Symantec
A Division of Broadcom

Product Brief

Symantec® Data Center Security: Server Advanced

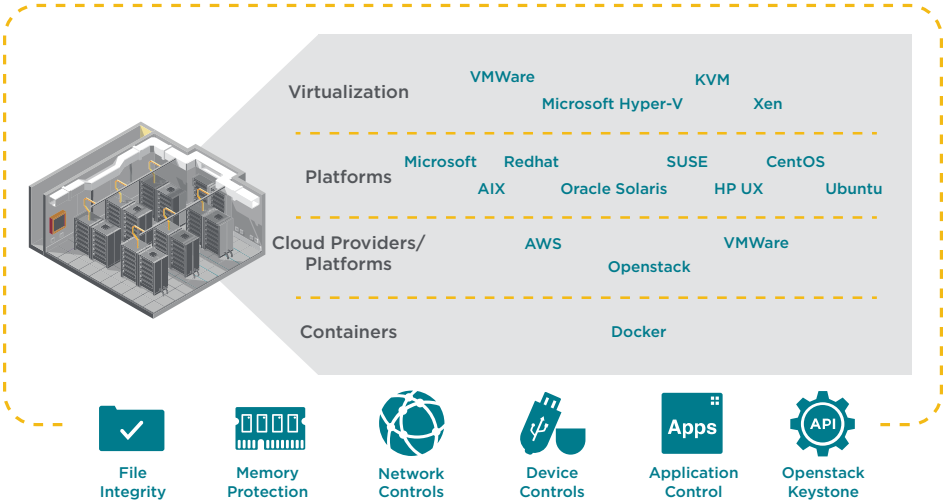
Protection and Hardening for Advanced Threats

Solution Overview

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

- Protect and harden your heterogeneous virtual and physical server environments?
- Protect and harden critical applications running on legacy and end-of-life (EOL) platforms?
- Achieve visibility, harden, and protect Docker environments?
- Effectively deliver security while migrating off EOL server platforms?
- Quickly respond to critical vulnerabilities and unauthorized application configuration changes?
- Secure your organization's critical server infrastructure against zero-day threats and new vulnerabilities?
- Secure your OpenStack Keystone implementation?
- Execute and monitor application and instance-level security in your organization's AWS, Azure, and OpenStack cloud deployments?
- Quickly provision application-centric security hardening for newly created physical and virtual workloads?
- Embed security provisioning and hardening into your organization's IT processes?

Solution Overview



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 IPS Policies: Prebuilt policies for Windows 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.

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 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 a combination of 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 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 cyber security and compliance
- Provide visibility, compliance, hardening, and management of Docker containers
- Simplified policy creation in learn mode helps build rules via 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

Server Advanced also includes all the features in Data Center Security: Server:

- 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

Overview of Symantec Data Center Security Solutions

Symantec DCS:SA
Symantec DCS:SA combines agent-less 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-prem, hybrid, and cloud-based data centers by delivering the following:

- Application and protected whitelisting
- Fine-grained intrusion detection and prevention
- File, system and admin lockdown
- File integrity and configuration monitoring

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.

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.

Symantec Cloud Workload Protection (CWP)
Symantec CWP allows enterprises to secure their critical workloads wherever they are—public clouds, private clouds, and physical on-premises data centers—all from a single, centralized console. CWP is a native cloud SaaS offering that automates workload security, providing discovery, visibility, and protection against advanced malware and threats across multiple cloud service providers (AWS, Azure, GCP, OCI). Automatic identification of workload security posture and software services, including visibility into infrastructure changes and flow logs, enables automatic policy recommendations and deployment.

Symantec Cloud Workload Protection (CWP) (cont.)
CWP provides multi-layered protection for cloud compute instances including anti-malware scanning, application control and isolation to help block exploits targeting known and unknown vulnerabilities, OS hardening that helps to stop zero-day threats, and real-time file integrity monitoring (RT-FIM) that helps to prevent unauthorized system changes. Docker containers and Orchestration applications are also supported.

Cloud-native integration with public cloud platform APIs allows CWP to both share and consume information in real-time, along with any changes to cloud infrastructure and security settings. Public cloud API integration also enables DevOps practitioners to build security directly into service deployment workflows, ensuring that workloads are protected, and that security scales automatically with dynamic cloud infrastructure. The CWP cloud console can also be used to manage Symantec DCS agents on virtualized and physical on-premises servers.

Symantec CWP for Storage

- Protects Cloud Storage Against Threats and Discovers Sensitive Data
- Automatic discovery and scanning of Amazon S3 buckets
- Uses SEP anti-malware technologies including reputation analysis and advanced machine learning to remediate threats
- Alerts when S3 buckets are misconfigured or exposed to the public internet to protect against data breaches
- Applies Symantec Data Loss Protection (DLP) policy to data stored in Amazon S3 buckets to discover and tag sensitive information
- Data never leaves the protected environment during malware or DLP scanning
- Creates custom alerts based on events and view results and security posture in a single intuitive dashboard
- Industry-first solution for in-tenant anti-malware and DLP scanning of cloud storage

Symantec™
A Division of Broadcom

For product information and a complete list of distributors, visit our website at: broadcom.com

SED-DCS-Server-Adv-PB100 December 17, 2020