



Symantec's Altiris* Management Solutions for Notebook and Desktop PCs with Intel® vPro™ Technology

Solution Brief

Symantec's Altiris Client Management Suite*

Altiris Real-Time System Manager Solution*

Altiris Out-of-Band Management Solution*

Altiris Network Discovery*

Intel® Core™ i5 vPro™ processor

Intel® Core™ i7 vPro™ processor

Company	Symantec is a leading provider of service-oriented management solutions that help reduce the cost and complexity of IT ownership through automation.
Business Challenge	Reducing costly manual processes, improving IT service levels, and providing increased network security.
Technology Solution	Symantec's Altiris Client Management Suite,* Altiris Real-Time System Manager Solution,* Altiris Out-of-Band Management Solution,* Altiris Network Discovery,* and other Altiris solutions.
Enhanced By	Notebook and desktop PCs with Intel® Core™ i5 vPro™ processors and Intel® Core™ i7 processors.



Reduce IT costs by significantly reducing desktide visits, enforcing compliance, and improving security

Symantec and Intel are working closely to help IT administrators reduce the cost and complexity of IT services for notebook and desktop PCs. IT administrators can now use Symantec's Altiris* solutions¹ to improve remote problem resolution, security updates, quarantining, and compliance – even for PCs that are powered off or whose OS is unresponsive².

When Symantec's Altiris solutions are used on notebook and desktop PCs with Intel® vPro™ technology, IT technicians can perform faster, more automated security and management tasks. This can translate into improved compliance with government and other regulations, reduced desktide visits, improved service efficiencies, and lower costs for business.



Today's challenges

Today's PCs have traditionally been difficult to remotely or automatically inventory, diagnose, and rebuild 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. Updates also generally can't be deployed to all systems at the same time—sometimes because PCs are powered off, or because users refuse a patch. Since viruses can move fast, the longer it takes to quarantine the compromised systems, the greater the threat to the network.

The solution: Symantec's Altiris solutions used on notebook and desktop PCs with Intel® vPro™ technology

Symantec is improving security and management tasks by taking advantage of new hardware-based capabilities built into notebook and desktop PCs featuring Intel® Core™ i5 vPro™ processors and Intel® Core™ i7 vPro™ processors.² Symantec's Altiris solutions now offer more secure, encrypted communication with the PC over a hardware-based channel that runs outside the OS. This communication channel allows IT technicians to use powerful new capabilities—such as encrypted remote power-up, remote boot, and console redirection as well as hardware-based filtering for network traffic—even if PC power is off, an OS is unresponsive, or management agents are missing.²

Fast call for help and hardware-based KVM help reduce deskside visits

When used on notebook and desktop PCs with Intel vPro technology, Symantec's Altiris solutions can help significantly reduce the deskside

visits and service-depot calls traditionally required to resolve software problems. IT technicians can now securely and remotely reboot a PC to reset its state or boot the PC to a healthy image on a remote drive when the system can't be booted from its own local hard drive.

Once a user has initiated a connection, technicians can use secure, encrypted console redirection utilizing breakthrough hardware-based KVM³ to troubleshoot and resolve problems without user participation. This is true even for notebook and tablet PCs located outside the corporate firewall; users can initiate a secure tunnel for remote management and repair of the system.⁴ Hardware-based KVM allows technicians to maintain control of the user's keyboard, video, and mouse throughout the boot process regardless of the OS state, giving the technician visibility into any boot errors. All this happens in a fully encrypted session with configurable user consent. For example, a technician could push new copies of .DLL files to the PC or rebuild the system—without leaving the service center. Users can be back up and working faster and with less frustration, while technicians reduce costly deskside or service-depot visits. And with more diagnostic and rebuild services performed remotely, IT service efficiencies can significantly improve.

Eliminating many diagnostic visits for hardware failures

Hardware failure resolution is also easier since an authorized technician can access information stored in protected memory about the make and model of components in order to identify a specific component (such as a hard drive) that must be replaced. Improved accuracy of

Use case without Intel® vPro™ technology	Use case with Intel® vPro™ technology	Intel® Core™ i5 vPro™ processor and Intel® Core™ i7 vPro™ processor allow authorized IT technicians to: ²
<ul style="list-style-type: none"> ▪ Unencrypted wake on LAN, not trustworthy across multiple subnets ▪ Manual patching is required for PCs that aren't powered on 	<ul style="list-style-type: none"> ▪ Encrypted, remote software update 	<ul style="list-style-type: none"> ▪ Remotely and securely power up PC to receive a critical patch or update
<ul style="list-style-type: none"> ▪ PC vulnerable during boot process ▪ Quarantine typically a manual process if OS or security application is already compromised 	<ul style="list-style-type: none"> ▪ System isolation and recovery even if OS is unresponsive 	<ul style="list-style-type: none"> ▪ Protect systems even before OS or security agents are loaded ▪ Filter network traffic even after the OS is inoperative ▪ Remotely quarantine PCs even if OS is already unresponsive
<ul style="list-style-type: none"> ▪ Management agent is vulnerable to typical security threats that affect OS and other applications ▪ Network traffic restricted at the server level ▪ Manual remediation is typically required after malicious attack 	<ul style="list-style-type: none"> ▪ Hardware-based virtualization on desktop PCs while OS is up and running³ 	<ul style="list-style-type: none"> ▪ Restrict network traffic during normal operations based on PC "posture" ▪ Recover more quickly after a malicious attack

Table 1. Use cases for improved security

Use case without Intel® vPro™ technology	Use case with Intel® vPro™ technology	Intel® Core™ i5 vPro™ processor and Intel® Core™ i7 vPro™ processor allow authorized IT technicians to: ²
<ul style="list-style-type: none"> ▪ Deskside visit required to diagnose and repair software problem 	<ul style="list-style-type: none"> ▪ Remote diagnosis and repair for software problems ▪ Supports industry-wide management standards, including DASH and WS-MAN 	<ul style="list-style-type: none"> ▪ Remotely control PC via secure console redirection with hardware-based KVM, even if OS is unresponsive ▪ Resolve many OS problems by securely and remotely rebooting PC to clean state ▪ Resolve more complex problems by securely redirecting PC's boot device to a clean image on a remote drive ▪ Remotely push new copies of critical system files, such as .DLL files, to PC ▪ Remotely rebuild system, even if PC's OS is inoperative ▪ Resolve application/BIOS conflicts by securely and remotely changing BIOS settings ▪ Improve accuracy of problem diagnosis by accessing protected event log
<ul style="list-style-type: none"> ▪ Deskside visit required to diagnosis hardware problem. Second deskside visit required to install hardware. 	<ul style="list-style-type: none"> ▪ More accurate remote diagnosis of hardware problems 	<ul style="list-style-type: none"> ▪ Identify hardware failures remotely by watching as BIOS loads ▪ Improve accuracy of problem diagnosis by accessing protected event log
<ul style="list-style-type: none"> ▪ Manual inventory for PCs that have missing software agents or are powered down or inoperable 	<ul style="list-style-type: none"> ▪ Remote hardware and/or software asset tracking 	<ul style="list-style-type: none"> ▪ Remotely discover PCs, even after reimaging or configuration changes ▪ Inventory hardware assets, regardless of agent presence, OS state, or power state ▪ UUID in non-volatile flash prevents double counting of PC assets

Table 2. Use cases for remote problem resolution and asset tracking

remote diagnosis can enable IT to eliminate many of the deskside or service-depot visits traditionally required to diagnose hardware failures.

Pushing updates and managing virtualized software licenses, even for PCs that are powered off

Notebook and desktop PCs with Intel vPro technology include a remote power-up capability to help improve automation, after-hours updates, and other maintenance tasks. Unlike current technologies, this power-up capability is authenticated and can be encrypted by third-party software.⁵

Symantec's Altiris solutions now allow IT administrators to deploy policy-based updates anytime. When the polling process discovers a PC that is powered off, Symantec's Altiris solutions remotely power up the system, roll out the update, and return the PC to the state in which the user left it: on, off, hibernating, or sleeping. Users can see less interruption, while the network as a whole can become more stable.

First and last line of defense for the PC

Notebook and desktop PCs with Intel vPro technology offer IT administrators a first line and last line of defense against security threats. The programmable hardware filters in these PCs can examine inbound and outbound network traffic behavior before packets are passed from the hardware to the OS or out to the network. Symantec's Altiris solutions use these filters to allow IT administrators to define policies that are triggered by certain packet behavior.

Because hardware-based filters work regardless of system state, the PC is protected, even during the boot process, before the OS comes up, and before virus scan and other security software loads. The use of these filters closes some of the security holes in today's PC environment and creates a new first line of defense against malicious attacks.

Even with the increased security embedded in the PC, IT administrators still need powerful tools to prevent new and evolving threats from penetrating the network. To this end, the filters also offer a new last line of defense for systems. Because the filters are based in hardware, they are not as susceptible to the problems that typically affect an OS or security application, such as being disabled or turned off by a user, hacker, or virus.

Even after an OS or security agent is disabled, the hardware-based filters can rate-limit or stop incoming or outgoing network traffic, based on IT-defined policies. And even though the network data path might be cut off, Symantec's Altiris solutions remediation ports can remain open. This allows technicians to remotely communicate with the PC, correct the problem, and bring the machine back onto the network quickly and without a costly deskside visit. Technicians no longer need to ask users to unplug the PC's network cable to help stop a virus from spreading. Instead, they can use the Altiris network filtering capability to isolate the system remotely.

Knowing which agents are being monitored— even if the OS is inoperative

Notebook and desktop PCs with Intel vPro technology also include innovative hardware-based “watchdog” timers for agent presence checking. Software agents (and applications) can check in with these timers to verify that they are active. Symantec’s Altiris solutions take advantage of this capability by querying the Intel® Management Engine to find out and report on which agents are being monitored by the hardware. For example, if the presence of two security applications is being automatically checked by notebook and desktop PCs with Intel vPro technology, IT administrators could concentrate their resources on other agents that have less visibility.

Secure access to hardware-based capabilities

Symantec supports a range of security options for the hardware-based capabilities of notebook and desktop PCs with Intel vPro technology. These options range from simplified security for small and medium businesses to enterprise-grade security with certificate-based authentication and encryption.⁶

Summary

Symantec’s Altiris solutions used on notebook and desktop PCs with Intel vPro technology help IT administrators reduce desk-side visits, solve more service challenges through automation, protect PCs more effectively, and improve corporate compliance with government and other regulations¹. IT can now perform more work off-hours or at other times that don’t interfere with users. Together, Symantec’s Altiris solutions and notebook and desktop PCs with Intel vPro technology can help IT administrators reduce both the cost and complexity of IT services for notebook and desktop PCs.¹

For more information about notebook and desktop PCs with Intel vPro technology, visit www.intel.com/go/businesspc

For more information about Symantec’s Altiris solutions, visit www.altiris.com/vpro

SOLUTION BENEFITS

- Increase automation of security and management processes
- Reduce desk-side visits and service-depot calls for software and hardware problem resolution
- Increase compliance with government and other regulations
- Reduce cost of owning technology

¹ All content regarding Altiris solutions was provided by Altiris, now part of Symantec.

² Intel® vPro™ technology includes powerful Intel® Active Management Technology (Intel AMT). Intel AMT requires the computer system to have an Intel AMT-enabled chipset, network hardware and software, as well as connection with a power source and a corporate network connection. Setup requires configuration by the purchaser and may require scripting with the management console or further integration into existing security frameworks to enable certain functionality. It may also require modifications of implementation of new business processes. With regard to notebooks, Intel AMT may not be available or certain capabilities may be limited over a host OS-based VPN or when connecting wirelessly, on battery power, sleeping, hibernating or powered off. For more information, see www.intel.com/technology/manage/iamt.

³ KVM Remote Control (Keyboard Video Mouse) is only available with dual-core Intel® Core™ i5 vPro™ processors and i7 vPro™ processors with active integrated graphics. Discrete graphics are not supported.

⁴ Systems using client-initiated remote access require wired LAN connectivity and may not be available in public hot spots or “click to accept” locations. For more information on client-initiated remote access visit, www.intel.com/products/centrino2/vpro/index.htm.

⁵ Intel® Virtualization Technology (Intel® VT) requires a computer system with an enabled Intel® processor, BIOS, virtual machine monitor (VMM), and, for some uses, certain platform software enabled for it. Functionality, performance, or other benefits will vary depending on hardware and software configurations and may require a BIOS update. Software applications may not be compatible with all operating systems. Please check with your application vendor.

⁶ For detailed information about the security methodologies and technologies used to secure the capabilities of Intel® Centrino® Pro processor technology and Intel® vPro™ technology, refer to the Intel® Active Management Technology Deployment and Reference Guide, Intel 2006, at www.intel.com/technology/vpro/index.htm.

Copyright © 2010 Intel Corporation. All rights reserved. Intel, the Intel logo, Intel Core, vPro, and Core Inside are trademarks of Intel Corporation in the U.S. and other countries.

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

