Real-World Guide

Embedded Security in the 3rd Generation Intel® Core™ vPro™ Processor
Helping IT Managers Gain Added Protection with Intelligent Performance

Why You Should Read This Document

This guide explains how the built-in security of the 3rd Generation Intel® Core™ vPro™ processor provides the additional layer of protection IT managers need to address the four pillars of IT security:

- Preventing viruses and malware through threat management, including rootkits and escalation-of-privilege attacks
- Strengthening authentication and protecting passwords through stronger identity and access security
- Improving data protection through faster encryption of sensitive business data and online transactions, and mitigating the risk of lost or stolen PCs
- Extending monitoring and remediation capabilities with powerful remote support, regardless of the operational state of the PC
Real-World Guide
Embedded Security in the 3rd Generation Intel® Core™ vPro™ Processor
Helping IT Managers Gain Added Protection with Intelligent Performance
MAY 2012

Sponsors of Tomorrow.™
Contents

3  Time for Change in IT Security
4  Managing Threats
6  Strengthening Identity and Access
8  Protecting Data
11  Monitoring and Remediation
13  Innovative Design—Without Sacrificing Security
15  Next Steps
16  Intel Resources for Learning More
Time for Change in IT Security

Today’s rapidly changing business landscape is taking client security challenges to a new level. Security threats have grown far beyond the annoying viruses and amateur hacking of the past. From rootkit attacks to international security breaches and everything in between, the threats are far more advanced and stealthy. There are also far more of them: There has been a substantial increase in the number of unique pieces of malware and malicious web sites discovered each month.

Complicating matters is the evolution of a more mobile and socially connected workforce. IT must adopt new delivery models, such as cloud computing and desktop virtualization, which bring a brand-new set of security risks to the table. And yet another difficulty is the growing number of tech-savvy workers who are putting pressure on IT to support new mobile clients with seamless connectivity.

Added Protection from the 3rd Generation Intel Core vPro Processor

To meet the needs of this fast-moving environment and stay ahead of sophisticated security threats, you need a comprehensive PC security solution. And that solution must address the four pillars that define IT security for most enterprise operations: threat management, identity and access, data protection, and monitoring and remediation.

While software-based solutions are at the foundation of most PC security management systems, there’s a way to increase that protection at the hardware level, below the operating system. By using the embedded security technologies available in the 3rd Generation Intel® Core™ vPro™ processor, you can gain an added layer of protection across each pillar to strengthen your existing PC security.

The Purpose of This Guide

The purpose of this guide is to show you how the built-in security technologies in the 3rd Generation Intel Core vPro processor can help you stay ahead of today’s sophisticated security threats. By incorporating these embedded technologies as part of your PC security strategy, you can gain the additional protection you need below the operating system.

This guide describes how the 3rd Generation Intel Core vPro processor can help you:

- Proactively navigate today’s sophisticated threat landscape.
- Address the four pillars of IT security with additional hardware-based support.
- Offer new innovative form factors that your users want, without sacrificing security.

Four Pillars of IT Security

- **Threat management** is about preventing viruses and malware, such as rootkits and escalation-of-privilege attacks.
- **Identity and access** pertains to strengthening authentication and protecting passwords; a simple user-name and password solution is no longer enough.
- **Data protection**, arguably the most critical IT security need, is about encryption for sensitive business data in the cloud as well as for online transactions, and mitigating the risk of lost or stolen PCs.
- **Monitoring and remediation** extends across all the pillars with powerful remote support capabilities for proactive security management, monitoring, and remediation—regardless of the operational state of the PC.
Managing Threats

The first line of defense, threat management, starts with the prevention of viruses and malware. Although software-based solutions have been a successful prevention resource, today’s escalating threat landscape requires a new approach. Organizations need to guard against advanced persistent threats and an explosion of malware that is growing every day.

Prevent Rootkit Attacks

Rootkit attacks—one of the most serious forms of malware—can be difficult to detect using traditional antivirus strategies. These attacks give a hacker root-level access to a computer that can occur without detection and proceed to infect key system components such as hypervisors. Complex threats like this underscore the need to establish additional protection for both your virtual and your physical computing environments. With Intel vPro processor technologies, you can gain built-in protection against the persistent threat of rootkit attacks and other forms of malware.

How It Works

Intel Trusted Execution Technology\(^1\) (Intel TXT) and Intel Virtualization Technology\(^4\) (Intel VT) perform regular integrity checks on client system components to actively prevent viruses and malware from entering your network. These technologies work below the operating system to validate the behavior of key client system components at start-up. This works to prevents threats, and also establishes a root of trust to create a protected, measured launch environment.

Moreover, Intel VT can help boost security in a virtualized environment, as well as alleviate some of the issues associated with software-based virtualization, such as poor performance and excessive overhead. It works by shifting much of the burden of software-based virtualization to the hardware to simplify virtualization, reduce overhead costs, and significantly improve performance to near-native levels.

More about Intel® Trusted Execution Technology

Keep Attacks from Taking Hold

Taking this one step further is the need to prevent attacks from digging in below the operating system, where they can do the most damage. One example of this is escalation-of-privilege attacks, which occur when a hacker gains elevated access to your network and its associated data and applications to put all of your sensitive business data at risk. In a vertical attack, the hacker can grant himself higher privileges and run unauthorized code in your environment. In a horizontal attack, you are at risk of confidential data loss or identity theft when the hacker assumes the identity of another user with similar privileges.

How It Works

With Intel OS Guard, you can help protect your operating system from escalation-of-privilege attacks and gain broad security for your clients. This built-in security technology works constantly to deliver extensive, automatic "blanket" protection that helps defend against these sophisticated attacks and prevents viruses from taking hold deep in your system.

Securing Evolving Compute Models

Intel® Trusted Execution Technology (Intel TXT) improves security in virtualization environments with these key capabilities:

- Protects information from software-based attacks by allowing software to build a chain of trust from the "bare-metal" hardware to a fully functional virtual machine monitor (VMM)
- Shields security credentials during power transitions
Strengthening Identity and Access

The next line of defense, identity and access, is about strengthening authentication and protecting passwords. Strong authentication is no longer an option for the enterprise—it’s a requirement. Whether it is for securing VPN access or protecting access to software-as-a-service (SaaS) applications, a simple username and password solution is no longer adequate.

Many enterprises have long deployed strong authentication solutions, such as one-time-password (OTP) credentials or public-key infrastructure (PKI) certificates, either on tokens, on smart cards, or via software-only provisioning. However, recent data breaches have exposed vulnerabilities with these traditional forms of account protection, illustrating just how aggressive fraud has become with the installation of key-logging and screen-scraping malware into enterprise networks.

Validate Using Two-Factor Authentication

With two-factor authentication from Intel vPro technology, you gain a simple way for web sites and business networks to validate that a user is logging in from a trusted PC. Embedded support for identity and access security helps enterprise IT departments protect their access points while reducing costs over traditional hardware-token or smart-card methods.

How It Works

Intel Identity Protection Technology (Intel IPT) provides hardware-based two-factor authentication. Intel IPT is embedded in the processor and works with industry-leading authentication solutions to support hardware-based storage of tokens or certificates. By eliminating the need for a separate physical token, it simplifies the VPN login process, and more importantly, ensures that the PCs accessing your VPN are those assigned to your employees. Because the credential is secured inside the platform, it cannot be compromised or removed from a particular PC.
Comparing Intel® Identity Protection Technology to Token-Based Authentication

- Token-based authentication solutions require additional costs, ranging from the costs of the back-end service or software and physical tokens, to the management costs of shipping, tracking, and activating replacement tokens.
- Intel Identity Protection Technology (Intel IPT) protects consumer assets, employee VPNs, suppliers, and partners—without requiring separate token hardware.
- Intel IPT helps minimize the common burdens of two-factor authentication, such as having to resend new tokens and users mistyping their one-time-password (OTP).

Block Screen-Scraping Attacks

Another critical step to protecting confidential company data is the ability to prevent screen-scraping attacks. With Intel vPro processor technology, you can bolster protection by offering safety in random numbers: The technology displays to the end user a secure PIN pad with randomly placed numbers. This PIN pad is created by the graphics hardware within the processor, making it invisible to the operating system.

How It Works

Intel IPT with protected transaction display prevents man-in-the-browser or man-in-the-middle malware from scraping a PC’s display by verifying a human presence at the PC. Because this screen is part of the integrated graphics within the processor, you can work confidently knowing it is never exposed to the software layer. Then, the ID and password are sent directly to the processor for authentication. Because Intel IPT is embedded in the hardware, there is nothing to lose or break.
Protecting Data

The third IT security need, and arguably the most critical, is data protection. Protecting sensitive company, employee, and customer information remains one of the biggest IT security challenges for organizations worldwide. The onset of cloud computing combined with the ever-increasing number of mobile PCs in today’s business environment has compounded the risk of data loss.

Encrypt Sensitive Business Data

When you have sensitive business data in the cloud, you need a fast, reliable technology in place to protect it. Encryption is a well-established method of protecting critical data, and it’s especially important for information covered by compliance regulations and standards, such as the Health Insurance Portability and Accountability Act (HIPAA) and Sarbanes-Oxley. The downside? Deploying a comprehensive PC encryption policy typically comes with a performance trade-off. However, with accelerated encryption technology built into the processor, you get faster data protection without any system slowdown.

How It Works

The accelerated encryption technology of Intel Advanced Encryption Standard New Instructions (Intel AES-NI®) encrypts data up to four times faster, and works quietly in the background without slowing performance or interfering with user productivity. Because the encryption blocks are executed in the hardware within the microprocessor, it reduces the possibility of side-channel attacks. In addition, the acceleration provided by Intel AES-NI allows the system to execute larger key sizes, therefore making data transfers more secure.

More about Intel® Advanced Encryption Standard New Instructions

Guard Your Online Transactions

Another important aspect of protecting business data is securing it as it moves over networks. Whether it’s online authentication over the Internet or e-commerce transactions, there is a critical need to ensure security and privacy while protecting against identity theft. This is another area where hardware-based encryption is critical.

How It Works

Intel SecureKey provides this built-in technology, which generates higher-quality random numbers so that data encryption is made even more secure for safer online interactions. This technology delivers:

• High-quality random numbers from a high-volume entropy source, making the numbers unpredictable

• High performance that is faster than most entropy sources available today

• Easy access, with instruction available to all applications and at any privilege level

• Secure hardware-based implementation that isolates the entropy source from software attack
Prepare for the Inevitable: Lost or Stolen PCs

Finally, perhaps the biggest risk of data loss is with a lost or stolen PC. With users on the go and laptop thefts on the rise, this risk has become a harsh reality. Aside from the obvious threat of confidential data loss, there is a risk of financial and legal exposure as well as a potential breach of compliance with regulations regarding data privacy. With embedded anti-theft support built right into the processor, you can protect laptops by rendering them useless to thieves.

How It Works
With Intel Anti-Theft Technology 4.0, you have the response power of an embedded intelligent client that works proactively to protect your data in the event of such loss. First, the client is smart enough to automatically disable itself locally if it detects someone attempting to hack into it, even before the user has realized that it has been lost or stolen. Second, if the PC is discovered lost or stolen but no hacking attempt has been made, IT can remotely access and disable it.

More on Intel® Anti-Theft Technology


Mitigating Costly IT Investigations with Intel® Anti-Theft Technology

- Tamper-resistant anti-theft security is built right into the PC hardware.
- Nondestructive protection makes the laptop easy to reactivate without harming hardware or data.
- The screen displays a unique recovery message that includes contact information to return the laptop to its owner.
Monitoring and Remediation

PC management has changed. The reality of today’s mobile business environment is that desk-side IT support visits are no longer a practical option. Users are working from any number of remote locations, while others are traveling worldwide and constantly on the go. And while software-based monitoring tools have long been a reliable resource for help-desk staff, the ever-growing trend of IT consumerization is reducing IT’s ability to control security.

The last line of defense, monitoring and remediation, extends across all aspects of IT security management. Hardware-based remote monitoring and remediation capabilities give you the ability to simplify IT management and enforce security for all of your users, regardless of their location. With powerful remote support tools, you can stay one step ahead of critical security threats by pushing updates to any PC at any time. And remote remediation tools make it easier to manage mobile PCs, whether it’s to diagnose a minor problem or to manage a possible security breach.

Simplify IT Management with Remote Support

Let's say you have a user who is traveling and suddenly unable to log in. Based on the information they've provided, you suspect that their PC has a virus. Security breaches like this can occur anytime, whether the user is sitting in their office or on the go, and they can result in potential data loss. When a breach or suspicious activity does occur, you need the ability to respond at any time, with the right resources in place for remediation. With Intel vPro processor technologies, these remote monitoring and remediation capabilities are embedded into the processor.

How It Works

Intel Active Management Technology 8.0 (Intel AMT) allows your help-desk staff to access and control any user’s computer, with the ability to resolve issues through all states, including reboot. You can proactively manage threats by pushing security updates to users before a breach occurs, and you can diagnose, isolate, and repair infected clients after a breach takes place.

Saving Costs—and IT Resources—with Intel® Active Management Technology

- Track all asset information remotely, whether the PC device is powered on or off.
- Work proactively by sending updates at any time and monitoring for potential problems.
- Use a remote IT console to manage issues, helping to reduce system maintenance costs and reduce the burden on IT resources.
- Reduce energy consumption with the ability to automatically power PC devices off during nonbusiness hours.
Moreover, you can do all of this work with minimal impact to user productivity. For the traveling user who is unable to log on, you can reboot their PC remotely. Then you can give that user the ability to read and respond to e-mail as you continue to work on the problem using “invisible” remediation tools, such as virus scans and other diagnostics. With "always available" access to system information, you can:

- Remotely poll wired and wireless PCs, regardless of power state.
- Write asset data into protected memory, including hardware asset data and software version information.
- Identify and remediate noncompliant PCs to simplify compliance management.

More about Intel® Active Management Technology

Innovative Design—Without Sacrificing Security

The built-in security and performance of Intel vPro processor technology is now available in a range of innovative form factors to meet the needs of any organization. From the compact all-in-one computer designs to thin and light laptops, these form factors deliver the power and style to appeal to your most discriminating users—without any sacrifices to IT security and control.

All-in-One Designs

For office environments with limited space, the all-in-one computer designs are a perfect fit with a compact, elegant design. These include all the embedded security technologies and intelligent performance capabilities of Intel vPro processor technology.

Ideal for creating, managing, and consuming content, all-in-one designs include Intel Turbo Boost Technology, Intel Hyper-Threading Technology, and Intel HD Graphics Turbo. The simplified design means simplified manageability: A locked configuration model helps minimize IT issues. Employees can get up and running quickly and increase productivity with wireless connectivity and intuitive interaction tools, such as a multitouch screen and convenient stylus for capturing notes and signatures.

Everything You Need: All-in-One

- High performance with greater power efficiency
- Lightweight, space-saving design
- Simplified manageability and smarter security
- Intuitive touch screen with multiple user interaction
- Increased productivity
Thin and Light Laptops

Things are looking up for mobile users. A new range of ultrathin laptops is designed to deliver the portability that users want with the compute power they need. These sleek, highly responsive PCs are thinner, lighter, and faster than previous models—all with an extended battery life to fit a mobile lifestyle.

With smarter, faster processors in a lightweight design, these laptops offer the perfect balance of style and performance:

- Intuitive performance boost as needed
- Highly responsive for running simultaneous tasks
- Enhanced battery life and powerful performance
- Embedded security with enhanced data protection
- Smooth high-definition (HD) video and audio

With a thin and light laptop, your users can get the convenience of a portable PC with the compute power to do any task.

Go Anywhere, Do Anything: Thin and Light Laptops

- Easy to carry and stow
- Sleek, stylish designs
- Powerful performance and security
- Highly responsive with an extended battery life
Next Steps

By incorporating these intelligent PCs into your computing environment, you can give users the flexibility and power they need while still maintaining full IT control. But it’s more than control; it’s about staying one step ahead of a changing threat landscape. A comprehensive PC security solution that includes embedded security within the hardware works proactively below the operating system to address the four pillars of IT security:

- Threat management
- Identity and access
- Data protection
- Monitoring and remediation

Find out how the embedded security technologies in the 3rd Generation Intel Core vPro processor can give you the additional layer of protection you need combined with the intelligent performance you expect from Intel.

### Intel vPro Technologies Overview

<table>
<thead>
<tr>
<th>Technology</th>
<th>Capabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intel® Trusted Execution Technology (Intel TXT)</td>
<td>Establishes hardware-based root of trust to defend against software attacks at launch</td>
</tr>
<tr>
<td>Intel Virtualization Technology (Intel VT)</td>
<td>Works with Intel TXT to deliver built-in protection against malware and rootkit attacks</td>
</tr>
<tr>
<td>Intel OS Guard</td>
<td>Delivers automatic “blanket” protection to defend against escalation-of-privilege attacks</td>
</tr>
<tr>
<td>Intel Identity Protection Technology (Intel IPT with public-key infrastructure (PKI))</td>
<td>Protects access points by working with authentication solutions to support hardware-based storage of tokens or certificates inside the platform</td>
</tr>
<tr>
<td>Intel Advanced Encryption Standard New Instructions (Intel AES-NI)</td>
<td>Encrypts data up to four times faster without slowing performance or interfering with user productivity</td>
</tr>
<tr>
<td>Intel SecureKey</td>
<td>Generates high-quality random numbers to enhance encryption for online transactions</td>
</tr>
<tr>
<td>Intel Anti-Theft Technology</td>
<td>Offers tamper-resistant security to detect potential theft with the capability to automatically disable PCs</td>
</tr>
<tr>
<td>Intel Advanced Management Technology (Intel AMT)</td>
<td>Provides remote support for proactive threat management and diagnosing, isolating, and repairing an infected PC, regardless of operational state</td>
</tr>
</tbody>
</table>
Intel Resources for Learning More

About the Intel Core vPro Processor Family

Security White Paper: The 3rd Generation Intel® Core™ vPro™ Processor
Read all about the embedded security features in the 3rd Generation Intel Core vPro processor in this white paper.

Overview: The 3rd Generation Intel® Core™ vPro™ Processor
Watch this animation to learn about the embedded security and hardware-enabled manageability of the 3rd Generation Intel Core vPro processor.

3rd Generation Intel® Core™ vPro™ Processors
Learn how intelligent clients can help you solve IT’s toughest challenges with hardware-based security and manageability.

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

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

Find out more about the embedded security technologies in the 3rd Generation Intel Core vPro processor.

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

**Intel® AES New Instructions Demo**

**Intel® Active Management Technology**
intranet.com/technology/platform-technology/intel-amt/

**Access Accounts More Securely with Intel® Identity Protection Technology**
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. 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/tpm.

4. Intel VT requires a computer system with an enabled Intel processor and BIOS, and a 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/technology/virtualization.

5. No system can provide absolute security. Requires an Intel OS Guard–enabled system with a 3rd Generation Intel Core vPro processor and an enabled operating system. Consult your system manufacturer for more information.

6. 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.

7. 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 intel.com/technology/vipt.

8. 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 intel.com/technology/vipt.

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

10. 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.

11. No system can provide absolute security. Requires an Intel SecureKey–enabled PC with a 3rd Generation Intel Core vPro processor and software optimized to support Intel SecureKey. Consult your system manufacturer for more information.

12. 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 thereto. For more information, visit intel.com/technology/vpro/.

13. 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, as well as modifications or implementation of new business processes. For more information, visit intel.com/technology/vpro/

14. Requires a system with Intel Turbo Boost Technology capability. Consult your PC manufacturer. Performance varies depending on hardware, software, and system configuration. For more information, visit intel.com/technology/turbo.

15. Requires an Intel Hyper-Threading Technology–enabled system. Check with your PC manufacturer. Performance will vary depending on the specific hardware and software used. Not available on Intel Core i5-750. For more information, including details on which processors support Intel Hyper-Threading Technology, visit intel.com/info/hyperthreading.
More from the Intel® IT Center

Real-World Guide: Embedded Security in the 3rd Generation Intel® Core™ vPro™ Processor 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.

Share with Colleagues  
Join the conversation #CorevPro