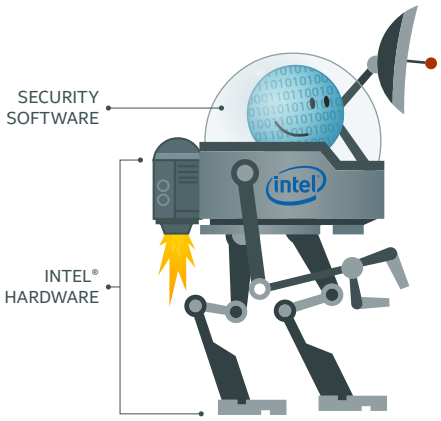
Hardware-Enhanced Protections Help Keep Your Infrastructure Resilient

Strengthen data protection with innovative technologies rooted in the chipset



Executive Summary

According to the IT Trust Curve 2013 global survey by Vanson Bourne, security breaches cost enterprises an average of $860,000 a year.[1] But here's an even more staggering statistic: downtime alone costs enterprises an average of $495,000 a year as they struggle to identify and block threats or repair any damage done.[1] This fact is critical as organizations attempt to defend an ever widening attack surface. Cloud computing, mobile devices, the bring-your-own-device (BYOD) trend, and constant connectivity open up more and more avenues to attack. It's no longer a matter of if a breach happens, but when it does and how much damage it leaves in its wake.

As a result, you need ways to minimize the damage and restore systems as quickly as possible. Traditionally, organizations rely on software-only solutions to security, prevention, and mitigation challenges, but those approaches typically fall short. That's because they usually rely on less-than-effective means of identifying stealth malware before it causes extensive damage. Even when they do find threats, software-only solutions often stop at identification, leaving the harder work of blocking and remediating to your security analysts. Software-only solutions are also ineffective for remediating remote PCs that are locked up or unable to boot, because they don't have any means of accessing unresponsive devices. Security professionals need a newer, more effective tactic for stronger, more proactive security that helps their organizations stay healthier and—when infected—recover faster.

Intel and its ecosystem of partners are helping to shift the balance in your favor with a new approach to keeping your endpoints, servers, data centers, and clouds resilient in the face of modern threats. Intel drives security closer to the chipset with technologies embedded in the platform hardware to provide stronger, more proactive and effective solutions. Innovative software and services from Intel, McAfee, and partners take advantage of those built-in hardware features to help keep systems resilient and minimize disruption and downtime.

Table of Contents

Executive Summary 1
Dealing with the Inevitable. 2
A New Approach to Faster Remediation. 3
Resiliency Helps Keep Your Enterprise Healthy. 3
Resiliency Begins in the Chipset . . 3
Three Steps to a Healthy Enterprise: Find, Freeze, and Fix. 4
Coordinate a Real-Time Response to Threats. 4
Reduce Downtime for Endpoints 4
Security through Resiliency 5

Dealing with the Inevitable

It's a typical morning for the IT department of a large hospital. Like most days, an assortment of malware-laden files hits the firewalls and servers. Security analysts start the day as they usually do: scouring the threat report generated by their anti-malware software. They focus on a few suspicious files, including one in particular that raises some red flags but is not listed as a known threat in any of the blacklisting databases. Being diligent, the team blocks the file at the firewall and continues to analyze the file over the course of the next several days.

Meanwhile, without their knowledge, copies of the file have already made their way onto client endpoints, where an advanced persistent threat (APT) has quietly migrated vertically into deeper layers of the client PCs, and laterally across the network to servers containing vital services and confidential patient data. By the time IT understands the nature of the threat, weeks have passed. The malware has activated its payload and begun to transfer sensitive information across the Internet to the perpetrators.

IT spends weeks trying to find and remove the threat, an effort that costs the hospital tens of thousands of dollars, months of man-hours, and possible fines due to lack of compliance with regulations.

Unfortunately, scenarios like this happen every month, causing many businesses to hemorrhage money. Security professionals are well aware of the damage done by malware when data or identities are stolen, but costs to the enterprise go well beyond the initial expense of a security breach. Once an advanced threat has infiltrated your defenses, it hides, spreads surreptitiously, and continues to quietly lurk in your systems, where it can remain undetected for days or even weeks. In fact, a 2013 Ponemon study determined that the average time to resolve a cyber-attack was 32 days, with an average cost to participating organizations of $1,035,769 during this 32-day period.[2] With each moment that passes after initial infection, dollars are stripped from your bottom line as compliance violations, support efforts, down time, and lost productivity accumulate.

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."

As cloud computing, mobile devices, BYOD, and constant connectivity become ubiquitous, malware attacks are essentially a given. Even if your network and devices are well protected, one unsuspecting employee who falls victim to a targeted social engineering attack might open a back door for threats to sneak inside.

Unfortunately, software-only approaches to security are typically inadequate for comprehensive prevention and remediation. Software solutions might flag suspicious files, for example, but leave you with the exhaustive work of scouring log entries while the unhindered threats burrow deeper into your infrastructure. Software-only solutions are also ineffective for resuscitating remote devices that are unresponsive or unable to boot. Given how pervasive and potentially costly malware attacks are, most enterprises would clearly welcome a new, more effective tactic for stronger, more proactive security that helps your enterprise stay healthier and—when necessary—recover faster.

A New Approach to Faster Remediation

Intel and its partners are upsetting the software-versus-software tradition with a new approach to resiliency that embeds security in the hardware of Intel® platforms: from the data center to users' pockets. Rooting security in the Intel chipset gives your business an advantage over software-only solutions by hardening protections, simplifying management, and providing more comprehensive, proactive solutions for maintaining or quickly restoring the health of your systems. Even before the operating system starts, Intel technologies help verify the integrity of the system to prevent tampering by advanced malware. McAfee® management solutions work with integrated Intel hardware-enhanced technologies to help you remotely access and remediate unresponsive devices. When your enterprise is resilient, you can reduce remediation costs, improve productivity, and increase confidence in meeting regulatory compliance mandates.

Resiliency Helps Keep Your Enterprise Healthy

A healthy enterprise is like a healthy body. When a person is physically fit, with an active, healthy immune system, and proper vaccinations, she is better able to ward off infections that others might succumb to. Even when illness does strike, an otherwise healthy body and immune system can fully recover much faster than one that is weaker from lack of exercise, malnutrition, low-grade infections, or other causes. When your clients, servers, and network infrastructure are fortified with mechanisms for faster detection, isolation, and remediation, you can better prevent or quickly recover from advanced threats while keeping damage and costs to a minimum. With comprehensive infrastructure monitoring, you can watch for deviations in vital signs for your enterprise and take additional steps when key indicators deviate from the norm. When the occasional, inevitable breach or exposure occurs, you can return your infrastructure to health quickly, with less chance of long-term damage.

Resiliency Begins in the Chipset

Hardware-enhanced security adds layers of protection that stay with the device regardless of how it is used or managed. Even before the operating system starts, deeper layers of security are working to help defend against stealth malware. For example, during the initial Windows 8.1* boot process, Intel® Device Protection Technology with Boot Guard helps prevent unauthorized software and malware from taking over boot blocks that are critical to a system's function, and Intel Device Protection Technology with BIOS Guard helps prevent unauthorized modification of a system's BIOS code.[3]

Together, these advanced technologies help prevent the deepest levels of your system—critical to both the operating system and the applications above—from being tampered with, even if malware infects the device.

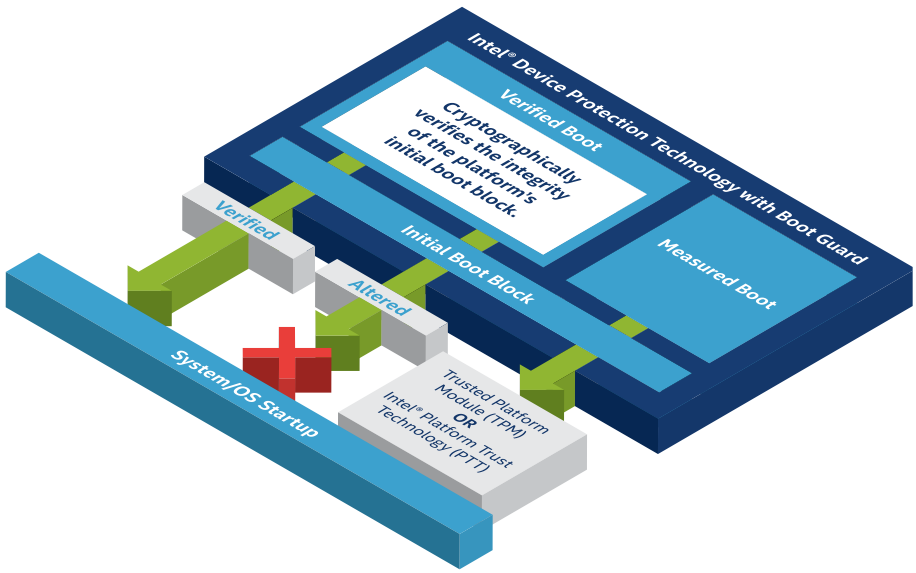


Figure 1: Intel® Device Protection Technology with Boot Guard[3]

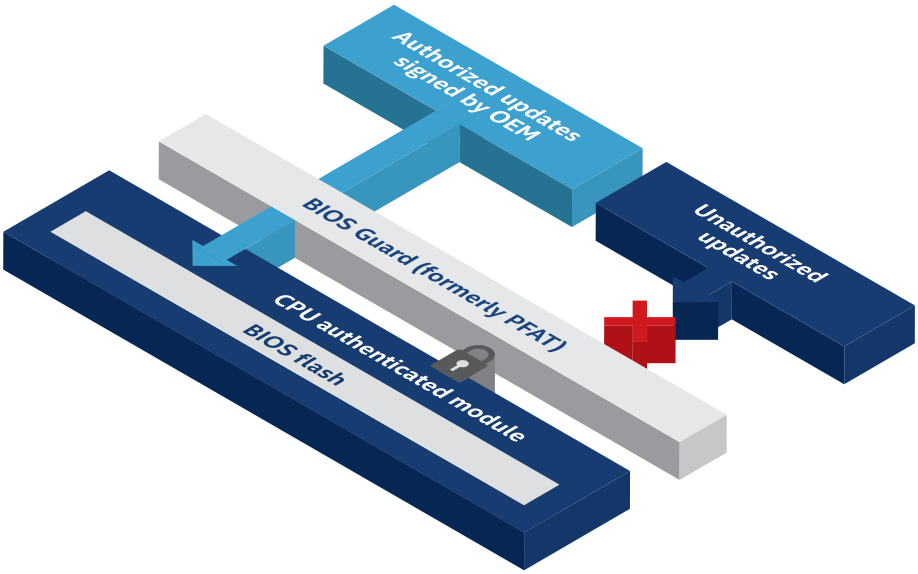


Figure 2: Intel® Device Protection Technology with BIOS Guard[3]

Intel Technology	Description
Intel® Device Protection Technology with Boot Guard[3]	Helps maintain boot integrity by working to prevent execution of unauthorized software and malware in the boot blocks.
Intel Device Protection Technology with BIOS Guard[3]	Helps protect the BIOS flash from modification without platform manufacturer authorization.

Table 1: Hardware-enhanced security technologies from Intel help protect your devices at startup

Three Steps to a Healthy Enterprise: Find, Freeze, and Fix

There is no shortage of firewalls, antivirus applications, and other solutions designed to identify or block malware. Each solution, however, must be configured and monitored separately, as individual components to a larger, interconnected ecosystem. To stay healthy overall, you wouldn't want to care diligently for your teeth and eyes, while allowing pneumonia to take hold and spread. Total health requires a wider perspective of all systems, and the ability to react quickly to prevent or limit infections when they are detected. Similarly, to keep your enterprise infrastructure healthy, you need a holistic approach that helps you to comprehensively find (quickly and accurately identify), freeze (block and quarantine), and fix (rapidly remediate) advanced threats before they establish a foothold in your organization.

Intel hardware-enhanced technologies not only help protect your system, they also 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 help provide the holistic approach to security you need to stay healthy.

Coordinate a Real-Time Response to Threats

Traditional malware defense solutions rely on signatures or sandboxing, which only offer partial protections without remediation. McAfee offers a comprehensive, layered approach to protecting your network, data center, servers, and clients that is designed to address even sophisticated, advanced malware attacks. In-line network security products like McAfee® Network Security Platform and McAfee® Web Gateway examine incoming traffic at your network perimeter for threats.

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.

Reduce Downtime for Endpoints

Even when you proactively detect and block malware, at some point you might need to remotely remediate or support endpoints. To minimize disruptions and remediation costs, you need a way to more securely access those remote PCs, even if a client operating system is inoperative or powered off.

With McAfee ePO™ Deep Command, administrators can more securely access remote PCs—even if they are powered

Intel Technology	Description
McAfee® Network Security Platform	Helps discover and block sophisticated malware by using advanced threat detection techniques for fast, accurate responses to network-borne attacks.
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	Uses multiple proven methods, including behavioral and signature analysis, and a dynamic, stateful firewall to help block emerging attacks.
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. Also helps find advanced malware and zero-day threats and seamlessly integrates with McAfee network security solutions to quarantine the infected hosts. Works with Real Time for McAfee® ePolicy Orchestrator® to initiate a fix or remediation action.
Real Time for McAfee® ePolicy Orchestrator® (McAfee ePO™)	Collects security status in real time from endpoints managed with McAfee technologies; helps administrators to quickly identify and remediate under-protected and noncompliant endpoints.

Table 2: Intel® hardware-enhanced technologies work with McAfee® appliance and software solutions to help keep your enterprise resilient

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) to access endpoints without relying on the operating system. By using McAfee® KVM Viewer, you can use Intel AMT to more securely control a remote PC's keyboard, video, and mouse to greatly simplify remediation. Because McAfee ePO Deep Command communicates directly with the hardware, you can control the remote PC through power cycles and operating system reboots without breaking the connection.

Intel Technology	Description
Intel® Active Management Technology (Intel® AMT)[4]	Enables remote repair of business PCs with keyboard, video, and mouse (KVM) controls, even if the remote device is out of band or unresponsive.
McAfee ePO™ Deep Command	Allows security administrators to configure and remediate remote endpoints from a central site, using McAfee® ePolicy Orchestrator® (McAfee ePO™).

Table 3: McAfee and Intel integrated solutions help you recover quickly to stay resilient

Security through Resiliency

In today's security-conscious environment, threat prevention and risk management are integral to enterprise initiatives. As a result, security professionals now find themselves as the driving force in enabling business by mitigating risks, reducing costs, ensuring compliance, and eliminating barriers to efficiency and productivity. Intel helps security practitioners like you fulfill your mission by embedding security features in the platform hardware of devices across the enterprise.

Even with the strongest protections, bad stuff from bad people will inevitably infiltrate your ecosystem. By using the combined technologies of Intel hardware-enhanced security and McAfee software security solutions, you can maintain the health of your enterprise ecosystem by more quickly finding, freezing, and fixing threats before they spread and cause widespread damage. This innovative approach helps you reduce costs and risks associated with exposure to threats by helping keep devices and enterprise infrastructure resilient.

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

> Security practitioners exist "to enable business—to help deliver IT capabilities that provide competitive differentiation."[5]
>
> *- Malcolm Harkins, Intel Chief Security and Privacy Officer*

Hardware-Enhanced Protections Help Keep Your Infrastructure Resilient

[1] Vanson Bourne. "IT Trust Curve 2013 Global Survey." Commissioned by EMC. http://www.emc.com/collateral/other/emc-trust-curve-es.pdf.

[2] Ponemon Institute. "Cost of Cybercrime Study, 2013." Sponsored by HP. http://www.hpenterprisesecurity.com/ponemon-study-2013.

[3] 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/.

[4] 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.

[5] 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 330366-001US