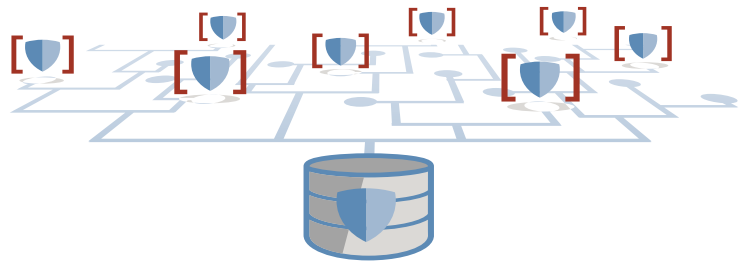


Protect Your IT Infrastructure from Zero-Day Attacks and New Vulnerabilities

Protecting a business's IT infrastructure is complex. Take, for example, a retailer operating a standard multi-tier infrastructure with both customer and partner portals. The infrastructure typically employs a mix of databases, in-house applications, third-party applications and web services, running in a heterogeneous OS environment and is constantly changing as technology advances and new business applications are added.

To ensure a base level of security and compliance, IT installs antivirus and uses a complex series of static network zones to protect the infrastructure.



This approach makes it difficult and slow to deploy new business applications and only provides protection from a casual attacker. The architecture becomes more complex as more applications and business services are introduced. Increasing IT infrastructure complexity also exacerbates existing challenges in protecting the environment from zero-day threats and from malicious actors eager to take advantage of newly discovered vulnerabilities.

Zero-day Attacks and New Vulnerabilities

Recent security breaches highlight the growing threat surface and the increasing sophistication of the cyber attacks that organizations like the Retailer face today, including:

- i. Sophisticated malware toolkits to enable customized spying - An advanced piece of malware, known as Regin, has been used in systematic spying campaigns against a range of international targets since at least 2008. A back door-type Trojan, Regin is a complex piece of malware whose structure displays a degree of technical competence rarely seen. Customizable with an extensive range of capabilities depending on the target, it provides its controllers with a powerful framework for mass surveillance and has been used in spying operations against government organizations, infrastructure operators, businesses, researchers, and private individuals. Symantec believes that the threat is installed through a Web browser or by exploiting an application.

Confidence in a connected world.  **Symantec™**

- ii. Watering hole attacks - A watering hole attack is a method of targeting sites that are likely to be visited by targets of interest. The attacker will compromise the site and inject JavaScript or HTML to redirect victims to additional malicious code. The compromised site is then left “waiting” to infect the profiled victim with a zero-day exploit, just like a lion waiting at a watering hole. Symantec has published research on watering hole attacks (The Elderwood Project) that details targets, growing trends and attack platforms seen since 2009.
- iii. Cross-site injection attacks - Cross-site scripting (XSS) is a security exploit in which the attacker inserts malicious coding into a link that appears to be from a trustworthy source. Cross-Site Scripting (XSS) attacks occur when:
 - (1) Data enters a web application through an untrusted source, most frequently a web request.
 - (2) The data is included in dynamic content that is sent to a web user without being validated for malicious content. The malicious content sent to the web browser often takes the form of a segment of JavaScript, but may also include HTML, Flash or any other type of code that the browser may execute. The variety of attacks based on XSS is almost limitless, but they commonly include transmitting private data, like cookies or other session information, to the attacker, redirecting the victim to web content controlled by the attacker, or performing other malicious operations on the user’s machine under the guise of the vulnerable site.

New vulnerabilities and zero-day attacks demand more proactive security monitoring and hardening approaches that take advantage of software-defined capabilities.



Confidence in a connected world.  **Symantec™**

Symantec Data Center: Server Advanced Protects the IT Infrastructure Against Zero-day Threats and New Vulnerabilities

Customers, like the Major Retailer, are using Symantec Data Center Security: Server Advanced to protect its web infrastructure against recent vulnerabilities. These threats include:



Bash Vulnerability (also known as “Shellshock”) affects most versions of the Linux and Unix operating systems. This vulnerability allows an attacker to gain control over a targeted computer if exploited successfully



Sandworm, which affects Windows OS and allows attackers to embed Object Linking and Embedding (OLE) files from external locations. Malicious hackers can exploit this vulnerability to download and install malware onto the target’s computer.



Regin, a multi-staged Trojan, in which each stage is hidden and encrypted. Regin has been used in systematic spying campaigns against a range of international targets since at least 2008.

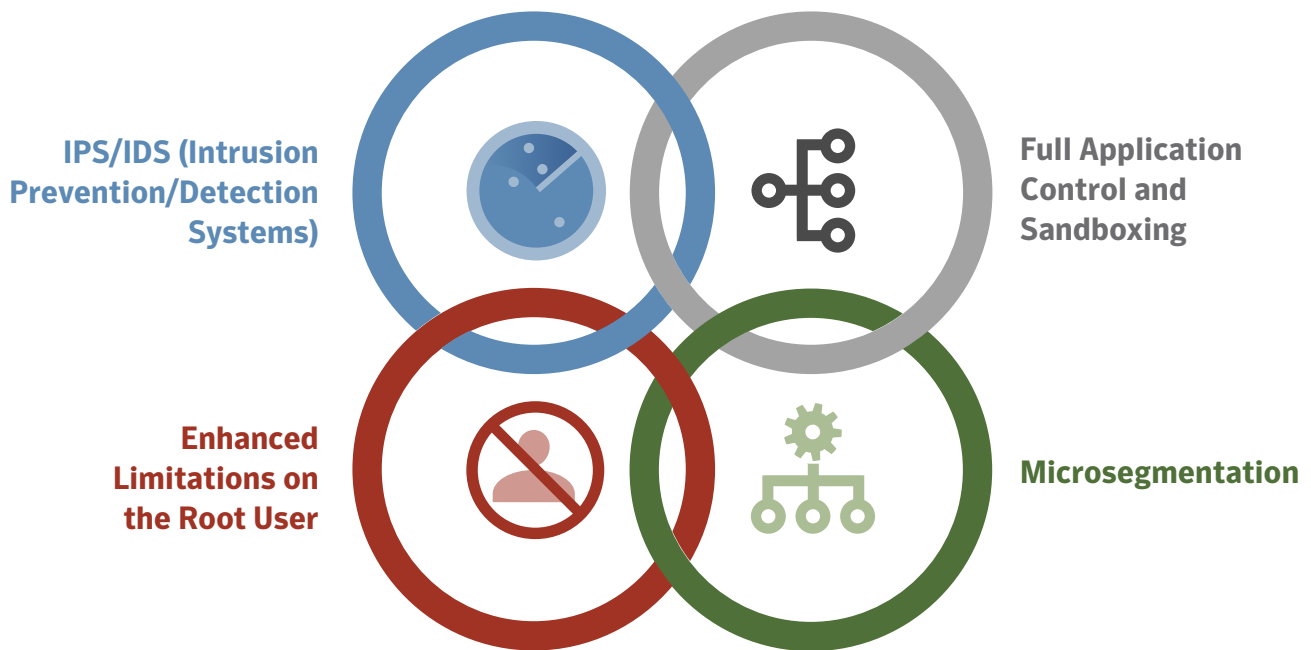


The Retailer is using Symantec Data Center Security: Server Advanced to proactively secure and harden its web infrastructure. With this approach, IT enables the web infrastructure to keep up with the business and maintain its service levels, yet still protect the environment against zero-day threats and new vulnerabilities.

Confidence in a connected world.



The Retailer is taking advantage of the following Symantec Data Center Security: Server Advanced capabilities to execute its objectives:



IPS/IDS

Turning on Symantec Data Center Security: Server Advanced IPS capabilities provide a first-line defense against zero-day vulnerabilities.

Protecting Windows Systems

Using the most basic intrusion prevention policy, Symantec Data Center Security: Server Advanced protects the online Retailer's Windows systems against Sandworm by automatically preventing Sandworm from entering the data center, by protecting critical Windows control points such as the 'runonce' registry key in this case. Symantec Data Center Security: Server Advanced prevention ensures protection even if IT has not yet applied the Windows Sandworm security patch, and even before security research knows the vulnerability exists.

Confidence in a connected world.  **Symantec**[™]



Protecting Unix/Linux Systems

In scenarios similar to the Bash vulnerability, which attacks Linux and Unix systems, customers can set IPS to monitoring mode in order to alert the customer to activities that it would normally restrict or block. This enables the customer to quickly detect and set alerts for unusual and suspicious activity without taxing application performance. The customer can also set prevention policies so that the configuration files of both the *NIX OS and common Daemons/Applications, such as Apache, remain read only and when Apache runs Bash it is limited to Apache and cannot read and or modify anything else on the system.

IT can also use the standard IDS Unix Baseline policy to monitor and run important checks such as Privileged Command, Bash History Monitor and System Hardening Monitor. These checks help IT detect potentially unwanted activity.

Protecting the Infrastructure from Exposed Hosts

For exposed hosts, IT can also adjust policy settings with Symantec Data Center Security: Server Advanced so that vital files are made “read only” to any user or process (including ROOT), and changes are limited to specific management applications, hosts or IP addresses. Customers can tie policies to their change control procedures.

Policy Management

Customers can also run checks to help detect potentially unwanted activity. To minimize the potential impact of IDS checks on performance, customers will have to do some fine-tuning to remove all check options and reduce event traffic. Policies can be tied into a customer’s Change Control Procedures so that the first and more secure version of this policy is live 99 percent of the time. When changes are necessary or threats subside, the second version can then be applied if desired.



Full Application Control and Sandboxing

IT can use Symantec Data Center Security: Server Advanced to perform full application control and address vulnerabilities such as Bash, Sandworm and Mimikatz. Symantec Data Center Security: Server Advanced protects web servers against malware that uses the common gateway interface (CGI) to launch attacks by limiting processes in the affected servers to only perform their required functions or by preventing CGI from running altogether.

IT can also utilize Symantec Data Center Security: Server Advanced to prevent attacks like Regin from running on unprotected platforms by using the published Regin hash signature (MD5) to create blacklists.

Symantec Data Center Security: Server Advanced provides out-of-the-box protection for Apache. However, customers are advised to ensure they have properly configured the sandbox for their environment. Customers have to properly configure the file resource lists so that only Apache has access to the web content.

In many instances Apache web services are installed by default, but not used. In this scenario, IT can configure Symantec Data Center Security: Server Advanced to block these unused Apache web services.


Limiting the Root User

Symantec Data Center Security: Server Advanced can be used by customers to limit the root user's capabilities on Unix systems. Customers are advised to tune their Unix Prevention policy to ensure that the root user limits can be enforced even when the vulnerability is installed, thus preventing accidental exposures.

Microsegmentation

When the web infrastructure is compromised, the "kill chain" prescribed for zero-day and advanced threats depends on the "hard shell, chew center" of the traditional perimeter-enforced physical networks. With Symantec Data Center Security: Server Advanced, customers can manually create micro-segments (asset groups) of security containers per application instance and apply the right policies to the asset groups.

Confidence in a connected world.  **Symantec**™



Customers that have both VMware NSX and Data Center Security: Server Advanced can replace their rigid perimeter-centric security zones and predominantly manual processes with policy-based, automated, application-specific security models. Customers can use this integration to orchestrate security settings across Server, Server Advanced and third-party tools that are registered with VMware Service Composer, starting with Palo Alto Networks firewalls.

Customers that utilize microsegmentation will realize faster and more dynamic response times to advanced threats, and can stop the malware from accessing critical applications, even within the compromised physical hosts.

Protect Your Web Infrastructure with Symantec Data Center Security: Server Advanced


Symantec Data Center Security: Server Advanced will help customers protect their customer facing web infrastructure so that they can:

- Protect the corporate brand by delivering secure business services to customers and business partners.
- Provide faster response times to detect, monitor and protect its web infrastructure against zero-day attacks and new vulnerabilities.
- Maintain compliance with security standards and fulfill regulatory obligations such as PCI-DSS.

Symantec Data Center Security: Server Advanced offers the following capabilities:



Confidence in a connected world.  **Symantec**™



In addition to delivering protection against zero-day threats and new vulnerabilities, IT can use Symantec Data Center Security: Server Advanced to:

- Harden and secure critical applications running on legacy systems (such as your Windows 2003 Servers).
- Quickly enable security for newly provisioned physical and virtual assets.

With Symantec Data Center Security: Server Advanced, customers can ensure their IT infrastructure is secure and compliant regardless of where they are in the life cycle of their software-defined data center.

Click for more information on [Symantec Data Center Security: Server Advanced](#).

Confidence in a connected world.

