Technology Blueprint

McAfee®
An Intel Company

# NO SLEEP FOR SECURITY

Using Intel's Active Management Technology for remote support and reliable security updates

# Using Intel's Active Management Technology for remote support and reliable security updates

## The Situation

You are not scanning your enterprise for malware often enough. Nobody is. Informal polls of customers and security professionals show that "Wednesday at noon" is the typical schedule for a full virus scan. The explanation for this timing boils down to "people are usually in the office on Wednesday and eating lunch around noon." Some outlier responses are "at night" or "every day at noon."

Why aren't more people scanning at night? Because IT finds users are shutting desktop systems down, so the scans cannot take place.

Why is "every day" not an acceptable practice? Performance. Users complain when they feel their systems are affected by security products. Oddly enough, they don't complain when their computers are slow due to 18 open web browser windows, but that's part of the challenge you face managing operational security.

## Driving Concerns

External regulations and internal expectations demand that you keep end user systems up to date, patched, and free of viruses, while users want systems running smoothly, with no noticeable performance impact. Although a highly secure and smooth-running environment should include daily virus definition updates and full scans, keeping desktop systems up to date and healthy has a number of complications:

- **User impact.** Any time you scan a file system, be it for search indexing or checking for viruses, you create I/O overhead. This drives the need to select a time that will least affect users. Lunch time is usually a good window, but after hours would be much better if you could guarantee all systems will execute the scan.
- **Limitations of built in scheduling.** Updates and scan with built in scheduling tools are usually limited to either simple tasks or hand crafted batch files. This labor-intensive approach adds management and troubleshooting overhead.
- **Green computing.** Most organizations striving for a "greener" work environment implement power conservation plans on end user systems. A powered down system will typically skip scheduled scans.
- **Regulatory compliance.** New and updated government and industry regulations are prescribing that organizations keep up to date with security functions, scanning, and virus definitions.

### Security Connected

The Security Connected framework from McAfee enables integration of multiple products, services, and partnerships for centralized, efficient, and effective risk mitigation. Built on more than two decades of proven security practices, the Security Connected approach helps organizations of all sizes and segments—across all geographies—improve security postures, optimize security for greater cost effectiveness, and align security strategically with business initiatives. The Security Connected Reference Architecture provides a concrete path from ideas to implementation. Use it to adapt the Security Connected concepts to your unique risks, infrastructure, and business objectives. McAfee is relentlessly focused on finding new ways to keep our customers safe.

Another sticky issue that IT Operations has to deal with involves resolution of end-user issues. Anyone who has spent any amount of time trying to troubleshoot a problem over the phone knows how much more difficult it is than being physically at the device. Remote access applications offer some utility, but with major limitations:

- **Connectivity.** This is really the biggest hurdle when it comes to remote access. Most remote access tools require networking to be functioning properly on the target system. If a user is having problems connecting to the network, IT will likely have difficulty launching or maintaining a remote desktop access session.
- **Misconfiguration.** What if a firewall rule has been deployed incorrectly or the user disabled (or worse, deleted) their network adapter?
- **No help during a reboot loop.** Troubleshooting someone's mail settings remotely is one thing, but how do you fix someone's system when their system won't even boot up due to a corrupted file or failed system update? Sometimes there are problems that can only be solved by booting to a known "good image." This is one of those really tough situations where help is definitely needed, usually from a location physically in front of the system.

### Decision Elements

These factors could influence your architecture:

- Do you have regular scan times that must be maintained?
- Does your helpdesk team have immediate physical access to all machines they are required to support?
- Do you have users that work remotely?
- Does your company have power savings and Green initiatives?

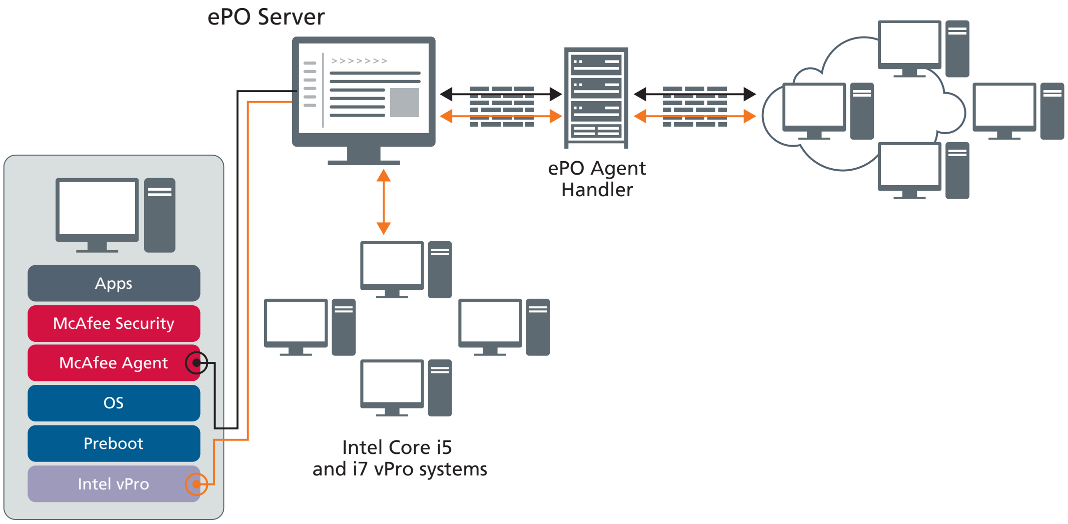
## Solution Description

All of these limitations can be overcome with the appropriate systems management technology. McAfee recommends an approach that can exist outside the operating system (OS) and can give you remote control over power. There are a few key requirements:

- **Remote power access.** To solve the problem of systems not being scanned due to being powered off, we need a solution that can either force the power on or provide reliable scheduling. Ideally, the solution would be able to follow a power on command with a security update and full antivirus scan, and then return the system to its previous state.
- **Remote console access.** If you've ever tried to help someone troubleshoot a problem, you know that sometimes the easiest and quickest way is to have a remote view into the troubled system. For constant visibility, console level access should allow the remote administrator to have access to BIOS or see start up error messages. In cases where the OS is damaged, the solution should allow the administrator to remotely boot the system to a shared disk image.
- **Operating system independent.** Most operating systems have some form of scheduling and remote access built in. Unfortunately, these tools can run into any number of problems. An effective solution will work outside the operating system, closer to the hardware, so that the limitations of the OS do not constrain the security solution's ability to operate reliably and on schedule.
- **Manageability.** Your solution should allow you to implement, monitor, update, and report on all of your endpoints from within one dashboard. Policies should be easily configurable and applied consistently across endpoints. Scheduling of management procedures should be straightforward and include options for both regular and on-demand functions.

## Technologies Used in the McAfee Solution

While waking systems to scan and providing remote repair capabilities seem like very different issues, they are both solved through McAfee integration with Intel® vPro® Active Management Technology (Intel AMT). Leveraging the McAfee® ePolicy Orchestrator® (McAfee ePO™) agent and centralized management environment, McAfee ePO Deep Command™ runs on desktops and laptops with the second generation Intel Core™ i5 and i7 vPro technologies.



McAfee ePO Deep Command provides power management and remote access beneath the operating system.

### Intel Active Management Technology (AMT)

Intel AMT is a component of Intel vPro technology available on business laptops and desktops. It provides a secure method for businesses to monitor, maintain, update, and repair PCs without direct hands-on contact. AMT is part of the onboard chipset and uses a very small amount of power to remain "always on." It provides a lengthy array of features, but for the purposes of this discussion, we'll focus on power management and remote access.

AMT gives administrators complete remote control over the power state of a system. Administrators can initiate a remote power on, power off, or reboot. AMT also has the ability to power on a system on a set schedule, for example to permit security or OS updates.

AMT on Intel Core i5 and i7 vPro systems provides hardware based keyboard/video/mouse (KVM) (a version of VNC) that is always accessible, regardless of power state. This KVM sits below the OS, allowing direct console access into the systems. This direct access is extremely useful when it comes to troubleshooting an unresponsive system. It allows you to remotely examine the BIOS or look for pre-boot error messages.

Additionally, AMT provides the ability to remotely redirect the boot sequence of a system to a networked image. Instead of having a user bring or ship a system in to be reimaged, IT can simply point the system to a clean boot image and restore the system remotely.

### McAfee ePO Deep Command

McAfee ePO Deep Command allows IT and Security operations to take the features available in Intel's AMT and deploy them into the enterprise. The first step is to get an inventory of AMT-enabled systems in your environment by running an automated task within McAfee ePO. From there, AMT simply becomes another product you can manage within ePO. Just as with other ePO operations, you can now schedule ePO tasks. With ePO Deep Command, a typical task might include powering on the system, downloading the latest antivirus definitions, performing a full system scan, and then shutting the system back down.

This task either can run as a regularly scheduled event or be initiated ad hoc in the case of a virus outbreak or high severity threat. Instead of waiting for every user to power on their systems to receive a security update against a specific threat, you can force all your systems to boot, update, and shut down. This control allows you to remain up to date on security, compliant with regulatory requirements, and supportive of green initiatives.

Also, from within the McAfee ePO console you can tell a system to boot from a networked ISO archive file, allowing you to reimage or repair a system that has been compromised or damaged. Within the McAfee ePO console, this is done by simply selecting a system and pulling the redirect option from the context-sensitive menu.

### McAfee ePolicy Orchestrator (McAfee ePO)

McAfee ePO is the centralized policy and management environment used by McAfee products as well as many McAfee partner solutions. Using McAfee ePO Deep Command, ePO provides a reporting structure that lets you assess the overall readiness of your network for ePO Deep Command deployment. Default reports include what version of AMT systems are running, whether or not systems have been provisioned, which systems have AMT versions that support full KVM, and more.

The McAfee ePO Agent provides a constant line of communication between the McAfee ePO console and the AMT functions on the chip. The McAfee ePO Agent talks directly to AMT to schedule wake up times, update information, and run other maintenance tasks.

## Impact of the Solution

At the beginning of this paper we outlined some serious concerns that organizations are facing. You have to keep systems patched, secured, and running while also dealing with power savings guidelines and support challenges for remote users.

With McAfee ePO Deep Command and Intel AMT, you can reduce the power consumption of your organization, saving money while keeping systems up to date. You can move your scan times to off hours without worry about systems being powered down. With Intel AMT you just wake systems up on a set time and let the McAfee ePO Agent update definitions, run a full scan, and then shut back down. You can keep the systems secure and reduce the complaints from users.

With Intel's AMT, you gain the ability to have control outside the operating system. You can have full KVM access to a system just like it was sitting at your desk. Through ePO Deep Command, you can even boot the system to a networked image, allowing you to reimage systems remotely.

Intel AMT is a great tool, but needs a management infrastructure to make it beneficial to enterprises. Managing tens of thousands of systems from one central location is a McAfee ePO strength. Bringing AMT management into McAfee ePO provides a way for organizations to take full advantage of the tools provided by Intel in the vPro chipset. Unfortunately, we still don't have a solution for your users' systems being bogged down by 18 web browser windows and 45 open emails.

## Q&A

### Which systems support the latest version of AMT?

The second generation Intel Core i5 and i7 vPro support the latest version of AMT, giving you access to all the features mentioned in this document.

### Is the AMT communication channel secure?

Yes. Intel AMT provides a number of methods for securing the communication including TLS-PSK, Kerberos, and others.

## Additional Resources

www.mcafee.com/deepcommand
www.mcafee.com/epo
www.mcafee.com/kb
www.mcafee.com/producttrials
www.intel.com/vPro

For more information about the Security Connected Reference Architecture, visit:
www.mcafee.com/securityconnected

## About the Author

*Bruce Snell* is director of technical marketing at McAfee. In this role he uses face-to-face discussions and webcasts to help customers understand the latest security threats and how McAfee can help them address their concerns and priorities. He also serves as an expert guest for NBC News and PBS Newshour, discussing how Trojans and rootkits spread and what everyday computer users can do to protect themselves.

Bruce has been involved in security for nearly 20 years. Prior to McAfee, he worked as an SE for Entercept Security, the first company to provide Host Intrusion Prevention through system and API call interception. His prior work included security and network administration at organizations ranging from Fortune 100 to independent design firms and advertising agencies.

McAfee®
An Intel Company

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

The information in this document is provided only for educational purposes and for the convenience of McAfee customers. The information contained herein is subject to change without notice, and is provided "AS IS" without guarantee or warranty as to the accuracy or applicability of the information to any specific situation or circumstance.