DATA SHEET SYMANTEC DATA CENTER SECURITY: SERVER 6.5

Agentless antimalware and network IPS for your VMware environments.

Data Sheet: Security Management

Frictionless AV & Network IPS Protection

- Agentless AV and agentless network IPS
- Hypervisor-based security virtual appliance (SVA)
- Low OPEX – Fully integrated with VMware NSX
- Always On – Anywhere Protection
- Utilizing Symantec Best in Class AV and Insight Reputation
- **NEW: Guest Network Threat Protection & In-Guest File Quarantine**
- **NEW: Operations Director**
- **NEW: Unified Management Console**

Integrated with "Server Advanced"

- Scale up to Full Lock Down
- Wizard Driven Simplified Hardening
- Protected Application Whitelisting and Control
- **NEW: Security Monitoring for AWS and OpenStack clouds**
- **NEW: Security Hardening for OpenStack Keystone**

Security Response
Insight Reputation

Virtual Data Center

Symantec Security Virtual Appliance

Symantec Security Virtual Appliance

vmware

vmware

Data Center Security Service for VMware NSX

Threat Landscape Overview

More than 317 million new pieces of malware were created in 2014, or close to 1 million new pieces of unique malware each day. The overall total number of malware is now over 1.7 billion. (Figure 1) Malware authors have various tricks to avoid detection; one is to spot security researcher by testing for virtual machines before executing their code. In 2014, up to 28 percent of all malware was "virtual machine aware.". *Source: "Symantec Internet Security Threat Report", Volume 20 (April, 2015).*

2014	**317 Million** +26%
2013	**252 Million**

New Malware Variants (Added in Each Year)
Source: Symantec
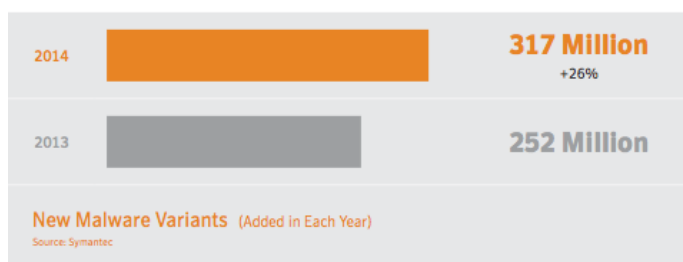
Solution Overview

Symantec™ Data Center Security (DCS): Server 6.5 delivers agentless antimalware protection, agentless network IPS, and file reputation services for VMware environments. It enhances operational effectiveness in the data center by providing a single-instance security service per host, protecting all virtual machines within that host.

Symantec™ DCS: Server 6.5 introduces Operations Director, a new feature that enables customers to automate and orchestrate security provisioning of anti-malware and network IPS services at the application-level across VMware NSX environments. This capability enables organizations to transition from traditional perimeter-centric security models that mimic physical security infrastructures into

✓ Symantec.

dynamic, software-defined security models. By leveraging its out-of-the-box integration with VMware vCenter and VMware NSX, Symantec™ Data Center Security: Server extends the ability to automate and orchestrate application-centric security across third-party security tools that are registered with VMware NSX Service Composer, starting with Palo Alto Networks.

Symantec™ DCS: Server 6.5 also features Unified Management Console (UMC), a new web-based console appliance that delivers a consistent management experience across the Data Center Security products. Customers will use UMC to register and configure features,

reports, and products in Symantec™ Data Center Security (DCS).

Operations Director and Unified Management Console are the new software-defined security capabilities that are being rolled out across the Symantec™ Data Center Security Product family. These enhanced capabilities are based on the core tenets of embedding security into the platform, integrating and simplifying point technologies, and automating and orchestrating security across the data center. These enhanced capabilities enhance operational efficiencies and mitigate the dreaded security tax by enabling security to keep up with the speed of the business and IT operations.

Why Symantec™ Data Center Security: Server?

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

- How do I dynamically provision application-level security for newly created virtual workloads?

- How do I deliver dynamic and operationally efficient antimalware and network IPS protection without taxing network resources and application performance?

- How can I provision security so that it is able to keep up with the speed of business and IT?

- How can I scale out security as I scale my infrastructure and applications?

- How can I leverage my planned and current investment in VMware NSX to enhance security in my software-defined data center?

- How can I reduce the resource impact associated with scanning and definition file updates, such as scan and update storms?

What's New in Symantec™ Data Center Security: Server 6.5?

- **Agentless network-based threat detection and protection (Network IPS).** DCS: Server 6.5 leverages network introspection for data packet inspection to detect threats. Security admins will have several options for defining security policies that can be applied to

workloads. Customers can optimize network performance and reduce disk IOPS by creating application-specific Network IPS policies.

- **Operations Director.** This new feature delivers out-of-the-box security intelligence and automates policy-based security orchestration within the Symantec Data Center Security product family. Operations Director automates the security provisioning workflow, enables application-centric security services, and seamlessly integrates with VMware NSX. Operations Director leverages its out of the box integration with Vmware vCenter and NSX Service Composer to extend these capabilities into partner products like Palo Alto Networks NextGen Firewall.

- **Unified Management Console (UMC).** UMC is new web-based console appliance that delivers a consistent management experience across Data Center Security products. Customers will use UMC to register and configure features, reports, and products in the Symantec™ Data Center Security (DCS) product family.

- **In-guest file quarantine.** This feature enables admin to set rules on the number of days for files to age and purge, as well as rules to purge folders based on count of files or on the size of the folder and generate alerts. This feature supports regulatory mandates and internal data retention policies.

- **Enhanced scan caching.** This feature improves the performance of agentless malware detection.

- Support for NSX 6.1.2 and vSphere 5.5 U2.

Symantec™ Data Center Security: Server Standard Features

- Agentless antimalware threat protection.

- Integrates with Symantec DeepSight providing reputation security technology to files and URL's.

- Auto-deployment and provision of Security Virtual Appliance to ESX host in a cluster.

- Integrates at the hypervisor, providing real-time detection and remediation of malware infection.

- Always-on security with the best-of-breed security protection technology

- Supports VMware vSphere 5.5 and NSX 6.1.

Customer Benefits

- Optimize network and application performance of guests and hosts via agentless antimalware and agentless network IPS.

- Improve network performance by having single definition updates.

- File and URL reputation services to complement the agentless malware protection service.

- Auto-deployment of virtual appliances enables the workloads to scale while minimizing any additional OpEx cost.

- Increase operational effectiveness by providing a single-instance security service per host.

  – Eliminate virus scanning on each virtual machine by providing security at the hypervisor

  – Centralized management of virus definitions eliminates the need for virus updates to each and every guest VM

- Enable always-on security during new workload provisioning, thus reducing the security tax.

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 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 Corporation (NASDAQ: SYMC) is an information protection expert that helps people, businesses, and governments seeking the freedom to unlock the opportunities technology brings—anytime, anywhere. Founded in April 1982, Symantec, a Fortune 500 company operating one of the largest global data intelligence networks, has provided leading security, backup, and availability solutions for where vital information is stored, accessed, and shared. The company's more than 20,000 employees reside in more than 50 countries. Ninety-nine percent of Fortune 500 companies are Symantec customers. In fiscal 2014, it recorded revenue of $6.7 billion. To learn more go to www.symantec.com or connect 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

21347665 06/15

✓Symantec.™