PRODUCT BRIEF

Symantec® Data Center Security: Server Advanced

Protection and Hardening for Advanced Threats

CUSTOMER BENEFITS

- Comprehensive server protection providing visibility, compliance, hardening, and management.
- Automated threat response with out-of-box recipes to protect against critical vulnerabilities and unauthorized application configuration changes.
- Virtualization-technology agnostic and broad platform support to secure workloads regardless of where it resides and protect entire data centers including legacy, unpatchable systems.

STANDARD FEATURES

- **Out of the Box Host IDS and Intrusion Prevention System (IPS) Policies:** Prebuilt policies for Windows environments that will monitor and prevent suspicious server activity.
- **Sandboxing and Process Access Control:** Prevention against a new class of threats utilizing comprehensive IPS protection.
- **Host Firewall:** Control inbound and outbound network traffic to and from servers.
- **Compensating Host Intrusion Prevention System (HIPS) Controls:** Restrict application and operating system behavior using policy-based least privilege access control.
- **File and System Tamper Prevention:** Lock down configuration, settings, and files.
- **Application and Device Control:** Lock down configuration settings, file systems, and use of removable media.

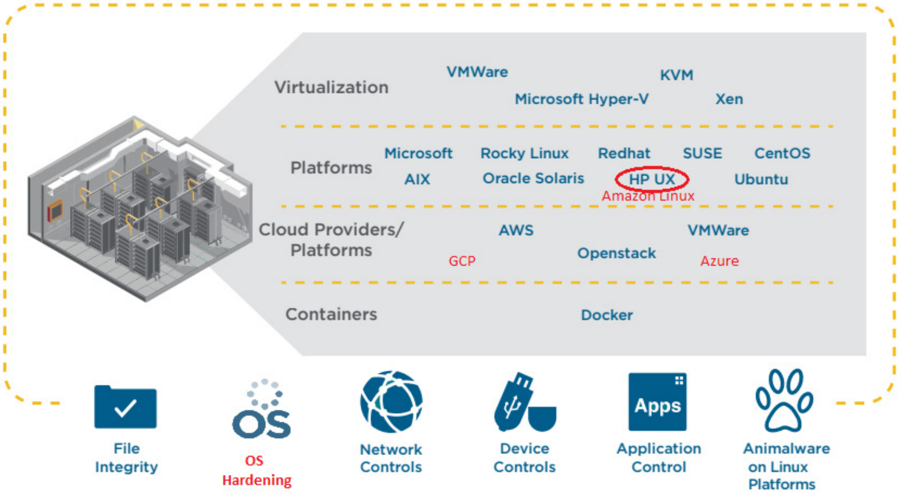
Solution Overview

Symantec® Data Center Security: Server Advanced (DCS:SA) provides complete server protection. Full application control enables microsegmentation, administrator privilege de-escalation, patch mitigation, and protection against zero day threats in today's heterogeneous private and public cloud data centers.

Does your current solution measure up to the capabilities of DCS:SA?

- Protects and harden heterogeneous virtual and physical server environments
- Protects and hardens critical applications running on legacy and end-of-life (EOL) Windows and Linux platforms
- Achieves visibility, hardens, and protects Docker environments
- Effectively delivers security while migrating off EOL server platforms
- Quickly responds to critical vulnerabilities and unauthorized application configuration changes
- Purpose-built to secure an organization's critical server infrastructure against zero-day threats and new vulnerabilities
- Secures OpenStack Keystone implementation
- Executes and monitors application and instance-level security in an organization's AWS, Azure, and OpenStack cloud deployments
- Quickly provisions application-centric security hardening for newly created physical and virtual workloads
- Embeds security provisioning and hardening into an organization's IT processes
- Detects and eradicates known and unknown malware on broad Linux platforms, regardless where they are hosted

Symantec DCS:SA Provides Complete Server Protection



Product Capabilities

- Protect servers from zero-day attacks including an added ability to integrate DCS:SA into the customer's data center toolset to quickly deploy additional monitoring and targeted hardening to applicable servers through REST APIs
- Secure unpatched applications and systems running on legacy and end-of-life platforms
- Monitor and protect physical and virtual data centers using a combination of host-based intrusion detection and intrusion prevention (HIPS), and least-privilege access controls.
- Fully instrumented REST API provides corresponding API for all console activities to enable full internal and external cloud automation
- Enable the secure migration and operationally cost-efficient migration from end-of-life platforms
- Mitigate patching for new and legacy systems
- Enable application and instance level security for public and hybrid cloud deployments
- Gain continuous monitoring of data center infrastructure for cybersecurity and compliance
- Provide visibility, compliance, hardening, and management of Docker containers
- Simplified policy creation in learn mode helps build rules through automated sandboxing
- Reduce operational costs with the new application centric security groups
- Additional platform support
- Monitor OpenStack data center infrastructure
- Easily identify abnormal event activity and also monitor your key performance indicators using dashboards
- Heterogeneous and exotic or EOL operating system (AIX, HP-UX, Solaris, Win2008) support

DCS:SA

DCS:SA combines malicious code protection along with intrusion detection, file integrity, and configuration monitoring. Customers are also able to monitor OpenStack-based data centers including configuration changes, access monitoring, and Keystone data.

DCS:SA protects both physical and virtual servers in on-premises, hybrid, and cloud-based data centers by delivering the following functionality:

- Application and protected allow listing
- Fine-grained intrusion detection and prevention
- File, system and admin lockdown
- File integrity and configuration monitoring
- Real-time detection and eradication of known and unknown malware

DCS:SA helps minimize time and effort and reduce operational costs by using out of the box monitoring and hardening for most common data center applications. Protect your OpenStack-based data centers using file integrity monitoring of all OpenStack modules and with full hardening of the Keystone identity service module.

- Anti-malware on vCNS and vShield platforms
- IPv6 support and block list/allow list support in NIPS

Data Center Security: Server

DCS:SA also includes all the features in Data Center Security: Server.

For more information, please visit:
www.broadcom.com/products/cyber-security/endpoint/hybrid-cloud/data-center-security

BROADCOM®
connecting everything®

For more information, visit our website at: www.broadcom.com