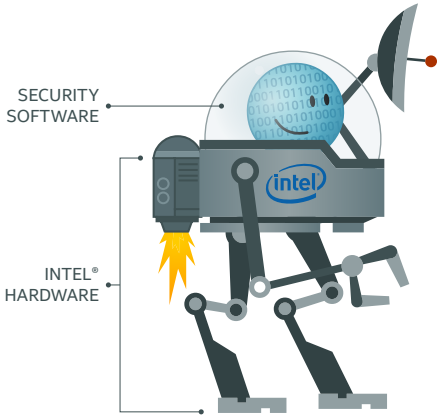
Hardware-Enhanced Security Strengthens Anti-Malware Defenses

Start, run, and stay secure with technologies embedded in platform hardware



Executive Summary

Can your company afford to pay $9.4 million to restore its reputation in the wake of a malware attack? In a recent study, the Ponemon Institute identified that figure as the average cost to restore a corporate brand following one of the most devastating types of malware attacks—the Advanced Persistent Threat (APT)—a sophisticated attack that targets high value assets and is difficult to detect.[1] A single APT incident also incurs the costs of technical support, loss of user productivity, and revenue loss and business disruption. And it doesn't end there. Your organization might face fines associated with lack of legal compliance, expend funds on recovery efforts, and suffer incalculable losses from theft of intellectual property and user credentials.

As malware continues to proliferate at breakneck speed, businesses are challenged to defend themselves using software-only solutions. Yet software alone cannot effectively protect your enterprise from the more sophisticated attacks—particularly APTs. Intel is shifting the balance in your favor with its hardware-enhanced security technologies. Innovative software and services developed by Intel partners take advantage of those built-in hardware technologies to help keep your business safe.

Using this new, hardware-enhanced approach to security, you can take a more proactive stance to enable business. Show C-level executives that security does not detract from the bottom line—rather, that it can be the framework that helps your business to thrive. Indeed, as APTs grow ever more sophisticated, security can become a vital differentiator between your enterprise and those that have not evolved.

Unmasking Advanced and Persistent Attacks

An organized crime ring begins to methodically launch an APT attack on a large bank. The countdown begins:

T minus 12 months: *Seasoned experts mine the bank's website and social networking sites for organization charts and the contact information of the bank's senior personnel. Meanwhile, a different team scans the bank's perimeter networks to identify its Internet-facing hosts.*

T minus 9 months: *The crime ring uses the stolen data to orchestrate social engineering attacks, such as targeted phishing e-mail campaigns aimed at several of the bank's executives, introducing malware that compromises their laptop operating systems. Undetected by antivirus software, the malware slowly proliferates across the business and waits until its moment to strike.*

Table of Contents

Executive Summary 1

Unmasking Advanced and Persistent Attacks 1

How Software-Only Solutions Can Fall Short 3

How Hardware-Enhanced Solutions Enable Business 3

Anti-Malware Technologies from Intel 3

- Guard PCs before Start Up or Wake Up 3
- Protect the BIOS 4
- Prevent Privilege Escalation. . . . 4
- Enhance Windows* Protections at Startup 4
- Defend a Broader Surface Area 5

Hardware-Enhanced Anti-Malware Solutions from McAfee 5

- Coordinate a Real-Time Response to Threats. 5
- Block Malware below the Operating System 6
- Securely Manage Remote Endpoints. 6

Differentiating Your Business from the Competition. 7

T minus 7 months: *The malware injects custom code to entrench itself in all infected systems, including those of several key contractors who regularly work on site at the bank. It begins to morph and infiltrate servers, slowly and steadily stealing network topology diagrams, security polices, and password datasets. The crime ring uses this information to launch even more offensives across the enterprise network.*

0 months: *The crime ring executes a targeted data exfiltration over eight weeks, downloading the bank card information of more than 50 million customers and causing incalculable damage before the IT department finds out about the breach from a partner organization.*

On average, a diminished brand or reputation caused by a single APT incident costs enterprises an estimated $9.4 million.[1] In addition, enterprises lose an average of $2.5 million in technical support costs, $3.1 million in diminished employee productivity, and $3.0 million in revenue loss and business disruption costs.[1] Additional losses include fines associated with compliance violations, funds spent on recovery efforts, and the incalculable damage incurred by theft of intellectual property and user credentials.

As software-only protections against malware evolve, so does the malware. In 2013, about 10 million new malware strains came to light.[2] Malware continues to proliferate as cybercriminals find more surface area to attack: enterprises are moving their data to the cloud and users are augmenting desktop PCs with mobile devices. The bring-your-own-device (BYOD) phenomenon is now ubiquitous: by 2018, more than one billion employee-owned smart phones and tablets will exist in the enterprise.[3] In addition, software, services, and people will never be infallible. For example, spear-phishing is nothing new, but it is prevalent because today it is easy to find personal and professional information via social media and other channels—and this information can be used to craft a more convincing message and persuade an unsuspecting employee to click a link in an e-mail.

Enable Business with Hardware-Enhanced Security

As security threats grow ever more sophisticated, security can become a vital differentiator that separates businesses that have evolved from those that have not.

Intel is working to strengthen security as a business enabler by embedding security features into the hardware across four fundamental pillars of enterprise security:

- Anti-Malware: Deeper protections help eliminate places malware can hide
- Identity: Easier access with enhanced security
- Data Protection: Stronger protection helps keep data safe from theft or alteration
- Resiliency: Help keep systems up-to-date and resilient

For more information, see the white paper "Hardware-Enhanced Security: Change Your Security Paradigm to Enable Business while Reducing Risks and Costs."

How Software-Only Solutions Can Fall Short

Although businesses can catch basic malware exploits using standard security software, the more sophisticated attacks—particularly APTs—are designed to evade software-only detection. Once an APT has compromised a system, it uses evasion techniques that allow it to shape shift and fly under the radar. It can then steal and exfiltrate data from systems across an enterprise over prolonged periods. Even if security software detects run-time threats, an APT can reassert itself the next time a system is restarted. Boot and wake from sleep are high-risk times when pre-operating system code executes before security software gets up and running. BIOS or firmware-resident malware can execute during this window of vulnerability.

A full 63 percent of respondents to a Ponemon Institute survey said that they discovered an APT by accident, and it took an average of 225 days for their companies to detect them.[1] 72 percent reported situations where APTs evaded their intrusion prevention systems (IPSs), and 76 percent reported that their antivirus solutions were also evaded.[1] As common news headlines illustrate, using software to fight software is not effective enough.

How Hardware-Enhanced Solutions Enable Business

Intel and its ecosystem of partners are helping to shift the balance in your favor with stronger protections against both basic malware and sophisticated APTs. Security technologies embedded in the chipset help protect the deepest levels of the system, before software-only protection even starts. Innovative software and services take advantage of those built-in hardware features to keep systems safer.

This new, hardware-enhanced approach to security helps you take a more proactive stance. Instead of fighting software with software, you can better protect and enable business using hardware-enhanced technologies that strengthen your defenses by pushing security down into lower levels of the computing stack. This approach can help your business to thrive and can differentiate your organization from those whose approach to security has not evolved.

Anti-Malware Technologies from Intel

Intel offers the following hardware-based anti-malware technologies:

Intel Technology	Description
Intel® Device Protection Technology with Boot Guard[4]	Helps verify boot integrity by helping to prevent execution of unauthorized code in the device BIOS.
Intel Device Protection Technology with BIOS Guard[4]	Helps protect the BIOS from modification without platform manufacturer authorization.
Intel Device Protection Technology with OS Guard[4]	Helps prevent privilege-escalation attacks that allow attackers to take control of the OS.
Intel Device Protection Technology with Trusted Execution Technology (TXT)[4]	Helps protect sensitive data in virtual and cloud ecosystems by validating a trusted compute environment.

Table 1: Hardware security technologies from Intel

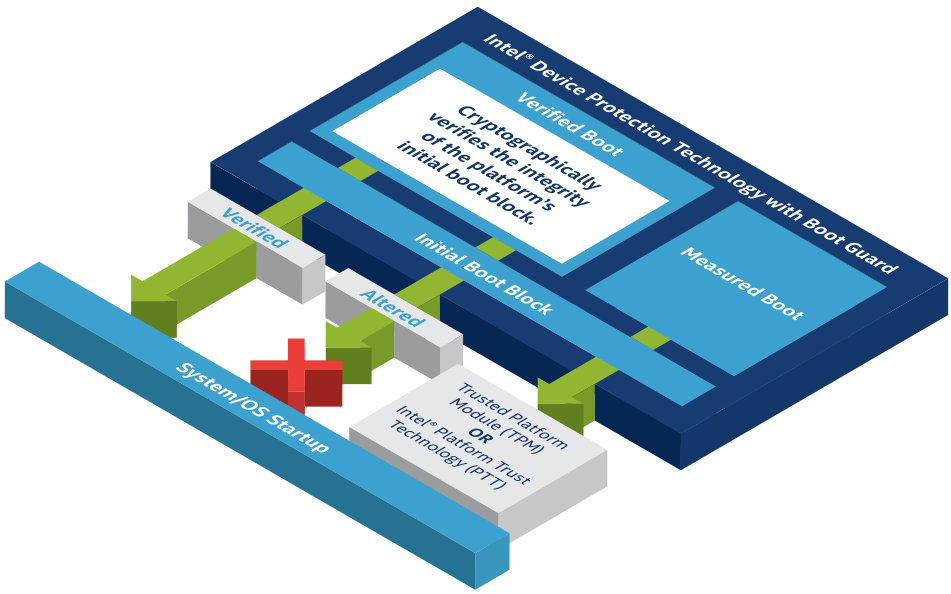


Figure 1: Intel® Device Protection Technology with Boot Guard[4]

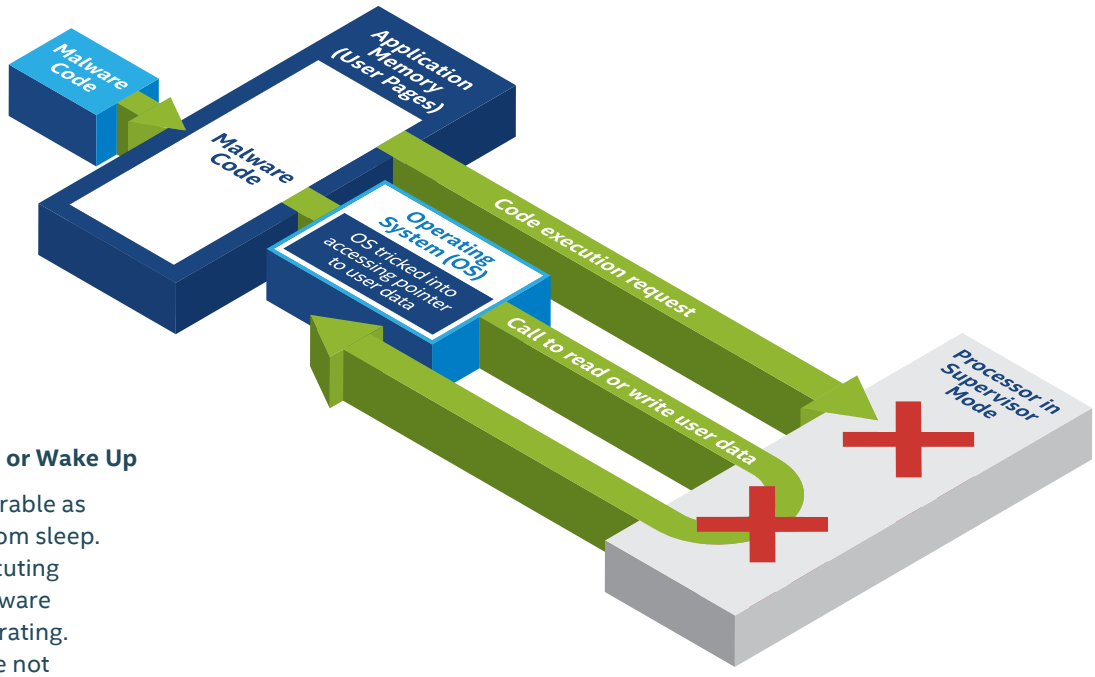


Figure 2: Intel® Device Protection Technology with OS Guard[4]

Guard PCs before Start Up or Wake Up

A PC is perhaps most vulnerable as it begins to boot or wake from sleep. In these states, code is executing but software-only anti-malware protections are not yet operating. Software-only solutions are not enough to defend against attacks that target devices in these states. Intel® Device Protection Technology with Boot Guard helps verify that only authorized firmware and an authorized operating system are running on a device.[4] Because it helps block malware from repurposing the platform to run unauthorized software, it can help to spare your organization the enormous costs of an APT incident.

Protect the BIOS

You have seen the headlines about targeted attacks on point of sales (POS) terminals, interactive vending machines, and ATMs. To avoid detection, attackers are now digging deeper into the platforms of such devices, all the way down to the BIOS, which is contained in a privileged space that is invisible to antivirus software. In addition, once malware infects a BIOS, it doesn't go away, even after a cold boot. Intel Device Protection Technology with BIOS Guard helps to defend the BIOS by blocking software-only attempts to update it without the platform manufacturer's authorization.[4] For retailers and enterprises seeking to protect proprietary data, security begins with the BIOS.

Prevent Privilege Escalation

Privilege escalation allows attackers to gain complete control of a computer's operating system. To better protect operating systems from this type of attack, your IT department can take advantage of two hardware-enhanced security technologies from Intel:

- Intel Device Protection Technology with OS Guard
- Intel Device Protection Technology with Enhanced OS Guard

Intel Device Protection Technology with OS Guard can help protect your enterprise against privilege escalation attacks.[4] These types of attacks occur in two steps: first, they compromise an application running in user mode, or trick an employee into installing malware. Second, they use a system call to exploit a vulnerability in the operating system while the processor remains in supervisor mode, giving the malware full control of the system. Intel Device Protection Technology with OS Guard helps block these memory access attempts from supervisor mode to user mode.[4]

Intel Device Protection Technology with Enhanced OS Guard helps to prevent access to an operating system and applications from a device's System Management Mode (SMM) software.[4] This hardware-enhanced security can help protect your enterprise by clearly isolating any SMM code from inadvertently accessing the operating system and applications on the device.

Enhance Windows* Protections at Startup

Intel® hardware-enhanced security works with newer security features in Windows 8.1* to help provide a trusted environment at startup. Windows 8.1 Trusted Boot uses the Unified Extensible Firmware Interface (UEFI) root of trust to help verify that the rest of the boot components are secure and have integrity. At the same time, Windows 8.1 Measured Boot takes measurements of each component—from firmware up through the boot start drivers and even anti-malware drivers—and locks away the measurements in a trusted platform module (TPM), such as Intel

Device Protection Technology with Platform Trust. Intel Device Protection Technology with Platform Trust offers a more secure, firmware-based TPM solution built to rigid standards established by the Trusted Computing Group, an industry consortium led by Intel, Microsoft, and others. The measurements collected by Measured Boot can be accessed from Intel Device Protection Technology with Platform Trust by third-party security software in order to compare the current state of the system against the known-good state established by UEFI Secure Boot.[4] By establishing and verifying a trusted state, you can better assess the integrity of the system and help identify and block malware before it takes root.

Each time the device is started, these combined technologies help ensure that the deepest levels of the system are not tampered with, allowing you to detect and block malware before it can infiltrate and steal your confidential assets.

Defend a Broader Surface Area

As more enterprises store data in the cloud, cybercriminals have exponentially more surface area to attack. IT can combat their efforts using trusted compute pools built on Intel® Platform Protection Technology with Trusted Execution Technology (TXT).[4]

Threats to your organization's data centers with physical, virtual, and cloud environments might already be keeping you up at night. Your IT department needs to protect personal, financial, or other sensitive data on behalf of your employees and customers, but in virtual and cloud ecosystems this can be hard to accomplish without new tools and techniques.

By establishing trusted compute pools, IT can better protect critical workloads. Trusted compute pools are built on a foundation provided by TXT, which creates a measured launch environment (MLE) to help verify the integrity of firmware, BIOS, and operating system or hypervisor code on servers powered by Intel® Xeon® processors. By using attestation capabilities, along with virtualization and security policies, IT can detect which platforms in your virtual pool have passed or failed integrity verification by TXT. IT can then combine the verified systems into trusted pools and can better ensure that sensitive workloads run only on trusted computing resources. Figure 3 shows how trusted compute pools work.

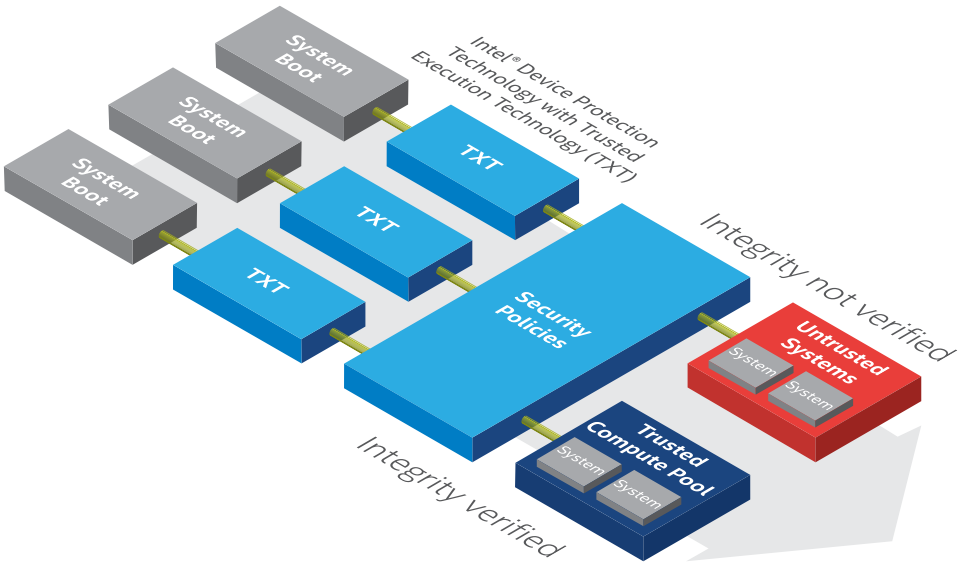


Figure 3: Trusted Compute Pools with Intel® Device Protection Technology with Trusted Execution Technology (TXT)[4]

Hardware-Enhanced Anti-Malware Solutions from McAfee

In addition to the deeper protections they provide, Intel hardware technologies build a foundation for layering stronger software protections above. McAfee offers a comprehensive collection of technologies that are designed to complement or integrate with Intel technologies to better protect your enterprise from advanced threats.

Together, the combined solutions cut across multiple Intel security pillars to provide a more holistic approach to security. For example, integrated McAfee solutions can help you combat malware by enabling you to better find (quickly and accurately identify) and freeze (block and quarantine) threats. Additional technologies give you the tools you need to better fix (rapidly remediate) threats before they establish a foothold in your organization. Because no single solution is enough to fend off increasingly sophisticated attacks, only a holistic approach can help ensure a healthy computing environment.

Coordinate a Real-Time Response to Threats

Traditional software-only solutions rely on signatures or sandboxing, which do not effectively block APTs. McAfee offers a more comprehensive, layered approach to protecting your network, data center, servers, and clients. Beginning at the edge of your network, in-line network security products like McAfee® Network Security Platform and McAfee® Web Gateway examine incoming traffic at your network perimeter for threats.

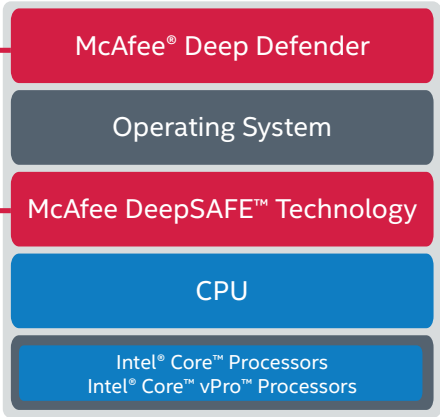


Figure 4: McAfee® Deep Defender gains a new vantage point on threats by using McAfee DeepSAFE™ technology, which resides between the CPU and the operating system

If these solutions are unable to determine if a particular file is malicious, they pass the file on to McAfee® Advanced Threat Defense—a centrally located appliance that can handle incoming files for threat analysis from multiple sources on your network. McAfee Advanced Threat Defense uses signatures, threat reputation, and emulation engines to more accurately detect a broad spectrum of advanced threats in real time.

If a threat is discovered, integration with McAfee® Host Intrusion Prevention for Server, and other sensors and gateways, helps freeze the threat by blocking future penetration attempts and quarantining the infected endpoint. Finally, Real Time for McAfee® ePolicy Orchestrator® (McAfee ePO™) examines all systems for other instances of the detected malware so you can initiate remediation.

Block Malware below the Operating System

McAfee also offers several software solutions that take advantage of Intel hardware technologies to help collectively identify and block threats before they can cause widespread damage. McAfee® Deep Defender uses Intel® Virtualization Technology (Intel® VT-x) to go beyond the operating system to help detect, block, and remediate advanced, hidden attacks in real time. McAfee Deep Defender is enabled by McAfee DeepSAFE™ technology, a solution jointly developed by McAfee and Intel. McAfee Deep Defender runs below the operating system, enabling stronger hardware-enhanced protection for systems.

Securely Manage Remote Endpoints

With McAfee ePO Deep Command, administrators can more securely access remote PCs—even if they are powered off or disabled—to deliver beyond-the-operating-system security management. The solution lets you control endpoints to execute security updates, deploy software and policies, or remediate system problems more securely from across the office, continent, or globe.

McAfee ePO Deep Command uses Intel® Active Management Technology (Intel® AMT), found in systems powered by Intel® Core™ vPro™ processors, to access endpoints without relying on the operating system.[5] McAfee ePO Deep Command lets you set up automatic provisioning, reporting, and configuration of endpoints. You can even schedule policies to power on groups of remote systems, execute security tasks, and then return the endpoints to their previous power states.

No matter how strong and effective your defenses are, at some point you might need to move beyond the find and freeze approach to anti-malware defense and cross into remediation solutions. This holistic approach to security helps keep your ecosystem healthy even when a threat infiltrates your borders. Advanced McAfee technologies let you remotely remediate infected endpoints to reduce downtime and prevent more widespread damage. With the McAfee® KVM Viewer, you can use Intel AMT to help securely control a remote PC's keyboard, video, and mouse to remediate the device even if it is inoperative or powered off. With McAfee ePO Deep Command communicating directly with the hardware, you can control the remote PC through power cycles and operating system reboots without breaking the connection.

By providing centralized, more secure remediation and management of endpoints, McAfee ePO Deep Command helps you reduce support, remediation, and maintenance costs, strengthen your security posture, and maintain efficiency and productivity for your users.

Intel Technology	Description
Find, freeze, and fix advanced threats	
McAfee® Network Security Platform	Moves beyond mere pattern matching to help find threats to your network with extreme accuracy.
McAfee® Web Gateway	Analyzes the nature and intent of all content and code entering the network from requested web pages, helping to immediately find malware and other hidden threats.
McAfee® Host Intrusion Prevention for Server	Helps freeze malware using a firewall and an intrusion protection system (IPS).
McAfee® Advanced Threat Defense	Helps freeze stealth attacks by initiating an immediate and comprehensive response whenever a threat is identified, quarantining the infected hosts or applications to help prevent further infection.
Real Time McAfee® ePolicy Orchestrator® (McAfee ePO™)	Helps IT to identify and remediate under-protected and noncompliant endpoints.
Go below the operating system to protect against rootkits	
McAfee® Deep Defender	Built on McAfee DeepSAFE™ technology, it goes below the operating system to help detect rootkits and other threats that propagate code or attack specific areas.
McAfee DeepSAFE™ technology and Intel® Virtualization Technology (Intel® VT-x)[6]	Jointly developed by Intel and McAfee, it helps protect virtual machines (VMs) by isolating their execution environments and monitoring memory, so malware existing in or attempting to invade one VM environment cannot affect another VM on the same host.
Securely access remote endpoints	
McAfee ePO Deep Command	Enables remote security management access to PCs, even if they are unresponsive or unable to boot. Helps reduce security operations costs while enhancing security posture.

Table 2: Software security technology from McAfee

> Security practitioners exist "to enable business—to help deliver IT capabilities that provide competitive differentiation."[7]
>
> *- Malcolm Harkins, Intel Chief Security and Privacy Officer*

Differentiating Your Business from the Competition

APTs and other malware threats will continue to proliferate because software and the people who use it will always be vulnerable. With more and more APT incidents making the news, enterprises must prove to current and prospective customers that they are taking the right steps to better secure identities and data. The software-only approach simply isn't effective against newer, more sophisticated attacks.

Intel and its partners offer you a game-changing approach that couples hardware-enhaced security technologies with innovative anti-malware software and services. Now, you can better protect devices, platforms, and servers from the moment they start. You can also help defend an ever growing surface area, from the cloud down to the device in an employee's pocket. By taking this new approach to security, you no longer react to threats, but help prevent them—and ultimately help to ensure the future success of your business.

Visit www.intel.com/enterprisesecurity/ to learn more.

[1] Ponemon Institute. "The State of Advanced Persistent Threats." December 2013. http://buildingtrust.trusteer.com/Ponemon_Study_December_2013.

[2] SoftPedia. "10 Million New Malware Strains Identified So Far in 2013, Q3 Study Shows." November 2013. http://news.softpedia.com/news/10-Million-New-Malware-Strains-Identified-So-Far-in-2013-Q3-Study-Shows-404043.shtml.

[3] Infosecurity. "One Billion Mobile Devices to Spur Mass BYOD Security Investment." November 2013. http://www.infosecurity-magazine.com/view/35863/one-billion-mobile-devices-to-spur-mass-byod-security-investment/.

[4] No computer system can provide absolute security under all conditions. Built-in security features available on select Intel® processors may require additional software, hardware, services and/or an Internet connection. Results may vary depending upon configuration. Consult your system manufacturer for more details. For more information, see https://security-center.intel.com/.

[5] Requires activation and a system with a corporate network connection, an Intel® AMT-enabled chipset, network hardware and software. For notebooks, Intel AMT may be unavailable or limited over a host OS-based VPN, when connecting wirelessly, on battery power, sleeping, hibernating or powered off. Results dependent upon hardware, setup and configuration. For more information, visit http://www.intel.com/content/www/us/en/architecture-and-technology/intel-active-management-technology.html.

[6] Intel® Virtualization Technology requires a computer system with an enabled Intel® processor, BIOS, and virtual machine monitor (VMM). Functionality, performance or other benefits will vary depending on hardware and software configurations. Software applications may not be compatible with all operating systems. Consult your PC manufacturer. For more information, visit http://www.intel.com/go/virtualization.

[7] Harkins, Malcolm. Managing Risk and Information Security: Protect to Enable. Apress Media, LLC. December 2012. http://www.apress.com/9781430251132.

Printed in USA 0414/MS/PRW/PDF ♻ Please Recycle 330365-001US