevent advanced attacks on Windows from the firmware level.

Devices using Intel Hardware Shield, exclusive to the Intel vPro platform, provide protections against attacks at the firmware level as specified by the Microsoft Secured-core PC specification.

Security Technologies: Intel

Intel® Hardware Shield: security benefits of 10th Gen Intel® Core™ vPro®-based systems

Business-class devices based on the Intel vPro platform with Intel Hardware Shield provide hardware-enhanced security that enterprises demand, and meet and exceed the requirements of Microsoft Secured-core PCs.

New Windows 10 security features work with the hardware-based security capabilities of Intel Hardware Shield and make a compelling case for businesses to continually refresh and update their investments in Windows 10 and workplace hardware. It launched with 8th gen Intel Core vPro processors and is available on select SKUs. Intel Hardware Shield continues to evolve the hardware-based security features built into the Intel vPro platform. Devices with Intel Hardware Shield allow organizations to fully utilize security features included in Windows 10 and provide more support to address today's security issues and threats.

Intel Hardware Shield's below-the-OS security features:

Intel® Boot Guard and Intel® BIOS Guard
Intel Boot Guard and Intel BIOS Guard were previously part of Intel® Security Essentials and incorporated into every system. Now a part of Intel Hardware Shield,

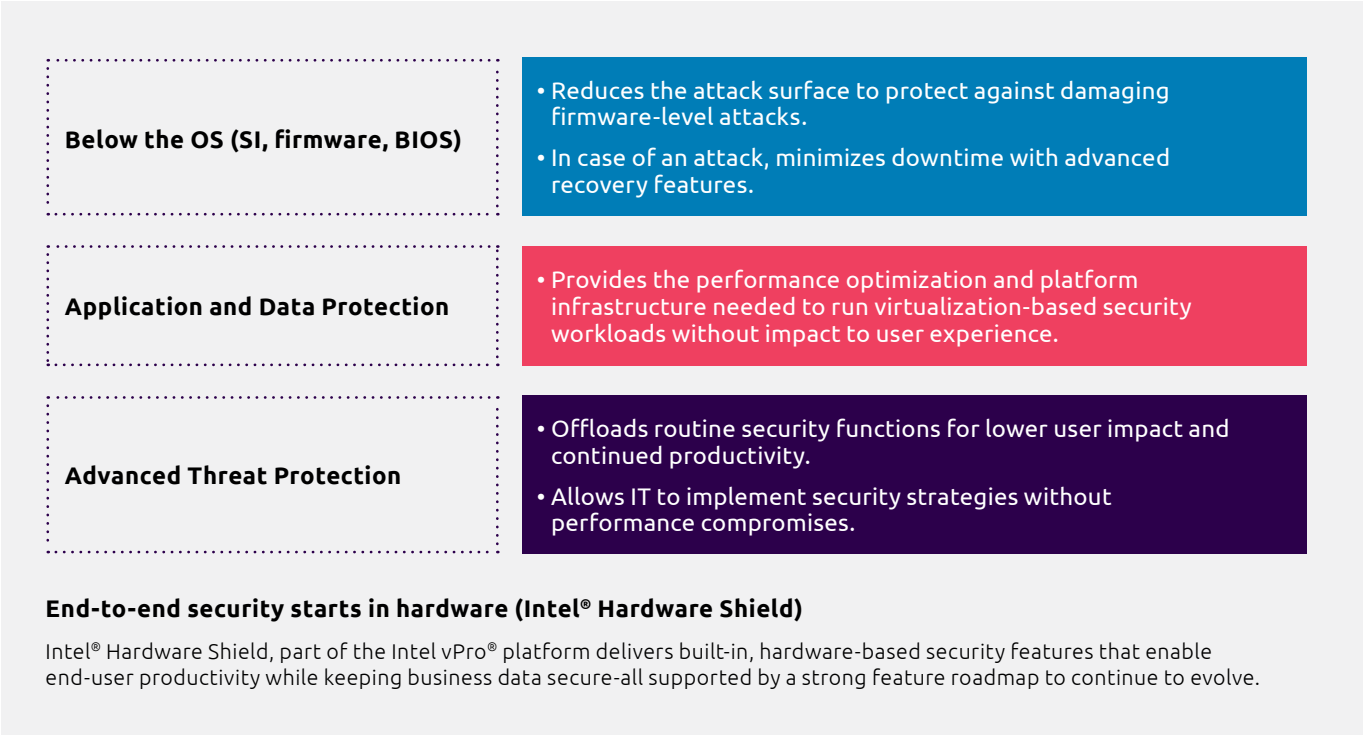

Figure 6: Intel® Hardware Shield.

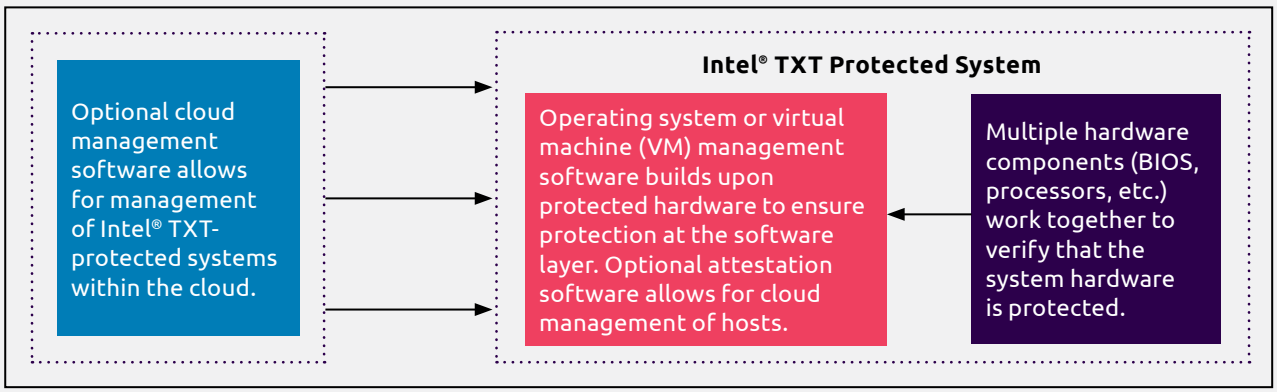

Figure 7: Intel® Trusted Execution Technology (Intel® TXT).

Intel Boot Guard provides hardware-based boot integrity protection and prevents unauthorized software and malware of boot blocks critical to a system's function, thus providing an added level of hardware-based platform security.

Intel BIOS Guard protects the BIOS flash from modification without platform manufacturer authorization, which helps defend the platform against low-level denial of service (DoS) attacks and restores the BIOS to a known good state after an attack. Intel BIOS Guard enables a hardware-based static root of trust for measurement and verification of boot integrity by checking hardware and system firmware for malware before the OS boots up for resilient hardware-based OS security.

Intel® Trusted Execution Technology (Intel® TXT)
Intel TXT simplifies the firmware integrity measurement process at startup to help remove the firmware's access to critical system resources. Intel TXT measures the platform components in the boot and launch environment, such as the BIOS, OS loader, and virtual machine managers (VMMs), to provide a trusted, tamper-resistant position to evaluate the integrity of the system components and enable assurance through secure comparison against expected measurements. Utilizing these comparisons during the boot and launch sequence, the system can block the launch of unrecognized software and enforce "known good" launch time configurations. Intel TXT can ensure Windows 10 is running on legitimate hardware, that has not been tampered with without your knowledge and prevent execution of unauthorized code should tampering be detected. This hardware-based solution provides the foundation on which trusted platform solutions can be built to protect against the software-based attacks that threaten system integrity, confidentiality, reliability, and availability.

Intel® Runtime BIOS Resilience
Intel Runtime BIOS Resilience (IRBR) uses the CPU to help 'lock' the page table in SMM/BIOS to reduce the risk of malicious software being injected into the BIOS. When IRBR is implemented with SMM/BIOS page table without access to the memory used by the OS, it reduces the risk that malware could use the BIOS/SMM to gain visibility into the OS, as the CPU has 'locked' the page table in the BIOS/SMM. IRBR also contributes Intel System Resources Defense by providing part of the mechanism enforcing memory-DRAM access.

Intel® System Security Report
Intel System Security Report provides unique and increased visibility on what system hardware and resources may be used or accessible by firmware SMI handlers. Intel System Security Report works with Intel TXT to provide this information in a trusted manner. Without this capability, the OS's hypervisor or Measured Launch Environment (MLE) does not have any visibility into what system hardware or resources may be accessible from firmware SMI handlers.

Intel® System Resources Defense
Intel System Resources Defense is a mechanism that can enforce policy on what type of system resources can be accessed by firmware SMI Handlers from within System Management Mode (SMM). When Intel System Resources Defense is implemented with policy that limits resource accesses to only things that BIOS/SMM needs, it helps to reduce the attack surface and improves platform security. Intel system resources covered by Intel System Resources Defense include memory - DRAM, memory - MMIO, CPU model specific registers (MSR), and IO ports. Platform Configuration Registers are NOT included. Intel System Resources Defense receives its enforcing memory-DRAM access enforcement mechanism from IRBR.

Intel Hardware Shield's application and data protection features:

Intel VT for IA-32, Intel® 64 and Intel® Architecture (Intel® VT-x)
Intel VT-x is a series of extensions for hardware virtualization that adds migration, priority, and memory handling capabilities to Intel-based hardware. Intel VT-x provides the hardware and software foundation to prevent unauthorized software from being installed on a system by virtualizing the hardware resources providing security to prevent malicious code from being injected above the OS.

Intel® Virtualization Technology (Intel® VT) for Directed I/O (Intel® VT-d)
Intel VT-d manages device and IO virtualization. Intel VT-d provides a separate engine that provides the ability to automatically map Direct Memory Access (DMA) from real devices to specific memory locations as well as direct interrupts directly to certain cores. This provides the ability to assign physical devices to VMs. Giving them direct access allows them to direct DMA to memory for that VM, and to direct interrupts to specific cores assigned to that VM. This takes the burden away from the hypervisor and provides good security and performance.

Intel® VT-d allows multiple OSs and applications to run in independent partitions on a single computer. Using virtualization capabilities, one physical computer system can function as multiple virtual systems. Intel VT improves the performance and robustness of today's VM solutions by adding hardware support for efficient VMs.

Intel VT-d helps the VMM better utilize hardware by improving application compatibility, and reliability, and providing additional levels of manageability, security, isolation, and I/O performance. By using the Intel VT-d hardware assistance built into Intel's chipsets, the VMM can achieve higher levels of performance, availability, and trust.

Mode-Based Execution Control (MBEC)
MBEC is an update to the Extended Page Tables (EPT) to provide an additional level of protection from malware attacks with control of execute permissions. MBEC can enable hypervisors to more reliably verify and enforce integrity of code accessing the kernel. With MBEC, the previous Execute Enable (X) bit is turned into Execute Userspace page (XU) and Execute Supervisor page (XS). The processor selects the mode based on the guest page permission. With proper software support, hypervisors can take advantage of this to ensure the integrity of kernel-level code. MBEC also protects the system from memory corruption attacks and provides protection from unauthorized access.

Intel Hardware Shield's advanced threat protection features:

Intel® Threat Detection Technology (Intel® TDT)
Intel TDT is a threat detection software development kit that allows Intel's partners in the security software industry to build solutions that help accelerate and offload some of the most CPU-demanding workloads to the GPU. Intel TDT is a suite of hardware-assisted technologies that can be incorporated into ISV security solutions, augmenting their existing capabilities to improve the detection of advanced cyber threats and exploits.

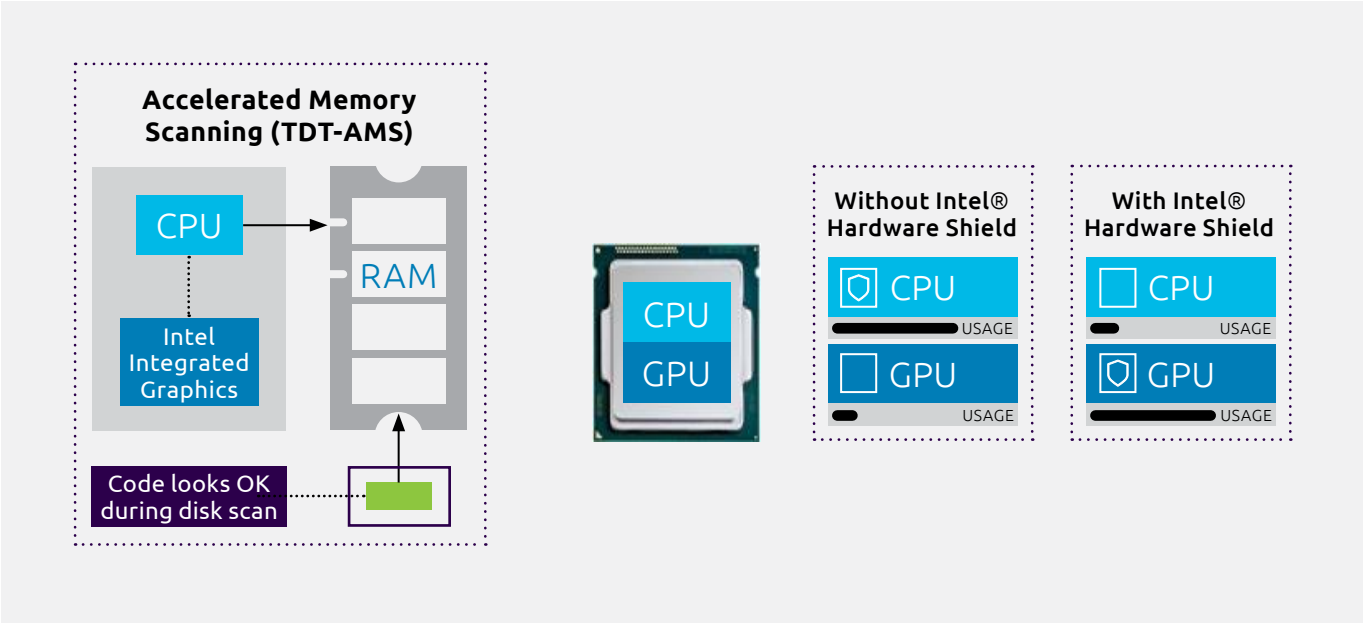

Figure 8: Intel® Threat Detection Technology (Intel® TDT).

The following capabilities of Intel TDT are currently offered:

- Silicon acceleration like accelerated memory scanning for security workloads
- Exploit detection using Advanced Platform Telemetry
- Silicon-Assisted Threat Detection - CPU telemetry coupled with ML heuristics to detect hard-to-isolate malware attacks amd improve ISV efficacy

Intel TDT Accelerated Memory Scanning (AMS)
Intel TDT AMS harnesses hardware telemetry and acceleration capabilities to help identify threats and detect anomalous activity that many modern exploits use to escape detection by offloading the memory scan to the integrated GPU—the onboard graphics engine. This method helps improve memory scanning efficiency while lowering performance overhead, and it also helps expand detection coverage of malware hiding in system memory. One such example is where malware attempts to reside in (and then change) system memory avoiding detection from signature-based disk scanning processes. Intel TDT AMS can help address the gaps that current traditional anti-malware protection solutions offer. AMS enables the ISV to do more frequent scans to improve the overall system security and uncover hard-to-detect file-less attacks to the memory layer.

Intel TDT Exploit Protection
Intel TDT offers exploit detection with targeted detection that combines artificial intelligence (AI) with hardware telemetry unique to Intel 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.

Intel Hardware Shield—a look ahead to security in future Intel vPro platform-based systems

As an Intel Alliance Partner and global systems integrator, Intel often gives us a look ahead to the future technology it is working on. The following security features are coming on 11th Gen Intel Core vPro-based systems.

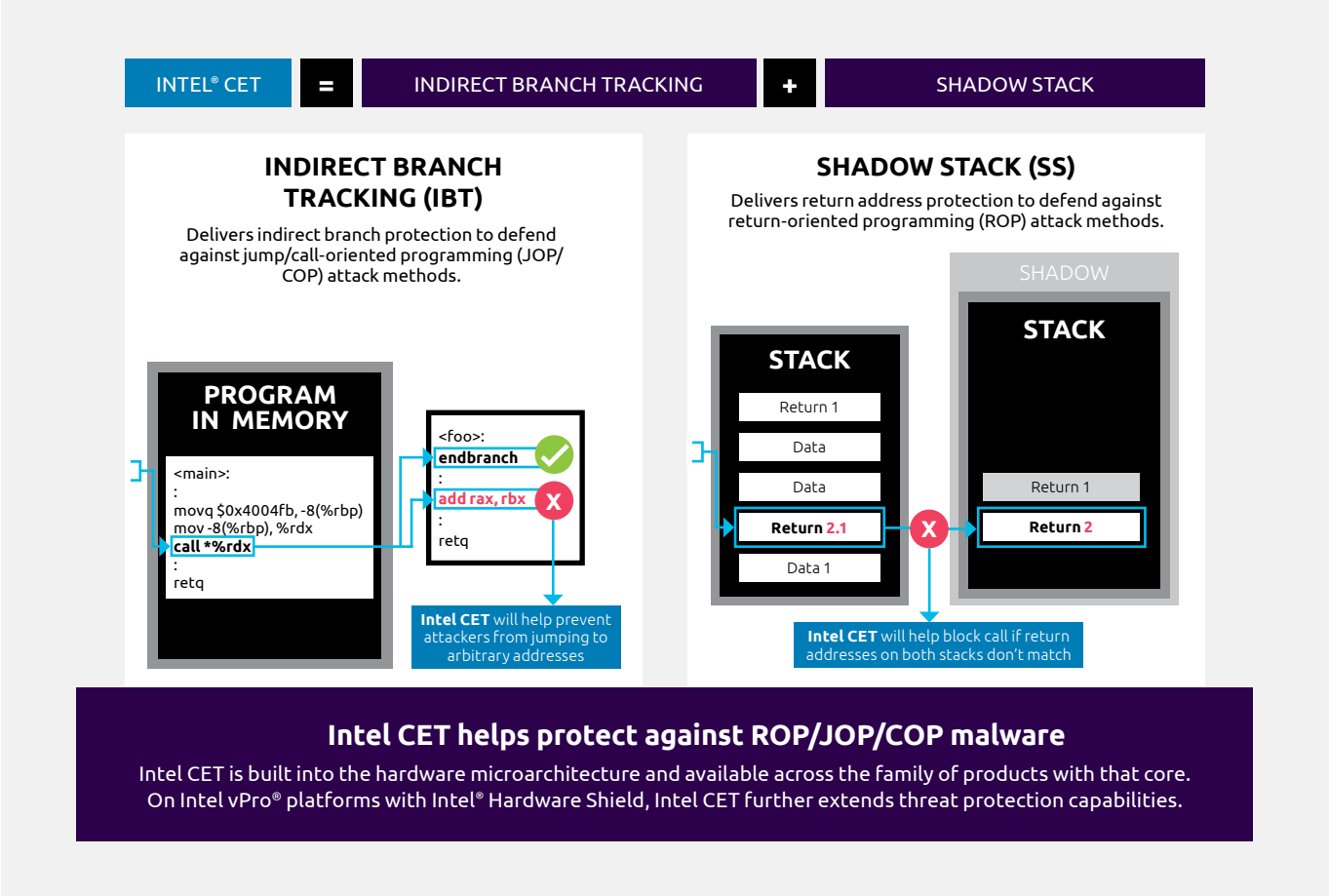

Figure 9: Intel® Control-flow Enforcement Technology (Intel® CET).

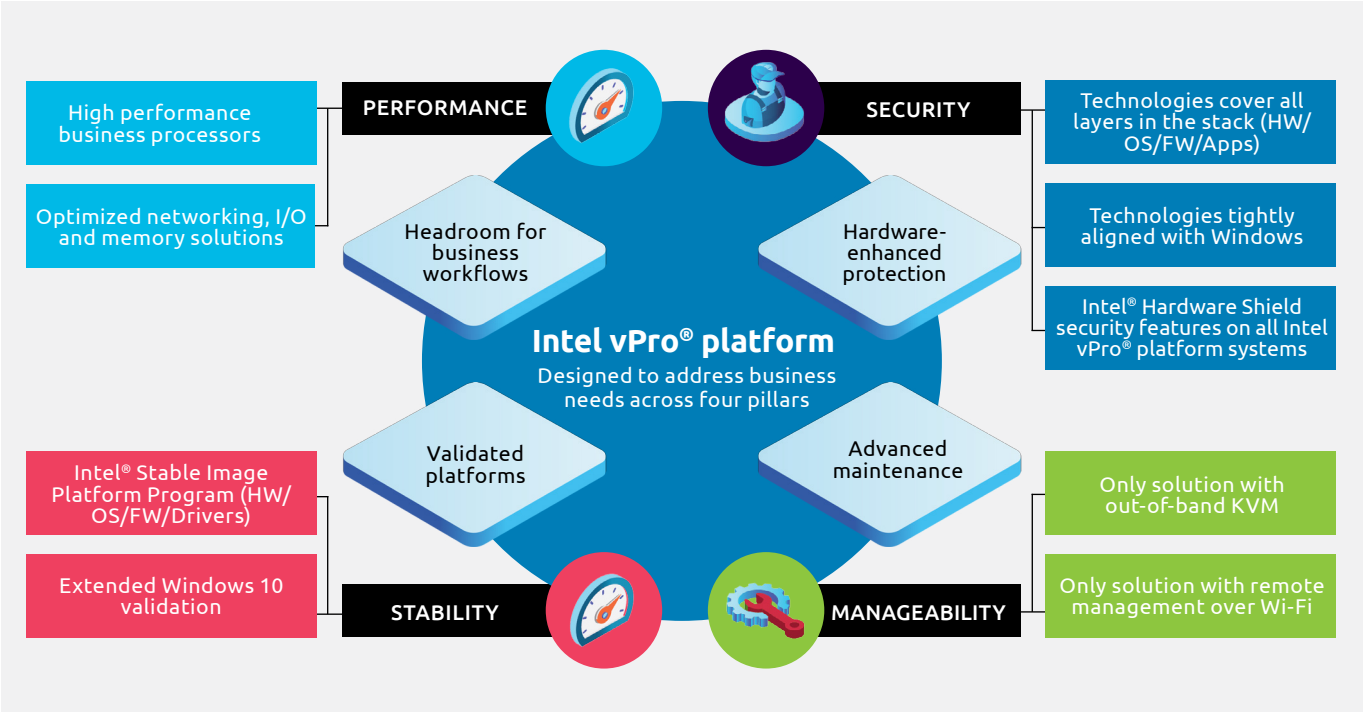

Figure 10: Intel vPro® Technology.

Intel® Control-flow Enforcement Technology (Intel® CET)
Intel has been working closely with Microsoft to prepare Windows 10 and developer tools so applications and the industry at large can offer better protection against control-flow hijacking threats. Intel CET is designed to protect against the misuse of legitimate code through control-flow hijacking attacks–widely used techniques in large classes of malware. 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 return-oriented programming (ROP) attack methods.

These types of attack methods are part of a class of malware referred to as memory safety issues and include tactics such as the corruption of stack buffer overflow and use-after-free. For technical details, see A Technical Look at Intel's Control-Flow Enforcement Technology.

Microsoft's upcoming support for Intel CET in Windows 10 is called Hardware-enforced Stack Protection. This new hardware-enforced stack protection feature only works on chipsets with Intel CET instructions. It relies on a new CPU architecture that is compliant with Intel CET specifications.

The significance of Intel CET is that it is built into the microarchitecture and available across the family of products with that core. While devices based on the Intel vPro platform with Intel Hardware Shield already meet and exceed the security requirements for Secured-core PCs, Intel plans to further extend CET advanced threat protection capabilities.

Beyond security implementation

Intel® Active Management Technology (Intel® AMT)
Intel Core vPro-based systems include Intel® AMT, which allows IT or managed service providers to better discover, repair, and protect their networked computing assets. With Intel AMT, you can manage and repair PC assets, workstations, and entry servers, utilizing the same infrastructure and tools across platforms for management consistency. For embedded developers, this means that devices can be diagnosed and repaired remotely, ultimately lowering IT support costs. Intel AMT lets you manage and monitor your investment and offers peace of mind knowing you can check and manage the status of the Intel Hardware Shield security features. Intel AMT offers additional support to supplement your security practices with features like Intel Remote Secure Erase and Out of Band management. Intel AMT and Intel Hardware Shield are features of the Intel vPro platorm and are available on mobile, desktop, and workstation devices.

Conclusion

Endpoint security decisions start at the PC. To fully protect your organization, you need to protect your PC endpoints. It is imperative that organizations continue to update and patch their Windows 10 systems and evolve from traditional antivirus protections. But that's only half the story. In addition to software-based attacks, hackers have begun targeting firmware,

below what the OS can see and monitor, which can serve as a conduit to system memory and the virtualization-based security environment. Enterprise businesses need fully integrated software and hardware solutions, which is where Intel Hardware Shield comes in.

Intel Hardware Shield is the cornerstone of a more secure PC fleet, delivering protections against firmware attacks for increased platform protection. As part of the Intel vPro platform, Intel Hardware Shield helps ensure that the OS runs on legitimate hardware. Intel Hardware Shield also offers application and data protection through virtualization-based security features and advanced threat protection features in partnership with key security ISVs and partners like Microsoft. With the hardware-to-software security visibility Intel Hardware Shield provides, the OS can enforce a more complete security policy.

As technology advances, so do the skills of cyber intruders. It is prudent to take advantage of safer and more efficient technology, and for that we need to adapt and also change human behavior. Business Reimagined's Dave Coplin says: "If you can't help people change, technology changing all around them won't make the slightest difference."[1]

Every day there is a new test on the security of your infrastructure, as hackers look to take advantage of zero-day exploits, and work down the hardware stack to compromise systems in harder to detect ways. To combat these threats, technology experts must get smarter as well, and need to expand their focus from morethan just perimeter security to include endpoint security in their overall strategy.

Maintaining your Windows 10 systems and refreshing your PC fleet with the latest Intel vPro processor-based devices, as well as helping your key development and security resources learn to effectively apply, manage and monitor these capabilities, increases security to protect your valuable systems, data, and, ultimately, your business.

How to get started

Sogeti can enhance how you manage your approach to cybersecurity, aligned with specific business strategies and risk profiles to help protect your business. We can offer endpoint security configuration options to provide hardening of your systems, and systems monitoring and rapid incident response to prevent any attacks from spreading. Each service is tailored to the unique needs of each client, from the services themselves, to our flexible deployment models. Consult with Sogeti to create a monitoring and management solution to monitor, detect, respond and protect your valuable endpoints with a solution and security strategy aligned to your business priorities.

Get in touch

Contact our experts and learn more at: www.sogeti.com/services/cybersecurity/ and www.capgemini.com/service/cybersecurity-services/

About Sogeti

Sogeti is a leading provider of technology and engineering services. Sogeti delivers solutions that enable digital transformation and offers cutting-edge expertise in Cloud, Cybersecurity, Digital Manufacturing, Digital Assurance & Testing, and emerging technologies. Sogeti combines agility and speed of implementation with strong technology supplier partnerships, world class methodologies and its global delivery model, Rightshore®. Sogeti brings together more than 25,000 professionals in 15 countries, based in over 100 locations in Europe, USA and India. Sogeti is a wholly-owned subsidiary of Capgemini SE, listed on the Paris Stock Exchange.

Capgemini is a global leader in consulting, digital transformation, technology and engineering services. The Group is at the forefront of innovation to address the entire breadth of clients' opportunities in the evolving world of cloud, digital and platforms. Building on its strong 50-year+ heritage and deep industry-specific expertise, Capgemini enables organizations to realize their business ambitions through an array of services from strategy to operations. Capgemini is driven by the conviction that the business value of technology comes from and through people. Today, it is a multicultural company of 270,000 team members in almost 50 countries. With Altran, the Group reported 2019 combined revenues of €17billion.

Visit us at

www.sogeti.com

Author:
Darren W Baker, Sogeti
Special Thanks and Assistance from:
Katie Anderson, Microsoft
Sumera Baker, Georgetown University
Joe Lurie, Microsoft
Kim Sterkendries, Intel

[1]Business Reimagined, Author Dave Coplin, published by Harriman House 2013, **ISBN-10:** 0857193317