McAfee ePO Deep Command

Reducing the cost of security operations with "beyond the OS" security management

Call a halt to desk-side visits, truck rolls, and endless helpdesk calls due to security incidents or outbreaks. Finally, security administrators can deploy, manage, and update security on powered off and disabled endpoints. McAfee® ePolicy Orchestrator® (McAfee ePO™) Deep Command™ employs Intel® vPro® Active Management Technology (AMT) for automated, beyond-the-operating system management, reducing operational costs, enhancing security and compliance, and enabling "green" practices for idle PCs.

Key Points

Optimize security
- Put protection in place ahead of threats, even if systems are powered off or using encryption

Enforce compliance
- Ensure powered off, remote, and mobile endpoints adhere to policies and configurations

Reduce IT costs
- Eliminate frequent desk-side visits and lengthy service calls

Save time
- Improve security response time through immediate access to endpoints regardless of network access status

Go green and clean
- Maintain management access and enforce compliance of powered off systems, while conserving energy

Security administrators are assailed by increasing costs, threats, and business requirements. Each desk-side visit caused by malware or other threats can cost $250. That's expensive. It's also a challenge to physically reach every user's desk. Remote offices, teleworkers, and mobile employees depend on service desk calls and overnight shipments to the service depot. These busy users often ignore problems, working on noncompliant, vulnerable systems until a catastrophic failure, a lockout, or disruption by malware.

At the same time, the endpoint threat landscape grows more dangerous by the day. Cybercriminals move quickly to exploit each new vulnerability, using botnets and websites to propagate stealthy and zero-day malware. And some malware can now deactivate operating system (OS)-level countermeasures, giving attackers command of system resources.

Adding complexity, CIOs under pressure to cut energy consumption see idle desktops as a "green" field. They would like to power off unused systems, yet need a reliable way to manage security and compliance and run IT processes—scans and updates—when these activities will least bother users.

Remote management to the rescue

Now, security administrators can communicate with and take low-level control of their endpoints, using automation and remote management to enforce security and policy compliance and reduce security operational costs. In addition to a better security posture, these controls allow adoption of power management programs to conserve energy.

Using Intel vPro AMT technology, McAfee ePO Deep Command will access endpoints without relying on the operating system. This hardware level access enables administrators to power on systems, execute security tasks, and then return the endpoints to their previous power states. McAfee ePO Deep Command can even initiate the boot process from a network disk image or execute arbitary commands. These operations can all happen automatically through the alarm clock or on demand.

By communicating with endpoints at a level beyond the operating system, ePO Deep Command allows you to configure and remediate hard-to-manage endpoints from a central site, with the familiar management platform, McAfee ePO.

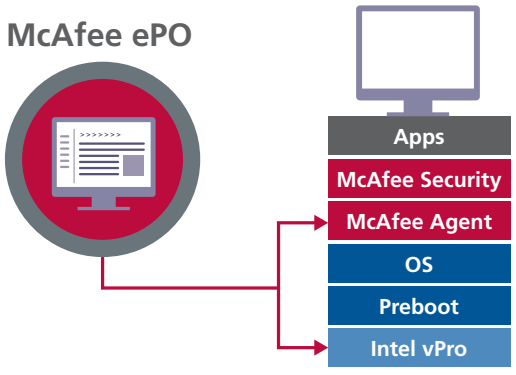

Figure 1. McAfee gains low-level control via Intel vPro.

System Requirements and Specifications

- McAfee ePO 4.6 (Discovery and Reporting Module); ePO 4.6 P1 (McAfee ePO Deep Command)
- McAfee Agent 4.5 or higher
- Supports Windows XP, Vista, Windows 7, Server 2003, and Windows 2008 operating systems
- Supports Intel vPro AMT versions 4.2, 5.2, 6.1.2, 7.0, and 7.1.4

Unlock the power of Intel vPro

McAfee ePO Deep Command helps you get the value of Intel vPro technology by leveraging the Intel Active Management Technology (AMT) alarm clock, remote wake up capabilities, and serial over LAN connections, as well as IDE Redirection.

First, the McAfee ePO Deep Command Discovery and Reporting module discovers any AMT-capable PCs in your environment. Detailed reports ensure you know exactly which PCs should receive the ePO Deep Command agent. Once ePO Deep Command is installed on provisioned AMT PCs, you are ready to begin remotely managing these PCs beyond the operating system, at the hardware level.

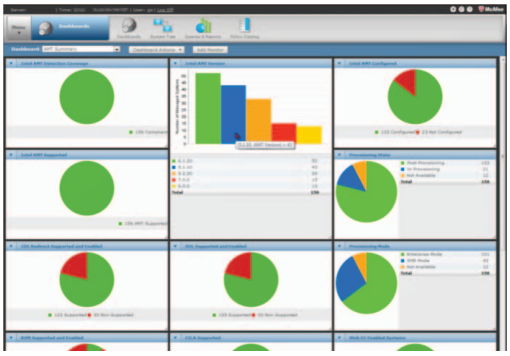

Figure 2. Dashboards can show custom query results for an overview of vPro/AMT-enabled endpoints.

Wake and execute

Administrators can now conduct security maintenance or time-intensive tasks during off hours, when end users will not be disrupted. Using the AMT Alarm Clock, security administrators can power on and wake up a PC to execute a defined series of security tasks, including:

- Security and configuration updates (including DATs)
- On-demand scans
- Scheduling of on-demand scans

Security ahead of the threats

With this broad control, security teams have new options for protecting endpoints ahead of emerging threats. Systems can be updated before a potential threat reaches them and countermeasures can be activated remotely, preventing any impact on user productivity and keeping data safe.

Out-of-band recovery of disabled endpoints

When there are problems, such as when an operating system has been disabled or a hard drive has failed, both administrators and end users will appreciate the convenience of integrated management activated by McAfee ePO Deep Command. Whether the PC is local or remote, the administrator can connect to the disabled PC via AMT to conduct a remote boot from another .ISO image on the network.

The Intel AMT Fast Call for Help function gives users an easy way to contact McAfee ePO administrators for help. The McAfee ePO administrator can quickly:

- Redirect the PC to boot from an image from another location on the network
- Collect forensics on malware
- Clean and repair infected, disabled, or quarantined systems without hands-on access

Enterprise scalability and reporting

McAfee ePO Deep Command enhances the McAfee ePO management framework, which is proven to scale to hundreds of thousands of endpoints. Designed to support distributed architectures and security management teams, McAfee ePO provides a unified security policy management and reporting environment for your entire McAfee security infrastructure. Now, it can take your policies and compliance initiatives beyond the operating system, too.

By extending the information you can include in McAfee ePO dashboards and reports, you can increase your visibility into each endpoint's compliance as well as the organization's overall security posture. Correlated data makes audit time easy.

Going green and clean

Since McAfee ePO Deep Command can wake up PCs, update policies, and then securely return them to a low power state, your business can safely embrace energy savings programs and pursue industry incentives to cut power consumption without compromising security.

Learn more at www.mcafee.com/deepcommand

McAfee
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

37802ds_epo-deep-command_1011_ETMG