New Security Solutions Using Intel® vPro™ Technology

Intel IT security specialists have identified significant new enterprise security use cases that we can implement using Intel® vPro™ technology. We focused on three high-priority, high-value categories—e-Discovery and investigations, data protection and loss prevention, and system health and updates—and successfully performed lab tests to validate each use case. Potential benefits include fewer labor-intensive deskside visits, increased security, and greater user productivity. As we continue to deploy Intel vPro technology throughout our environment, we plan to further investigate these use cases for enterprise implementation.

Dennis Morgan and Frank A. Engelman, Intel Corporation

February 2009

IT@Intel

Executive Summary

To increase our ability to maintain, manage, and protect PCs while reducing management costs, Intel IT is undertaking a multi-year program to implement Intel® vPro™ technology throughout our environment.

Intel vPro technology delivers new abilities to securely manage PCs over networks. It also provides an infrastructure and a set of capabilities that can be used to implement a broad range of additional management and security functions.

With this in mind, a team of Intel IT security specialists set out to identify significant new security use cases that we could implement using Intel vPro technology. The team focused on high-priority, high-value areas and identified a total of 10 use cases in three main categories:

- e-Discovery and investigations

- Data protection and loss prevention, including preventing malicious use, wiping corporate data from PCs, and detecting dual-boot systems and unauthorized peripherals

- System health and updates

With Intel vPro technology, we can perform each of these security uses remotely using features such as remote, redirected boot; console redirect; and agent presence checking. This could deliver benefits such as fewer labor-intensive deskside visits, increased security, and greater user productivity.

We successfully conducted lab tests to validate each use case. As we continue to install PCs with Intel vPro technology throughout our environment, we plan to further investigate these use cases for enterprise deployment.

> Intel® vPro™ technology delivers new abilities to securely manage PCs over networks. It also provides an infrastructure and a set of capabilities that can be used to implement a broad range of additional management and security functions.

Contents

Background

Intel's worldwide computing environment includes more than 100,000 PCs in 120 countries. At Intel, as at most companies, managing and securing these PCs consumes considerable IT resources.

To increase our ability to maintain, manage, and protect our PCs while driving down management costs, we are undertaking a multi-year program to implement Intel® vPro™ technology throughout our environment.

Intel vPro technology is a hardware-based technology that provides us with new abilities to securely manage PCs over networks (see sidebar). By the end of 2008, we had deployed about 40,000 PCs with Intel vPro technology.

Our initial deployments of Intel vPro technology have focused on a small number of management use cases that are relatively easy to implement and quickly deliver a positive return on investment (ROI). However, once deployed, Intel vPro technology provides an infrastructure and a

set of capabilities that can be used for a much broader range of management and security functions, delivering a correspondingly greater set of benefits to the enterprise. Large-scale deployment of Intel vPro technology is still relatively new, and additional usage models continue to be developed.

With this in mind, a team of Intel IT security specialists set out to identify potential new security use cases that we could implement using Intel vPro technology. The team focused on high-priority, high-value areas such as e-Discovery, protecting corporate data, and system health. Once we had identified a list of valuable new security use cases, we performed lab tests to validate each one.

Use Cases

In developing new use cases, we focused on three areas: e-Discovery and investigations, corporate data protection and loss prevention, and system health and updates.

Our use cases rely on specific Intel vPro technology capabilities including:

- **Secure access with authentication.** The network can authenticate a PC before the OS and applications load, and before the PC is allowed to access the network. In security-related use cases, this authentication is critical for helping ensure secure management of the PC using the out-of-band capabilities of Intel vPro technology.

- **Remote power-up.** Previously, it was impossible to manage systems when they were powered

down. With Intel vPro technology, we can remotely power up PCs, perform management functions, and then power down.

- **Remote, redirected boot.** Integrated drive electronics redirect (IDE-R), a more powerful and secure capability than wake on LAN (WOL), allows IT technicians to redirect the boot device for a problem PC. This enables us to remotely boot the PC using a clean, secure OS image on a trusted server.

- **Console redirection.** Through serial over LAN (SOL), IT staff have remote keyboard and video

console control of a PC outside of standard OS control. This allows IT to remotely perform tasks such as editing BIOS settings and system files without user participation.

- **Agent presence checking.** Regular, automated checking determines whether specific programs are active on a PC without the need to repeatedly poll the PC over the network. To enable agent presence checking, PCs with Intel vPro technology include a programmable "heartbeat" presence check built into the Intel® Management Engine. The Intel Management Engine can notify third-party software upon completion of the specific program. We can use this to remotely determine whether a security scan or other security task has completed on the managed PC.

Category 1. e-Discovery and Investigation

e-Discovery is a growing burden for many businesses. Ever-changing legal and regulatory requirements increase the need to be able to track and retrieve a wide variety of data from corporate PCs, including documents and e-mail messages. Examples of these laws include the Sarbanes-Oxley Act, industry-specific laws such as the Gramm-Leach-Bliley Act for the financial services industry, and regulations for individual states.

Additionally, businesses may need to conduct internal investigations to determine whether insiders have carried out malicious activities.

Use Case 1.1. Copy Data for e-Discovery or Investigation

Today, gathering data for e-Discovery and investigations involves labor-intensive manual processes. Without Intel vPro technology, it is difficult to reliably and securely control PCs down the wire.

Current process

Security teams often make deskside visits to remove physical hard drives from client PCs. The drives are transported to corporate storage facilities where the data they contain can be analyzed.

Process with Intel vPro technology

We could remotely copy all the data from the PC.

1. Remotely shut down the client system.

2. Boot using IDE-R from a clean, secure OS image that resides on a server.

Intel® vPro™ Technology

Intel® vPro™ technology is designed to address many of the most costly challenges IT organizations currently face in deploying, maintaining, managing, and securing clients. It enables support teams to securely access and manage PCs over networks even when an OS is unresponsive, a software agent is missing, or a hard drive has failed.

It also contains other features that can enhance a wide range of client management functions. A partial list includes persistent and protected storage for event logs and asset information, configurable hardware-based traffic filters, and programmable triggers and responses for protecting Internet-connected PCs.

3. Copy the contents of the PC's hard drive to a drive on a corporate server.

4. Shut down the PC.

Benefit

This would significantly reduce manual effort, eliminating costly, time-consuming deskside visits. It would enable better use of our limited investigation and e-Discovery resources.

Category 2. Data Protection and Loss Prevention

All businesses are concerned about the threat of losing corporate data and intellectual property. This can happen in many ways, some of which are not adequately protected using existing tools. For example, protected information may be vulnerable because it is stored on client systems in breach of corporate security rules. Data may also be stolen by copying it onto portable storage devices. Protecting corporate data and intellectual property is a primary goal of a well-designed security program.

Use Case 2.1. Wipe Hard Drive When System is Refreshed

Intel refreshes tens of thousands of PCs each year, and we need to make sure that the old systems do not contain corporate data when they leave the company. We must also remove all corporate data from PCs on employees' last days of employment.

Current process

In many cases physical drives are removed and then destroyed, but this reduces the resale value of the PC. If we want to increase resale value by keeping the hard drives, it is essential to remove all corporate data from the systems. One option is to manually clean the drive using a data wipe utility, but this is time- and labor-intensive.

Process with Intel vPro technology

With Intel vPro technology, we could completely remove all corporate data from hard drives.

1. Remotely boot using IDE-R from a clean, secure OS image that resides on a server.

2. Clean the system using a disk wipe utility in the image.

Benefit

Using Intel vPro technology would significantly reduce hands-on effort, decreasing cost and increasing PC resale value.

Use Case 2.2. Wipe Deleted Data from Current System

In the course of their everyday work, employees continually create and delete data on their PCs. Deleted data is placed in the recycle bin and subsequently is "permanently" deleted by the system. The hard drive space once occupied by deleted data is then available for reuse. In actuality, however, the data still resides on the system. Forensic kits available on the Internet can recover even this permanently deleted data, which may include protected intellectual property or personally identifiable information. We could make systems more secure by completely wiping hard drive free space so that data cannot be retrieved in this way.

Current process

Most companies don't currently have a process for doing this.

Process with Intel vPro technology

We could remotely wipe the system.

1. Boot using IDE-R from a clean OS image that resides on a server.

2. Use a wipe tool.

3. Shut down the system.

Benefit

Wiping deleted data would reduce the threat of unwanted access to corporate or personal information.

Use Case 2.3. Prevent Client System Access by Malicious Users

Corporations may not discover malicious intent until a user begins behaving suspiciously within the environment. IT staff must then prevent the user from accessing valuable data on the user's own client system. Isolating the client from the network is not enough: The user could still potentially remove large amounts of data from the client system using portable devices such as flash drives.

Current process

Current methods are labor-intensive and sometimes inadequate. For instance, if users are logged on, we can isolate them from the network but not from data on their own systems.

Process with Intel vPro technology

We could immediately isolate users, even when they are logged on and actively using the network, and prevent subsequent system access.

1. Remotely shut down the client system.

2. Use SOL to boot the system into BIOS.

3. Change the PC's BIOS settings so the user cannot reboot the system.

4. Shut down the client.

Benefit

Security would be improved and the risk of data loss reduced because the user would be immediately disconnected from corporate resources and data on the client PC.

Use Case 2.4. Validate Client Adherence to Data Protection Requirements

On servers, policy and software protection mechanisms are used to control access to intellectual property and other classified documents. However, these protection mechanisms typically are not used on clients. As a result, there is no mechanism to restrict storage and verify policy adherence for information on client systems.

Current process

Companies typically rely on employee adherence to data protection policy. They do not check for protected and classified content on client systems.

Process with Intel vPro technology

We could protect corporate data.

1. Remotely boot the client system from a clean server-based OS image using IDE-R.

2. Map one or more drives to the employee's system.

3. Scan the drives to search for known protected documents.

The process can be configured to include various actions, such as notifying a security team member, removing the classified files, or moving the files to a protected space.

Benefit

This would improve security by reducing the threat to intellectual property and other classified information.

Use Case 2.5. Investigate Unauthorized Peripheral Devices

Portable high-capacity peripherals, such as flash drives or hard drives that connect to USB ports, make it easier to transfer large amounts of valuable data from corporate systems.

Portable network interface cards (NICs) are also a risk. By plugging a portable NIC into a USB port on a client system, a user could connect to a second network. This could allow information to pass from the corporate network to a less-secure network through the client.

Current process

Companies do not generally scan to determine whether unauthorized peripherals are connected to client systems. Instead, they typically rely on employees to adhere to corporate policy.

Process with Intel vPro technlogy

We could detect unauthorized peripherals.

1. Remotely boot the system from an OS image on a server.

2. Review the connected devices.

Benefit

This would improve security by enabling companies to scan for peripherals that violate corporate policy.

Use Case 2.6. Detect Dual-Boot Systems

IT groups typically create, deploy, and support specific client software builds. One goal is to help ensure that clients running the software can be managed and that they meet corporate security requirements. However, installing a second OS to create a dual-boot system allows the client to be used without enforcing corporate policies and controls, making the system vulnerable to attack. As a result, corporate data could be copied, removed, or corrupted.

An additional threat is that malware writers are becoming more adept at creating and installing underlying OSs that are invisible to the user but capable of stealing corporate data.

Current process

Companies do not generally scan for dual-boot systems.

Process with Intel vPro technology

We could scan systems to identify those with dual-boot capability.

1. Shut down the system.

2. Boot from a server using IDE-R.

3. Scan for multiple partitions.

If we identify a system with dual-boot capability, we could shut it down. We could also use Intel vPro technology to remove the OS.

Benefit

This would improve security by detecting and preventing use of dual-boot capability.

Category 3. System Health and Updates

Keeping client systems up to date and healthy is the foundation of a strong security program. In addition to delivering updates and patches, we must frequently scan for malware and back up data.

Use Case 3.1. Run Security Services When System Is Not in Use

Applications that perform security services such as malware scans and network backups are processor-intensive and can slow PCs, hindering user productivity. In general, users want security services to be unobtrusive.

Current process

These tasks are often performed during normal working hours, impacting user productivity.

Process with Intel vPro technology

We could reliably perform these tasks overnight or when an employee is not using the system.

This use case employs Intel vPro technology agent presence checking capability in a new way. Typically this feature is used to monitor critical services to help ensure that they continue to

run on the client system. However, in this use case, agent presence checking detects when a security service has completed, at which point we shut down the employee's PC.

1. Use IDE-R to remotely boot the PC from a server-resident OS image. This OS contains a watchdog timer that monitors the desired security task, such as a virus scan.

2. Initiate the scan. The watchdog timer continually checks for the presence of the security service. When the service completes, the watchdog detects that the service is no longer running.

3. Shut down the system.

Benefit
This would enable greater employee productivity and help ensure that systems stay current.

Use Case 3.2. Check File System to Validate System Integrity

Malware writers have increasingly focused on modifying OSs and applications as a way to attack systems while escaping detection and making the malware harder to remove. Examples include

rootkits and patches to legitimate executables in order to spy on corporate systems. This means there is a growing need to validate system files and applications to check that they have not been compromised or patched.

Current process
Most companies currently install only antivirus software on employees' PCs. Antivirus products typically do not perform file integrity checks. Though established integrity-check products exist, they are typically not installed on users' PCs.

Process with Intel vPro technology
We could reliably scan systems by remotely running a file system integrity check.

1. Remotely shut down the system.

2. Boot from a server using IDE-R.

3. Run the integrity check.

4. Report the results to the security team.

Benefit
This would improve security by more reliably detecting malware.

Tests

We performed lab tests to validate each use case. A summary of the use cases and the test steps we executed is shown in Table 1.

Test Environment and Test Plan

We used the Manageability Developer Tool Kit, available for free download at http://software.intel.com, to test our use cases. This set of tools helps designers, developers, and testers understand the benefits of Intel vPro technology and assists in developing and testing applications based on Intel vPro technology.

Tools we used included:

- **Manageability Commander Tool.** A sample management console that enables users to interact with Intel vPro technology functions, including remote connection, power control, agent presence management, watchdogs, SOL, IDE-R, and many more.

- **Manageability Outpost Tool.** A sample client agent that provides a local link from a client's Intel

Table 1. Use Cases and Test Steps

| Use Case	Current Process	Process with Intel® vPro™ Technology	Benefit	Tested Steps
1.1 Copy Data for e-Discovery or Investigation	Typically, remove and transport the hard drive.	Remotely copy data to corporate server.	Reduced effort; better use of limited e-Discovery resources.	1. Remotely shut down system. 2. Boot using integrated drive electronics redirect (IDE-R) from a clean, secure OS image that resides on a server. 3. Copy entire contents of local disk to network share. 4. Shut down system.
2.1 Wipe Hard Drive When System Is Refreshed	Remove and destroy hard drive or manually wipe.	Remotely wipe drive.	Reduced effort; increase in resale value.	1. Boot from image server using IDE-R. 2. Wipe drive using wipe tool in image. 3. Shut down system.
2.2 Wipe Deleted Data from Current System	Typically not done.	Remotely wipe free space.	Increased security.	1. Boot from image server using IDE-R. 2. Wipe free space on PC drive using wipe tool.
2.3 Prevent Client System Access by Malicious Users	Lock account and use manual processes to force re-authentication.	Remotely shut down and disable user's system.	Faster and more reliable; much less manual effort.	1. Shut down system. 2. Boot system into BIOS using serial over LAN (SOL). 3. Change BIOS settings, disabling the system so it cannot reboot locally. 4. Shut down system.
2.4 Validate Client Adherence to Data Protection Requirements	Typically not done.	Remotely scan user's PC for protected documents.	Increased security.	1. Boot from server using IDE-R. 2. Map one or more drives to user's PC. 3. Search for protected documents. 4. Remove files. 5. Shut down system.
2.5 Investigate Unauthorized Peripheral Devices	Typically not done.	Remotely detect unauthorized devices.	Increased security.	1. Shut down system. 2. Boot from server using IDE-R. 3. Review connected devices. 4. Shut down system.
2.6 Detect Dual-Boot Systems	Typically not done.	Remotely scan system.	Increased security.	1. Shut down system. 2. Boot from server using IDE-R. 3. Scan hard drive for multiple partitions and types. 4. Identify systems with dual-boot capability. 5. Shut down system.
3.1 Run Security Services When System Isn't in Use	Processor-intensive security scans and backups typically take place during office hours and can hinder employee productivity.	Remotely perform security tasks when system is not in use.	Greater employee productivity.	System is initially in a down state. 1. Boot from server using IDE-R. Watchdog timer starts. 2. Start security service. Watchdog timer detects when service completes (is no longer running). 3. Shut down system using Microsoft Windows* system tools.
3.2 Check File System to Validate System Integrity	Typically not done.	Remotely check file integrity.	Greater security due to better malware detection.	1. Shut down system. 2. Boot from server using IDE-R. 3. Run file system integrity check. 4. Report results and shut down system.
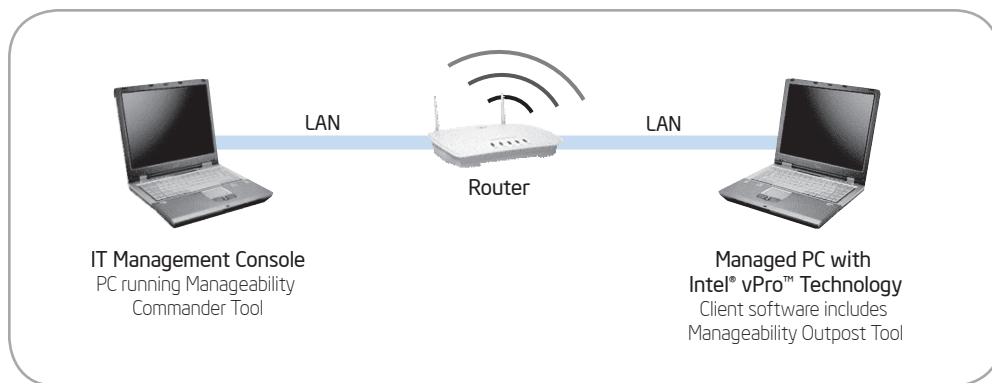
Figure 1. Test environment for new security solutions using Intel® vPro™ technology.

vPro technology firmware to the same client's OS. This remote agent allows the management console to perform OS-level functions through SOL even when the Microsoft Windows* network driver is disabled.

We set up a test environment, shown in Figure 1. The managed client was a notebook PC with Intel® Centrino®2 with vPro™ technology running Microsoft Windows XP SP3* and Manageability Outpost Tool. Our management console was a notebook PC running Microsoft Windows XP SP3 and Manageability Commander Tool. Our environment also included a router, which supplied Dynamic Host Configuration Protocol (DHCP) addresses to the PCs.

We performed the tests over both wired and wireless LANs within our enterprise network. Each test consisted of a series of steps designed to determine whether the use case is feasible. We verified that each step completed successfully.

Results

We successfully tested all the use cases.

Conclusion

Intel vPro technology provides a set of capabilities that we can use to implement a broad range of security and management capabilities.

We identified significant new security uses for Intel vPro technology and validated them through testing. In a production environment, many of the use cases could be automated. These uses deliver potential benefits including reduced manual effort and increased security.

As we continue to install and provision Intel vPro technology throughout our environment, we expect to further investigate these use cases for enterprise deployment.
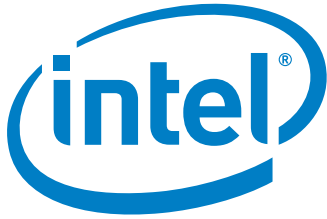
www.intel.com/IT

Authors

Dennis Morgan is a senior security specialist with Intel IT.

Frank A. Engelman is an enterprise architect with the Intel® IT Innovation Centre.

Acronyms

DHCP	Dynamic Host Configuration Protocol	**ROI**	return on investment
IDE-R	integrated drive electronics redirect	**SOL**	serial over LAN
NIC	network interface card	**WOL**	wake on LAN