McAfee ePolicy Orchestrator* Deep Command*

Industry

IT security management across industries

Business Challenge

Comprehensive security management solution allowing complete security control, even if PCs are powered off or inaccessible through in-band channels

Technology Solution

McAfee ePolicy Orchestrator Deep Command

Enterprise Hardware Platform

PCs running the Intel® Core™ vPro™ processor family

BUSINESS AND SOLUTION DETAILS

MEETING MARKETPLACE DEMANDS

McAfee ePolicy Orchestrator Deep Command enables IT and security organizations that deploy PCs running the Intel® Core™ vPro™ family of processors to reduce costs and maintain security for endpoints that are disabled or powered off. This solution represents a new way to deliver security management beyond the operating system by enabling enterprise environments to:

- **Optimize security.** Put protection in place ahead of threats, even if systems are powered off or using encryption.
- **Reduce power usage.** Maintain management access and enforce compliance of powered off systems while conserving energy.
- **Reduce IT costs.** Eliminate frequent desk-side visits and lengthy security service calls.
- **Enforce compliance.** Ensure powered-off, remote, and mobile endpoints adhere to policies and configurations.
- **Save time.** Improve IT service levels with immediate access to endpoints regardless of network access.

BUSINESS CHALLENGE

Recent high-profile security breaches were the result of unpatched systems. The need to correctly identify systems, and the ability to apply security patches regardless of their power state, become must-haves for any organization. Since malware can move fast, the longer it takes to quarantine the compromised systems, the greater the threat to the network.

Today's PCs have traditionally been hard to remotely or automatically inventory, diagnose, and update when their power is off or their operating system (OS) is down. Users, hackers, viruses, and various threats can also disable or remove management and security agents, so IT administrators no longer have visibility or control of the PC or its hardware and software assets.

Endpoint administrators are assailed by increasing costs, threats, and business requirements. Each desk-side visit can cost USD 250 or more, accounting for the technical resources involved and user downtime .[1] It may also be a challenge for IT to 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 hang, a lockout, or disruption by malware.

Security has high operating costs and chief information security officers (CISOs) want to increase security while maintaining or reducing those costs. Also, organizations need to reduce their power consumption to lower costs and reduce the company's carbon footprint, but still need to have security access for updates and security patches, even when a PC is powered off.

Further complicating the situation, PCs using endpoint encryption can be awakened but not updated without pre-boot authentication. This increases costs and lowers overall security on endpoints due to missing patches and updates, forcing companies to choose between security management access all the time or encrypting data for security purposes.

A final thought on the common challenges faced with endpoint security management: IT operations and security staffs generally have their own tools and frameworks for monitoring and managing the same endpoints. It can be hard for one team to share its knowledge of those endpoints with the other's frameworks to keep up to date on system and application inventories. With different and separate management frameworks, operations and security teams have little visibility into the impact their actions may have on the other team's view of the environment. For instance, a security configuration change can result in unintended blockage of legitimate application activity or result in security alerts on new traffic flows.

SOLUTION OVERVIEW

McAfee is improving security management by taking advantage of hardware-based capabilities built into notebook and desktop PCs featuring Intel Core i5 and i7 vPro processors. These systems have Intel® Active Management Technology (Intel® AMT) to enable out-of-band management. McAfee ePolicy Orchestrator Deep Command uses Intel AMT to enable beyond-the-operating system security management, allowing security administrators to reduce operating costs while enhancing security. Regardless of a PC's power state, you can remotely remediate compromised systems, enable power-saving initiatives, wake and patch even encrypted systems, and apply proactive security beyond the operating system.[2]

As shown in Figure 1, McAfee ePolicy Orchestrator Deep Command communicates with both the McAfee agent and Intel AMT. The communications can occur whether internal to a corporate environment or across the Internet.

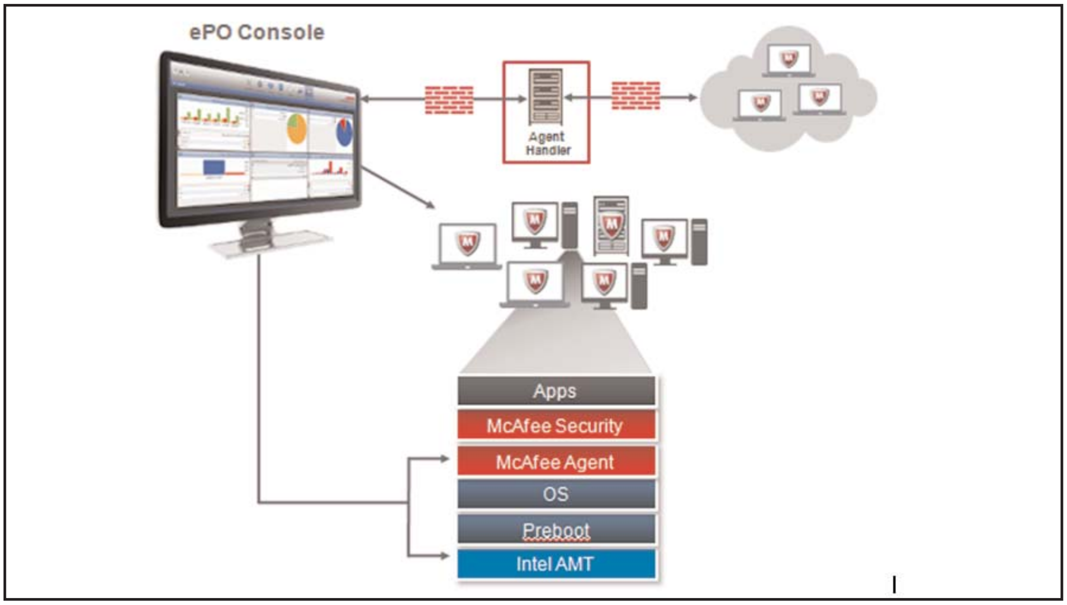


Figure 1. ePolicy Orchestrator Deep Command Connection via the Intel AMT Functionality

This new approach enables McAfee ePolicy Orchestrator users and McAfee Security Innovation Alliance (SIA) members to apply the McAfee ePolicy Orchestrator Deep Command use cases shown in Table 1.

Table 1. McAfee ePolicy Orchestrator Deep Command Use Cases

Use Case	How ePolicy Orchestrator Deep Command Is Used
Rapidly identify which computers in your organization have Intel vPro technology and Intel AMT	ePolicy Orchestrator Deep Command's free discovery and reporting module, distributed via the ePolicy Orchestrator Software Manager, identifies Intel AMT-capable systems and the versions and configuration status of those machines, plus other useful information for directing your rollout.
Deploy updated security ahead of an attack if endpoints are powered off	ePolicy Orchestrator Deep Command can contact and apply updated security policies to all Intel AMT-enabled systems before a potential threat outbreak, regardless of their power state.
Remote remediation of compromised or failed systems	ePolicy Orchestrator Deep Command enables the administrator to boot the compromised system from a remote remediation disk image, allowing full cleaning and repair of the system disk.
Reduce power consumption while still meeting security and compliance regulations	ePolicy Orchestrator Deep Command can apply security updates, patches, and new products or policies to systems by using the Intel AMT PC Alarm Clock and remote wake-up capabilities.
Users of encrypted PCs forget their passwords	McAfee ePolicy Orchestrator Deep Command and Endpoint Encryption enable remote password reset for encrypted drives via secure AMT connection.[2]
Wake and patch encrypted machines	ePolicy Orchestrator Deep Command can temporarily unlock encrypted machines for wake and patch activities.[2]
Correct misconfigured policy settings such as an accidental host firewall change limiting network connectivity	ePolicy Orchestrator Deep Command connects to the system using Intel AMT and allows remote reconfiguration of the faulty policy to reestablish normal traffic flows to and from the operating system environment.[2]

This solution is ideal for IT and security departments looking for more security management control of notebook and desktop PCs featuring Intel Core i5 and i7 vPro processors. Such companies will improve their security posture by applying beyond-the-operating-system communication and control facilities. The solution is also well suited for businesses that need to address endpoint security while simultaneously reducing power consumption, enabling them to power off computers as needed. Businesses will also gains benefits by reducing the cost of IT security operations and configuration. For McAfee users with installed McAfee Endpoint Encryption*, this solution provides an enabling framework to remotely and securely unlock the hard drive.

SOLUTION ARCHITECTURE

McAfee ePolicy Orchestrator Deep Command is an add-on module that plugs into McAfee ePolicy Orchestrator. McAfee ePolicy Orchestrator allows IT administrators to centrally manage industry-leading security for systems, networks, data, and compliance solutions from McAfee and McAfee Security Innovation Alliance (SIA) member portfolios.

McAfee ePolicy Orchestrator provides powerful workflow capabilities to increase administrators' effectiveness so they can more quickly define and deploy security as well as respond to events and issues as they arise. With McAfee ePolicy Orchestrator, administrators share information, create escalation paths, and automate remediation tasks. McAfee ePolicy Orchestrator eliminates boundaries between security, processes, and people to drive down the costs of managing security while strengthening protection.

Figure 2 shows the architecture of McAfee ePolicy Orchestrator. This distributed architecture allows for scalability and resiliency that enterprises require when managing their security. Combined with the McAfee ePolicy Orchestrator Deep Command module, even systems with a crashed hard drive, a locked operating system, or that are turned off are still accessible to perform basic system management tasks.

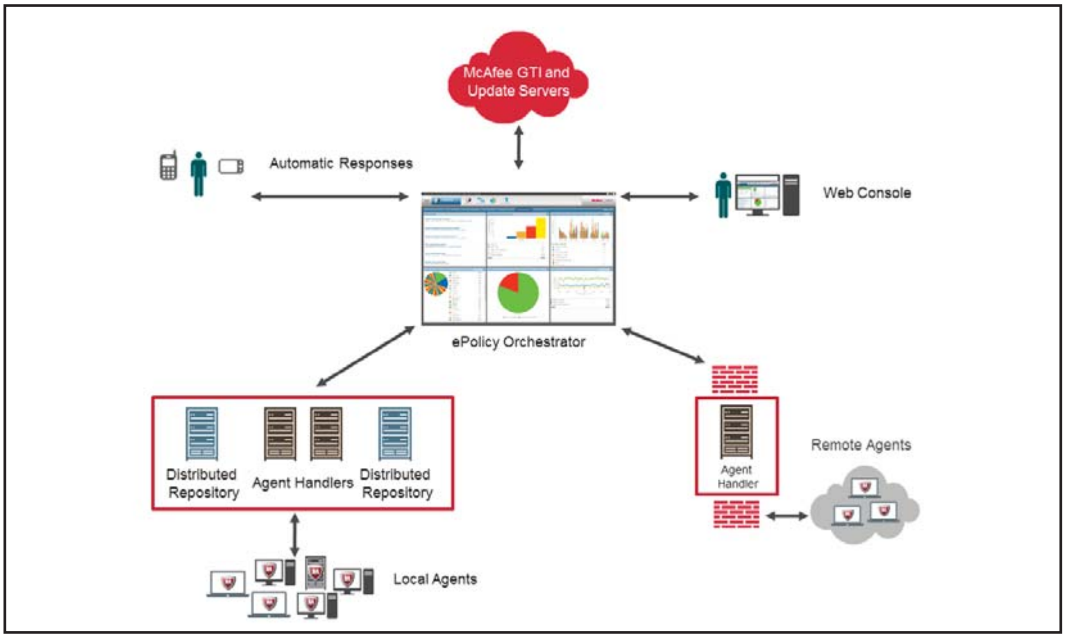


Figure 2. McAfee ePolicy Orchestrater Architecture

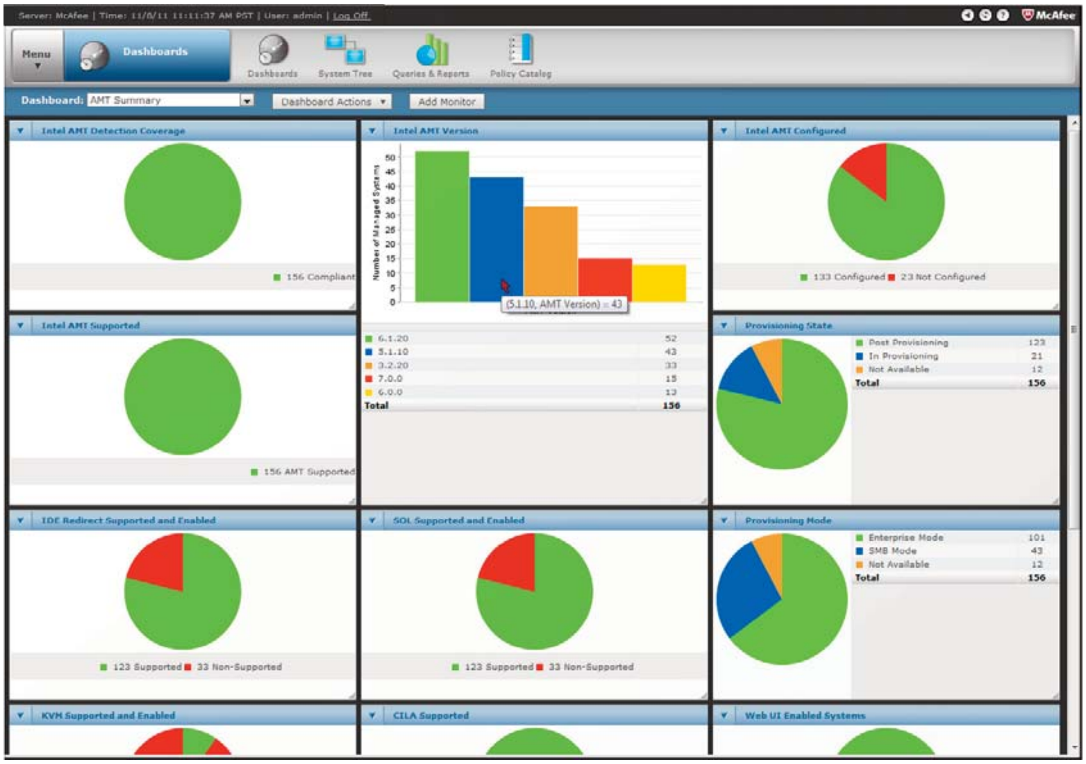
USER EXPERIENCE

The McAfee ePolicy Orchestrator Deep Command Discovery and Reporting module can be used to identify Intel AMT systems, regardless of their present configuration state. Figure 3 is a screenshot example of the AMT summary dashboard. ePolicy Orchestrator administrators can quickly identify which computers in their organization have Intel Core vPro processors, as well as the version and status of Intel AMT on each. This dashboard answers major questions for IT administrators today:

- Do I have Intel AMT-enabled systems?
- Where are they?
- What level of Intel AMT do they have?
- What is the configuration status?

This discovery module is freely available to all McAfee users via the Software Manager within ePolicy Orchestrator 4.6 or higher.

Using the dashboards shown in Figure 3, McAfee ePolicy Orchestrator users are able to identify which endpoints are enabled with Intel AMT and ready to be remotely managed with ePolicy Orchestrator Deep Command. Simply by clicking on a dashboard element, or by selecting a system from within the ePolicy Orchestrator system tree, administrators get a wealth of information at their fingertips.


Server: McAfee | Time: 11/8/11 11:11:37 AM PST | User: admin | Log Off
McAfee
Menu
Dashboards
Dashboards
System Tree
Queries & Reports
Policy Catalog
Dashboard: AMT Summary
Dashboard Actions
Add Monitor
Intel AMT Detection Coverage
🟩 156 Compliant
Intel AMT Version
Number of Managed Systems
50
45
40
35
30
25
20
15
10
5
0
(5.1.10, AMT Version) = 43
Intel AMT Configured
🟩 133 Configured 🟥 23 Not Configured
Intel AMT Supported
🟩 156 AMT Supported
Provisioning State
IDE Redirect Supported and Enabled
🟩 123 Supported 🟥 33 Non-Supported
SOL Supported and Enabled
🟩 123 Supported 🟥 33 Non-Supported
Provisioning Mode
KVM Supported and Enabled
CILA Supported
Web UI Enabled Systems

🟩 6.1.20	52
🟦 5.1.10	43
🟧 3.2.20	33
🟥 7.0.0	15
🟨 6.0.0	13
Total	**156**

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

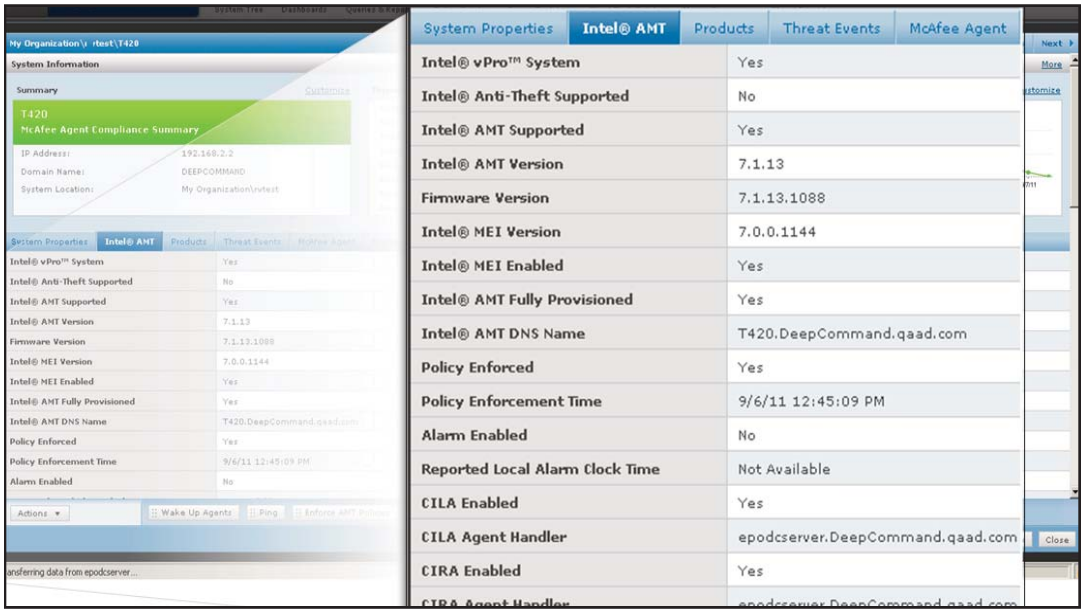
🟩 Enterprise Mode	101
🟦 SMB Mode	43
🟧 Not Available	12
Total	**156**

Figure 3. ePolicy Orchestrator Deep Command Summary Dashboard

Figure 4 shows some of the detailed information returned by ePolicy Orchestrator Deep Command's Discovery and Reporting module. ePolicy Orchestrator administrators can use this data to drive automatic provisioning, reporting, and configuration of Intel AMT-enabled systems.

Intel AMT must be enabled and operating to allow ePolicy Orchestrator Deep Command to securely interact beyond the operating system to the hardware level. Intel AMT is a hardware-based solution that uses out-of-band communication for basic management of client systems.

Figure 5 is an example of a serial over LAN connection launched from ePolicy Orchestrator to perform maintenance or remediation beyond the operating system on a PC. In this case, the administrator has used ePolicy Orchestrator Deep Command to boot a remote PC to its BIOS screen to check on a configuration setting without physically touching the target system.



My Organization\rvtest\T420

System Information

Summary

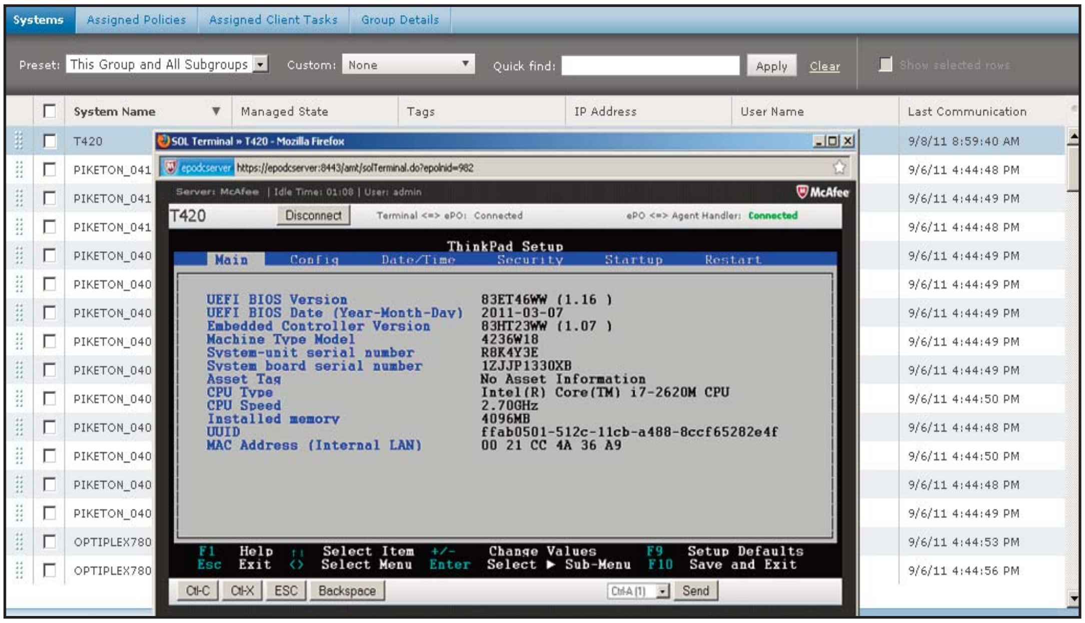
T420
McAfee Agent Compliance Summary

IP Address: 192.168.2.2
Domain Name: DEEPCOMMAND
System Location: My Organization\rvtest

Intel® vPro™ System	Yes
Intel® Anti-Theft Supported	No
Intel® AMT Supported	Yes
Intel® AMT Version	7.1.13
Firmware Version	7.1.13.1088
Intel® MEI Version	7.0.0.1144
Intel® MEI Enabled	Yes
Intel® AMT Fully Provisioned	Yes
Intel® AMT DNS Name	T420.DeepCommand.qaad.com
Policy Enforced	Yes
Policy Enforcement Time	9/6/11 12:45:09 PM
Alarm Enabled	No
Reported Local Alarm Clock Time	Not Available
CILA Enabled	Yes
CILA Agent Handler	epodcserver.DeepCommand.qaad.com
CIRA Enabled	Yes
CIRA Agent Handler	epodcserver.DeepCommand.qaad.com

ansferring data from epodcserver...

Figure 4. Intel AMT Properties



Preset: This Group and All Subgroups Custom: None Quick find:

System Name	Managed State	Tags	IP Address	User Name	Last Communication
T420					9/8/11 8:59:40 AM
PIKETON_041					9/6/11 4:44:48 PM
PIKETON_041					9/6/11 4:44:49 PM
PIKETON_041					9/6/11 4:44:48 PM
PIKETON_040					9/6/11 4:44:49 PM
PIKETON_040					9/6/11 4:44:49 PM
PIKETON_040					9/6/11 4:44:49 PM
PIKETON_040					9/6/11 4:44:49 PM
PIKETON_040					9/6/11 4:44:49 PM
PIKETON_040					9/6/11 4:44:50 PM
PIKETON_040					9/6/11 4:44:48 PM
PIKETON_040					9/6/11 4:44:50 PM
PIKETON_040					9/6/11 4:44:48 PM
PIKETON_040					9/6/11 4:44:49 PM
OPTIPLEX780					9/6/11 4:44:53 PM
OPTIPLEX780					9/6/11 4:44:56 PM

SOL Terminal » T420 - Mozilla Firefox

https://epodcserver:8443/amt/solTerminal.do?epoInid=982

Server: McAfee | Idle Time: 01:08 | User: admin

T420 Terminal <=> ePO: Connected ePO <=> Agent Handler: Connected

```
                         ThinkPad Setup
   Main       Config      Date/Time     Security      Startup      Restart

   UEFI BIOS Version                   83ET46WW (1.16 )
   UEFI BIOS Date (Year-Month-Day)     2011-03-07
   Embedded Controller Version         83HT23WW (1.07 )
   Machine Type Model                  4236W18
   System-unit serial number           R8K4Y3E
   System board serial number          1ZJJP1330XB
   Asset Tag                           No Asset Information
   CPU Type                            Intel(R) Core(TM) i7-2620M CPU
   CPU Speed                           2.70GHz
   Installed memory                    4096MB
   UUID                                ffab0501-512c-11cb-a488-8ccf65282e4f
   MAC Address (Internal LAN)          00 21 CC 4A 36 A9

  F1   Help  ↑↓  Select Item  +/-    Change Values      F9   Setup Defaults
  Esc  Exit  <>  Select Menu  Enter  Select ▶ Sub-Menu  F10  Save and Exit
```

Figure 5. Serial over LAN Connection Launched from ePolicy Orchestrator for Maintenance or Remediation beyond the OS on a PC

SECURITY CONNECTED: EPOLICY ORCHESTRATOR DEEP COMMAND

The McAfee Security Connected framework provides a strategic approach using centralized management and McAfee Global Threat Intelligence* to synchronize security, mitigate risk, and enable a comprehensive, proactive threat response across endpoints and networks, and in the cloud. McAfee ePolicy Orchestrator Deep Command supports the McAfee Security Connected framework by providing complete integration and threat response for all PCs that have been powered down or disabled, allowing security to be connected across all endpoints. By enable enterprise security both via the McAfee agent and beyond the operating system, all endpoints, whether powered on or off, from a reactive to an optimized state, enable businesses to reduce the effort and cost of managing security and make the most effective use of resources.

MORE INFORMATION

To learn more about McAfee ePolicy Orchestrator Deep Command, visit www.mcafee.com/deepcommand.

To learn more about about Intel Core vPro processor and Intel Active Management Technology, visit www.intel.com/vpro.

[1] "Using Total Cost of Ownership to Determine Optimal PC Refresh Lifecycles," Wipro Technologies, March 2009 (www.wipro.com/industryresearch). Based on an Intel Corporation-sponsored survey of 106 firms in North America and representing 15 different industries; projections are based on a model company developed by Wipro Technologies.

[2] Future function dependent on security point product.

*Other names and brands may be claimed as the property of others.

Intel, Intel Core, Intel vPro, and the Intel logo are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

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. For more information go to http://www.intel.com/performance.

Intel® Active Management Technology (Intel® AMT) 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/technology/platform-technology/intel-amt.

1111/SS/PDF