SOLUTION BRIEF
Hardware-based Security Solutions
Healthcare Information Security

Healthcare Security: User Experience, Compliance, and Risk

David Houlding, CISSP, CIPP
Healthcare Privacy and Security Lead Architect
Intel Corporation

Raj Samani
Vice President, Chief Technology Officer EMEA
McAfee

Nancy Vuckovic
Senior Health Researcher
Intel Corporation

Introduction

Healthcare is in the midst of a perfect storm of change that is being driven by healthcare, consumer, IT, and security trends.

These trends promise major benefits that will empower healthcare workers, including doctors and nurses, by improving the quality and reducing the cost of patient care. However, these trends also increase privacy and security risks that must be managed to avoid security incidents, such as breaches. Compounding this challenge are the ongoing cost-reduction pressures in healthcare and the limited budget available for privacy and security measures.

Security controls must mitigate risks in a way that preserves an optimum user experience for the healthcare worker; otherwise, workers may seek alternatives that can circumvent or disable security. Healthcare workers now have access to many tools that provide powerful, but potentially risky, alternatives such as personal smartphones, tablets, USB keys, social media, apps, file transfer services, and even personal email. Use of these alternatives can lead to non-compliance issues and create significant additional risk (Table 1).

Implementing a proactive, preventative approach to privacy and security—one that includes technology together with administrative and physical controls—is a practical strategy that healthcare organizations can use to manage risk. To meet the future security needs of healthcare, security solutions must be high performance, robust, usable, and cost effective. Vertically integrated security solutions that make use of hardware-assisted security (HAS)—from Intel and McAfee—can deliver strong security with a great user experience, enabling healthcare workers to deliver effective patient care without the need for risky alternatives.

Practical Strategies for Security

Security breaches averaged over USD 5.2 million per event in 2011.[1] Given the devastating business impact that these types of security incidents can cause, the only practical approach to privacy and security is a proactive, preventative one. In this way, healthcare organizations can identify trends that are driving change, incorporate risks associated with these changes in their risk assessments, and apply

TRENDS DRIVING PRIVACY AND SECURITY RISKS

Medical Trends

- Migration to electronic health records
- Health information exchange and data proliferation
- Mobile health
- Regulations, breach notification rules, and breaches
- Cost-reduction pressure

Consumer Trends

- Consumerization/bring your own device
- Social media

IT and Security Trends

- Cloud computing
- Sophisticated, targeted malware attacks
- Big data and evolving research requirements

Table 1. Considerations for implementing security controls in a healthcare environment

Goal	Challenge
Healthcare Deliver great patient healthcare	▪ Privacy and security are not the focus ▪ Cumbersome security controls impede healthcare
Compliance Deliver an optimal user experience for healthcare workers	▪ Attractive, but risky alternatives; non-compliance with policy ▪ Increased risk to healthcare organizations
Security Deliver security that performs effectively and is robust and usable	▪ Limited mobile device compute power ▪ Surge in sensitive data to protect ▪ Many alternatives

safeguards proactively to mitigate the risks to acceptable levels. Risk assessments done well, and regularly, can also help healthcare organizations maximize the value of the limited budget and resources available for privacy and security, thereby providing additional value beyond regulatory or standards compliance. Once adequate safeguards are in place, if a security incident does occur, the business impact can be avoided or minimized.

Historically, many healthcare organizations have taken a perimeter approach to privacy and security, depending heavily on perimeter defenses such as network firewalls and physical buildings, with little or no security applied within this perimeter. However, this approach is becoming increasingly inadequate due to several factors, including the following:

- Emerging trends, such as mobile health, provide anywhere and anytime access to sensitive healthcare data inside the perimeter.
- Cloud computing moves the sensitive data out of the traditional perimeter of the healthcare organization and into the cloud provider's data center.
- Sophisticated malware outbreaks often occur within the perimeters of healthcare organizations.

A practical strategy is to secure the sensitive data directly, wherever that data is—at rest or in transit—even within the traditional security perimeter. For example, it is unwise to assume that a database containing sensitive healthcare data doesn't need to be encrypted simply because it is inside the firewall or protected by the physical security of the data center building.

While the importance of protecting confidentiality in healthcare information is generally well accepted, given the media's attention to breaches, the need to protect the integrity of sensitive healthcare data—for example, to enable its use in evidence-based medicine—is less understood. Risks such as medical claims fraud can compromise both the integrity of the patient medical record and the quality of care that a patient subsequently receives. Similarly, protecting the availability of sensitive healthcare data is important for urgent patient care, an area in which delayed or unreliable access to patient records can also compromise the quality of patient care.

Safeguards chosen to mitigate risk should be considered from the standpoint of confidentiality, availability, and integrity. For example, thin-client models can effectively mitigate the risk of breach resulting from the loss or theft of mobile devices by storing sensitive healthcare data on strongly managed and secured back-end servers, instead of on mobile clients. However, thin-client models can introduce availability risks if networks are not 100-percent available or are not responding efficiently.[2]

Keeping privacy and security policies up to date, accurate, and complete is critical to establishing strong privacy and security practices. Risk assessments that are undertaken based on this policy foundation can provide value in regulatory or standards compliance and also serve as a practical tool, guiding the allocation of funds available for privacy and security in a prioritized and measured way that reduces the most business risk.[3] Beyond risk assessments, improving the security posture of a healthcare organization depends on addressing security deficiencies identified in the risk assessments and implementing any prescribed security controls.[4]

The human factor is critically important in privacy and security procedures. Even with the best technical security in place, users must comply with these procedures; otherwise, they can become the weakest link in security. This is especially important given trends such as consumerization/ bring your own device, and social media

that are empowering end users with many attractive and powerful, but potentially risky, alternatives. Strong administrative controls, including policy, procedures, training, auditing, and compliance, can help mitigate these risks. Robust privacy and security procedures increasingly also require good detect-and-respond capabilities in order to identify and resolve potential vulnerabilities and security incidents, eliminating or minimizing their impact on the business.

User Experience

Every healthcare worker's primary goal is to provide high-quality health care to patients. However, if security controls stand in the way of delivering that care, clinicians may seek other ways to access the information they need, even if those methods create security risks.

Our experience conducting ethnographic research in healthcare over the last six years provides some real-world examples of the choices clinicians make when faced with the conflict between dealing with what they view as burdensome security systems and providing patient care.

- When attempting to access records, the process of full disk encryption may create extended wait times. This delay may be unacceptable during times when medical attention is urgently needed or visit times are condensed. Clinicians may resort to writing notes on paper, which can increase the risk of loss or a privacy breach. Other strategies to improve ease of access to data, such as storing data on portable drives or personal devices, are similarly prone to loss and exposure.
- A login that requires two-factor authentication with a separate hardware token is cumbersome and adds to clinician workload. We have observed clinicians sharing an authentication token to allow entry into the electronic medical records, after one of them lost his authentication token. The clinician was reluctant to report the lost token because he had already lost another token earlier in the month. Others have reported breaking tokens and forgetting them, and nearly all complain that using tokens is time consuming and frustrating.
- Clinicians who have access to more than one electronic health record (EHR), such as specialists who consult with multiple health systems, express frustration over having to remember and enter a different user ID and password each time they access patient records. To save time, they write down the passwords and keep them in their wallet or at their desk, leading to the possibility of loss or inappropriate use.
- The inability to effectively manage a large fleet of PCs, some of which may be powered down, inoperable, or in the hands of remote clinicians, can create vulnerabilities and increase risk. For example, during our field work with mobile clinicians, we observed one healthcare worker whose PC had a backlog of 64 patches waiting to be installed.

In an effort to streamline workflows and deliver timely medical care, clinicians have begun using personal smartphones, tablets, USB keys, and other devices. These devices may contain both professional and personal data and apps and may even have multiple users, including family members. For example, we have observed clinicians using personal email and file transfer services to confer with colleagues or transmit patient data. A hospital-based nurse we interviewed said she used her personal phone to text orders from physicians, but then had to remember to delete the texts before leaving work for the day.

Use of alternatives can lead to a proliferation of data—including files on USB keys, undocumented repositories of data, or undeleted emails—that inventory processes may inadvertently overlook,

Clinician Security System Challenges

- ❑ When attempting to access records, the process of full disk encryption may create extended wait times.
- ❑ A login that requires two-factor authentication with a separate hardware token is cumbersome and adds to clinician workload.
- ❑ Clinicians with access to more than one EHR must remember and enter a different user ID and password each time they access patient records.
- ❑ Inability to effectively manage a large fleet of PCs can create vulnerabilities and increase risk.

leaving that data unsecured. Implementing security methods that provide an excellent level of performance, are robust and usable, and enable an optimum user experience will in turn lead to improved compliance and lower risk. Challenges to achieving this goal include addressing the compute demands of strong security controls and the limited compute power of mobile devices, and protecting the surge of sensitive data on servers and in the cloud, driven by trends such as migration to EHRs, health information exchange, genomics, and high-resolution digital pathology.

Hardware-Assisted Security

HAS can help improve the healthcare user experience of security by improving technical security controls with acceleration, hardening, improving usability, or lowering the total cost of ownership (TCO). Intel® technology, available today for healthcare organizations, can be a part of this solution and can become a critical component of an HAS approach.

Acceleration

A good example of technology that uses performance acceleration is Intel® Advanced Encryption Standard - New Instructions (Intel® AES-NI),[5] which accelerates encryption and decryption. Another example is Intel® Solid-State Drives with AES embedded encryption. These technologies help to enable the strong protection of encryption while preserving performance.

Hardening

The use of HAS can also help harden security controls and make them robust, helping to deter increasingly sophisticated malware. By protecting security controls, healthcare systems are kept healthy, so they are always up and running when healthcare workers need them.

- Intel® Trusted Execution Technology (Intel® TXT).[6] Measures the firmware, BIOS, and hypervisor, and compares values to known good values stored in a Trusted Platform Module to ensure they have not been compromised by sophisticated malware such as rootkits.
- Intel® Virtualization Technology (Intel® VT).[7] Enables the detection, blocking, and removal of sophisticated malware such as kernel mode rootkits, even beyond the OS in security solutions such as McAfee Deep Defender* and McAfee DeepSAFE* technology.
- Intel's Execute Disable Bit (XD).[8] Helps prevent certain classes of malicious buffer overflow attacks when combined with a supporting OS.
- Intel® OS Guard. Protects the OS from applications that have been hacked by preventing an attack from being executed from application memory.
- Intel® Secure Key.[9] A hardware-based random number generation technology that provides high-quality, high-performance entropy and random number generation that can be used for generating high-quality keys for cryptographic protocols used in encryption.
- Intel® Anti-Theft Technology.[10] A robust, hardware-based remote locking technology that helps IT lock lost or stolen laptops, even if thieves attempt to re-image the OS, change boot order, or install a new hard drive.

Usability

HAS can also improve the usability of security safeguards. For example Intel® Identity Protection Technology (Intel® IPT)[11] helps enable strong two-factor authentication without the use of separate hardware tokens that can introduce usability issues and become lost, stolen, or broken.

Healthcare solutions often run on remote PCs, workstations, or entry-level servers that may be powered down or inoperable. Intel® vPro™ technology[12] with Intel® Active Management Technology (Intel® AMT)[13] enables such systems to be securely and remotely managed, even if they are in a powered-down state, or inoperable because of an OS crash or malware infection. Through secure remote management for tasks such as patching, inventory, remediation, and diagnostics, healthcare solutions on these systems can be kept up and running, creating a reliable and optimum user experience for healthcare workers.

Cost

HAS can also improve the user experience from a TCO standpoint. HAS technologies were previously implemented using separate hardware, which incurred additional costs for healthcare organizations. For example, separate encryption and decryption accelerator cards or appliances were traditionally used to accelerate encryption and decryption. Intel AES-NI, which meets those same needs, is now embedded in the latest generations of Intel® Core™ and Intel® Xeon® processors. The use of Intel IPT also helps further cost reduction by making a separate hardware token for two-factor authentication unnecessary, thereby eliminating associated separate hardware costs, and provisioning and decommissioning costs.

Vertically Integrated Solutions

Maintaining the confidentiality of patient data is not only a legal and regulatory requirement, but also crucial in maintaining a patient's confidence in his or her healthcare provider. Security solutions from McAfee have been protecting healthcare organizations worldwide for many years, helping to preserve the confidentiality, integrity, and availability of information. These solutions include the deployment of encryption on devices that healthcare professionals use.

Remote healthcare workers must have support for local storage of patient information on mobile systems, which pose a risk to the healthcare provider should a lost or stolen device result in a breach of patient confidentiality. To help mitigate this risk, McAfee Endpoint Encryption encrypts data while it is stored at rest on the device. This approach helps ensure patient confidentiality even if a device is lost or stolen.

McAfee Endpoint Encryption has been successfully deployed throughout many industries, including healthcare. Intel AES-NI accelerates and hardens McAfee Endpoint Encryption, producing a vertically integrated encryption solution that performs efficiently, enabling healthcare workers to access healthcare information more quickly. This encryption solution is also resilient to sophisticated attacks such as side channel attacks, helping to maintain the confidentiality of sensitive healthcare data and to avoid security breaches.

To ensure adherence to privacy and security policies and data governance rules, the implementation of data loss prevention (DLP) technology has been prevalent in healthcare. In addition to helping prevent breaches from accidental disclosure of sensitive healthcare data, DLP is used to educate healthcare workers through "teachable moments" about potential security incidents and the policies and data governance rules within the healthcare organization.

When integrated with classification software, the DLP solution is able to interact with healthcare professionals to prompt the classification of newly created files. Moreover, any attempt to circumvent policies can raise an exception that may require the user to explain the reasons for his or her actions. This is important in ensuring that technology does not prevent healthcare workers from conducting their daily activities, but does hold them accountable for their actions, with deviations from policy tracked in support of auditing and compliance activities. The McAfee Data Loss Prevention 4400* appliance is vertically integrated with Intel® Xeon® processors X5660. These processors also have HAS, including Intel AES-NI, Intel VT, Intel TXT, and XD, that can help to accelerate and harden security for a better end-user experience.

Medical devices, such as diagnostic tablet computers, heart rate monitors, and MRI scanners, are just as susceptible to malware as standard laptop computers. To protect medical devices, McAfee offers solutions that help prevent unauthorized changes and help keep devices malware-free. McAfee Integrity Control* locks down a medical device, allowing only authorized executables and changes. This low-footprint solution helps protect against malware, unauthorized applications, and system changes. It also provides the ability to capture an audit trail of authorized changes, facilitating compliance and reporting. McAfee Integrity Control provides unique read/write protection for added data protection of field devices. This feature blocks the view and alteration of system data and configuration files from any application other than the original creator of the data. For manufacturers of medical devices, McAfee offers these same capabilities with McAfee embedded security solutions.

McAfee ePO* software Deep Command* is vertically integrated with Intel vPro technology with Intel AMT and provides secure remote management access to PCs, even those that may be powered off or disabled. Tasks such as patching can be conducted in a more efficient manner, accelerating time to patch saturation and reducing the window of opportunity for malware based on new vulnerabilities.

Some organizations have experienced malware outbreaks that have resulted in the loss of availability for key systems. In healthcare organizations, these types of incidents can negatively affect healthcare professionals, and ultimately the patient, especially in the case of urgent patient care. The threat landscape for malware based on the "McAfee Q1 2012 Threat Report" suggests the volume of malware is increasing.[14]

The proliferation of malware across multiple devices appears to be continuing with a corresponding increase of malware for mobile platforms. To manage and protect against the many threats, McAfee has implemented Global Threat Intelligence (GTI), which provides predictive security by forecasting or predicting

> Going into 2012 we had collected more than 75 million samples in our combined "malware zoo," but with the tremendous growth this quarter we have already topped 83 million pieces of malware. We don't know when we will top the 100 million mark, but it will certainly happen in the next few quarters. With increases in rootkits and their functionality, signed malware, and rampant growth across most other threat vectors, 2012 might prove to be a bumpy year on the security superhighway.
>
> *McAfee Threat Report Q1 2012*

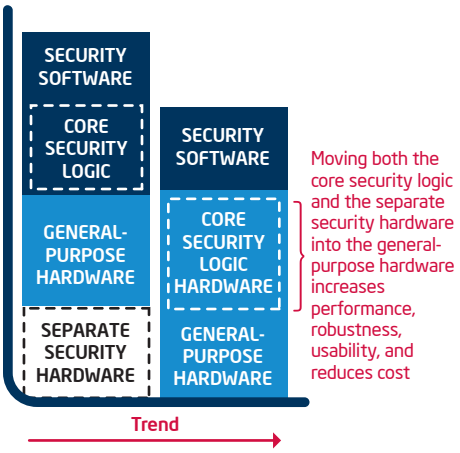


Figure 1. Future trends in hardware-assisted security.

the potential threats based on prevalence, reputation, and the type of content. By taking advantage of the collective intelligence gathered across all threat vectors—network, Web, email, and vulnerabilities—and with millions of real-time sensors deployed, McAfee can identify threats and deliver protection mechanisms potentially even before the threats get to the user.

McAfee released McAfee DeepSAFE technology, a vertically integrated solution that is designed to protect the stack against advanced malware, such as rootkits. McAfee and Intel jointly developed McAfee DeepSAFE technology, which uses Intel VT, enabling McAfee to use HAS that enables a deeper security footprint. This provides a new method to block sophisticated advanced persistent threats and stealth techniques in real time. Moreover it provides the ability to uncover threats that traditional OS-based security does not detect.

The Security Connected for Healthcare Providers strategy enables McAfee customers to manage day-to-day security issues more efficiently. By moving from a reactive mode, they can respond in real time to real world threats, diverting their resources to more valuable work. This strategy also helps healthcare organizations improve day-to-day processes, enhance productivity, and meet their business objectives. Implementing an integrated, correlated security approach can actually reduce costs by 62 percent, making it a business as well as an IT initiative.[15]

Looking Forward to the Future

McAfee and Intel remain committed to close collaboration on security to continue delivering leading vertically integrated security solutions that provide strong security suitable for healthcare, while also enabling a great healthcare worker user experience, improved compliance, and lower risk. HAS security is targeted for future processors across the compute continuum, from smartphones to tablets, laptops, Ultrabook™ devices, and servers. As major advances in hardware such as Intel® 22nm 3-D Tri-Gate Transistor Technology are delivered, HAS will deliver even better performance and more power efficiency, enabling improved user experience across the compute continuum.

In the future, more core security logic will be implemented in hardware, providing improved performance, robustness, usability, and lower cost, as shown in Figure 1. This technology will also include consolidation of separate security hardware, such as separate encryption acceleration hardware and two-factor authentication tokens, into core security logic embedded in processors across the compute continuum. Core security logic provides a maximally standards-compliant, open platform that software ecosystem can integrate with in order to implement vertically integrated security solutions, such as those from McAfee and Intel.

BEST PRACTICES CHECKLIST FOR IMPLEMENTING MOBILE DEVICES

1. Awareness

- ❑ What are your trends and privacy and security risks?
- ❑ Risk assessment: What safeguards do you need?
- ❑ What is hardware-assisted security, and how can it help you?

2. Inventory

- ❑ What hardware platforms do you have with hardware-assisted security?
- ❑ What McAfee products and versions do you have that can make use of hardware-assisted security?

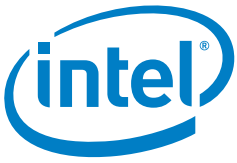
3. Activations

- ❑ Configuration completed; for example, BIOS switch
- ❑ Setup steps completed

Learn more about security technologies and products

PRODUCT	URL
Intel® Advanced Encryption Standard - New Instructions (Intel® AES-NI)	www.intel.com/content/www/us/en/architecture-and-technology/advanced-encryption-standard--aes-/data-protection-aes-general-technology.html
Intel® Solid-State Drives with advanced encryption standard embedded encryption	www.intel.com/content/www/us/en/solid-state-drives/solid-state-drives-320-series.html
Intel® Trusted Execution Technology (Intel® TXT)	www.intel.com/content/www/us/en/architecture-and-technology/trusted-execution-technology/malware-reduction-general-technology.html
Intel® Virtualization Technology (Intel® VT)	www.intel.com/content/www/us/en/virtualization/virtualization-technology/hardware-assist-virtualization-technology.html
McAfee Deep Defender*	www.mcafee.com/us/products/deep-defender.aspx
McAfee DeepSAFE* technology	www.mcafee.com/us/solutions/mcafee-deepsafe.aspx
Intel's Execute Disable Bit (XD)	www.intel.com/technology/xdbit/index.htm
Intel® OS Guard and Intel Secure Key®	http://download.intel.com/newsroom/kits/core/3rdgen/vpro/pdfs/3rdGen_Core_vPro_FactSheet.pdf
Intel® Anti-Theft Technology	www.intel.com/content/www/us/en/architecture-and-technology/anti-theft/anti-theft-general-technology.html
Intel® Identity Protection Technology (Intel® IPT)	www.intel.com/content/www/us/en/architecture-and-technology/identity-protection/identity-protection-technology-general.html
McAfee Endpoint Encryption*	www.mcafee.com/us/products/endpoint-encryption.aspx
McAfee Data Loss Prevention* (DLP)	www.mcafee.com/us/products/data-protection/data-loss-prevention.aspx
McAfee Integrity Control*	www.mcafee.com/us/products/integrity-control.aspx
McAfee embedded security solutions	www.mcafee.com/us/solutions/embedded-security/embedded-security.aspx
McAfee ePO* software Deep Command*	www.mcafee.com/us/products/epo-deep-command.aspx
McAfee Q1 2012 Threat Report	www.mcafee.com/us/resources/reports/rp-quarterly-threat-q1-2012.pdf
Global Threat Intelligence (GTI)	www.mcafee.com/us/mcafee-labs/technology/global-threat-intelligence-technology.aspx
Security Connected for Healthcare Providers	www.mcafee.com/us/resources/solution-briefs/sb-security-connected-for-healthcare-providers.pdf
Intel® 22nm 3-D Tri-Gate Transistor Technology	www.intel.com/content/www/xa/en/energy/intel-22nm-3-d-tri-gate-transistor-technology.html

For more information on IT best practices for healthcare, see:
http://premierit.intel.com/community/ipip/healthcare



[1] Ponemon research, "2011 U.S. Cost of a Data Breach Study." www.symantec.com/content/en/us/about/media/pdfs/b-ponemon-2011-cost-of-data-breach-us.en-us.pdf

[2] Learn more about consumerization and protecting healthcare data by reading the Intel white paper "Healthcare Information at Risk: Consumerization of Mobile Devices." www.intel.com/content/dam/www/public/us/en/documents/solution-briefs/securing-mobile-devices-in-healthcare-solution-brief.pdf

[3] Learn more about improving risk assessments in healthcare organizations by reading the Intel white paper "Improving Risk Assessments to Maximize Security Budgets." http://premierit.intel.com/servlet/JiveServlet/download-Body/6498-102-1-9661/Improving%20Healthcare%20Risk%20Assessments%20to%20Maximize%20Security%20Budgets.pdf

[4] "Improving Your Healthcare Organization's Security Posture," Intel Healthcare IT Professionals blog post (May, 2012.) http://premierit.intel.com/community/ipip/healthcare/blog/2012/05/23/improving-your-healthcare-organization-s-security-posture

[5] AES-NI is a set of instructions that consolidates mathematical operations used in the Advanced Encryption Standard (AES) algorithm. Enabling 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. For availability of AES-NI enabled processors or systems, check with your reseller or system manufacturer.

[6] No computer system can provide absolute security under all conditions. Intel® Trusted Execution Technology (Intel® TXT) requires a computer system with Intel® Virtualization Technology, an Intel TXT-enabled processor, chipset, BIOS, Authenticated Code Modules, and an Intel TXT-compatible measured launched environment (MLE). Intel TXT also requires the system to contain a TPM v1.s. For more information, visit www.intel.com/technology/security.

[7] 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 www.intel.com/go/virtualization.

[8] Enabling Execute Disable Bit functionality requires a PC with a processor with Execute Disable Bit capability and a supporting operating system. Check with your PC manufacturer on whether your system delivers Execute Disable Bit functionality.

[9] No system can provide absolute security. Requires an Intel® Secure Key-enabled PC with a 3rd generation Intel® Core™ vPro™ processor and software optimized to support Intel Secure Key. Consult your system manufacturer for more information.

[10] No computer system can provide absolute security under all conditions. Intel® Anti-Theft Technology (Intel® AT) requires the computer system to have an Intel AT-enabled chipset, BIOS, firmware release, software and an Intel AT-capable service provider/ISV application and service subscription. The detection (triggers), response (actions), and recovery mechanisms work only after the Intel AT functionality has been activated and configured. Certain functionality may not be offered by some ISVs or service providers and may not be available in all countries. Intel assumes no liability for lost or stolen data and/or systems or any other damages resulting thereof.

[11] No system can provide absolute security under all conditions. Requires an Intel® Identity Protection Technology-enabled system, including a 2nd gen Intel® Core™ processor enabled chipset, firmware and software, and participating website. Consult your system manufacturer. Intel assumes no liability for lost or stolen data and/or systems or any resulting damages. For more information, visit http://ipt.intel.com.

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

[13] 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 www.intel.com/technology/platform-technology/intel-amt/

[14] "McAfee Threats Report: First Quarter 2012." McAfee Labs. www.mcafee.com/us/resources/reports/rp-quarterly-threat-q1-2012.pdf

[15] Insight Express survey, June 2007. "Thinking Security Connected: The Essential Guide to Mitigation Risk and Optimizing Your Enterprise." McAfee. www.mcafee.com/uk/campaign/security-connected

Printed in USA 0712/DHOU/KC/LP/250 ♻ Please Recycle 327473-001US