SOLUTION BRIEF
Intel® Core™ vPro™ Processors
Endpoint Encryption

Keep Your Client PCs Safer, Wherever They Go

Hardware-enhanced solutions from Intel and McAfee help you protect and manage remote PCs and data

The modern, mobile work style lets users access data any time from almost anywhere. But with devices and data scattered outside your physical offices, it's difficult to ensure adequate protection and secure remote management for your enterprise.

Intel and McAfee have collaborated to provide strong, hardware-enhanced security features integrated with comprehensive security management software. The result is a unique 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.

Accelerate and Manage Encryption across Endpoints

Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI)[1] is an instruction set found in Intel® Core™ processors and latest-generation Intel® Atom™ processors that increases encryption and decryption performance and reduces processor load. Intel AES-NI forms the secure backbone of McAfee® Endpoint Encryption technologies by helping users maintain productivity while protecting data on PCs, network files, removable USB storage devices, and CDs/DVDs. McAfee Endpoint Encryption also benefits from Intel® Secure Key: hardware-enhanced technology that generates truly random numbers on the processor chip to greatly strengthen encryption algorithms. And full integration with McAfee® ePolicy Orchestrator® (McAfee ePO™) software means you can centrally manage deployments, policies, password recovery, reporting, and auditing for consistent protection and lower total cost of ownership (TCO).

Securely Manage Remote PCs

With McAfee ePO™ Deep Command, you can monitor and control remote endpoints at the hardware level, even if PCs are powered off, disabled, or encrypted. Intel® Active Management Technology (Intel® AMT)[2] provides unique out-of-band management technology at the heart of McAfee ePO Deep Command. When you deploy PCs powered by Intel® Core™ vPro™ processors,[3] you can use ePO Deep Command in conjunction with Intel AMT to schedule security policies that power on, update, and then power off groups of remote systems. Even if PCs are encrypted with McAfee Endpoint Encryption, you can wake them with pre-boot authentication credentials to schedule and perform tasks.

The same technology can help you significantly reduce remediation costs by giving you the power to remotely repair PCs. Users with disabled operating systems don't have to wait for an on-site visit because administrators can quickly and conveniently troubleshoot problems or restore infected systems from a central location.

Quickly Reset Encryption Passwords Remotely

If a user forgets a password, an administrator can use McAfee ePO Deep Command and the McAfee ePO console to send a password reset command directly to the remote client. On the client side, the integration of McAfee Endpoint Encryption with Intel AMT provides a fast, secure mechanism for resetting the user password in seconds. With this unique, out-of-band feature, what used to be a distracting, time consuming task can now be completed in the time it takes your user to call IT for help.

Configure PCs to Boot Automatically Based on Location

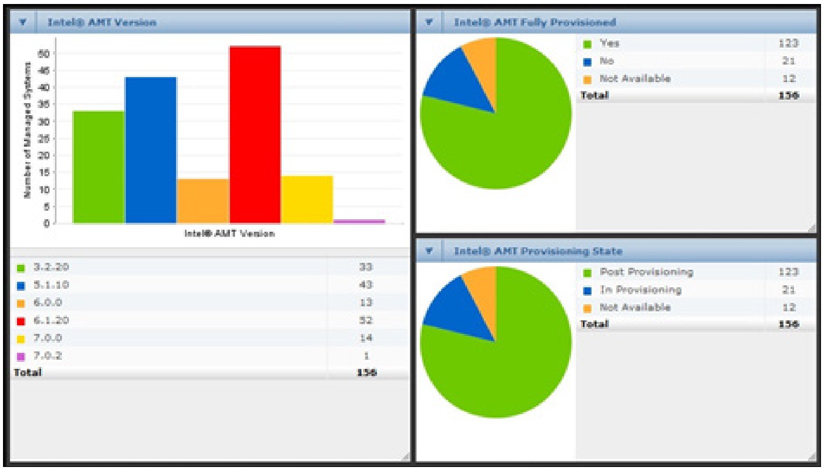
Location-aware pre-boot authentication lets you configure PCs to boot directly into the operating system based on location, seemingly without a pre-boot environment. Behind the scenes, the PC is still fully protected by encrypted authentication, but users do not need to manually authenticate as long as their PCs are on the local office network. As soon as they leave the secure environment, they are required to authenticate normally. Location-aware pre-boot authentication is also a boon to productivity and usability for employees who share computers in secure environments, such as hospitals or office meeting rooms.

Simplify Discovery and Provisioning of Intel AMT

Most enterprise IT environments comprise a wide variety of PCs. By using McAfee ePO Deep Command, administrators can quickly poll endpoints to determine which ones are equipped with Intel AMT, what versions of Intel AMT they are running, and whether the Intel AMT PCs have been provisioned. After the non-provisioned PCs with Intel AMT have been identified, McAfee ePO Deep Command can help activate Intel AMT so administrators can enjoy the full benefits of secure, remote management with controls that go beyond the operating system.

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

Intel and McAfee are uniquely qualified to provide hardware-enhanced security with comprehensive management of remote devices. The combined protections and management features of Intel AMT, Intel Core vPro processors, McAfee Endpoint Encryption, and McAfee ePO Deep Command can make you a hero to your users and IT support staff, while the improved security operations' costs, enhanced security posture, and increased efficiency will make you a hero to your CIO.


Intel® AMT Version
Number of Managed Systems
0
5
10
15
20
25
30
35
40
45
50
Intel® AMT Version
Intel® AMT Fully Provisioned
Intel® AMT Provisioning State

🟩 3.2.20	33
🟦 5.1.10	43
🟧 6.0.0	13
🟥 6.1.20	52
🟨 7.0.0	14
🟪 7.0.2	1
Total	**156**

🟩 Yes	123
🟦 No	21
🟧 Not Available	12
Total	**156**

🟩 Post Provisioning	123
🟦 In Provisioning	21
🟧 Not Available	12
Total	**156**

Figure 1: With McAfee ePO™ Deep Command, you can use the McAfee® ePolicy Orchestrator® (McAfee ePO™) console to easily discover, provision, and activate PCs that are configured with Intel® Active Management Technology (Intel® AMT)

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® 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® processors. For availability, consult your reseller or system manufacturer. For more information, see http://software.intel.com/en-us/articles/intel-advanced-encryption-standard-instructions-aes-ni/.

[2] 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.

[3] 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.

Printed in USA 0513/JL/PRW/PDF ♻ Please Recycle 328957-001US