

Solution Brief

Symantec* Virtual Security Solution

Intel® vPro™ Technology

Symantec* Virtual Security Solution and PCs with Intel® vPro™ Technology



Company	Symantec* Corporation is a leading provider of solutions that help individuals and enterprises assure the security, availability, and integrity of their information
Business Challenge	Addressing the growing number of new PC threats and infection vectors, with a large percentage of these new attacks directed against the user's operating system and commonly used applications.
Technology Solution	Symantec* Virtual Security Solution ¹
Enhanced By	PCs with Intel® vPro™ technology

Increasing enterprise security through desktop virtualization

Symantec* and Intel are working together to provide innovative ways of using a virtual security solution to solve critical information technology (IT) challenges in desktop security. With this collaboration, Symantec will be able to take full advantage of the hardware-based virtualization capabilities built into PCs with Intel® vPro™ technology, to provide a new level of security for desktop PCs.² These capabilities allow critical security applications to run in the background in a virtual partition—or “virtual security solution”—even while users are working on their own compute-intensive tasks in their own user operating system (OS) environment. This helps keep vital security processes isolated from potential problems with the main OS. It also helps keep security processes isolated from threats that may arrive on the desktop PC through means other than network vectors.

When used on PCs with Intel vPro technology, the new virtualized Symantec security solution will help IT gain better control of endpoint security, and at the same time, take advantage of “always-on” security capabilities. For IT, a virtual security solution will simplify management, make better use of administrative resources, increase confidence in endpoint security, and help improve system and regulatory compliance of desktop PCs.

Today's challenges

The complexity, frequency, and malicious intent of security attacks from many sources are increasing in today's enterprise. Likewise, IT administrators are seeing a marked increase in vulnerabilities in the OS and applications. Successful attacks cost significant time and money to remediate.

Currently, the period between the announcement of a vulnerability and the introduction of an exploit for that vulnerability is about six days, and that time may continue to decrease.³ The threat landscape has reached a point at which exploits can arrive on almost the same day a vulnerability is uncovered—"zero-day" attacks. These attacks place a significant burden on IT to deploy patches as soon as possible, even before patches have been fully tested. Because an exploit can now arrive before a patch is deployed to guard against it, the desktop PC is increasingly vulnerable when only traditional protections are installed on the machine. What IT needs is a separate, proactive protection layer to help guard against zero-day threats.

To make the situation even more challenging, such protective solutions can themselves be threatened by running security in an OS that has been compromised with a successful infection. The infected desktop OS can then affect the performance—or even the availability—of the additional security solution.

With the security threat landscape in an enterprise changing on a daily basis, security vendors must develop more innovative ways to protect desktop endpoints. Evolutionary security enhancements have just managed to keep pace with threats, but it is clear that more revolutionary security models will be needed to secure the desktop in the future.

The solution: Symantec and PCs with Intel vPro technology

To make the next leap in enterprise security, Symantec is taking full advantage of the new hardware-based capabilities built into PCs with Intel vPro technology. These capabilities will help Symantec build a tamper-resistant virtual security solution for IT. The security functionality will "live" in a secure space that runs outside the user OS, where it will be unaffected by issues with the user OS. This solution offers IT a separate, stable environment from which to protect the desktop from intrusions, such as zero-day attacks.

When installed on PCs with Intel vPro technology, Symantec's security solution increases IT's confidence in desktop security,

and its ability to administer security services across all desktops in the enterprise.

A more efficient virtual model

Traditional virtualization on a PC has been both "heavyweight" and expensive. Its purpose is to create multiple virtual PCs on a single machine. Each virtual PC then has a full set of drivers, a complete complex OS, and full-featured user applications. For IT, traditional virtualization multiplies all the overhead requirements of a typical PC, from management to security, maintenance to repair.

PCs with Intel vPro technology can be used for traditional virtualization. However, IT does not need another complete PC to perform vital security tasks for an existing PC. IT needs a more secure, isolated environment where critical applications are protected, and where security services can be more effective in dealing with threats to the user OS.

In collaboration with Intel, Symantec will offer IT more efficient desktop security through a new type of security solution that will run in a separate, self-contained environment enabled on PCs with Intel vPro technology. It consists of dedicated-function application code, a relatively thin embedded OS, and select drivers. It runs outside the user OS, so it is invisible to users and well-secured from tampering. And, independent of the user OS, the virtual security solution is under the control of authorized IT administrators. With the Symantec security solution, IT now has a simplified, self-contained operating environment dedicated to a specific function (in this case, security), instead of having another full PC to manage and secure.

Virtual environment independent of the user OS

In today's threat landscape, virus scanning in the user OS is insufficient protection to secure desktop endpoints. In fact, many threats try to disable virus-scanning and other security applications as the first step in an attack.

When used with the Symantec virtual security solution, a PC with Intel vPro technology helps protect itself. Within these PCs, the security solution operates in an isolated virtual partition, protected from viruses, worms, and other threats that are normally targeted at the user OS. The security solution can now continue efficiently protecting the desktop endpoint with less interference from such threats.

Isolated from the user OS, the solution is also the first program to boot up and the last to shut down on the PC. This means the solution can monitor the boot-up and shut-down sequences of the user OS to help prevent interference from threats that target those processes when other security programs are not running.

The security solution is not only independent of the health, or “state” of the user OS, it is isolated even from differences in versions of the user OS. For example, even when the user OS is updated, the virtual security solution is independent of those updates and may not need to be modified. This provides IT with a stable space from which to operate and administer security processes.

Enforcing corporate and regulatory compliance

With hardware-based virtualization technology, Symantec can offer IT the hooks and levers inside the PC’s own architecture to better control and customize systems to their specific environments. This is particularly important as, from both a systems standpoint and a regulatory aspect, compliance management is increasingly important in today’s businesses.

By taking advantage of the isolated, tamper-resistant environment enabled by PCs with Intel vPro technology, Symantec’s virtual security solution helps enhance IT management. Because the solution works even if the user OS is compromised or down, IT can now receive more accurate information for compliance and day-to-day IT management reporting.

Addressing a fundamental shift in the threat landscape

One of the major trends in today’s PC environments is a shift in the threat landscape from attacks based on personal pride, to attacks meant to generate money or notoriety. Just three years ago, most attacks were perpetrated by individual hackers who wanted the glory of having broken into a company’s computing environment. Or, most hackers wanted the glory of having spread a virus around the world, with all the attendant media coverage that came with their actions. Today, the landscape has shifted to cyber-crime attacks designed to steal information to sell or threaten to shut down a company’s business if a ransom is not paid. Both these activities are examples of more malicious, targeted, silent attacks that are becoming a larger part of today’s threat landscape.

The virtualized solution, isolated from the user OS, offers IT an additional level of security that speaks to real business continuity gains and protections against these new, cyber-crime threats. This is a level of security IT has not had before, one based on hardware and “firmware” capabilities that are deeply embedded in the platform itself, and tamper-resistant to hackers and would-be thieves. By taking advantage of these hardware capabilities, the solution significantly improves the protection of security, management, and other IT agents from unauthorized access and malicious attacks.

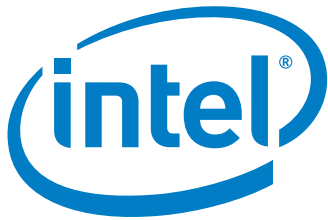
Summary

Symantec’s use of Intel’s hardware-based virtualization technology will offer a major step forward in enterprise security. For IT, the new security solution will deliver improved deployment, administration, threat mitigation, and trust, leading to better compliance. And, the cost of owning and managing PCs can be reduced. Interruptions in user productivity can be mitigated, infrastructure investments capitalized upon, and end-user systems better protected.

The Symantec virtual security solution will be seamlessly integrated with other Symantec solutions and the powerful new, hardware-based capabilities built into PCs with Intel vPro technology. This is not just another security solution. It is an innovative approach that demonstrates Symantec’s continued leadership in pioneering IT security models, and which creates a new layer of security that will be more effective in protecting critical information and applications.

SOLUTION BENEFITS

- **Resilient security through a dedicated, tamper-resistant virtual solution**
- **A more stable environment, which translates into reduced management complexity**
- **Always-on security model that helps ensure system and regulatory compliance**
- **Isolation of the security solution from the health of the user OS**



For more information

PCs with Intel vPro technology give IT administrators critical, hardware-based security and manageability capabilities not available in software-only solutions. When provisioned with third-party software, these PCs make it easier for IT to manage and secure desktop systems directly from the IT console, regardless of PC power state or the health of the OS.⁴

For more information about PCs with Intel vPro technology, visit
www.intel.com/vpro

For more information about this Symantec security solution, visit
www.symantec.com



¹ All content regarding the Symantec* virtual security solution was provided by Symantec.

² Intel® Virtualization Technology requires a computer 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.

³ Source: Symantec knowledge base.

⁴ PCs with Intel® vPro™ technology include Intel® Active Management Technology (Intel® AMT). Intel AMT requires the computer to have an Intel AMT-enabled chipset, network hardware and software, connection with a power source, and a network connection.

Symantec and the Symantec logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries.

Copyright ©2006 Intel Corporation. All rights reserved. Intel, the Intel logo, and Intel vPro are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

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