Symantec™ Critical System Protection

Maximum protection for physical and virtual data centers

Data Sheet: Endpoint Security

Overview

To secure physical and virtual data centers, IT professionals have relied on traditional protection technologies such as antivirus and whitelisting. These technologies, while important layers of defense on a laptop or desktop, do not sufficiently protect a server due to in-depth confidentiality, integrity, and availability requirements of each system. Without a way to customize the security for each unique server—Web, file, application, or database—organizations will continue to expose data centers.

Symantec™ Critical System Protection allows organizations to monitor and protect physical and virtual data centers using granular, policy-based controls. Through a combination of host-based intrusion detection (HIDS), intrusion prevention (HIPS), and least privilege access control, organizations can proactively safeguard heterogeneous server environments and the information they contain.

Unlike other technologies, Symantec's granular policy-based controls provide complete protection for VMware® vSphere™, protect against zero-day and targeted attacks, and real-time control and visibility into compliance.

Key benefits

Comprehensive protection for VMware® environments

In a virtual environment, applications and operating systems are subject to the same cyber attacks that are present in a physical environment. Even further, additional attack surfaces such as the hypervisor and management server need protection. When considering security in virtual environments it is important to select a technology that will defend against insider abuse and external threats across the virtual fabric without compromising performance. Critical System Protection is optimized to protect and monitor vSphere 5.0. Leveraging out-of-the box policies based on the latest vSphere hardening guidelines organizations are able to completely protect their environment at the management server, hypervisor, and guest. Key capabilities include:

- **VMware vCenter™ management server protection (New):** Harden vCenter based on VMware hardening guidelines.
- **VMware ESX® and VMware ESXi™ hypervisor protection (New):** Prebuilt policies to monitor and block malicious activity.
- **VMware ESX and ESXi guest protection:** Prebuilt policies to harden virtual machines based on unique workload.

Stop internal and external attacks to servers

Servers are frequently targeted by cybercriminals during in the incursion, discovery, and capture phases of a data breach. The techniques used against servers today range from sophisticated penetration techniques to unintentional configuration mistakes by insiders. Critical System Protection allows organizations to protect against internal and external attacks such as Microsoft SQL® injections, buffer overflows, and vulnerability exploits in addition to malicious insider abuse and system mis-configurations. By hardening the data center, stop further penetration and prevent the loss of sensitive information. Key capabilities include:

- **Targeted prevention policies**: One-click prevention policy that can be applied in a breach scenario, or as a way to move from monitoring to prevention.
- **Process Access Control (PAC) (New)**: Prevention against a new class of threats utilizing comprehensive IPS protection. PAC provides additional controls over a running process.
- **Out of the box IDS and IPS policies**: Prebuilt policies for Windows® environments that will monitor and prevent suspicious server activity.
- **Application and device control**: Lock down configuration settings, file systems, and use of removable media.
- **Host firewall:** Control inbound and outbound network traffic to and from servers.

- **Symantec™ Security Information Manager:** Compatibility with Symantec's leading security incident and event management solution.

Gain real-time visibility into IT compliance posture

To comply with external regulations such as PCI Data Security Standard 2.0 (PCI DSS), North American Electric Reliability Corporation (NERC) and others, organizations must routinely monitor their environment for policy violations and implement compensating controls. In a single solution, Critical System Protection enables organizations to perform real-time monitoring, consolidate event logs for reporting and analysis, while preventing further policy violations with granular policy-based controls. Demonstrate compliance with a centralized solution. Key capabilities include:

- **Real-time file integrity monitoring:** Identify changes to files in real-time including who made the change and what change occurred.
- **Configuration monitoring:** Identify policy violations and suspicious activity in real-time.
- **IT analytics cube integration (New):** Leverage flexible and enhanced dashboarding capabilities augmenting existing Critical System Protection reporting for increased visibility.
- **Consolidated event logging:** Consolidate and forward logs for long term retention, reporting, and forensic analysis.
- **File and system tamper prevention:** Lock down configuration, settings, and files.
- **Compensating HIPS controls:** Restrict application and operating system behavior using policy-based least privilege access control.
- **Symantec™ Control Compliance Suite:** Compatibility with Symantec's unified IT compliance solution.

Patch mitigation for new and legacy operating systems

Applying software patches to new and legacy operating systems improves security posture but also causes system downtime. In addition, paying for extended support for end of life operating systems can be costly and unsustainable. With Critical System Protection, reduce the maintenance costs associated with legacy system support and protect critical systems between patch cycles. By hardening the applications and operating systems of new and legacy systems, customers can ensure maximum security of data centers and maximize system availability. Key capabilities include:

- **System hardening:** Lock down configuration and settings of critical servers.
- **Least privilege access control:** Restrict the behavior of applications and operating systems using granular policy based controls.
- **Broad physical and virtual platform support:** Across VMware, Windows, RedHat®, Solaris®, Linux®, AIX®, HP-UX®, and additional server platforms.

More Information

Visit our website: http://enterprise.symantec.com

About Symantec

Symantec protects the world's information and is the global leader in security, backup, and availability solutions. Our innovative products and services protect the people and information in any environment—from the smallest mobile device to the enterprise data center to cloud-based systems. Our industry-leading expertise in protecting data, identities, and interactions gives our customers confidence in a connected world. More information is available at: www.symantec.com or by connecting with Symantec at: go.symantec.com/socialmedia.

Symantec World Headquarters

350 Ellis St., Mountain View, CA 94043 USA
+1 (650) 527 8000 | 1 (800) 721 3934 |
www.symantec.com