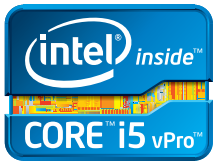
WHITE PAPER
Intel® Core™ vPro™ Processors
Endpoint Encryption

Protect Your Company's Data with Efficient Encryption and Secure Remote Management

Integrated hardware-software solutions from Intel and McAfee help you keep remote PCs and data safer with accelerated encryption and secure remote access to PCs powered by Intel® Core™ vPro™ processors.[1]



One of the top sales representatives from your company has just left a sales call in another city. She walks into a crowded downtown coffee shop, puts her laptop bag down on the floor while paying for her coffee, and then walks out without the laptop. Later that same day, a user in a remote office calls IT because his computer is infected with malware and won't start properly. And yet another user calls because he's forgotten his password.

Sound familiar? You're not alone. Companies are relying more and more on a highly mobile workforce. By 2015, the world's mobile worker population will reach 1.3 billion, representing 37.2 percent of the total workforce, according to a study by IDC.[2] But as companies become increasingly mobile, the risks of losing data from lost or stolen laptops will continue to grow, making it increasingly difficult for organizations to meet internal and regulatory security compliance requirements.

IT administrators need an effective way to protect laptops and keep data secure without dragging down user productivity. But those same protections also need to extend to files, folders, and removable drives in order to secure data in all locations and forms—whether at rest or in motion—to better protect the organization and meet government and industry compliance mandates.

Administrators and support staff also need to ensure that PCs—regardless of their location in the world—are kept up to date with operating system and security updates, in addition to driver and application patches. And in worst-case situations where problems arise or malware takes hold of a system, administrators need an effective way to support the remote system and remediate the threat quickly, without the high costs and lost productivity incurred from on-site visits or shipping remote PCs back to corporate headquarters.

Improve Data Protection and Simplify Security Management

Most of the device management and security solutions available today require piecing together software and hardware components from multiple vendors.

These fragmented solutions can be difficult and costly to configure, manage, and support and can leave risky gaps in your overall security posture.

Intel and McAfee (a wholly owned subsidiary of Intel) have collaborated to create a unique, integrated solution: strong, hardware-enhanced security features integrated with comprehensive security management software. The joint solution is built around PCs and Ultrabook™ devices powered by Intel® Core™ vPro™ processors. McAfee® Endpoint Encryption software takes advantage of the hardware-enhanced encryption provided by Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI) to deliver strong, efficient protection for your computer drives, files, folders, and even removable media, including USB drives, CDs, and DVDs.[3] When combined with McAfee ePolicy Orchestrator® (McAfee ePO™) Deep Command, the result is a comprehensive solution that delivers full control of remote PCs for out-of-band patch management, problem remediation, update distribution, and password resets—all with secure, pre-boot connectivity from a single management console.

By using innovative, integrated solutions from Intel and McAfee, you can reduce complexity and effort for your IT support staff, minimize downtime caused by malware remediation, and lower energy costs by remotely starting PCs for scheduled updates during non-peak hours. At the same time, the joint solution can help increase security, energy efficiency, productivity, and compliance, which can make you a hero to your cost- and reputation-conscious CIO.

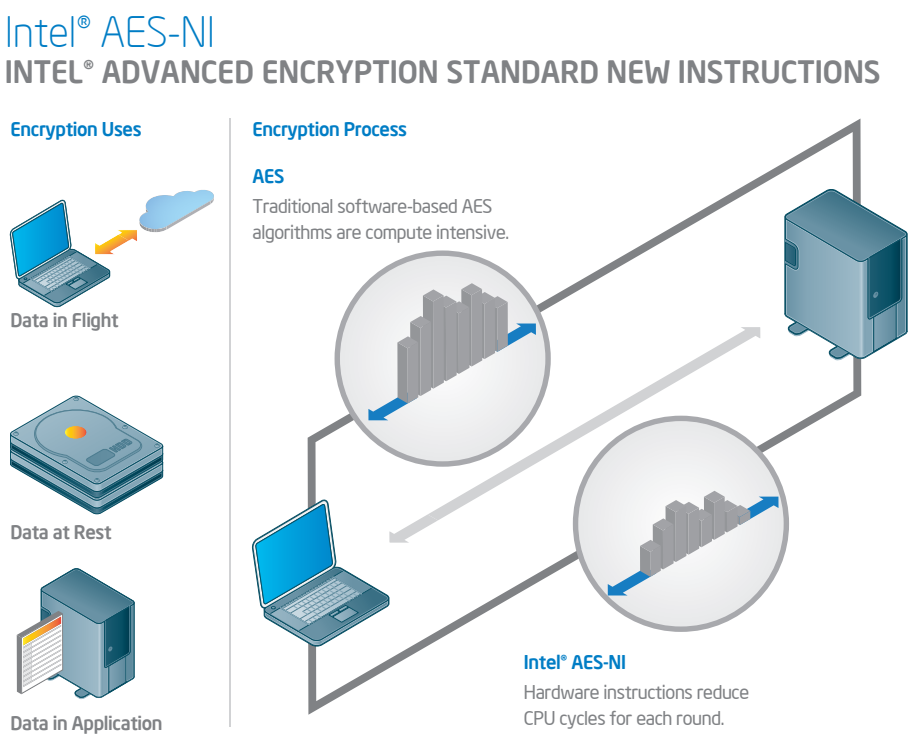


Figure 1: Intel® AES-NI accelerates encryption for efficient protections with faster performance

Accelerate Encryption for Drives, Folders, and Files

Encryption is at the heart of a complete endpoint security solution. When you safeguard the data, you reduce the risk of compromising sensitive customer or employee information, confidential files, and your company's reputation. According to a recent study by Gartner, "The encryption of information stored on endpoints is one of the most effective security controls to protect stored information from unauthorized access, especially when devices are lost or stolen."[4] Unfortunately, many organizations are hesitant to widely deploy encryption because it can significantly impair performance. Advanced Encryption Standard (AES), for example, has been used worldwide for years as a highly effective solution for protecting data, but the AES encrypting and decrypting operations can be resource intensive.

In response to this challenge, Intel has developed Intel AES-NI, an instruction set found in Intel® Core™ processors and latest-generation Intel® Atom™ processors that increases encryption and decryption performance and reduces processor load. As shown in Figure 1, by implementing some intensive substeps of the AES algorithm into the hardware,

Intel AES-NI accelerates execution of the AES application, while also reducing vulnerability to side-channel attacks.

When you deploy McAfee Endpoint Encryption solutions to devices powered by Intel Core processors, you automatically provide your users with strong, hardware-enhanced encryption from Intel AES-NI with minimal performance impact and no additional configuration effort. You can achieve even greater performance gains by combining Intel AES-NI accelerated encryption with high-performance, reliable, and efficient Intel® Solid-State Drives (SSD). Intel SSDs are ideal for achieving top performance with the advantages of enhanced encryption.

Intel AES-NI eliminates barriers to widespread adoption of encryption by significantly reducing performance bottlenecks—especially when paired with efficient Intel SSDs. By applying strong encryption to drives, files, folders, and removable media, you can better protect your company assets at rest or in motion.

Enjoy Stronger, Hardware-Based Encryption

Encryption relies on strong cryptographic keys for security. Most encryption products create those keys using software-based random number generators (RNGs). Keys generated with RNG protocols can be more vulnerable to attack due to predictable or poor quality random numbers. McAfee Endpoint Encryption takes a different approach for generating stronger cryptographic keys. The solution relies on Intel® Secure Key Technology: a digital random number generator that creates more secure, truly random numbers directly on the processor chip.[5] This hardware-based process greatly strengthens encryption algorithms to keep your data safer.

Deploy and Manage Encryption Across Your Endpoints

With McAfee Endpoint Encryption, you can maintain productivity while confidently protecting data stored on office desktop PCs, remote PCs and Ultrabook devices, and even on shared network files and removable USB storage devices. And because it's fully integrated with the McAfee ePO console, you can centrally manage deployments, policy administration, password recovery, monitoring, reporting, and auditing for consistent protection and lower total cost of ownership (TCO).

Simplify Activation of New Devices

McAfee Endpoint Encryption includes new features that make it easier to identify and activate compatible devices. With the offline activation feature, you can install McAfee Endpoint Encryption, apply a preconfigured policy, and encrypt a device that does not currently have a connection to McAfee ePO. Any machine activated while offline is essentially unmanaged, until it is connected to a network where it can communicate with the McAfee ePO server. Once communication with McAfee ePO has been established, the machine moves into a managed mode.

Another new feature, pre-boot smart check, tests your pre-boot environment to verify it will work as expected. An administrator can specify that a device cannot be activated and encrypted until it has passed a test sequence that determines and confirms a working configuration for a pre-boot environment. If no viable configuration can be determined, the test fails without installing pre-boot or encrypting the drive, and it reports the failed status to McAfee ePO for an administrator to remediate.

By quickly and automatically checking systems prior to deployment, administrators can easily determine the status of new devices attempting to join the network, regardless of those devices' locations. This benefit is particularly useful in a bring-your-own-device (BYOD) environment and can result in significant savings in time and support costs.

Securely Manage Remote PCs

Strong, efficient encryption adds a critical layer of protection for your assets, but you still need to provide updates, apply patches, and enforce policies to your endpoints. And unfortunately, there are times when you need to touch individual devices for remediation of software problems, removal of malware, or even a simple password reset.

With mobile or remote users across multiple locations, it can be difficult to keep systems up to date with the latest patches and drivers. And when a problem or malware strikes, it can be difficult and costly to troubleshoot or repair a remote PC. Typically you'd need to send a technician on site or have the affected users send in their computer, which can be risky, time-consuming, and costly from shipping expenses and lost productivity. Even worse, your affected users might delay addressing the issue while they're under pressure to make a sale or complete a project, which can increase the risk or lead to more catastrophic problems if malware is present.

Security can't sacrifice productivity or efficiency, either. To keep from disrupting users, you need to install patches and manage security during off hours. But that can be difficult if your organization powers down idle machines to cut energy costs.

With McAfee ePO Deep Command, you can monitor and control remote endpoints at the hardware level, even if the device is powered off, disabled, or encrypted. From one central control panel, you can enforce security and compliance policies, deploy power management programs to conserve energy, and remediate unresponsive PCs.

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.[6] By accessing McAfee ePO Deep Command entirely through the simple, comprehensive McAfee ePO control panel, administrators can schedule policies to power on groups of remote systems, execute security tasks, and then return the endpoints to their previous power states. Intel AMT also provides centralized remote keyboard, video, and mouse (KVM) controls and boot redirection. Through the power of Intel AMT, you can even securely initiate the boot process and unlock endpoints running McAfee Endpoint Encryption in order to conduct remote security tasks without the need for user authentication.

Remediate Disabled Endpoints

Intel AMT integration with McAfee Endpoint Encryption and McAfee ePO Deep Command can significantly reduce remediation costs by allowing a help-desk technician to remotely repair a PC anywhere in the world through a network connection. Users with disabled PCs don't have to wait for a personal, off-site visit because administrators can quickly and conveniently remediate problems or restore infected systems from a central location.

By using the McAfee KVM Viewer, you can securely and fully control a remote PC's keyboard, video, and mouse to greatly simplify remediation. With McAfee ePO Deep Command communicating directly to the hardware, you can control the remote PC through power cycles and operating system reboots without breaking the connection.

By providing centralized, 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.

Schedule Off-Hours Patching and Power Management with Secure, Remote Pre-Boot

McAfee ePO Deep Command allows you to connect to remote computers to conduct security maintenance or time-intensive updates during off hours, when users will not be disrupted.

In the past, the primary way to wake PCs remotely was by using the wake-on-LAN feature, where a wakeup call was sent to the network card and passed on to the PC. But this method would leave the PC stuck at the pre-boot authentication screen, requiring a user at the remote location to authenticate.

Today, McAfee ePO Deep Command and Intel AMT simplify the remote connection process and enable secure remote access—even to encrypted PCs. McAfee ePO Deep Command initiates the process with a wake request to the client, which will then contact McAfee ePO Deep Command to request permission to boot.

Intel® vPro™ Technology

Built-in security for greater protection

Today's rapidly evolving business environment is creating a new set of security challenges. To quickly respond to these challenges and stay ahead of high-level security threats, businesses need a comprehensive suite of security solutions that address critical areas of IT security.

Intel® vPro™ technology is a set of security and manageability capabilities built into the Intel® Core™ vPro™ processor family.

Intel® Active Management Technology (Intel® AMT) enables Intel vPro technology capabilities to be accessed and administered separately from the hard drive, operating system, and software applications—in a pre-boot environment. This makes management less susceptible to issues affecting these areas and allows remote access to the PC, regardless of the system's power state or operating system condition.

Intel vPro technology also accelerates data encryption/decryption using Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI), which can encrypt data up to four times faster than standard encryption without interfering with user productivity.

Based on configured policies, McAfee ePO will deny or allow the request. If McAfee ePO sends a denial or can't be reached, the client will remain at the pre-boot screen and will not start the operating system without authentication from a user. If McAfee ePO approves the request, it will also return cryptographic information to McAfee Endpoint Encryption to unlock pre-boot securely and allow the PC to start the operating system.

Once the connection is established and authenticated, you can securely patch, reset user passwords, or perform remote remediation. With the integrated capabilities of McAfee ePO Deep Command, Intel AMT, and McAfee Endpoint Encryption, routine scans, updates, and other tasks can be scheduled for individual PCs, groups of PCs, or all computers in your enterprise, regardless of their location or operating system state, even if they are encrypted. The secure wake and sleep capabilities also allow you to implement energy savings programs for your business and pursue industry incentives to cut power consumption without compromising security.

Securely Reset Passwords

Imagine that one of your remote users comes back from a two week vacation and discovers she can't remember her password. She's now stuck in pre-boot mode, calling the IT administrator for help. In the past, she'd have to call from the computer, exchange a 16-character string with the help desk, and hope neither person misreads or mistypes a character. With McAfee Endpoint Encryption, the administrator can easily locate the user in the McAfee ePO console and change the password to a one-time password that is sent to the remote PC using Intel AMT. The user can authenticate with the one-time password, and then immediately change it to a new one. With remote password reset, a distracting, time consuming task can now be completed in little more than the time it takes your user to call IT for help.

Configure PCs to Boot Automatically Based on Location

If you need to support shared computers in areas such as office meeting rooms or hospitals, you know how difficult it can be for different users to log on each time they need access. The joint Intel and McAfee solution includes a location-aware pre-boot option that enables a PC to boot directly into the operating system seemingly without a pre-boot environment, while still retaining the protections a pre-boot environment provides. This configuration is also useful for streamlining authentication in an office when a managed device is on the internal, corporate network. When the PC is in the office, there is no need to show the pre-boot. But as soon as it leaves the office for an insecure area, the user will be required to authenticate normally.

When a device is configured for location-aware pre-boot, it reaches out to McAfee ePO during startup and asks for boot permission. If a positive response is received, it simply boots into the operating system. However, if the device cannot reach McAfee ePO or is not on an allowed network location, it will automatically show the pre-boot authentication environment. This unique feature combines convenience and usability with the secure protections of the pre-boot environment.

Powerful, Secure Remote Access from Intel® Active Management Technology (Intel® AMT)

Intel® AMT allows IT or managed service providers to better discover, repair, and protect their networked computing assets by using integrated platform capabilities and popular third-party management and security applications. Intel AMT enables IT to remotely diagnose and repair PCs, ultimately lowering IT support costs.

Intel AMT is a feature of Intel® Core™ processors with Intel® vPro™ technology.

Simplify and Unify Your Enterprise Security Management and Reporting

McAfee ePO provides a software management framework that is capable of scaling to hundreds of thousands of endpoints. Designed to support distributed architectures and security management teams, McAfee ePO software provides a unified security policy management and reporting environment for your entire McAfee security infrastructure. Now, by taking advantage of Intel AMT capabilities, it can take your policies and compliance initiatives beyond the operating system. By extending the information you can include in McAfee ePO software dashboards and reports, you can increase your visibility into each endpoint's compliance in addition to the organization's overall security posture.

Protect Your Business with Efficiency, Manageability, and a Lower TCO

Intel and McAfee deliver hardware-enhanced security solutions that provide deeper levels of protection with unprecedented efficiency, scalability, and control. By combining the hardware foundation of security from Intel Core vPro processors with strong management, protection, and encryption software from McAfee and Intel, you can help lower your security operations' costs while enhancing your overall security posture and maintaining high performance and productivity for your users.

With this broad, centralized control, security teams have stronger, more efficient options for protecting endpoints ahead of emerging threats. Systems can be updated before a potential threat reaches them, and countermeasures can be initiated remotely, reducing any impact on users while keeping data safer. The result? Easier, more comprehensive management for IT, stronger, proactive protections with greater compliance for your business, an improved experience for your users, and a lower TCO for your company.

Learn More

For more information on comprehensive hardware-based security solutions from Intel and McAfee, visit the following web sites:

McAfee Endpoint Encryption:
www.mcafee.com/us/products/endpoint-encryption.aspx

McAfee ePO Deep Command:
www.mcafee.com/us/products/epo-deep-command.aspx

Intel AES-NI:
www.intel.com/content/www/us/en/architecture-and-technology/advanced-encryption-standard--aes-/data-protection-aes-general-technology.html

Intel vPro:
www.intel.com/vpro

Intel AMT:
www.intel.com/amt

[1] 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.

[2] IDC Worldwide Mobile Worker Population 2011-2015 Forecast, doc #232073, December 2011.

[3] 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.

[4] Gartner, "Comparing Endpoint Encryption Technologies," ID:G00250256. March 2013. http://www.gartner.com/id=2397415.

[5] No system can provide absolute security. Requires an Intel® Secure Key-enabled platform, available on select Intel processors, and software optimized to support Intel Secure Key. Consult your system manufacturer for more information.

[6] Security features enabled by Intel® AMT require an enabled chipset, network hardware and software, and a corporate network connection. Intel AMT may not be available or certain capabilities may be limited over a host OS-based VPN or when connecting wirelessly, on battery power, sleeping, hibernating, or powered off. Setup requires configuration and may require scripting with the management console or further integration into existing security frameworks, and modifications or implementation of new business processes. For more information, see http://www.intel.com/technology/platform-technology/intel-amt/.

Software and workloads used in performance tests may have been optimized for performance only on Intel microprocessors. Performance tests, such as SYSmark and MobileMark, are measured using specific computer systems, components, software, operations and functions. Any change to any of those factors may cause the results to vary. You should consult other information and performance tests to assist you in fully evaluating your contemplated purchases, including the performance of that product when combined with other products.

Printed in USA 0713/JL/PRW/PDF Please Recycle 328939-001US