Symantec virtual security application and PCs with Intel® Deskbrand technology

Company	Symantec, Inc., is the world leader in providing solutions to 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 against the user's operating system and commonly used applications.
Technology Solution	Symantec Security Virtual Application
Enhanced By	PCs with Intel® Deskbrand technology

Increasing enterprise security through desktop virtualization

Symantec and Intel are working together to create innovative ways of using a virtual security application to solve critical 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 Deskbrand Technology. These capabilities allow critical security applications to run in the background in a virtual partition -- or "virtual security application" -- even while users are working on their own compute-intensive tasks in their own user OS environment. This helps keep vital security processes isolated from potential problems with the main operating system (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 Deskbrand technology, the new virtualized Symantec security application 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 application will simplify management, make better use of administrative resources, increase confidence in endpoint security, and help ensure 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 is 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 gap continues to decrease. The industry has reached a point at which exploits arrive the same day a vulnerability is uncovered -- "zero day" attacks. These attacks places a significant burden on IT to deploy patches as soon as possible, even before patches have been fully tested. With an exploit

potentially arriving 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 guard against zero-day threats.

To make the issue even more challenging, such additional protection solutions can themselves be threatened by a successful infection in the operating system (OS) where they are installed. The infected desktop OS can then affect the performance -- or even the availability -- of the additional security solution.

With the security threat landscape in the 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 with Intel Deskbrand Technology PCs

To make the next leap in enterprise security, Symantec is taking full advantage of the new hardware-based capabilities built into PCs with Intel Deskbrand Technology. These capabilities allow Symantec to build a tamper-resistant virtual security application for IT. The security functionality will “live” in a secure space that runs outside the user OS, and where it will be unaffected by issues with the user OS. This application 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 Deskbrand Technology, Symantec's security application dramatically increases IT's confidence in desktop security, and their ability to deliver security management across all desktops in the enterprise.

A more efficient virtual model

Traditional virtualization on a PC has been both “heavyweight” and expensive. It’s purpose is to create multiple virtual PCs on a single machine, each virtual PC having 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 Deskbrand technology can be used for traditional virtualization. However, IT does not need another complete PC to perform vital security tasks. IT needs a 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 now offers IT the option of more efficient desktop security through a new, more efficient security application. This application runs in a separate, self-contained environment enabled on PCs with Intel Deskbrand 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 application is under the control of authorized IT. 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 application, a PC with Intel Deskbrand Technology helps protect itself. Within these PCs, the security application operates in an isolated virtual partition, protected from viruses, worms, and other threats that are normally targeted at the user OS. The security application can now continue efficiently protecting the desktop endpoint without interference from such threats.

Isolated from the user OS, the application is also the first program to boot up and the last to shut down on the PC. This means the application can offer high-level protection for PCs, for example, the application 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 application 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 appliance 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 Deskbrand technology, Symantec's virtual application enhances IT management. Because the application 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 income. Even 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 targeted, silent attacks.

The virtualized application, secure and 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 which provides hardware-based capabilities that are deeply embedded in the platform itself, inaccessible to hackers and would-be thieves. By taking advantage of these hardware capabilities, the application dramatically 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 application will deliver improved deployment, administration, threat mitigation, trust, and always-on operation leading to assured compliance. The cost of owning and managing PCs can be reduced. Interruptions in user productivity can be reduced, infrastructure investments capitalized upon, and end-user systems can be better protected.

The Symantec security application will be seamlessly integrated with other Symantec security solutions and the powerful new, hardware-based capabilities built into PCs with Intel Deskbrand Technology. This is not just another security solution; it is an innovative approach 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 application.
A more stable environment, which translates into reduced management complexity
Always-on security model that helps ensure system and regulatory compliance
Full isolation of the application from the health of the user OS.

For more information

PCs with Intel Deskbrand technology give IT critical, hardware-based security and manageability capabilities not available in previous generations of PCs or in software-only solutions. When provisioned[1] with the Symantec security application, these PCs can be managed and secured directly from the IT console, regardless of the health of the OS. For more information about Intel Deskbrand technology, visit www.intel.com\deskbrand.

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