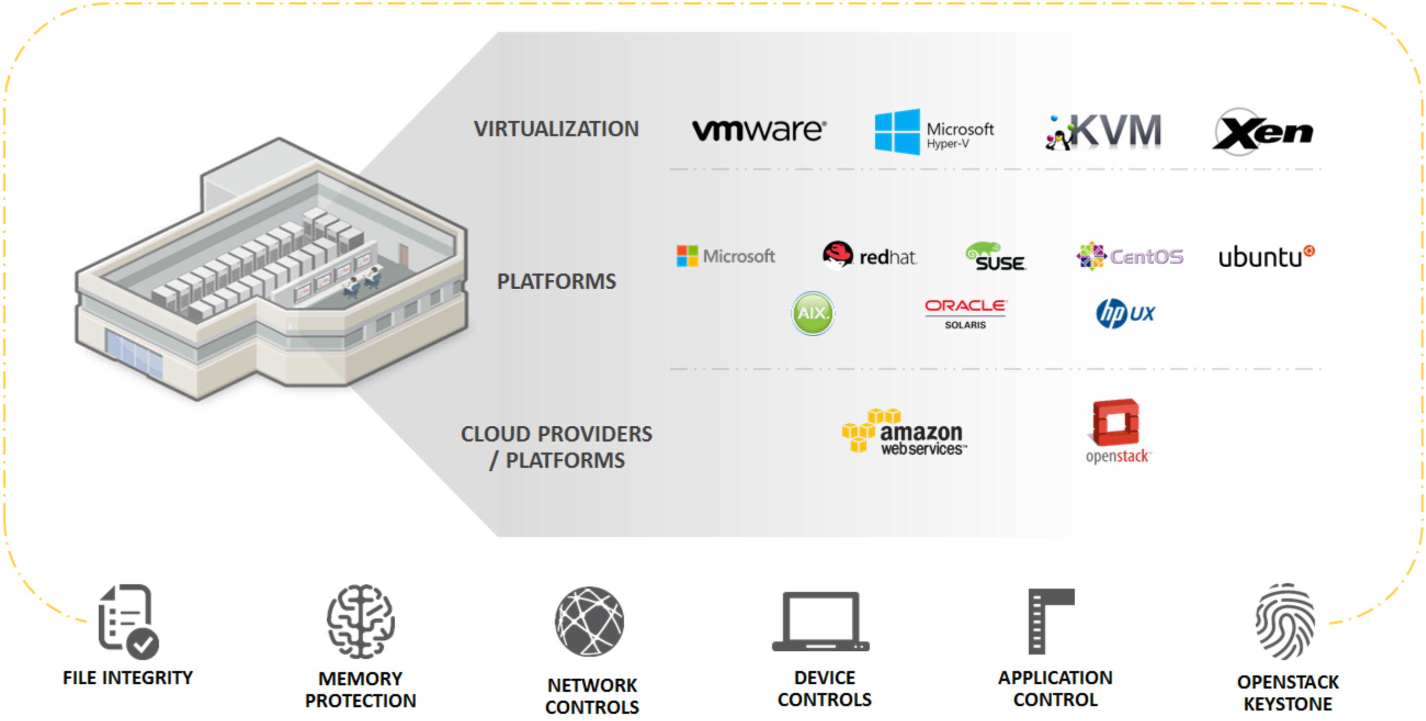
Symantec™ Data Center Security: Server Advanced

Protection and hardening for advanced threats

Data Sheet: Security Management

Solution Overview

Symantec™ Data Center Security: Server Advanced provides complete server protection. Full application control enables micro-segmentation, administrator privilege de-escalation, patch mitigation, and protection against zero day threat in today's heterogeneous private/public cloud data centers.



Can you:

- Protect and harden your heterogeneous virtual and physical server environments?
- Protect and harden critical applications running on legacy and end-of-life (EOL) platforms?
- 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 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?

Customer Benefits

- Protect server from zero day attacks including an added ability to integrate Data Center Security: Server Advanced into the customer's data center toolset to quickly deploy additional monitoring and targeted hardening to applicable servers via REST APIs.

- Unbreakable - Data Center Security: Server Advanced remains unbreakable in the five years that Symantec ran the "Capture the Flag" hacking challenge at the annual Black Hat Conference in Las Vegas, NV.
- Secure unpatched applications and systems running on legacy and End-of-life platforms.
- 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 means that customers can secure workloads regardless of where it resides and can protect entire data centers including legacy systems that cannot be patched.
- 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 cybersecurity and compliance.

What's New in v6.6

- Streamlined operational tasks with updated web-based UI
- Reduce operational costs with the new application centric security groups
- Minimize time to rollout hardening using guided tuning workflow
- Reduce time to harden your Unix workloads using Application discovery and hardening; Advanced Resilient Unix agent provides protection even as your environment evolves
- Platform Support: Ubuntu 14.0.4

Server Advanced also includes all the new features in Monitoring Edition 6.6 and Server 6.6:

- Monitor OpenStack Data Center Infrastructure
- Easily identify abnormal event activity and also monitor your key performance indicators using dashboards
- Agentless Network IPS for virtual servers on VMware NSX
- Anti-Malware on vCNS/vShield platforms
- IPv6 support and Blacklist/Whitelist support in NIPS
- Added Platform Support: vSphere 5.5/6.0, NSX 6.1.4, vCNS 5.5.4

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.

Overview of Symantec™ Data Center Security Solutions

Symantec™ Data Center Security: Server delivers agentless anti-malware, agentless network IPS, in-guest file quarantine, file reputation services for VMware hosts and virtual guests. It integrates with VMware vCenter, VMware NSX, Palo Alto Networks Next Generation Firewall and Rapid 7 Nexpose to automate and orchestrate application-level security throughout the lifecycle of an the workload.

Symantec™ Data Center Security: Monitoring Edition delivers security detection and monitoring capabilities for both physical and virtual server infrastructures. In addition to delivering agentless antimalware protection, Symantec™ Data Center Security: Monitoring Edition combines agent-less malicious code protection along with intrusion detection, file integrity and configuration monitoring. With Symantec™ Data Center Security: Monitoring Edition, customers are also able to monitor OpenStack based data centers including configuration changes, access monitoring, and Keystone data.

Symantec™ Data Center Security: Server Advanced protects both physical and virtual servers in on-prem, hybrid, and cloud-based data centers by delivering (1) application and protected whitelisting, (2) fine-grained intrusion detection and prevention, (3) file, system and admin lockdown, (4) and file integrity and configuration monitoring. Data Center Security: Server Advanced 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™ Control Compliance Suite enables asset and network auto discovery, automates security assessments and calculates and aggregates the CVSS/CIS risk scores. Customers use Control Compliance Suite to enable basic security hygiene, and gain visibility into their security, compliance, and risk postures. Customers use this intelligence to prioritize remediation and optimize security resource allocation.

Symantec™ Protection Engine delivers content scanning, antimalware, outbreak detection, anti-spam, insight and reputation services, and granular content filtering technologies for various types of data stores such as cloud storage, NAS, email, and AWS. Out-of-the-box support is available for NetApp NAS, Microsoft Exchange, and Sharepoint Data Stores, and a robust SDK enables custom integration for other data stores.

More Information

Visit our website

http://enterprise.symantec.com

To speak with a Product Specialist in the U.S.

Call toll-free 1 (800) 745 6054

To speak with a Product Specialist outside the U.S.

For specific country offices and contact numbers, please visit our website.

About Symantec

Symantec Corporation (NASDAQ: SYMC) is the global leader in cybersecurity. Operating one of the world's largest cyber intelligence networks, we see more threats, and protect more customers from the next generation of attacks. We help companies, governments and individuals secure their most important data wherever it lives.

Symantec World Headquarters

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