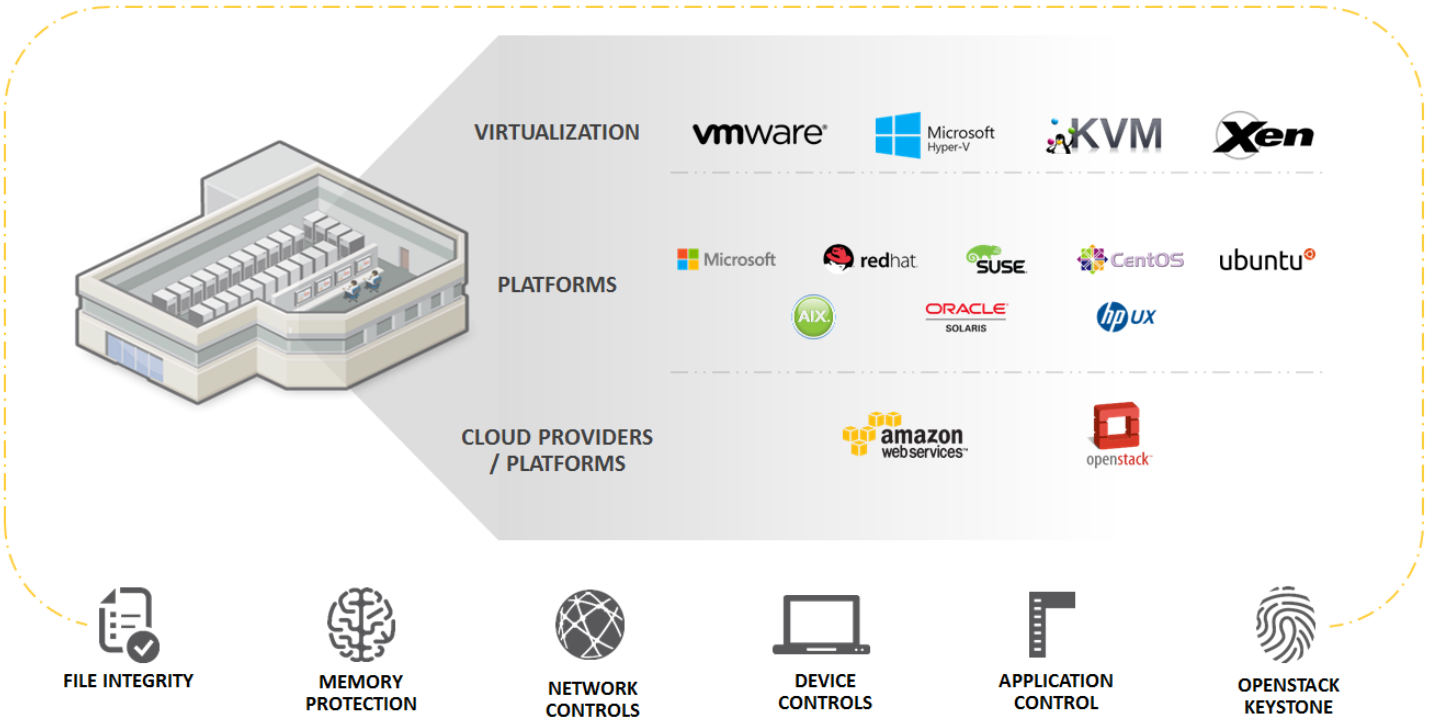
Symantec™ Data Center Security: Server Advanced

Protection and hardening for advanced threats.

Data Sheet: Security Management

Solution Overview

Symantec™ Data Center Security: Server Advanced enables organizations to secure and harden their physical and virtual servers, as well as secure and continuously monitor the security and compliance posture of their on-premises, public, and private 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?
- 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

Symantec

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 two 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.
- 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 v6.5

- Enhanced IDS including the ability to:
  - Secure OpenStack Keystone implementations.
  - Monitor extended file attributes and Access Control List (ACL) changes
  - Enable real-time File Integrity Monitoring (RT-FIM) support for Veritas File Systems (VxFS)
  - Support Windows and Linux agents on AWS Virtual systems
  - Enable security-Enhanced Linux (SELinux)/AppArmor
  - Support for Red Hat Enterprise Linux 7.0
- Enhanced IPS including:
  - Application Centric Hardening (database schema changes)
  - Linux Apache MySQL PHP (LAMP) support on UNIX (new sandboxes for MySQL and PHP in Unix policy)
  - Upgraded third-party components(OpenSSL, cURL, FIPSOPENSSL)
  - Prevention policy now supports no run exception list
  - Execution of files with non-executable extensions is blocked
  - Red Hat Enterprise Linux 7.0 and CentOS 7 support
  - ACL changes on Windows and UNIX
- Server Advanced includes all features in Monitoring Edition 6.5:
  - Security monitoring of OpenStack Data Centers
  - Expanded platform support to KVM, Ubuntu, and RHEL.
  - Security Monitoring across physical and virtual servers including:
    - Real-time file integrity monitoring
    - Configuration Monitoring
    - Consolidated Event Logging
    - File and System Tamper Prevention
- Server Advanced includes all features in Symantec Data Center Security: Server 6.5:
  - Agentless antimalware, agentless network IPS and file reputation services.
  - Auto-deployment and provision of Security Virtual Appliance to ESX host in a cluster.
  - Network based threat detection and protection (Network IPS).
  - Operations Director to automate and orchestrate security provisioning for newly created workloads.

- KVM, Ubuntu, RHEL support.
- Support for NSX 6.1.2 and vSphere 5.5 U2. (*DataCenter Security: Server Advanced does not require VMware NSX)*

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 friction-less threat protection with agentless anti-malware, network based IPS and file reputation services for the VmWare environments. It supports in-guest quarantine feature to isolate suspected malware files and remediate based on policy. Symantec Data Center Security: Server auto-delivers Security Virtual Appliances (SVA) that scales out, resulting in huge savings in OpEx costs.

Symantec™ Data Center Security: Monitoring Edition enables organizations to continuously monitor the security and compliance posture of its physical and virtual infrastructure, as well as its public (AWS) and private (OpenStack) clouds. It combines agent-less malicious code protection along with the IPS/IDS monitoring, file integrity monitoring, and configuration monitoring. This product is intended to enable customers automate and centralize their security operations and compliance monitoring and reporting objectives.

Symantec™ Data Center Security: Server Advanced delivers security detection, monitoring, and prevention capabilities for both physical and virtual server infrastructures. In addition to delivering agentless antimalware protection and security monitoring for virtual and physical infrastructures and across the AWS and OpenStack clouds, Symantec Data Center Security: Server Advanced protects both physical and virtual servers by delivering application and protected whitelisting, fine-grained intrusion detection and prevention; file, system and admin lockdown; and file integrity and configuration monitoring. It also supports full hardening of OpenStack Keystone.

Symantec™ Control Compliance Suite enables asset and network autodiscovery, 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 protects the world's information and is the global leader in security, backup, and availability solutions. Our innovative products and services protect 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

21347666-1 07/15