SOLUTION BRIEF

Strong Mobile Device Security Begins in the Hardware

STRENGTHEN YOUR MOBILE DEVICE SECURITY WITH HARDWARE-ENHANCED PROTECTIONS ON DEVICES POWERED BY INTEL® CORE™ PROCESSORS OR INTEL® ATOM™ PROCESSORS, WITH WINDOWS 8.1*

Mobile malware nearly doubled in number from second to third quarter 2012.[1]

Sometimes IT management can feel like a security treadmill—you respond to threats as they appear, but never gain any ground. It's hard enough responding to known threats on common platforms, but dealing with newer, more sophisticated attacks that target your PCs or mobile devices can lead to major headaches.

That challenge becomes even more daunting with the rapid increase in the consumerization of IT (CoIT) and bring your own device (BYOD) trends. You need to accommodate an increasingly wide range of mobile devices that don't easily integrate into your existing security infrastructure, but that are targets of a growing number of threats.

With so many security challenges, it can be costly trying to protect employees, customers, data, and your company's reputation. But of course the costs of ignoring the challenges can be much higher. In the second quarter of 2012, McAfee Labs reported the biggest increase in malware samples detected in the last four years.[2] And according to a 2013 Ponemon survey, malicious attacks were the root cause of 41 percent of the data breaches they examined.[3]

Mobile device management (MDM) solutions offer one approach to security across mobile device platforms. Windows 8.1* supports the Open Mobile Alliance Device Management (OMA DM) API, which enables you to manage devices through a low-overhead agent without needing to deploy a full management client on each device. But MDM products don't offer the same level of control as traditional domain-joined management solutions. Mobile devices commonly access both corporate and personal data and might be used to visit websites and download files for personal use without sufficient safeguards. These use patterns put mobile devices and their users at higher risk from identity theft, malware, and other stealthy threats that can infiltrate systems at deeper levels to steal data or even take control of a device.

Mobile Devices in the Enterprise

55 percent of enterprises surveyed rated concern for mobile devices a 4 or 5 out of 5, where 1 represented No Threat and 5 represented Significant Threat.[4]

Protecting Your Devices from the Silicon Up

To strengthen endpoint security, you need a more comprehensive approach that begins on the device itself. By using tablets, Ultrabook™ devices, 2 in 1 devices, and laptops powered by 4th generation Intel® Core™ processors and Intel® Atom™ processors running Windows 8.1, you can complement your MDM solution with strong, efficient security rooted in hardware. Hardware-assisted security adds layers of protection that stay with the device—regardless of how it is used or managed—to mitigate or even prevent the damages caused from malware compromising your system and stealing confidential assets. Deeper levels of protection can help you ensure your devices are secure before the operating systems even start. This unique approach helps you move from a reactive to a proactive security posture that can reduce risk, minimize downtime, and improve your ability to meet compliance mandates.

Layering Windows 8 Software on an Intel Hardware Foundation

Intel technologies provide a hardware foundation of security at startup and run time for Windows 8.1 and for the software components and applications that run on top of Windows. Integrated and complimentary features help prevent malware from infecting your system at the deepest levels, where attacks often go undetected, and can more easily spread to other parts of your infrastructure.

PROTECT AT STARTUP

The key to enabling a more proactive approach to security is to establish a root of trust in the hardware chipset—before the operating system and software even start. During the initial Windows 8.1 boot process, Intel® Platform Protection Technology with BIOS Guard and Boot Guard helps prevent unauthorized software and malware from taking over boot blocks that are critical to a system's function. Unified Extensible Firmware Interface (UEFI) Secure Boot continues early protections by ensuring only a properly signed operating system loader is used during startup.

Windows 8.1 Trusted Boot provides additional startup protections by using the UEFI root of trust to help ensure that the rest of the boot components are secure and have not been altered. 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 securely locks away the measurements in a trusted platform module (TPM), such as Intel Platform Protection Technology with Platform Trust. Intel Platform Trust offers a 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 securely accessed from Intel Platform Trust by third-party security software in order to compare the current state of the system against the known-good state established by secure boot. By establishing and verifying a trusted state, you can better ensure 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. But hardware-enhanced security doesn't end with the boot process. Intel® Platform Protection Technology with OS Guard helps protect the deepest levels of your system at run time, even if an application has been compromised. This unique Intel feature helps prevent hackers from remotely taking over a user's PC by preventing malicious code in compromised application memory from launching low-level, privilege escalation attacks.

ENCRYPT DATA EFFICIENTLY

Ultimately, security is about protecting your data. A comprehensive security solution relies on strong encryption to keep assets safe from prying eyes. But many organizations are reluctant to deploy strong

encryption technology, such as Advanced Encryption Standard (AES), because it can significantly drag down device performance. As shown in Figure 1, Intel helps remove that performance barrier with Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI), a new instruction set that accelerates data encryption and decryption on devices powered by Intel Core processors and Intel Atom processors. That enhanced performance allows wider use of strong encryption without a significant impact on productivity.

With Windows 8.1, Intel AES-NI accelerates the encryption used by BitLocker Drive Encryption* to more efficiently encrypt all user and system files on specified operating system drives, fixed data drives, and removable data drives. Once BitLocker is enabled on devices powered by Intel Core processors and Intel Atom processors, any file saved to a specified drive is encrypted automatically. That keeps your company data safer without any noticeable impact to the user.

STRENGTHEN ENCRYPTION WITH TRUE RANDOM NUMBERS

Intel doesn't just make encryption faster, it makes it stronger with Intel® Secure Key Technology. Typically, encryption keys are generated from software-based, pseudo-random number generators. Pseudo-random numbers offer complexity that seems secure, but actually can be replicated by sophisticated hackers who determine the procedure used to generate the numbers. Intel Secure Key responds to this challenge with a hardware-based solution that creates high quality, true digital random numbers on the processor chip.

Random numbers generated by Intel Secure Key can be used to create stronger encryption keys that help keep data secure anywhere that encryption is used on the device. For example, Intel Secure Key provides the isolated cryptography necessary to configure Windows 8.1 Pro and Enterprise systems as virtual smart cards for strong, two-factor authentication.

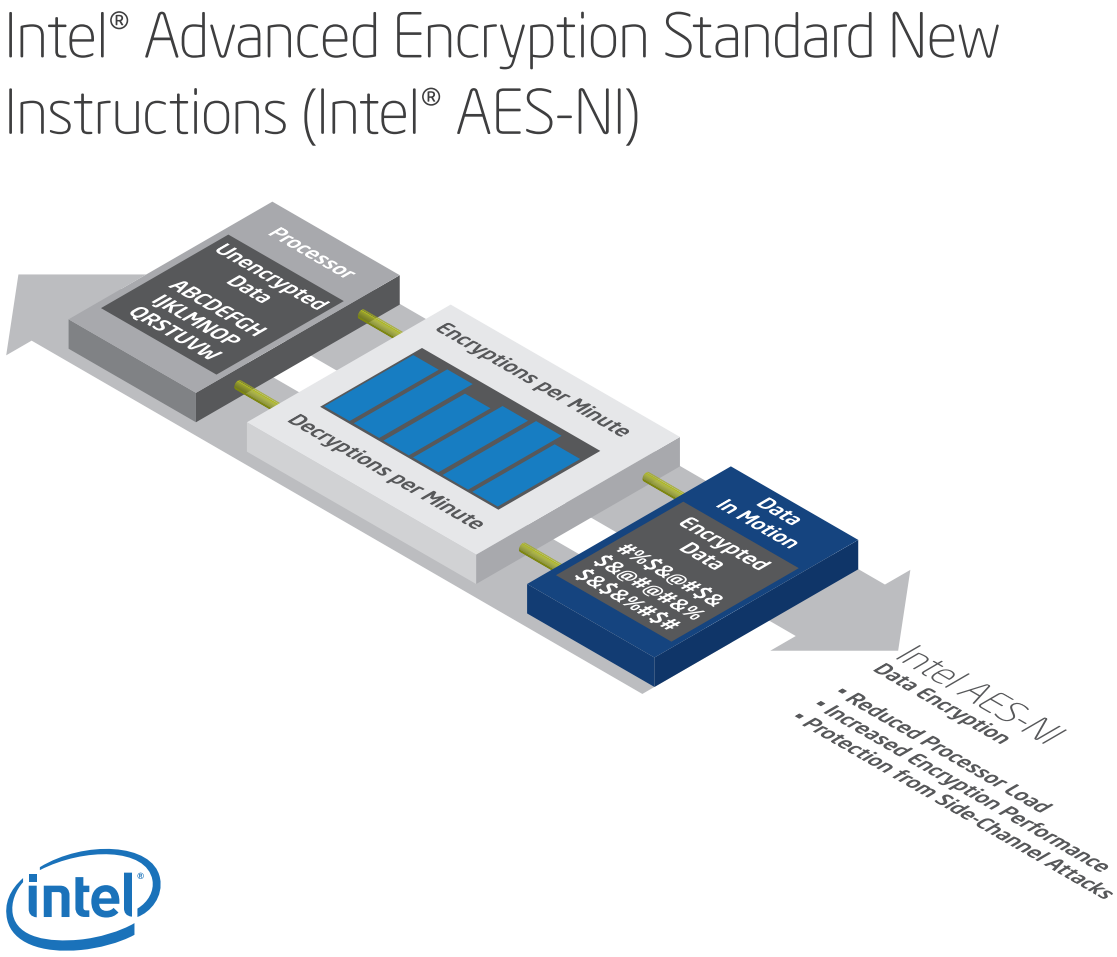

FIGURE 1: INTEL® ADVANCED ENCRYPTION STANDARD NEW INSTRUCTIONS (INTEL® AES-NI) ACCELERATES ENCRYPTION AND DECRYPTION PERFORMANCE TO ALLOW WIDESPREAD USE OF AES ENCRYPTION WITHOUT A SIGNIFICANT PERFORMANCE IMPACT

With this configuration, computers handle authentication the same as platforms with permanently inserted smart cards, while potentially reducing the costs and complexity associated with physical smart cards.

Provide Security with Power and Efficiency

Hardened protections shouldn't come at the expense of performance or efficiency. Intel factors manageability, performance, and power efficiency into every Intel Core processor and Intel Atom processor and chipset, while ensuring that the designs meet the form factor constraints of today's ultra-slim Ultrabook devices, 2 in 1 devices, and tablets. Speed and efficiency are critical for processing the cryptographic algorithms needed for the strong kernel protection offered with Intel® OS Guard and the enhanced, accelerated encryption provided by Intel AES-NI.

Don't Sacrifice Usability for Security

Today's modern workforce expects full remote access to the resources and tools users work with on desktop PCs in the office. Windows 8.1 tablets and 2 in 1 devices powered by Intel Core processors or Intel Atom processors are fully compatible with Microsoft Office* and other enterprise applications that are designed for Windows PCs. These devices provide the experience your users are familiar with, the mobility modern workers need, and the security technologies your CIO expects for keeping your company's assets safer.

As Table 1 shows, by complementing your MDM solutions with Intel hardware-assisted security technologies, you can keep devices powered by Intel Core processors and Intel Atom processors safer with the speed, efficiency, and user experience needed to satisfy your demanding workers.

TECHNOLOGY	BENEFIT	INTEL® CORE™ PROCESSORS	INTEL® ATOM™ PROCESSORS
UEFI Secure Boot	Provides a secure root of trust and prevents execution of an unverified bootloader	X	X
Intel® Platform Protection Technology with BIOS Guard	Protects the BIOS flash from modification without platform manufacturer authorization	X	
Intel® Platform Protection Technology with Boot Guard	Helps maintain boot integrity by preventing execution of unauthorized software and malware in the boot blocks	X	X
Intel® Platform Protection Technology with Platform Trust	Provides a standards-based TPM solution for securely storing measurements used to verify the integrity of the system	X	X
Intel® Platform Protection Technology with OS Guard	Helps prevent privilege-escalation attacks that allow attackers to take control of the operating system	X	X
Intel® Secure Key Technology	True digital random number generator with keys created more securely in the hardware	X	X
Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI)	Stronger, more efficient encryption that can be used with BitLocker Drive Encryption* for full disk encryption to keep data safer	X	X

Table 1: Hardware-assisted technologies strengthen security on devices powered by Intel® Core™ processors and Intel® Atom™ processors running Windows 8.1*

For more information on consumerization security:

http://www.intel.com/content/www/us/en/mobile-computing/consumerization-best-practices.html

For more information on Windows 8.1 security features:

http://technet.microsoft.com/en-us/library/dn344918.aspx

intel | Windows

[1] McAfee Labs, "McAfee Threats Report: Third Quarter 2012," 2012. http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q3-2012.pdf.

[2] McAfee Labs, "McAfee Threats Report: Second Quarter 2012," 2012. http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q2-2012.pdf.

[3] Ponemon Institute. "2013 Cost of a Data Breach Study: United States." May 2013. Benchmark research sponsored by Symantec. http://www.symantec.com/content/en/us/about/media/pdfs/b-cost-of-a-data-breach-us-report-2013.en-us.pdf.

[4] IDC, "Market Analysis Perspective: Worldwide Security Products, 2012," doc #231958, December 2012. http://www.idc.com/getdoc.jsp?containerId=238720.

Intel® vPro™ Technology is sophisticated and requires setup and configuration. Availability of features and results will depend upon the setup and configuration of your hardware, software, and IT environment. To learn more about the breadth of security features, visit http://www.intel.com/technology/vpro.

Intel® Advanced Encryption Standard–New Instructions (Intel® AES-NI) requires a computer system with an AES-NI-enabled processor, as well as non-Intel software to execute the instructions in the correct sequence. AES-NI is available on select Intel® Core™ processors. For availability, consult your system manufacturer. For more information, see http://www.intel.com/content/www/us/en/architecture-and-technology/advanced-encryption-standard--aes-/data-protection-aes-general-technology.html.

No computer system can provide absolute security under all conditions. Built-in security features available on select Intel® Core™ processors may require additional software, hardware, services and/or an Internet connection. Results may vary depending upon configuration. Consult your PC manufacturer for more details. For more information visit www.intel.com/technology/security.

Intel® OS Guard requires an Intel® OS Guard-enabled system with a 3rd gen Intel® Core™ vPro™ processor and an enabled operating system. Consult your system manufacturer for more information.

Intel® Secure Key requires an Intel® Secure Key-enabled PC with a 3rd gen Intel® Core™ vPro™ processor and software optimized to support Intel Secure Key. Consult your system manufacturer for more information.

Printed in USA 1113/PC/PRW/PDF Please Recycle 329623-001US