Symantec
by Broadcom

PRODUCT BRIEF

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-the-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 they reside and protect entire data centers including legacy, unpatchable systems.

STANDARD FEATURES

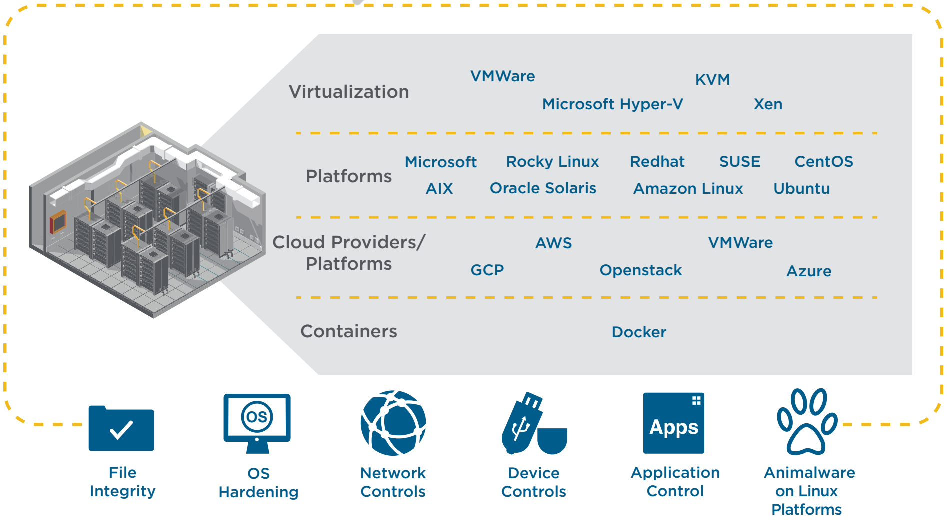
- **Out-of-the-box Host IDS and IPS policies:** Prebuilt policies for Windows and Linux environments that will monitor and prevent suspicious server activity.
- **Sandboxing and Process Access Control (PAC):** Prevention against a new class of threats utilizing comprehensive IPS protection.
- **Host firewall:** Control inbound and outbound network traffic to and from servers.
- **Compensating 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.

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/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



Data Center Security: Server Advanced

PRODUCT CAPABILITIES

- Protect servers from zero-day attacks including the ability to integrate DCS:SA into the data center toolset to quickly deploy additional monitoring and targeted hardening to applicable servers via REST APIs
- Secure unpatched applications and systems running on legacy and end-of-life platforms
- Monitor and protect physical and virtual data centers using host based intrusion detection (HIDS), intrusion prevention (HIPS), and least-privilege access control.
- Fully instrumented REST API provides corresponding API for all console activities to enable full internal and external cloud automation
- Enable the secure and 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
- Visibility, compliance, hardening, and management of Docker containers
- Simplified policy creation in learn mode helps build rules via automated sandboxing
- Reduce operational costs with new application-centric security groups
- Monitor OpenStack data center infrastructure
- Easily identify abnormal event activity and monitor key performance indicators using dashboards
- Heterogeneous and exotic/EOL operating system (AIX, Solaris, Win2008) support

Server Advanced also includes all the features provided by Data Center Security: Server:

Symantec DCS:SA

Symantec DCS:SA combines agentless malicious code protection 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-premise, hybrid, and cloud-based data centers by delivering the following:

- Application and protected allow listing
- Fine-grained intrusion detection and prevention
- File, system, and administrator 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 OpenStack-based data centers using file integrity monitoring of all OpenStack modules, plus full hardening of the Keystone identity service module.

- Agentless Network IPS for virtual servers on VMware NSX
- Anti-Malware on vCNS/vShield platforms
- IPv6 support and block list/allow list support in NIPS

Symantec DCS: Server

Symantec DCS: Server delivers agentless anti-malware, agentless network IPS, in-guest file quarantine, and file reputation services for VMware hosts and virtual guests. It integrates with VMware vCenter and VMware NSX to orchestrate security throughout the lifecycle of the workload.

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

BROADCOM®
connecting everything®

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