Planning Guide

Improve IT Efficiency with Intelligent PCs
Using Intelligent Clients for Hardware-Based Security and IT Management

Why You Should Read This Document

This guide explains how IT managers can use intelligent clients to do more with less. Intelligent clients based on Intel® vPro™ technology deliver an additional layer of hardware-based security and improve IT management by:

- Extending automation and control with out-of-band management capabilities for critical operations, such as alerting, agent presence checking, and remote booting
- Adding a deeper, robust layer of hardware-based security for proactive security management, automatic monitoring, and convenient after-hours patching
- Incorporating remote support capabilities for general help-desk tasks, remote reimageing, and “invisible” remediation, as well as security and compliance management
- Improving accuracy and speed of asset management by easily tracking universally unique identifier (UUID) data, hardware asset data, and software asset information
Planning Guide
Improve IT Efficiency with Intelligent PCs
Using Intelligent Clients for Hardware-Based Security and IT Management

APRIL 2012
Contents

3  The New IT Imperative: Do More with Less
4  Built-in PC Security and IT Management—a Smarter Solution
5  Incorporating Intelligent Clients into Your IT Strategy
8  Stay Ahead with Intel® vPro™ Technologies
9  Intel Resources for Learning More
The New IT Imperative: Do More with Less

Today’s IT managers are facing some of their biggest challenges yet. A turbulent economy has led to flat budgets and a changing business environment that requires greater flexibility and even tighter security. There are a growing number of mobile corporate PCs to manage within an evolving security threat landscape, making IT agility and security management more important than ever. Complicating matters are tech-savvy users who have high expectations for connectivity, performance, and fast IT support.

To stay ahead, IT departments must figure out how to do more with less. And it’s more complex than simply improving productivity. In addition to accelerating help-desk processes, IT staff must support and manage security for countless mobile and remote users from any location, on any PC device. They must be prepared for advanced security threats that are emerging with a new level of sophistication and greater frequency, from rootkit attacks to international security breaches and other intricate forms of malware. Finally, IT staff must be able to simplify and speed up time-consuming routine tasks, such as asset management.

Although software-based solutions have traditionally been successful resources for accelerating help-desk processes, today’s business landscape requires a smarter solution. IT managers need practical yet innovative ways to further improve efficiencies while bolstering security and reducing the time spent on hands-on support.

The Purpose of This Guide

This planning guide describes how you can incorporate the use of intelligent clients based on Intel® vPro™ technology into your IT strategy to gain an additional layer of hardware-based security and improve IT management across your organization.

The first section, “Built-in PC Security and IT Management—a Smarter Solution,” discusses how you can gain the incremental IT efficiencies you need to stay ahead with hardware-based tools that leverage out-of-band management capabilities. The second section, “Incorporating Intelligent Clients into Your IT Strategy,” discusses how you can use intelligent clients to add a new layer of built-in security, optimize help-desk efficiencies, and improve speed and accuracy of inventory management. The final sections provide an overview of Intel vPro technologies and resources for more information.

Defining “Intelligent Client”

This guide uses the term “intelligent client.” Intel defines an intelligent client as a client device that provides the following:

- Hardware-based security capabilities
- Advanced IT manageability
- Energy-efficient performance capabilities
Built-in PC Security and IT Management—a Smarter Solution

As security threats continue to expand in number and complexity, IT organizations must prepare for what might be around the corner. And while many have come to depend on software solutions, the maintenance and upgrades for those solutions can be a drain on IT resources. Budget cuts have invariably led to fewer employees, and many IT departments are struggling just to provide day-to-day support to users. As a result, routine maintenance tasks such as software updates can get pushed aside.

With hardware-based PC security and IT management tools in place, you can gain another layer of protection and achieve the incremental IT efficiencies you need to stay ahead.

Out-of-Band Management Capabilities

By design, traditional software-based control features use in-band communications that operate through the software stack in the operating system, and are secured through the operating system features. Because the operating system and software stack can be compromised via removal of security applications or by simply not being kept up-to-date, it means that in-band communication is also at risk.

Hardware-based IT management tools extend automation and control capabilities beyond what can be offered by software alone, helping to dramatically increase help-desk efficiencies and increase productivity. In fact, PCs with built-in management enabled can reduce software-related deskside visits up to 58 percent.4

With these hardware-based control features, you can more effectively support remote PCs by using an out-of-band communication tunnel to the remote PC. The out-of-band tunnel sits “below” the operating system and applications, goes through the TCP/IP firmware stack, and is secured with hardware-based Transport Layer Security (TLS) encryption and other robust methodologies. The out-of-band tunnel allows critical systems communication and operations, such as alerting, agent presence checking, and remote booting.
Incorporating Intelligent Clients into Your IT Strategy

By incorporating intelligent clients as part of your larger IT strategy, you can work with a smarter solution that is designed to improve IT efficiencies. Work proactively with access to hardware-based controls that reside on the processor, below the operating system, to:

- Implement a new layer of built-in security enforcement checkpoints.
- Provide convenient remote support for PCs unreachable by software solutions alone.
- Streamline and improve accuracy of PC and software inventory.

Gain an Additional Layer of Hardware-Based Security

Because today’s threat landscape is more sophisticated than ever, it’s posing new security challenges to IT organizations everywhere. Maintaining software-based solutions is a time-consuming process that can eat away at IT productivity, or even occasionally take a back seat to more pressing tasks. Moreover, common security measures such as antivirus software and operating system-level security features are vulnerable to tampering and removal—whether accidentally by a user, or with malicious intent. It is an ideal time to supplement the tried-and-true software security solutions that have worked so well in the past to help ensure adequate protection against current risks.

By implementing an additional hardware-based layer of protection, organizations can achieve a deeper layer of security. Built-in security features give you the ability to automatically prevent and respond to threats, all the while increasing the overall efficiency of security management. This extra layer of security comes from robust intelligent-device capabilities that are at the processor level, below the operating system.

Automatic Monitoring of Suspicious Behavior

Gain peace of mind with automatic monitoring. With built-in controls in place, you can establish policies that continuously monitor all inbound and outbound network traffic on corporate-owned PCs—regardless of the state of the PC. If the hardware detects suspicious behavior, it triggers the PC to port isolate or cut off its own network data to quarantine a virus and prevent its proliferation.

Automated Security Agent Polling and Alerts

Verifying security agents doesn’t have to be a drain on network bandwidth or dependent on the operating system. Hardware-based polling with Intel vPro technology works out of band, based on regular intervals set by you and your staff. Registered agents report to the Intel vPro chipset to indicate they are present and healthy. If the agent fails to report into the chipset, an alert is sent to the administrator that identifies a problem.

Convenient After-Hours Patching

Run security patches at your convenience, without disrupting user productivity. With after-hours patching capabilities, you can push critical security updates to PCs at any time, regardless of their power state—whether they’re on, off, hibernating, or on standby.

Key Security Questions to Consider

Think about security management at your organization and consider the following questions:

- How do you address inherent vulnerabilities that network-connected PCs pose?
- What steps can you take to prevent your business assets from being undermined by inside or outside forces?
- Are there simple solutions that can add extra layers of security?
Extend Your Remote Support Capabilities

Software-based solutions for automated support have become essential IT tools, but they don’t necessarily eliminate the need for deskside visits or user assistance. In spite of improved management tools, almost 20 percent of problem tickets still require user intervention to resolve the problem. Plus, certain support issues, such as the need to service remote PCs that are powered off or have nonfunctioning operating systems, are beyond the scope of software-based solutions. For companies with a large number of remote users, these common challenges can be expensive and time-consuming to fix.

With hardware-based remote support enabled by out-of-band management capabilities, you can quickly and efficiently manage remote PCs that sit beyond the reach of customary software management tools. Hardware-based remote controls make it possible to troubleshoot, diagnose, and correct errors on remote PCs—regardless of their operational state.

Cost Savings with KVM Remote Control

Imagine never again having to go to a user’s desk or call to ask them, “What do you see?” Hardware-based keyboard-video-mouse (KVM) remote control capabilities extend traditional software-based KVM capabilities by allowing you to remotely access and control the PC as if you were on a deskside visit.

Unlike software-based KVM, hardware-based KVM remote control allows IT staff to resolve issues with BIOS, start-up and shutdown, blue screens, operating system freezes, disk failure, and network software issues—through all states, including reboot. This cost-saving technology helps IT departments resolve complex issues in less time, without requiring user assistance, and users are able to get back to work quickly.

Remote Reimaging: Fast for IT and Users

In the event of corrupt software or an operating system problem, the fastest resolution is often to reimagine the operating system or disk. Because most software-based solutions can’t remotely access a PC in this state, resolution requires either a deskside visit from the technician or a help-desk visit by the user. With hardware-based disk reimaging capabilities, technicians can handle this work remotely to reduce resolution time and get the user up and running quickly.

“Invisible” Remediation—and Get Back to Work

Traditionally, when users contact the help desk with concerns about a virus, technicians must take control of the user’s PC to run a virus scan—leaving the user unable to work. With hardware-based remediation features and Microsoft Outlook Web Access with virus scan, they can give the user access to read and respond to e-mail. As the user continues to work productively, the technician can run “invisible” diagnostics, virus scans, and other utilities in the background and resolve any issues that are detected.

After-Hours Updates

For nearly every IT department, pushing software updates to user PCs is a routine but necessary task. Typically, these updates take place during business hours and are therefore disruptive to users—not to mention time-consuming for IT staff. With hardware-based control, your staff has the flexibility to push these updates after hours, even when PCs are powered down. This flexible update capability helps ensure that all your PCs are in compliance, and at the same time, minimizes interruptions.

How Does KVM Remote Control Work?

With keyboard-video-mouse (KVM) remote control, you can see exactly what users see through all states—without leaving your desk. To use KVM remote control:

1. Access the administrator console to connect to the user’s PC.
2. Get the six-digit user consent code from the user and plug it into your console.
3. See what the user sees and remediate the problem using almost any IT support kit.
Although software-based solutions have helped to streamline asset management, it remains one of the most time-intensive and difficult IT tasks. In fact, software inventories for laptops fail up to 62 percent of the time because they are powered off or otherwise inaccessible.

Because a substantial segment of PCs are beyond the reach of software tools, reporting inaccuracies result. In other words, a significant percentage of corporate PCs are not in compliance. This underreporting can expose corporate officers to liability issues, such as noncompliance with Sarbanes-Oxley and other government regulations.

Collecting accurate asset data is critical to meeting compliance regulations, improving life-cycle management, and reducing software licensing fees and liability. By incorporating the use of hardware-based inventory controls in intelligent clients, you can gain “always available” access to system information. This includes performing accurate remote discovery and inventory of wired or wireless PCs and software, both inside and outside the corporate firewall:

- Universally unique identifier (UUID) data – Collect UUID information that is persistent across reconfiguration, reimaging, and operating system rebuilds.
- Hardware asset information – Collect and automatically update hardware asset information, such as manufacturer and model.
- Software asset information – Collect and store software version information, .DAT file information, pointers to database information, and other data stored by third-party vendors that is available in the persistent memory space provided by Intel vPro technology.

**Realize Substantial Savings on Inventory Costs with Intel® vPro™ Technology**

- Improve your ability to inventory previously undetected software by up to 47 percent, and reduce laptop asset inventory failures by up to 62 percent.
- Improve accuracy of automatic hardware asset inventory by up to 22 percent.
- Improve the overall success rate of automated inventories by up to 16 percent.

**Hardware-Based Asset Management: Remote, Secure, and Automatic**

By using the asset management capabilities available in 2nd Gen Intel® Core™ vPro™ processors, IT managers can:

- Write asset and other information (or pointers to asset information) into protected memory.
- Power on PCs to perform inventory, push management agents to the system, and remotely power off when finished.
- Identify and remediate noncompliant PCs even if management agents have been disabled, and push replacement agents to bring PCs back into compliance before allowing further network access.
- Remotely poll wired and wireless PCs—regardless of power state—for software and hardware asset information stored in protected memory.
Stay Ahead with Intel® vPro™ Technologies

By using intelligent clients based on 2nd Gen Intel Core™ vPro processors, you can extend security and efficiency beyond what can be achieved with traditional software-based solutions alone. Intel vPro technology delivers complete, embedded security and IT manageability built right into the hardware. With these intelligent-client device capabilities, IT managers can leverage the smart performance features they expect from Intel vPro technology—and extend IT efficiencies even further to do more with less.

Embedded Security Technology Overview

Intel Active Management Technology® (Intel AMT) – Provides remote support for proactive threat management and diagnosing, isolating, and repairing an infected PC, regardless of operational state.

Intel Advanced Encryption Standard New Instructions® (Intel AES-NI) – Encrypts data up to four times faster\(^1\) without slowing performance or interfering with user productivity.

Intel Trusted Execution Technology® (Intel TXT) – Establishes hardware-based root of trust to defend against software attacks at launch.

Intel Virtualization Technology\(^3\) (Intel VT) – Works with Intel TXT to deliver built-in protection against malware and rootkit attacks.

Intel Identity Protection Technology\(^4\) (Intel IPT) – Helps protect access points by working with authentication solutions to support hardware-based storage and protection of tokens or certificates inside the platform.

Intel Anti-Theft Technology\(^5\) – Offers tamper-resistant security to detect potential theft with the capability to automatically disable PCs.
Intel Resources for Learning More
Use the following resources from Intel to learn more about Intel vPro technologies.

About the Intel Core™ vPro Processor Family

*Intel® Core™ vPro™ Processor Family Animation: More Secure, Manageable, and Responsive*
Watch a demo to find out how Intel vPro technology can simplify IT management and improve the user experience with built-in security technologies and intelligent performance.

*2nd Generation Intel® Core™ vPro™ Processor Family Overview*
Learn how intelligent clients can help you solve IT’s toughest challenges with hardware-based security and manageability.
intel.com/assets/PDF/prodbrief/2ndgenIntelCorevPro_Brief.pdf

*Intel® vPro™ Technology: Reference Guide*
Read a comprehensive reference guide on Intel Core vPro technology.

*Intel® Core™ vPro™ Processor Family Software Catalog*
Explore a catalog of software using Intel vPro processor technology and search by type of software or functionality, such as remote diagnosis and repair, remote asset management, or desktop virtualization.
intelsalestraining.com/vprosoftwareguide/content.htm

*Intel® vPro™ Processor Activation*
Find out how to activate your PCs with an Intel vPro processor in just six steps.

Learn more about the embedded security and IT management technologies available with the Intel Core vPro processor:

*Helpdesk Automation: IT Perspectives on KVM Remote Control*
in tel.com/content/www/us/en/remote-support/core-vpro-it-perspectives-kvm-remote-control-video.html

*Demo: KVM Remote Control*
in tel.com/content/www/us/en/remote-support/core-vpro-kvm-remote-control-demo-video.html
**Intel® vPro™ Solution Reference Design—Instant Back to Work**

**Accelerated Encryption with Intel Advanced Encryption Standard Instructions (AES-NI)**

**Access Accounts More Securely with Intel® Identity Protection Technology**

**Technology Overview: Intel® Trusted Execution Technology**

Find out how Intel IT leverages Intel vPro technology to achieve long-term business value and improve security.

**Managing a Factory IT Environment with Intel® vPro™ Technology**
Following a successful proof of concept, Intel IT uses Intel vPro technology to remotely manage PCs at select factory IT environments to realize significant results: 64 percent energy savings and up to 61 percent reduction in deskside visits.

**Achieving Long-Term Business Value with Intel vPro Technology**
Find out how Intel IT standardized its computing platform on PCs with Intel Core vPro processors to help address critical challenges, such as boosting employee productivity, enhancing security, and improving IT efficiency.

**Evaluating Intel® Anti-Theft Technology**
Intel IT completed a technology evaluation of Intel Anti-Theft Technology (Intel AT) and discovered that the technology will improve our ability to protect company-owned laptops as well as data and intellectual property.
Endnotes

1. Intel vPro technology is sophisticated and requires setup and configuration. Availability of features and results will depend upon the setup and configuration of your hardware, software, and IT environment. To learn more, visit intel.com/technology/vpro/.

2. No computer system can provide absolute security under all conditions. Built-in security features may require third-party software, hardware, or services and an Internet connection. Results may vary depending upon configuration. Consult your PC manufacturer for more details.

3. Results shown are from the 2007 EDS case studies with Intel vPro technology. For details, see the end of the video diagnose.wmv, found at intelsalesadvisor.com/asset/494.html.


6. KVM remote control is only available with Intel Core i5 vPro processors and Intel Core i7 vPro processors with active processor graphics. Discrete graphics are not supported.


9. Security features enabled by Intel AMT require an enabled chipset, network hardware and software, and a corporate network connection. Intel AMT may not be available or certain capabilities may be limited over a host operating system-based VPN or when connecting wirelessly, on battery power, sleeping, hibernating, or powered off. Setup requires configuration and may require scripting with the management console or further integration into existing security frameworks, and modifications or implementation of new business processes. For more information, visit intel.com/technology/manage/amt.

10. Intel AES-NI requires a computer system with Intel AES-NI–enabled processors, as well as non-Intel software to execute the instructions in the correct sequence. Intel AES-NI is available on select Intel Core processors. For availability, consult your system manufacturer. For more information, visit software.intel.com/en-us/articles/intel-advanced-encryption-standard-instructions-aes-ni.

11. 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.

12. No computer system can provide absolute security under all conditions. Intel TXT requires a computer with Intel Virtualization Technology, an Intel TXT–enabled processor and BIOS, a chipset, Authenticated Code Modules, and an Intel TXT–compatible measured launched environment (MLE). Intel TXT also requires the system to contain a TPM v1.s. For more information, visit intel.com/technology/security.

13. Intel VT requires a computer system with an enabled Intel processor and BIOS, and virtual machine monitor (VMM). Functionality, performance, or other benefits will vary depending on hardware and software configurations. Software applications may not be compatible with all operating systems. Consult your PC manufacturer. For more information, visit intel.com/go/virtualization.

14. No system can provide absolute security under all conditions. Requires an Intel IPT–enabled system, including a 2nd Gen or 3rd Generation Intel Core processor, an enabled chipset, firmware, software, and a participating web site. Consult your system manufacturer. Intel assumes no liability for lost or stolen data or systems or any resulting damages. For more information, visit http://ipt.intel.com.

15. No system can provide absolute security under all conditions. Requires an enabled chipset and BIOS, firmware, software, and a subscription with a capable service provider. Consult your system manufacturer and service provider for availability and functionality. Intel assumes no liability for lost or stolen data or systems or any other damages resulting thereof. For more information, visit intel.com/go/anti-theft.
More from the Intel® IT Center

Planning Guide: Improve IT Efficiency with Intelligent PCs is brought to you by the Intel® IT Center, Intel's program for IT professionals. The Intel IT Center is designed to provide straightforward, fluff-free, unbiased information to help IT pros implement strategic projects on their agenda, including virtualization, data center design, intelligent clients, and cloud security. Visit the Intel IT Center for:

- Planning guides, peer research, and vendor round tables to help you implement key projects
- Real-world case studies that show how your peers have tackled the same challenges you face
- Information on how Intel's own IT organization is implementing cloud, virtualization, security, and other strategic initiatives
- Information on events where you can hear from Intel product experts as well as from Intel's own IT professionals

Learn more at intel.com/ITCenter.