McAfee ePO Deep Command

Security management beyond the operating system reduces operational costs.

Reduce desk-side visits and help desk calls due to security incidents, outbreaks, or forgotten encryption passwords. Finally, security administrators can deploy, manage, and update security on powered-off, disabled, or encrypted endpoints. McAfee® ePO™ Deep Command software[1] uses Intel® vPro™ Active Management Technology (AMT) for automated, beyond-the-operating system management that helps reduce operational costs, enhances security and compliance, and accelerates remote PC and fixed-function device remediation.

Key Advantages

- **Quickly discover and provision Intel AMT:** Easily identify Intel vPro-equipped PCs, and then enable Intel AMT for streamlined activation.
- **Secure unlock**: When coupled with the McAfee Complete Data Protection suites, McAfee ePO Deep Command can securely unlock and gain access to the preboot environment of an encrypted endpoint.
- **Reduce remediation times:** Manage remote remediation to any PC or endpoint anywhere in the world with access from the hardware.
- **Improve user productivity:** Conduct resource-intensive tasks during off hours to limit impact to end users.
- **Lower IT costs:** Eliminate frequent desk-side visits and lengthy service calls.
- **Decrease endpoint power costs:** Adopt power savings program, but still maintain access for security or patching.

Security administrators are assailed by increasing costs, threats, and business requirements. Each desk-side visit resulting from malware infection or other threats can cost up to $250. In addition to the cost, 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, lockout, or disruption by malware occurs.

At the same time, the endpoint threat landscape offers more security challenges by the day. Cybercriminals move quickly to exploit new vulnerabilities, using botnets and websites to propagate stealthy and zero-day malware. And some malware can now deactivate operating system-level countermeasures, rendering a user's PC and fixed-function devices useless.

Adding to the 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, updates, or patches—when these activities will least impact users.

How to Discover and Enable Your Intel vPro Platforms

McAfee ePO Deep Command software helps you get the value of Intel vPro technology by leveraging the Intel AMT alarm clock, remote wake-up capabilities, and keyboard, video, and mouse (KVM), as well as IDE redirection. First, the McAfee ePO Deep Command discovery and reporting module discovers any AMT-capable PCs and endpoints in your environment. Detailed reports help you pinpoint exactly which PCs and endpoints should receive the McAfee ePO Deep Command agent. McAfee ePO Deep Command software also streamlines provisioning of Intel AMT to simplify the activation of Intel AMT. Once McAfee ePO Deep Command software is installed on provisioned AMT PCs and endpoints, you are ready to begin remotely managing these beyond the operating system, at the hardware level.

intel Security

System Requirements

- McAfee ePO software 4.6 (discovery and reporting module); McAfee ePO software 4.6 (McAfee ePO Deep Command); McAfee ePO software 5.0 and above
- McAfee agent 4.5 or higher
- McAfee Drive Encryption 7.0 and above (for remote encryption management capabilities)
- Supports Microsoft Windows XP, Vista, Windows 7, 8, Server 2003, and Windows Embedded XP, 7
- Supports Intel vPro AMT versions 2.2 and above
- Intel Setup and Configuration Software (SCS) 8.2 and above

Remote Management to the Rescue

Now, security administrators can communicate with and take control of endpoints at the hardware level, whether they are powered-off, disabled, or encrypted. This connection to the hardware allows for remote management for enforcement of security or compliance policy and reduction of security operational costs. In addition to a better security posture, these controls allow for adoption of power-management programs to conserve energy while still maintaining access to endpoints. Using Intel vPro AMT technology, McAfee ePO Deep Command software accesses 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 software can even securely initiate the boot process of endpoints running McAfee Complete Data Protection software (endpoint encryption), without the need for user authentication credentials to conduct remote security tasks. These operations can all occur automatically through the alarm clock "power on" or on-demand "power on."

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

Wake and Execute

Administrators can now conduct security maintenance or time-intensive tasks during off-hours, when users are not disrupted. Using the AMT Alarm Clock, security administrators can power on and wake up endpoints, even if encrypted, to execute security tasks including, but not limited to:

- Security and configuration updates (including .DATs).
- On-demand scans.
- Install additional security products.
- Event reporting.
- Patching applications or operating system.

Remote 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 users will appreciate the convenience of integrated management activated by McAfee ePO Deep Command software. Whether the endpoint or PC is local or remote, the administrator can connect to the disabled PC or endpoint and keyboard, video, and mouse (KVM) via AMT to conduct a remote remediation action, such as instructing the PC to boot from another .ISO image on the network. In most cases, the endpoint does not have to be hard-wired to the network. McAfee ePO Deep Command can manage secure Wi-Fi-enabled endpoints.

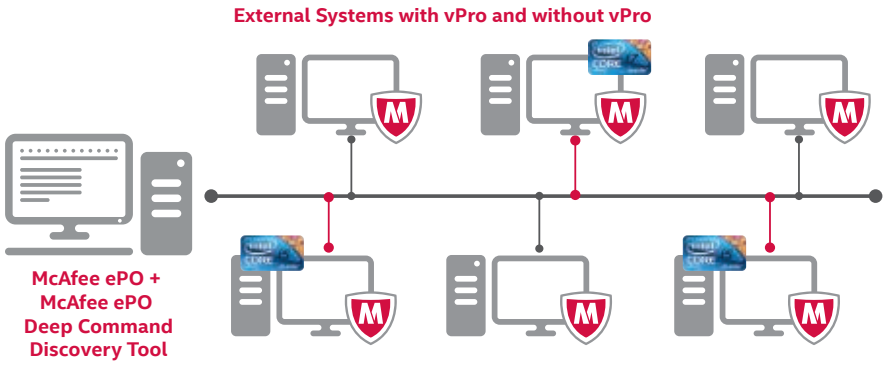

Figure 1. McAfee ePO Deep Command can discover vPro systems and deploy software to enable

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

- Redirect the endpoint to boot from an image from another location on the network.
- Completely control the local KVM.
- Reset the user's encryption password.
- Clean and repair infected, disabled, or quarantined systems without hands-on access.

Security That Stays Ahead of 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.

Lower Endpoint Power Costs

Since McAfee ePO Deep Command software can wake up endpoints, update policies, and then securely return them to their power state, your business can safely embrace energy savings programs and pursue industry incentives to cut power consumption without compromising security. Contact McAfee to see what your power savings could be.

Enterprise Scalability and Reporting

McAfee ePO Deep Command software enhances the ePolicy Orchestrator® (McAfee ePO™) software management framework, which can scale 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, it can take your policies and compliance initiatives beyond the operating system, too. By extending the amount of information you can include in McAfee ePO software 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.

Learn more at **www.mcafee.com/deepcommand**.

McAfee ePO Deep Command software is available as a standalone product and is also available in the McAfee Complete Data Protection suites. For more information, visit **www.mcafee.com/dataprotection**.

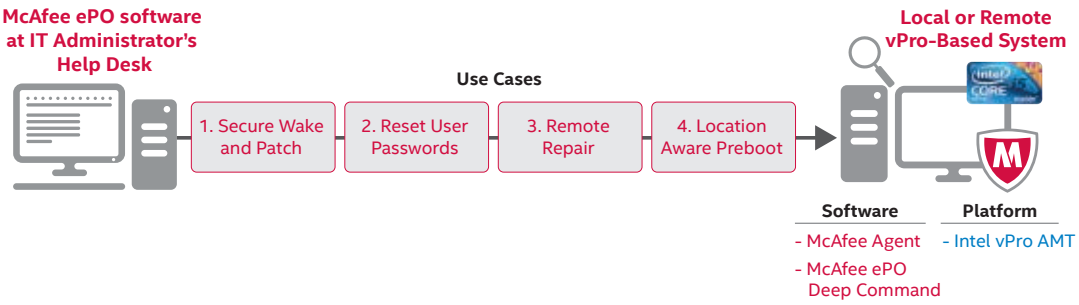

Figure 2. McAfee ePO Deep Command enables the help desk to perform a number of tasks, either locally or remotely.

1. McAfee ePO Deep Command software is available as a standalone product and is also available in the McAfee Complete Data Protection suites. For more information, visit **www.mcafee/dataprotection**.

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com

61371ds_epo-deep-command_1014_ETMG