White Paper

Intel® vPro™ Technology

Built-in Manageability and Proactive Security for Business Desktop PCs

Business desktop PCs with Intel® vPro™ technology provide down-the-wire proactive security and manageability capabilities—even for PCs whose power is off or whose operating system is down. These PCs also include virtualization capabilities that allow IT managers to enhance isolation of third-party applications. PCs with Intel vPro technology feature dual-core Intel® Core™2 Duo processors that deliver significantly improved performance for compute-intensive tasks—all in a power-efficient package that is Windows Vista* Premium Ready.

TABLE OF CONTENTS

Executive summary

Desktop PCs with Intel® vPro™ technology provide built-in, professional-grade management and security capabilities that meet critical business challenges. IT can lower maintenance costs while ensuring greater levels of IT compliance using Intel vPro technology's improved remote management, provisioning, problem resolution, off-hours maintenance, and proactive security capabilities—all directly from the IT console.

Most importantly, these hardware-based capabilities are available to authorized IT down-the-wire, even for PCs that are powered off or whose operating system (OS) is down. IT will now be able to remotely take accurate asset and hardware/software inventories, contain more security threats, resolve software and hardware problems faster, and increase user uptime.

PCs with Intel vPro technology also include additional, hardware-based capabilities that give IT the option of a lighter-weight form of virtualization for mainstream business. IT can now run critical security applications in a simplified, self-contained, dedicated virtual partition—or "virtual appliance"—even while users are working on their own compute-intensive tasks in the user OS.

These powerful new hardware-based capabilities are designed right into PCs with Intel vPro technology. And, every PC with Intel vPro technology uses the Intel® Core™2 Duo processor. The Intel Core 2 Duo processor gives IT the dual-core, 64-bit capable performance needed to run the latest compute-intensive applications and provide outstanding user responsiveness in multitasking environments—all in a power-efficient design that is Windows Vista* Premium Ready. IT can now spend less time on routine tasks, and can focus resources where they are most needed for better manageability and security of desktop PCs.

Intel® vPro™ technology

A new generation of desktop PCs meets the most pressing challenges of IT.

Today's IT challenges

Information technology (IT) managers have a critical need for capabilities that simplify security and manageability of desktop PCs.

Key IT challenges today include:

- A dramatic increase in malicious attacks on PCs.
- A critical need to reduce user downtime caused by malicious attacks; problem PCs; maintenance, upgrades, and other IT tasks.
- Financial and legal pressure to accurately inventory assets.
- Escalating demand for IT services that strain IT budgets.

Software-only management and security solutions for PCs can't work around a fundamental limitation: they cannot manage or secure a PC that is powered off or whose operating system (OS) is down.

A critical capability that would free IT to do more with the resources they have is the ability to remotely manage and effectively secure PCs regardless of machine power state or the health of the OS.

Built-in capabilities simplify remote management and improve security

Desktop PCs with Intel vPro technology are specifically designed to address the top IT challenges in manageability and security. These PCs provide simple remote management and tamper-resistant security capabilities, so IT has more control where they need it—at the IT console. Some of the capabilities enabled by PCs with Intel vPro technology are:

- Asset inventory. IT can now locate all PCs with Intel vPro technology, even if they are powered down or inoperative, so IT knows exactly which systems need to be managed or secured.
- Hardware and software inventory. IT can track and inventory hardware and software assets on a PC, including version information—even if the system is powered off or its OS is down. For example, software asset information includes version .dat information, while hardware information includes BIOS settings and make, model, and warranty information for hard drives, memory, add-in cards and other components.
- Remote problem resolution. IT can diagnose and resolve more problems remotely, regardless of PC power state or the state of the OS, reducing the cost of deskside visits, increasing user uptime, and saving IT resources for new services.
- Robust, hardware-based safety. IT can protect systems with two new layers of security, including virtualization, so third-party security software is always available when needed, and viruses, worms, and other threats can be identified faster and stopped more effectively.
- Higher performance. These PCs, powered by the state-of-the-art, 64-bit dual-core Intel® Core™2 Duo processor based on Intel® Core™ microarchitecture, are designed to deliver increased performance and responsiveness in a multitasking environment. IT can now run virus scans, email synchronization, backups, and other tasks in the background without bogging down user applications in the foreground.
- Energy efficiency. The Intel Core 2 Duo processor delivers power-optimized performance through an efficient design foundation based on Intel® Intelligent Power Capability. Intel Intelligent Power Capability uses ultrafine-grained power control to turn processor functions "on" only when needed, thus reducing processor power use.
- Ready for Windows Vista. PCs with Intel vPro technology are ready to be upgraded to the next-generation Windows Vista operating system, with built-in graphics and support for 64-bit applications.

Combined with third-party software solutions, Intel vPro technology allows IT to eliminate a significant number of deskside visits, reduce overspending on existing resources, and shift their focus from managing PCs to exploring new services and strategic initiatives.

Remote communication, tamper-resistant memory

With third-party software solutions running on PCs with Intel vPro technology, IT can more easily manage and secure PCs, regardless of their power state or the health of the OS. This is done by including Intel® Active Management Technology (Intel® AMT) and other advanced technologies directly in platform hardware.

Two Intel AMT capabilities are especially critical for remote IT tasks:

- A remote-communication channel that's always available to authorized IT.
- Persistent, nonvolatile memory where third-party application information can be safely stored.

Remote-communication channel

Traditionally in an enterprise network, manageability and security software can communicate with a PC only if the PC is powered up ("in band") and its operating system is working properly. Because these software-only solutions are installed at the same level as the OS, their management agents can be tampered with. Communication privacy is also an issue because the in-band, software-based communication channel they use is not secure.

In contrast, Intel vPro technology gives you two ways to communicate with a PC:

- The traditional, nonsecured communication channel, which sends network traffic through the software stack in the OS.
- A more secure, hardware-based communication channel that runs "below" the OS (refer to Figure 1), and is independent of the health of the OS. This "out-of-band" channel sends network communication through a stack built into the Intel AMT hardware and firmware. Even if PC power is off or the OS down, this communication channel is still available to authorized IT.

Because the Intel AMT communication channel is based in hardware, IT can have access to the machine anytime, as long as the PC is plugged into a power source and connected to the network. The channel allows critical system communication (such as alerting) and operations (such as remote booting) to continue, even if the OS is problematic.

IT can now troubleshoot, diagnose, and repair the PC whether it is on or off, whether its OS is working or down. IT can read event logs, check BIOS settings, access hardware asset information, and check the status of security and management agents anytime. Devices can be polled off-hours, and PCs can send critical system alerts to IT even if the PC itself is powered off. Systems can be powered up remotely from the IT console, and problem PCs can be rebooted, rebuilt, and repaired remotely even if their OS is down.

Persistent, nonvolatile memory

One of the main challenges in managing PCs is acquiring information that is typically lost or unavailable when a PC is powered down, reconfigured, rebuilt, or inoperative.

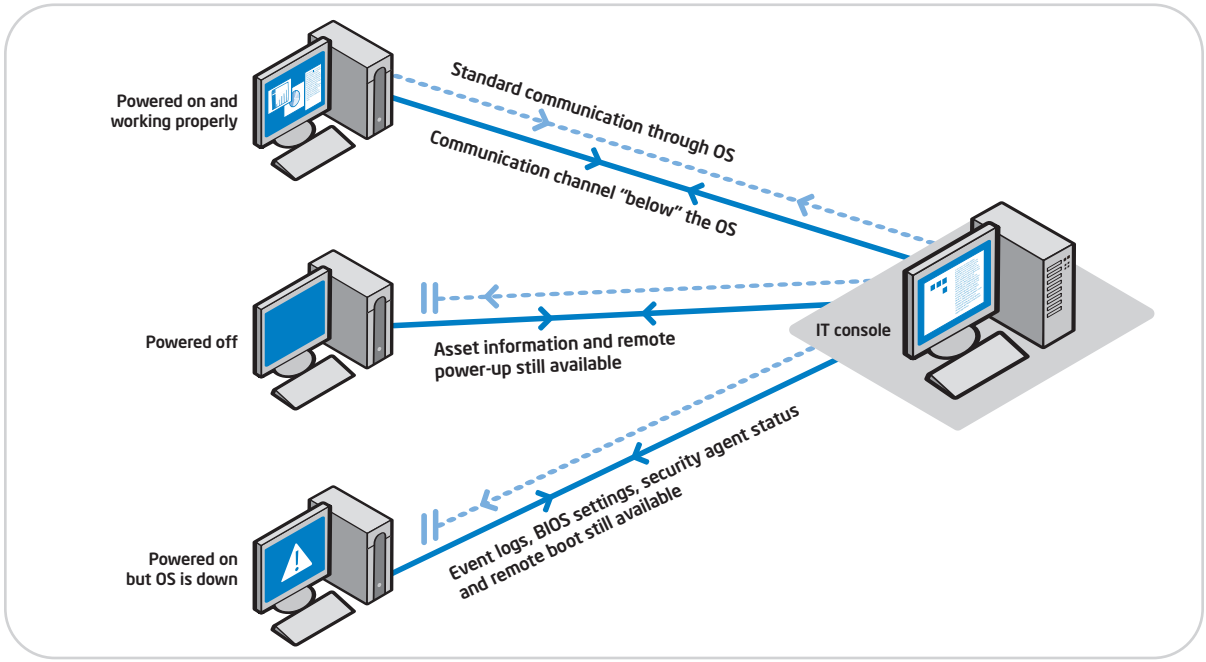


Figure 1: Remote-communication channel. The hardware-based communication channel runs outside the OS, so it remains available even when PCs are powered off or their OS is not available.

To address this problem, Intel vPro technology provides a more secure, nonvolatile memory in an execution environment that works below the operating system (refer to Figure 2). This nonvolatile memory is tamper-resistant to hackers, viruses, worms, and other security threats.

Nonvolatile memory is divided into three key areas:

- Storage for the signed, encrypted Intel vPro technology management engine and the information used by Intel AMT.
- Storage for hardware asset information, which is automatically updated each time power-on self-test (POST) runs.
- Storage that is configurable by authorized IT for use by third-party software for security, inventory, and other important information (or for pointers to information).

Critical system information is now available anytime, without IT having to "wake up" the system. Data also persists across OS builds, reimaging, and reconfigurations, so maintenance and disaster recovery is simpler.

Communication and memory are tamper-resistant

Even when an Intel vPro technology PC is powered off, the PC's management engine is not turned off as long as the system is plugged into a power source and connected to the network. Authorized IT can still access the PC.

Management and security capabilities are embedded in the hardware design of the PC platform. This "firmware" code is signed, encrypted, and stored in nonvolatile memory, and access to that space is controlled by an access control list (ACL), to help prevent unauthorized users, hackers, viruses, and other threats from accessing that space. (Third-party data is not encrypted in nonvolatile memory, but access to that data is controlled through the ACL.) At the same time, security for communication from the network to the management engine is provided through TLS and HTTP authentication, to help prevent Internet Protocol (IP) spoofing.

With these hardware-based measures, even when the PC is off or its OS is down, the confidentiality and authentication of the communication channel and the security of stored information remains in place.

Simpler remote management

On average, U.S. businesses can't find up to 20% or more of their PC assets at any given time, and the percentage of "missing" assets for overseas businesses is even higher.[1] Even with excellent asset-location applications and processes, IT still can't find 5% of their assets.[1] There is a critical need for accurate PC inventories, especially for PCs that are powered off or whose OS is inoperative.

Asset inventory: Finding systems remotely

Several situations have contributed to traditional problems with accurate PC inventories:

- It has been difficult to locate upgraded or reimaged PCs, because critical system information has not persisted after a rebuild.

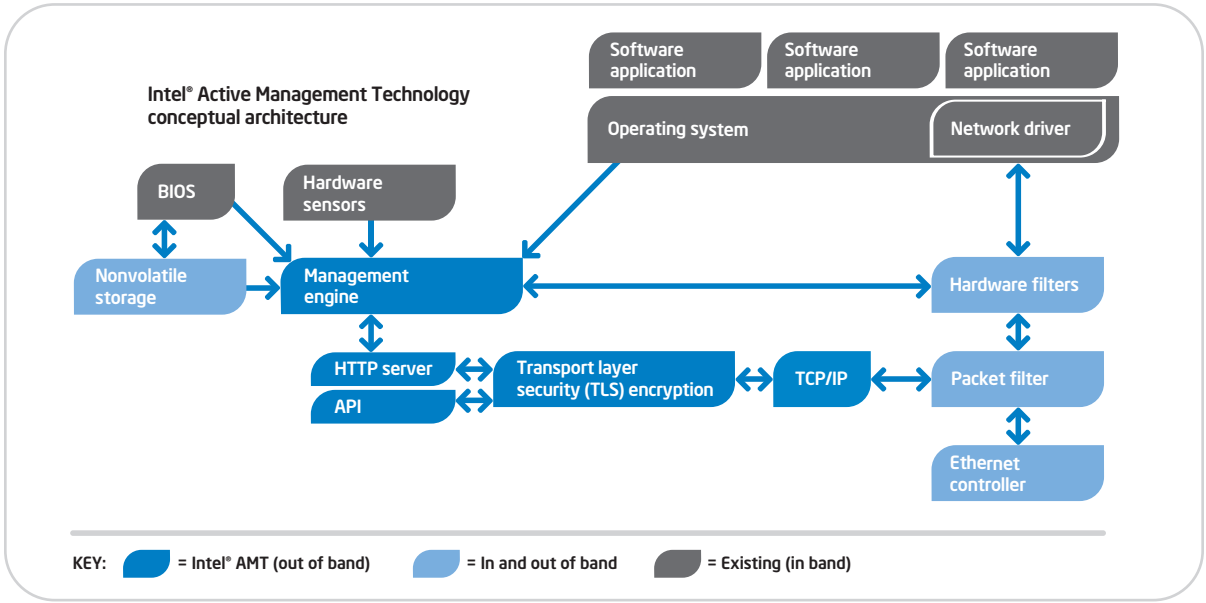


Figure 2: Intel® Active Management Technology simplified block diagram. Intel® AMT is a combination of hardware, software, and firmware.

- Users, hackers, and viruses often disable management agents, so systems can't be identified and brought back into compliance.
- IT may not be aware of new systems added to the network, so they can't apply corporate policies to the new systems before the PCs gain network access—a situation that exposes other PCs to malicious attacks from inside the network.
- PCs that are powered down or inoperative can't be located by software-only solutions.

Inaccurate inventories may also expose corporate officers to liabilities, such as from noncompliance with Sarbanes-Oxley and other government regulations.

Intel vPro technology: PC inventory capabilities built in

IT now has the ability to remotely and accurately inventory all PCs with Intel vPro technology (refer to Figure 3). This capability works even if third-party management agents are compromised or missing from the system.

Finding bare-bones PCs

For PCs with Intel vPro technology, inventory capabilities work even on bare-bones machines, before management agents have been installed. For example, a manager might buy and install 20 new machines, but forget to notify IT before plugging the PCs into the network. The result is a set of noncompliant machines that immediately expose the network to security threats, yet which can't be remotely managed because management agents aren't installed—IT can't recognize the PCs, let alone push security patches out.

Typically in these cases, a technician would go deskside to install the third-party software agents that enable remote management. With Intel vPro technology, that deskside visit is not necessary. Instead, the PC can be polled immediately as soon as it is plugged into a power source and connected to the network. When third-party polling software recognizes the noncompliant machines on the network, IT can be immediately alerted. IT can then remote-boot the machines from the IT console, read hardware asset information even before inventory agents are installed, and push the appropriate management, security, and other third-party applications out to the new PCs—all from the IT desk.

Hardware and software inventory for PC assets

Enterprises are under significant pressure to know how many software licenses to pay for, how many software and hardware assets to keep on maintenance contracts, which assets need recertification, and which need updating, securing, and/or upgrading. Unfortunately, assets which have been sold, discarded, lost, or retired, may not be automatically removed from maintenance contracts or license lists, a situation which causes underreporting of some assets and overpurchasing of others. On average, today's businesses overspend on asset maintenance and licensing services by a factor of 2.[1]

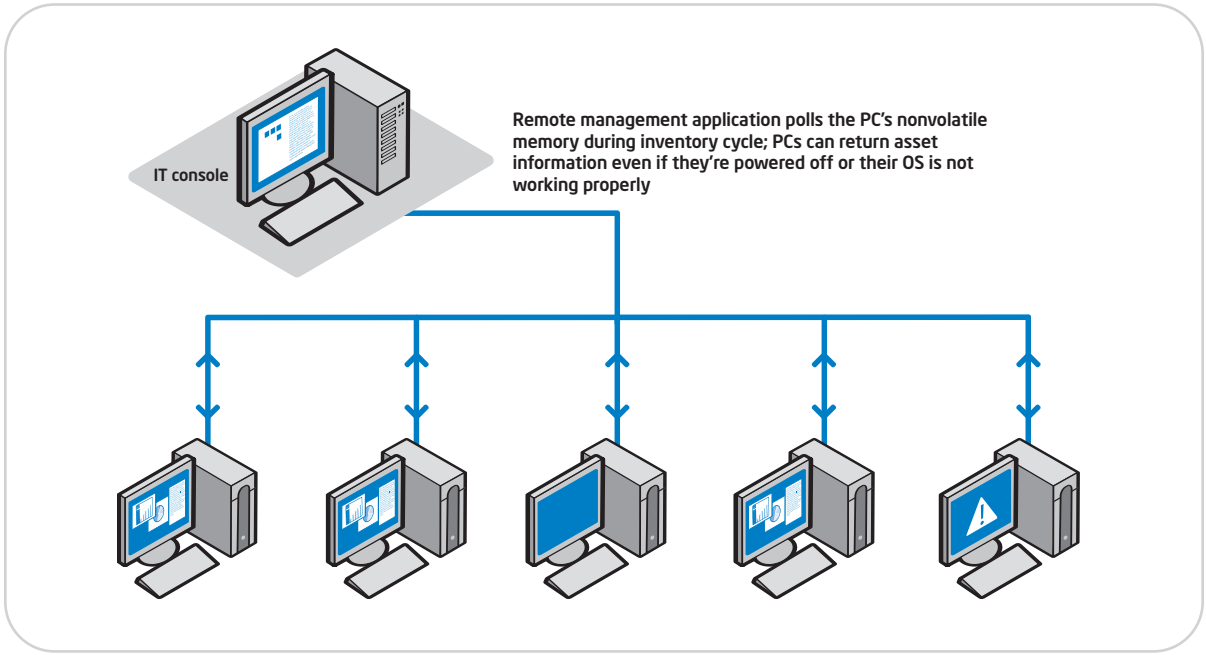


Figure 3: Inventory PCs anytime. IT can now inventory PCs and get hardware and software asset information even if management agents are not installed, PC power is off, or the OS is down.

Intel vPro technology: Hardware and software inventory capabilities built in

PCs with Intel vPro technology ease the hardware and software inventory burden by allowing third-party management applications and/or the IT console to use three main capabilities:

- Write asset and other information (or pointers to asset information) into persistent memory.
- Poll a system for asset information anytime.
- Power up PCs that are off, so IT can perform any necessary inventory tasks, and remotely power the PC back down to the state in which the user left it.

Tedious manual inventories can now be reduced, saving significant costs in labor. Unused software licenses can be appropriately reallocated to other resources, while hardware assets can be better utilized and warranties better managed. At the same time, businesses can be more confident that their audits are in compliance with government regulations.

Remote management for problem resolution

One of the most critical IT needs is to be able to remotely resolve PC problems, especially when a system is powered off or its OS is down. According to industry studies, deskside and service-center calls make up only 20% of PC problems in a typical business, but they take up 80% of the budget.[1] In fact, the cost of a deskside visit is seven times the cost of a remote problem resolution. According to an Intel study[1] of 44,000 trouble tickets, approximately 40% or more of the cost of deskside and service center calls could have been eliminated if IT had had better remote capabilities for problem resolution.

Remote problem resolution has traditionally been difficult, in part because boot failures can trigger costly, reactive management processes. User downtime is also exacerbated by time-consuming diagnostic visits, while deskside visits pull IT off other tasks. Even when problems can be diagnosed or resolved remotely, trying to talk a user through a troubleshooting process over the phone can be an exercise in frustration and inefficiency.

Intel vPro technology:
Remote manageability built in

PCs with Intel vPro technology can significantly reduce the number of deskside visits IT must make, by providing powerful hardware-based tools for remote problem resolution, even when the PC's power is off or its OS is unavailable:

- Remote boot through integrated device electronics redirection (IDE-R), a more powerful and secure capability than wake-on-LAN (WOL) and PXE (pre-execution environment).
- Persistent event logs, so IT can see what happened before a problem asserted itself; for example, a low-voltage power supply or a temperature zone too hot.
- Always-available asset information in a tamper-resistant space, so authorized IT can get software version information as well as hardware make, model, and warranty information to help troubleshoot, diagnose, and repair a PC without a deskside visit.
- Remote console redirection through Serial over LAN (SOL).
- Policy-based alerting that conforms to industry standards, for platform hardware sensors, hardware failures, OS lockups, and platform boot failures.

Resolving software problems remotely

An inoperative OS traditionally requires a deskside visit for reboot and rebuild. Intel vPro technology now enables IT to resolve many OS problems remotely.

For example, if a system becomes inoperable (refer to Figure 4), IT can use IDE-R to change the system's boot device to a CD or to an image located on a remote network drive, such as a service drive. IT can then establish a remote console session (using SOL) to walk the machine through a troubleshooting session. If a user application has become corrupted, the technician can remotely reimage the user's hard drive and restore the user's data from known-good files, overwriting corrupt or problem files. The user is back up and running as quickly and efficiently as possible.

Reducing deskside visits for hardware failures

Traditionally, when a hardware component (such as a hard drive) fails, the user calls IT, and a technician goes to the user's desk—sometimes several times—to diagnose the problem, find out the part's make and model numbers, install the new part, and perform the lengthy rebuild.

When using PCs with Intel vPro technology, IT can receive an immediate system alert when a hardware component fails, sometimes even before the user notices. IT can then remotely note the make, model, and warranty information for the component that needs replacing. The technician can then pick up the right part from inventory and reimage the drive right from the IT console. The technician might make only one deskside visit: to install the new hard drive to get the user back up and running.

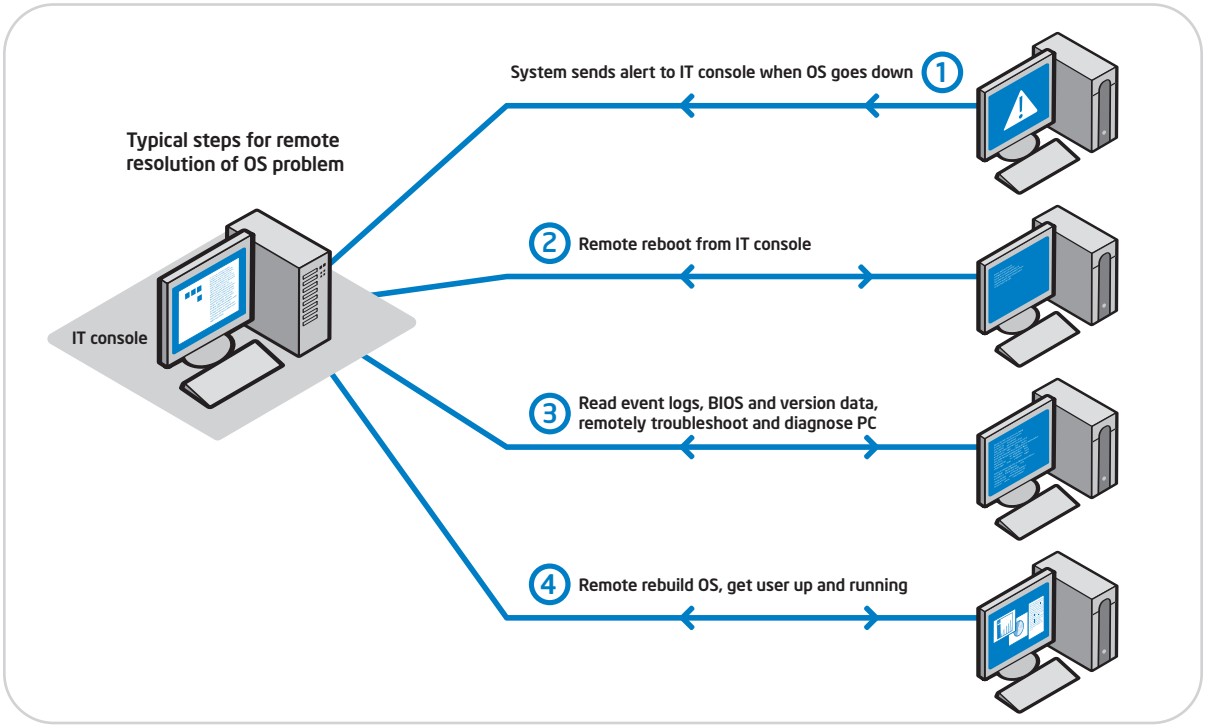


Figure 4: Remote problem resolution. IT can now boot, troubleshoot, diagnose and remediate PCs down the wire, even if the OS is inoperable.

Defining the alerts sent to the IT console

All system alerts generated by PCs with Intel vPro technology are written into the event log stored in nonvolatile memory. The tamper-resistant event log can be accessed anytime by authorized IT.

Third-party management applications define which of the alerts are also sent to the IT console and/or which will trigger an action (such as an immediate asset poll). This allows IT to specify the type of alerts they want to receive—so less critical alerts do not add substantially to network traffic—while remaining confident that low-priority alerts are not lost if a system is compromised or becomes problematic.

Managing a mixed environment

The management capabilities inherent in Intel vPro technology allow for a phased-in or integrated implementation of systems. PCs with Intel vPro technology use the same management console and the same communication mechanisms as other PCs, so the transition to a remotely managed environment is both easy and simple.

Proactive security

The most critical challenge in business today is securing PCs from malicious attacks. Even the best software-only solution can't manage or secure systems that are powered off or whose OS is unavailable.

Three layers of defense

Intel vPro technology gives IT two new layers of hardware-based security capabilities to deal with malicious attacks (refer to Figure 5). IT now has three distinct layers of protection for PCs, including hardware filtering of inbound and outbound network traffic, "heartbeat" presence checking of third-party agents, and other key capabilities:

- First line of system defense: filtering threats and isolating PCs. Programmable hardware-based filters examine network traffic to identify threats, while a hardware-based "switch" can now disconnect the network data path (or set a rate limit) to contain threats more quickly.
- Second line of system defense: third-party software security agents. Hardware-based capabilities deliver remote visibility of PCs, constant presence checking ("heartbeats") of security agents, and access to preboot BIOS settings—even when security agents are disabled or the system OS is compromised or down.
- Third line of system defense: nonvolatile memory and dedicated environments. Even if a threat gets past other defenses, IT now has access to persistent memory where critical information can be protected. IT can also use a self-contained, dedicated virtual environment to intelligently examine, isolate, and manage applications and data in the user OS. (Refer to the virtualization section beginning on page 11 for more information.)

These new layers of defense make it easier to identify threats faster and stop them more effectively before they begin to spread.

Filtering threats and isolating PCs

Software-based security applications typically rely on agents installed on top of the OS to secure a PC. The main problem in this approach is that users, hackers, and viruses can remove or disable security agents and alerts, creating critical vulnerabilities. When systems are compromised or unresponsive, IT can't usually push updates or enforce compliance remotely—or even locate the PC if other management agents have also been disabled.

Intel vPro technology enables third-party software to proactively:

- Identify more threats before they reach the OS.
- Isolate compromised systems more quickly.
- Ensure that security agents stay active.

Hardware-based filtering to contain threats

Intel vPro technology provides IT with programmable hardware filters for examining network traffic behavior. These filters examine packets passing into and out of the OS software stack. The PC itself can now help contain threats by implementing IT policy to filter inbound and outbound OS traffic.

Filtering is done by examining source, destination, and port address within the packet headers. Because the filters are programmable, management software can define the events triggered by proscribed packet behavior, such as log an alert, send an alert to IT, or trip a threat-containment "switch."

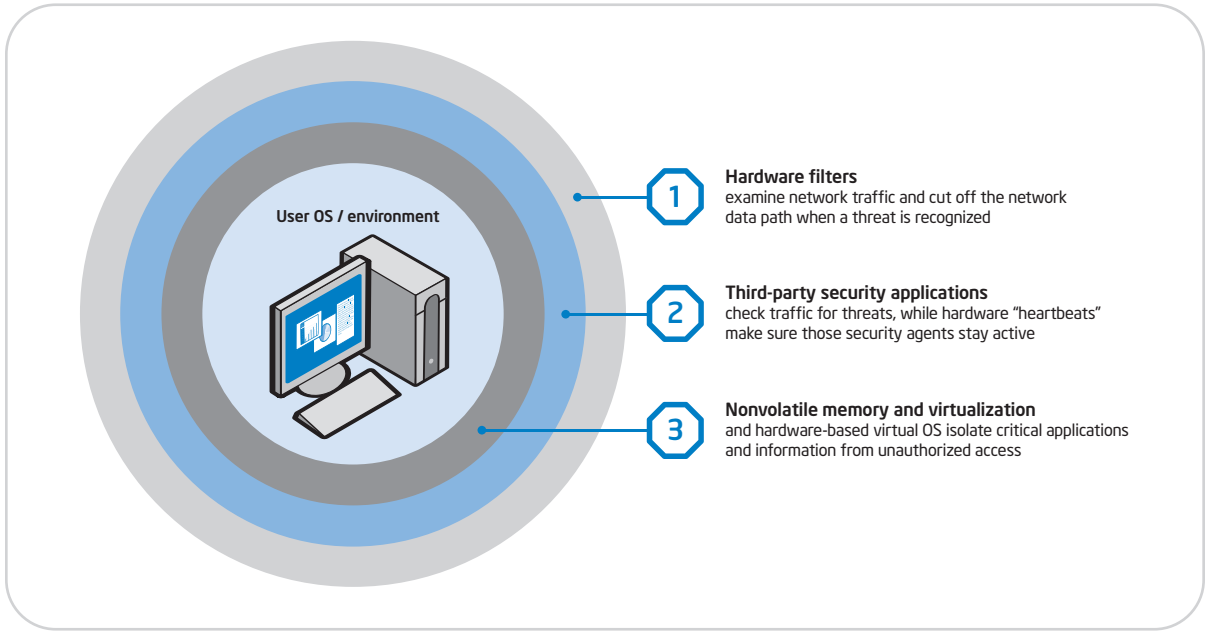


Figure 5: Three layers of defense. PCs with Intel® vPro™ technology have two new layers of defense against threats in inbound network traffic.

Switching off the network data path to contain threats

When a hardware filter identifies unauthorized packet behavior, PCs with Intel vPro technology can contain the threat by disconnecting their own OS from network communications (refer to Figure 6). The PC switches off the network data path at the OS software stack, before the network traffic actually comes into the OS. The system can also set a rate-limit for network traffic, to help IT investigate a potential threat.

IT can still communicate with the underlying hardware of the PC through the built-in, hardware- and firmware-based communication stack. IT can then use remediation software to correct the problem and bring the PC back into the enterprise network. Because only OS network communication is switched off, user applications (such as word processing and spreadsheets) can remain enabled, so user uptime is not affected. (Refer to the virtualization discussion beginning on page 11 for a description of how virtualization provides an additional level of isolation.)

Hardware heartbeats for third-party agents

Traditionally, IT has used serial polling to verify the presence of security agents. PCs with Intel vPro technology use a regular, programmable "heartbeat" presence check, which is built into the management engine. The heartbeat uses a "watchdog" timer so third-party security software (or other business-critical applications) can check in with the manage-

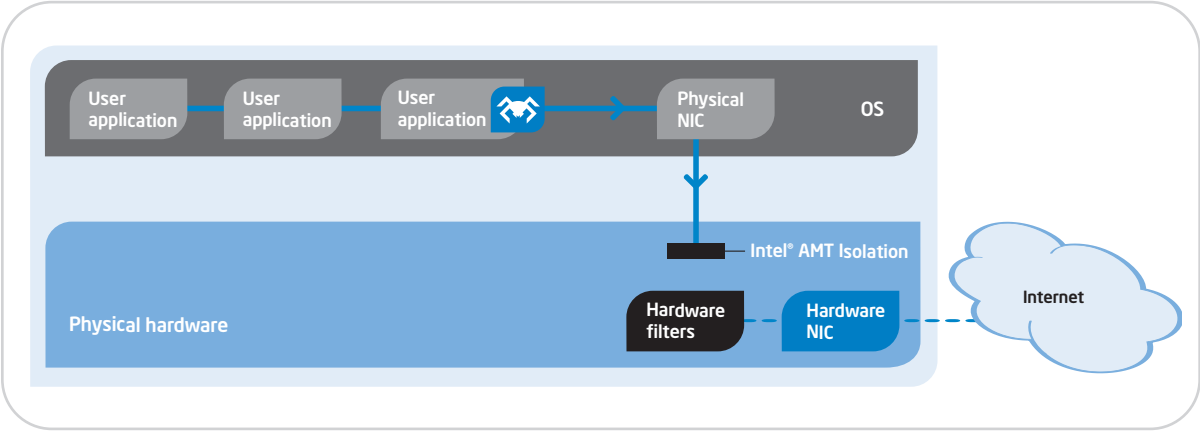


Figure 6: Hardware filters inspect outbound network traffic. When a threat is recognized, the PC can cut off its own network data path and quarantine itself—even if its OS is not available—to help prevent threats from spreading to the network.

ment engine at programmable, one-second intervals, to confirm that the agent is still active.

Each time an agent checks in, it resets its timer. If an agent hasn't checked in before the timer goes off, the agent is presumed removed, tampered with, or disabled. The management engine then automatically and immediately logs the alert and notifies (if specified) the IT console. A PC with Intel vPro technology can monitor up to 16 different agents.

With hardware-based heartbeats, the PC itself helps improve the reliability of presence checks and helps reduce the window of software vulnerability.

Security capabilities help PCs that don't have built-in filters or isolation

Because PCs with Intel vPro technology can reactively isolate and block themselves from the network, they help prevent threats from being passed to other PCs. In this respect, PCs with Intel vPro technology act like a buffer for other PCs, to help protect even those systems that do not include the advanced, hardware-based security of Intel vPro technology.

Using the existing management console to update filter policies

PCs with Intel vPro technology use the same management console and communication mechanisms as other PCs, so IT does not have to change their management console when deploying PCs with Intel vPro technology.

Push updates and patches down the wire regardless of PC power state

Before Intel vPro technology, IT could not remotely push updates to machines that were powered down. Instead, IT had to catch those PCs later, when they were powered up again—a process that allowed many systems to remain vulnerable to attack for dangerous lengths of time.

Critical update capabilities are built in

There are several methods in use today to wake a PC in order to push out an update, but those methods are not secure, or they work only when the OS is running properly.

For PCs with Intel vPro technology, IT can tell the system to wake up (or power down). Updates and patches can be done remotely and more securely, regardless of system power state or the health of its OS. IT can now:

- Check a PC's software version information and find out if anything needs updating, without waking up the PC.
- Remotely power up PCs from the IT console, so updates can be pushed even to machines that were originally powered off (or were in a sleep state) at the start of the maintenance cycle.

Ensuring compliance with corporate policies

PCs with Intel vPro technology let third-party applications store version and .dat file information in persistent memory, so authorized IT can check for compliance anytime. If a polling agent discovers software that is out of date, the third-party management application can remotely power up the PC, push the update, then remotely return the PC to its previous power state: on, off, hibernating, or sleeping, so users find their computers in the power state in which they left them. This allows IT to automate more management processes and make sure PCs with Intel vPro technology remain in compliance.

A dedicated virtual appliance

In PCs with Intel vPro technology, virtualization capabilities are built into the system's hardware. Third-party software vendors can now take advantage of these capabilities to build self-contained virtual environments, or "virtual appliances," that help manage and secure PCs. IT now has the option of using a dedicated tool to simplify and improve mainstream manageability and security for endpoint PCs.

Traditional virtualization

Virtualization technology is not new. It is actually a proven technology that allows IT to isolate and manage business-critical applications, operating environments, and information —even when all of those things are installed on a single PC. This helps improve trust in the integrity of management and security applications.

Until now, PC virtualization has primarily been an important niche model, where a specialized user needs to run more than one OS on the system. For example, a help-desk technician might use a partitioned PC to provide support for users on both Microsoft Windows* XP and Linux* OSs. A software developer might be required to maintain code for two versions of the same OS. Or, during an OS migration, both an old and new OS might be installed for an important user who must continue to use a legacy application.

Traditional PC virtualization has been both "heavyweight" and expensive (refer to Figure 7). It has meant building an entire "virtual PC" in each partition, from the heavy, underlying, complex OS, to the overlying set of full-featured user applications. This can require millions of lines of code and creates for IT all the maintenance issues of another PC.

And, because management and security agents are still installed inside the partitioned OS, they remain vulnerable to the problems that plague a typical OS.

Simplifying virtualization for mainstream use

In PCs with Intel vPro technology, virtualization capabilities are built into the hardware. IT can use these powerful systems for efficient, traditional heavyweight virtualization of multiple OS environments, such as Windows* XP, Windows* 2002 or Linux, all on the same machine. In fact, leading heavyweight VMM providers have already optimized their applications for these PCs.

However, although niche users may still need heavyweight virtualization on a PC, Intel's objective is to bring the advantages of virtualization to the mainstream business PC. To do this, Intel is focusing on addressing manageability and security concerns of IT.

Intel and leading third-party software providers are working closely to offer IT complete, self-contained, lightweight solutions for virtualizing management and security applications. These lightweight solutions will let IT run a user OS and a "service" OS at the same time. IT can now provide critical services to the user OS and network from a dedicated, tamper-resistant space.

What is a virtual appliance?

A virtual appliance is a self-contained operating environment dedicated to a particular function, such as manageability or security. It consists of dedicated-function application code, a relatively thin embedded OS, and select drivers (refer to Figure 7). The virtual appliance runs outside the user OS, so

Complementary types of outbreak containment

PCs with Intel vPro technology offer IT two powerful approaches for containing or isolating threats through Intel AMT or virtualization. Each approach has its benefits and capabilities. Each approach offers a different level at which to control threats, depending on the power state of the PC and the health of its OS:

Intel AMT	Virtualization
▪ Communication through the hardware- and firmware-based stack	▪ Communication through the OS software stack
▪ Options for responding to threat: log event, send alert, set rate-limit, switch off network data path before it reaches OS.	▪ Rich set of options for response to threat, based on capabilities of third-party virtual appliance
▪ Remote remediation from IT console based on hardware features	▪ Many remediation paths available, based on capabilities of third-party virtual appliance.
▪ Enabled even if PC power is off or the OS is down.	▪ Enabled when PC power is on and the OS is running.

Intel AMT and virtualization capabilities can be used together to provide a complete solution for managing and securing PCs. When an OS is enabled, the virtual appliance gives IT all the sophisticated control it needs for securing and managing endpoints. When an OS is disabled or PC power is off, Intel AMT lets IT remotely power up, boot, rebuild and remediate machines so the virtual appliance and other management or security applications can once again be used.

it is invisible to users and more secured from tampering. It is under the control of authorized IT.

The virtual appliance is like a gateway that sits between the user OS and the network. It provides a service to the user OS, and is the gateway through which all network communication passes. For example, if the virtual appliance detects a problem in network traffic or a deviation from IT policy, it can be enabled for the same type of sophisticated remediation as other third-party security or manageability applications. These responses include alerting, isolation of the user OS from the network, an integrity check of a management agent, or deployment of a local patch.

Sophisticated manageability and security

One of the main benefits of a virtual appliance is that it resides in a dedicated space that takes little to support or maintain, yet still delivers the sophistication of a third-party security or manageability application.

For example, to help secure endpoints, a security virtual appliance can now intelligently examine network traffic for malicious payloads or suspected intrusion attempts before the network packets are passed to the OS, where user applications might be affected. When the virtual appliance detects a problem or deviation from IT policy (refer to Figure 8), it can follow sophisticated remediation paths. These include proactive alerting, selective isolation of a particular communication port, hardware or software inventory, BIOS configuration reset, or deployment of a critical update. Because the virtual appliance is its own embedded OS, it can be programmed with a rich set of responses.

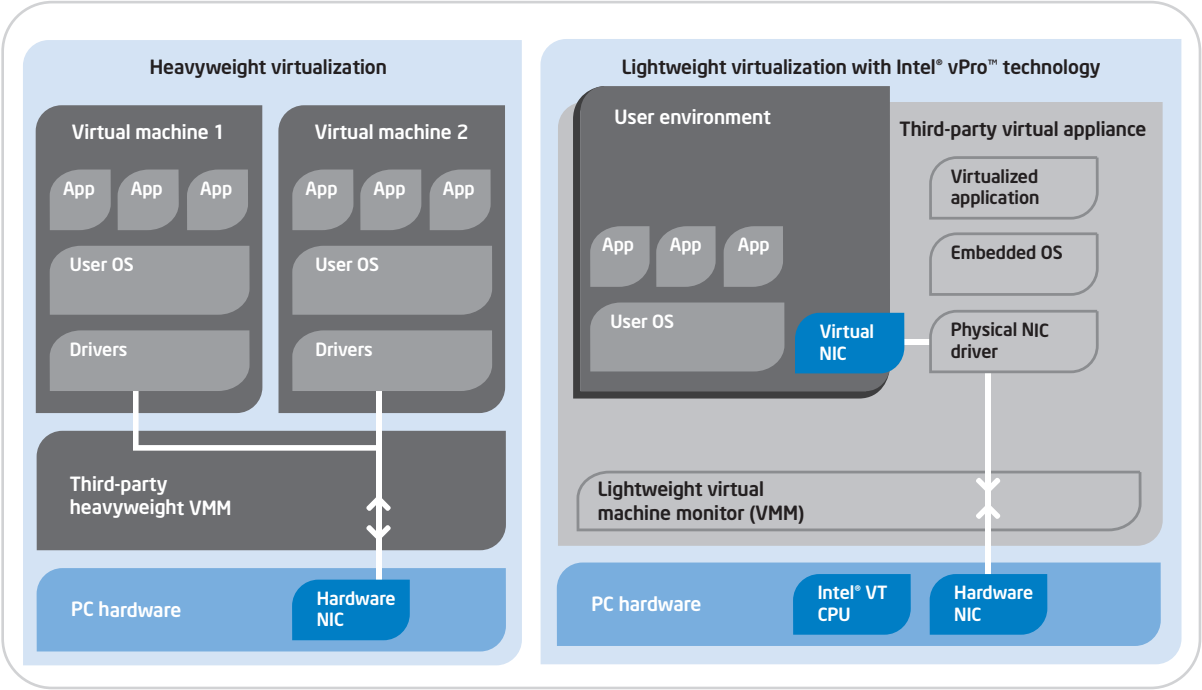


Figure 7: Heavyweight virtualization vs. lightweight virtualization. On PCs with Intel® vPro™ technology, virtualization is provided through a lightweight, dedicated-function third-party virtual appliance.

Isolation from the user OS

In order to remain under the control of IT and protected from threats, the virtual appliance is well-isolated from the user OS. Specifically, the user OS is not in direct control of the hardware. Instead, the user OS gains access to the network through a virtual network interface card (NIC). The physical NIC handles traffic between the virtual NIC in the user OS and the hardware NIC that passes communication on to the enterprise network (refer to Figure 7).

Isolated from hardware, the user OS and the virtual appliance run on top of a lightweight virtual machine monitor (VMM). The VMM acts as if it is another set of hardware—it abstracts the hardware for the OS, like an emulator (refer to Figure 9). The lightweight VMM convinces the user OS and its applications that the user OS "owns" the entire hardware platform. In these PCs, the virtual appliance is invisible to the user OS and under control of authorized IT.

Why choose to use a virtual appliance?

There are some powerful ways to use a virtual appliance to enhance security, manageability, or productivity:

- Protect critical agents. Install agents, critical business applications, and sensitive information within the virtual appliance, so they are more protected from tampering and/or removal. Even if a hacker could install a rogue application in the user OS, the virtual appliance would recognize that the rogue application was not authorized to access certain memory areas. The virtual appliance then prevents the rogue application from accessing sensitive files.
- Run tasks in the background. Isolate IT tasks in the virtual appliance, where they can be run outside of the user OS. This gives IT the ability to run tasks such as virus scan, antispyware, updates, and backups invisibly and unobtrusively, where they don't interfere with user applications or productivity.

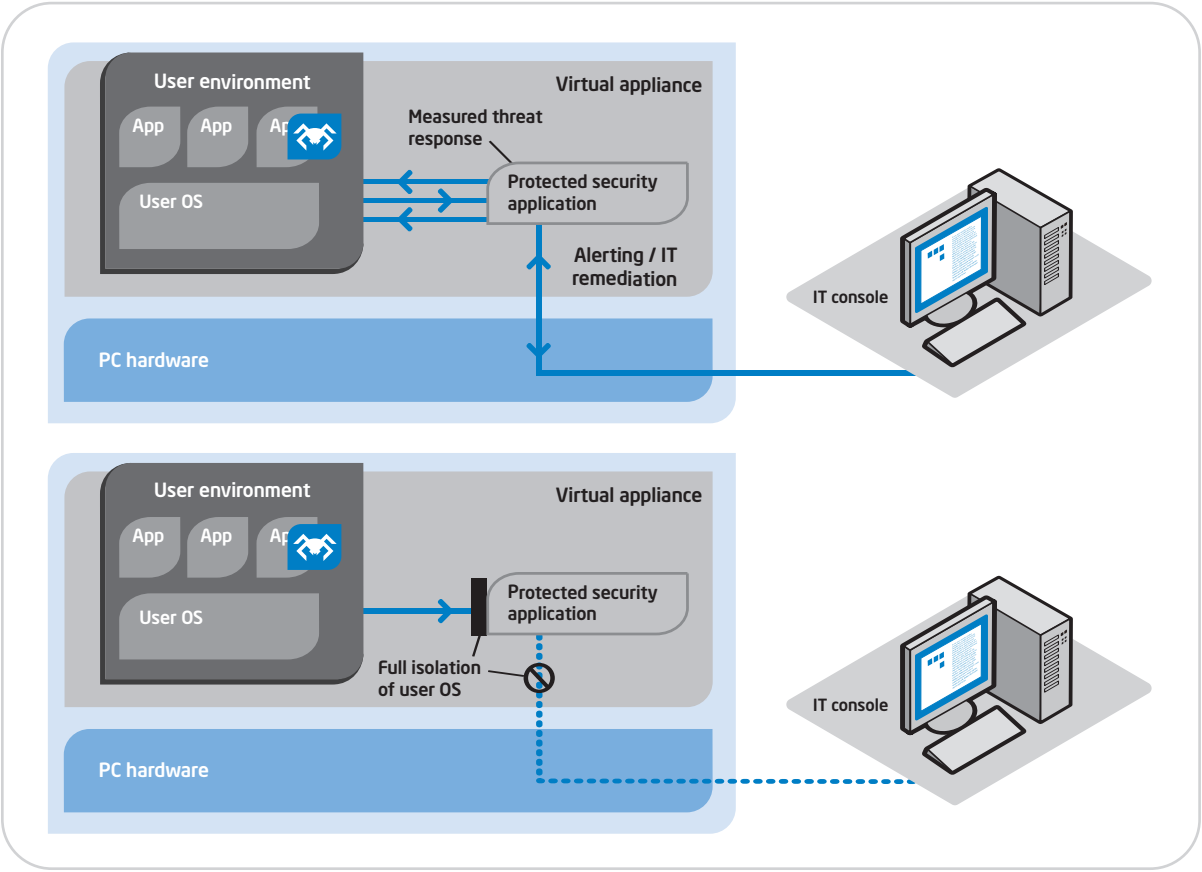


Figure 8: The virtual appliance offers sophisticated capabilities. Fully integrated application code offers IT a rich set of capabilities for management and security of the user OS. For example, a security virtual appliance can offer IT many remediation paths, from a measured response to full isolation of the user OS.

Virtualization is compatible with other technologies and third-party solutions

Intel has worked closely with market-leading security and manageability vendors to make sure third-party applications take full advantage of the power of Intel's hardware-based virtualization capabilities. For example, third-party vendors integrate the lightweight VMM, embedded OS, application, and Intel's virtualized NIC driver into their software solutions. This gives IT a turnkey solution that is easy to implement and simple to use.

Standard memory, storage, and graphics cards work with the virtualization technology. PCs with Intel vPro technology can also run off-the-shelf OSs and applications without IT having to perform special installation steps.

Finally, the hardware-based virtualization technology is designed to work with and complement other advanced Intel management and security technologies, such as Intel Active Management Technology.

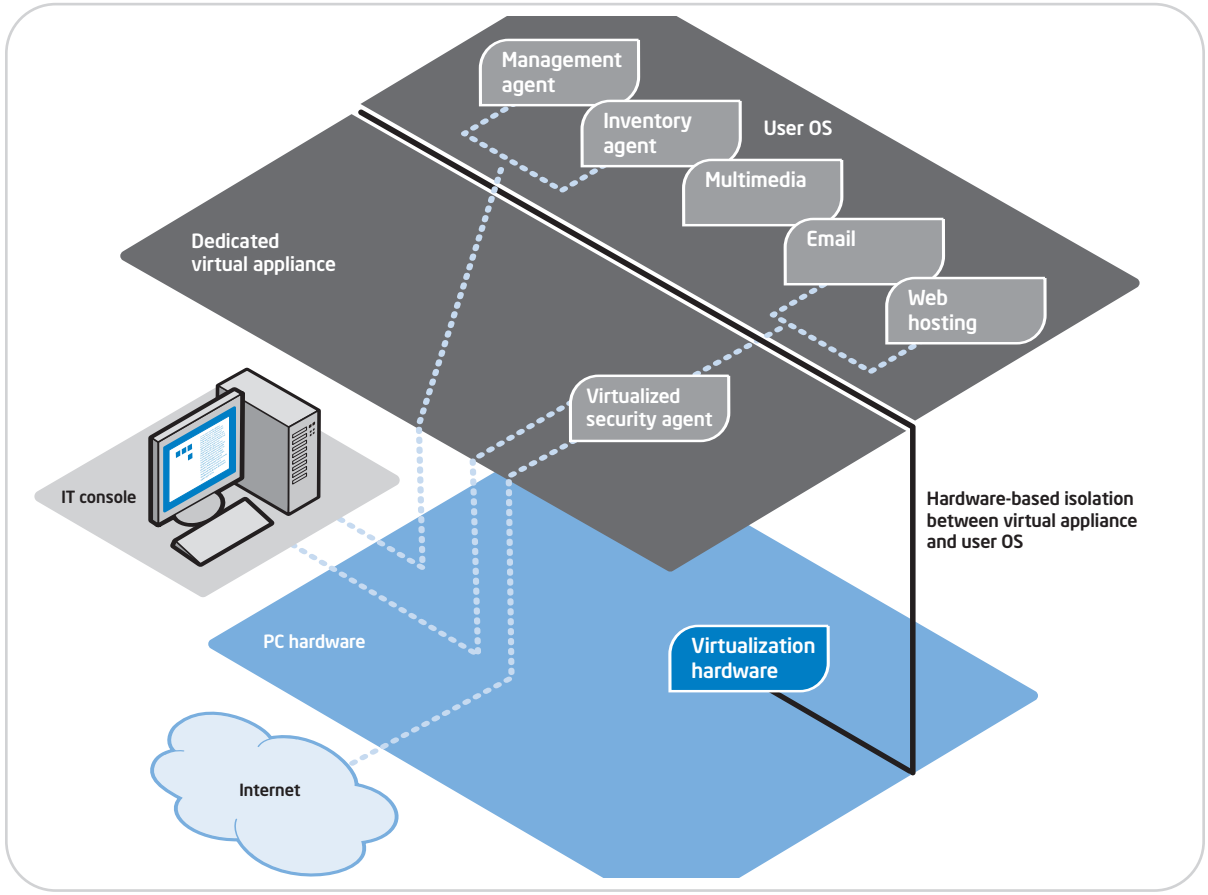


Figure 9: Virtualization "abstracts" the hardware from the software. IT can manage and improve the security of the PC through the stable, tamper-resistant virtualized environment—the virtual appliance—which runs outside the user OS.

Energy-efficient performance

In today's business environment, businesses need systems with the power to run IT tasks in the background while users run multiple applications in the foreground. At the same time, businesses can't afford to keep laying more power lines into their facilities just to provide users with the performance needed to get the job done. PCs with Intel vPro technology are designed to provide high performance in a power-efficient package.

The Intel® Core™2 Duo processor and Intel® Core™ microarchitecture

PCs with Intel vPro technology use the state-of-the-art, 64-bit, dual-core Intel Core 2 Duo processor based on Intel Core microarchitecture. This processor is optimized for improved multitasking responsiveness in 64-bit and 32-bit environments with significantly improved performance. The Intel Core 2 Duo desktop processor offers 40% more performance than previous generations and is more energy efficient.[2] For IT, this means that complex engineering programs (such as computer-aided design, or CAD), audio and video encoding, and other compute-intensive applications can be run simultaneously with IT background tasks like virus scans and antispyware. Critical IT tasks that help secure and manage PCs no longer need to interfere with user productivity. And, the new CPUs can operate at lower power, reducing power consumption and thus noise in the office.

Intel vPro technology: Cutting-edge performance and responsiveness built in

Energy-efficient platform technologies

Power coordination and thermal technologies allow PCs with Intel vPro technology to use less power while keeping the physical footprint to a minimum. Energy-efficient technologies also improve manageability for IT. For example, advanced fan-speed technology gives IT more accurate thermal measurements, more precise fan control and improved acoustics, better alerting, proactive system management, and improved problem resolution.

Stable and ready for the future, with broad industry support

PCs with Intel vPro technology are stable, standardized platforms with broad industry support, ready for future operating systems.

Windows Vista* Premium Ready

PCs with Intel vPro technology handle today's operating systems and are Windows Vista Premium Ready. This is important because a Windows Vista Premium Ready PC requires a configuration with at least 1 GB of system memory, support for the Windows Vista Aero* user interface and the Windows Vista Display Driver Model (WDDM), 128 MB of graphics memory and a modern processor (at least 1 GHz 32-bit or 64-bit processor). Since PCs with Intel vPro technology are Windows Vista Premium Ready, and the built-in graphics are ready to support the full Windows Vista Aero experience, migration to the new OS will be simpler.

The Intel Core 2 Duo processor provides the performance needed for the next-generation 2007 Microsoft Office*, including the performance for intense, always-on, text-based search indexing. For PCs with Intel vPro technology, upgrading and expanding to 2007 Microsoft Office is easier.

Broad industry support

New hardware technology doesn't mean much without software to take advantage of it. PCs with Intel vPro technology are already supported by major software vendors in management applications, security software, and business software. Desktop PCs with Intel vPro technology will be available from leading, worldwide desktop OEMs and will be supported by major IT outsourcers.

Stability and simplicity

PCs with Intel vPro technology are standardized in accordance with the Intel® Stable Image Platform Program (Intel® SIPP), so businesses can avoid unexpected changes that might force software image revisions or hardware requalifications. With Intel SIPP compliant PCs with Intel vPro technology, IT can be more assured of having a stable platform that simplifies the management and security of desktop PCs.

Intel vPro technology: Built-in manageability and improved security

Intel is uniquely positioned to provide critical business and IT capabilities on a desktop PC through extensive, breakthrough R&D, leading-edge manufacturing, and a unique ability to catalyze broad ISV support for creative solutions.

For IT, the result is the PC with Intel vPro technology, a professional-grade system designed from hardware to software with built-in capabilities that resolve the most critical challenges of business and IT—remote manageability and improved security—with energy-efficient performance.

With Intel built in, IT can address a wider range of enterprise needs and shift resources from managing and securing a fleet of PCs, to accelerating business into the future.

Enterprise capabilities on a small-business budget

For small businesses, Voice over IP (VoIP)[3] and high definition audio offer big-business functionality on a small-business budget.

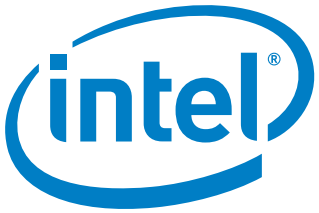
Voice over IP. PCs with Intel vPro technology include the latest Intel dual-core processor technology. These PCs deliver the performance users need to multitask while at the same time using VoIP applications for Internet telephony and business conferencing. Combined with the wide-band, high-fidelity audio built into PCs with Intel vPro technology, users will now experience a much higher quality of service. Even during conference calls and international calls, and even while users are multitasking with other applications, PCs with Intel vPro technology deliver a clear, crisp calling experience for today's business users.

Intel vPro technology lets business users with VoIP service:

- Call from anywhere they have Internet connectivity
- Check voicemail from a Web application
- Attach voice messages to email
- Make conference calls with up to 10 participants

High definition audio. Intel® High Definition Audio (Intel® HD Audio)[4] supports multiple audio streams and a microphone array, eliminating the need for a separate, discrete audio card for Internet telephony. Users can now conduct high-quality Internet phone calls—including conference calls—by plugging a standard, low-cost analog POTS ("plain old telephone service") headset into a PC with Intel vPro technology. Computer speakers remain active for system alerts, while the high definition audio handles rings.

Especially for small businesses, the telephony capabilities of the PC dial pad, speaker, and microphone eliminate the need for more expensive USB-based headsets.



To learn more about the built-in manageability, proactive security, and energy-efficient dual-core performance of Intel vPro technology, visit: www.intel.com/vpro

[1]Source: Intel White Paper: "Reducing Costs with Intel® Active Management Technology," published August, 2005. To download the white paper, visit www.intel.com/go/iamt.

[2]When comparing Intel® Core™2 Duo E6700 to Intel® Pentium® D Processor 960, performance based on SPECint*_rate_base2000 (2 copies) and power reduction based on Thermal Design Power (TDP).

[3]Voice over Internet Protocol (VoIP) capability requires a high-speed internet connection, PC headset or speakers and microphone as well as third party software. VoIP connectivity is provided by third party service providers and specific features may require you to purchase additional services. Internet services and/or VoIP services may not be available in all areas and are subject to compliance with all applicable laws and regulations.

[4]Intel® High Definition Audio—Some Intel® HD Audio functionality is dependent on actual implementation, controller, and codec.

Intel® Active Management Technology requires the platform to have an Intel® AMT-enabled chipset, network hardware and software, connection with a power source, and a network connection.

Intel® Virtualization Technology 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.

Printed in USA/0706/LKY/PMS/PP/13K Order Number: 311710-002US