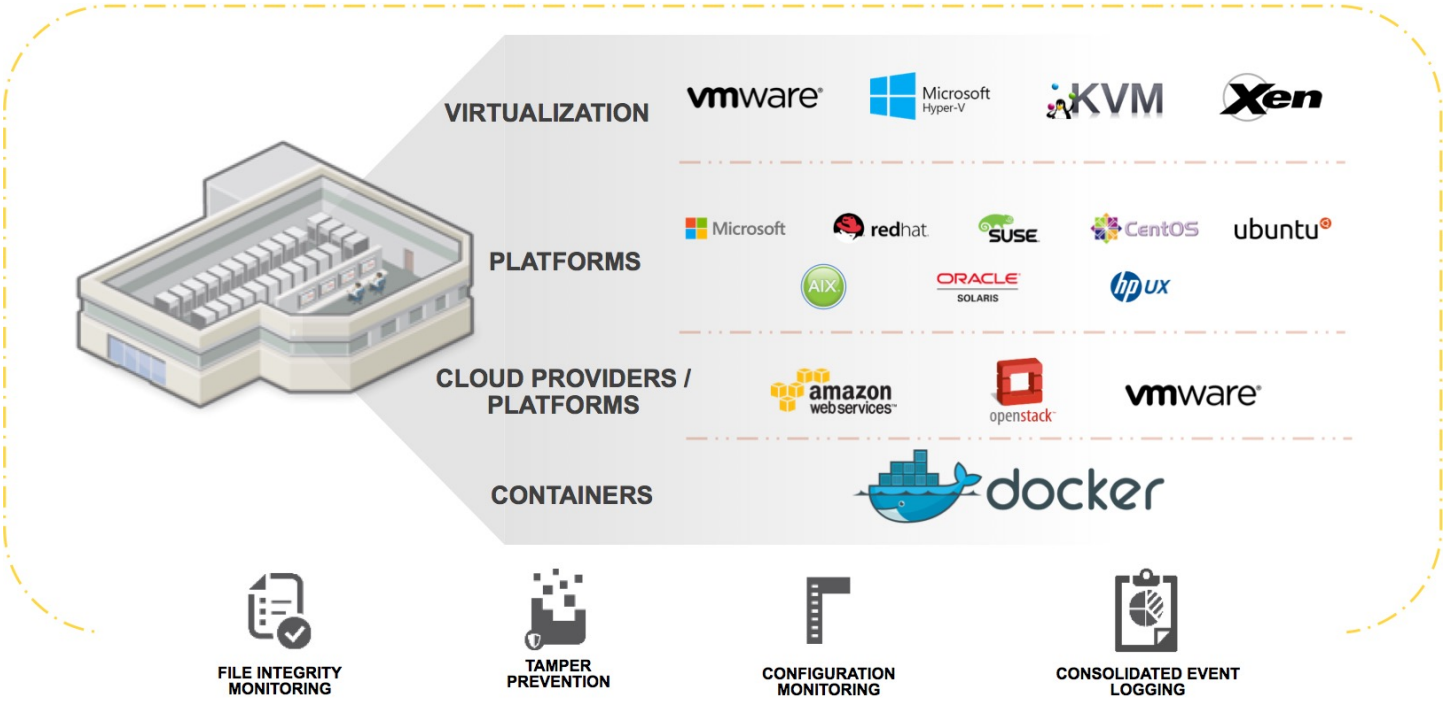
Symantec™ Data Center Security: Monitoring Edition

Simplify continuous security monitoring for physical and virtual servers as well as private and public clouds

Data Sheet: Security Management

Solution Overview

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) cloud deployments.



Symantec™ Data Center Security: Monitoring Edition provides out-of-the-box host intrusion detection policies across physical and virtual servers. It also extends security monitoring into Amazon Web Services (AWS) and all modules of the Openstack cloud. With Monitoring Edition, customers can monitor the file integrity and configuration, consolidate event logs, as well as employ whitelisting and application controls across its on-premises and off-premises data centers with a single tool.

Customers of Symantec™ Data Center Security: Monitoring Edition also have access to the functionalities available in Symantec™ Data Center Security: Server such as:

- Agentless antimalware
- Agentless network IPS
- Out-of-the-box integration with VMware
- Operations Director

For more information, refer to the Symantec™ Data Center Security: Server Datasheet

Why Symantec™ Data Center Security: Monitoring Edition?

Symantec™ Data Center Security: Monitoring Edition is a good fit for your organization if your team is asking any of the questions below:

- How do I effectively identify policy violations and suspicious activities at an application- or instance-level, in real-time, across my physical and virtual servers, as well as across my AWS and OpenStack clouds?
- How do I effectively monitor the security and compliance posture of my organization's AWS and Openstack cloud deployments at the application- and instance-level?
- How do I simplify continuous monitoring and compliance reporting across my physical and virtual servers, as well as across my AWS and OpenStack clouds?
- How do detect and identify changes to files in real-time across my physical and virtual servers, as well as across my AWS and OpenStack clouds?
- How can I provision security so that it is able to keep up with the speed of business and IT?

What's New In Data Center Security: Monitoring Edition 6.7?

- **Enhanced Visibility**
  - Security Administrators can view containers, their metadata and status, both online and offline
- **Stonger Compliance**
  - Security Administrators will be able to apply Unix real-time security and compliance monitoring policy to the Docker host. The host as well as the containers will be monitored, including real-time file monitoring of the Docker host and all containers
  - Security Administrators can insure files and services specified in the CIS Docker Benchmark are being monitored
- **Simplified Management**
  - Development operations will be able to integrate security and compliance into the container management process

Standard Features

- Security Monitoring across physical and virtual servers including:
  - Real-time file integrity monitoring: Identify changes to files in real-time including who made the change and what change occurred
  - Configuration Monitoring: Identify policy violations and suspicious activity in real-time
  - Consolidated Event Logging: Consolidate and forward logs for long term retention, reporting, and forensic analysis
  - File and System Tamper Prevention: Lock down configuration, settings, and files
  - Dashboards: Easily identify any abnormal event activity and monitor your key performance indicators
- Security monitoring of OpenStack Data center infrastructure including:
  - Configuration Changes: configuration files changes are monitored using real-time file integrity monitoring
  - Keystone Program files: Python files of modules are monitored to avoid file tampering of important system services.
  - Keystone Data: Changes to user account, role and tenant data are monitored closely to be aware of changes to identify data.
  - Access monitoring: Monitor user access through web interface
- Security monitoring of AWS public and hybrid clouds (VPCs) including:
  - Security configuration monitoring

  - File integrity monitoring,
  - Whitelisting with application control for on-premises and off-premises data centers,
  - Security automation across the cloud environment via REST API.
- Features and capabilities available in Symantec™ Data Center Security: Server including:
  - 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.
  - Unified Management Console (UMC) delivers a consistent management experience across Data Center Security products.

Customer Benefits

- Single tool to effectively identify policy violations and suspicious activities at an application or instance-level, in real-time, across the physical and virtual servers, as well as across AWS and OpenStack clouds.
- Simplify monitoring and compliance reporting of the security and compliance posture of AWS and Openstack cloud deployments at the application- and instance-level.
- Detect and identify changes to files in real-time across physical and virtual servers, as well as across AWS and OpenStack clouds.
- Optimize network and application performance of guest and hosts via agentless antimalware and agentless network IPS.
- Increase operational effectiveness by providing a single-instance security service per host that protects all virtual machines.
- Enable always-on security during new workload provisioning, thus reducing the security tax
- Monitor and protect physical and virtual data centers.
- Fully instrumented REST API provides corresponding API for all console actions to enable full internal and external Cloud automation.
- Simplify continuous monitoring and compliance reporting of hybrid data center infrastructures for cybersecurity and compliance.

Symantec™ Data Center Security Solutions

Symantec™ Data Center Security enables organizations to harden their physical and virtual servers, securely transition into software-defined data centers, and enable application-centric security across their public, private and private cloud environments.

The Symantec™ Data Center Security Product family includes:

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 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.

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

21347664-2 08/16