PRODUCT BRIEF

Data Center Security: Server

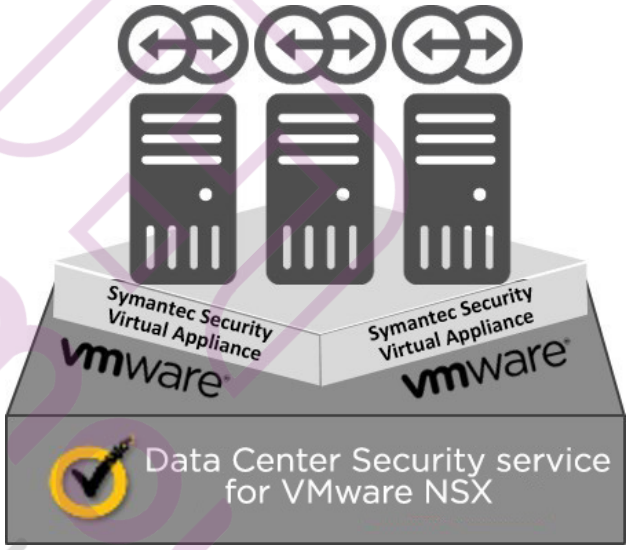
CUSTOMER BENEFITS

- An out-of-the box dashboard provides insight into the health and status of your data center.
- Agentless anti-malware and agentless network IPS help optimize the performance of networks and applications for guests and hosts.
- File and URL reputation services complement the agentless malware protection service.
- Automatic deployment of virtual appliances enables the workloads to scale while minimizing any additional OpEx cost.
- A single-instance security service for each host increases operational effectiveness.
- Security provided at the hypervisor level eliminates the need for virus scanning on each virtual machine.
- Centralized management of virus definitions eliminates the need for virus updates to every guest VM.
- Enable always-on security during new workload provisioning to reduce the security tax.

Overview

Symantec® Data Center Security: Server (DCS:S) is a purpose-built security offering for hypervisor, middleware, and guest VMs with agentless anti-malware protection, agentless network IPS, and file reputation services for workloads running on VMware NSX platforms. DCS:S enhances operational effectiveness in the data center by providing a single-instance security service for each host, protecting all virtual machines within that host.

Figure 1: Data Center Security: Server



Why DCS:S?

DCS:S is a good fit for your organization if your team is asking any of the following questions:

- How do I dynamically provision application-level security for newly created virtual workloads for NSX?
- How do I deliver dynamic and operationally efficient anti-malware 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 up security as I scale up infrastructure and applications?
- How can I manage and secure assets in a data center with minimal training for admins?
- How can I leverage a planned and current investment in VMware NSX to enhance security in a software-defined data center?
- How can I reduce the resource impact that is associated with scanning and updating definition files, such as in scan and update storms?

THREAT LANDSCAPE OVERVIEW

Hundreds of millions of new pieces of malware are created each year, and malware authors have various tricks to avoid detection. One trick is to spot security vulnerabilities by testing for virtual machines before executing their code. Some malware variants are also able to detect the presence of a virtualized environment.

What Is New in DCS:S?

The following features and capabilities are new in DCS:S:

- Easier deployment reduces the time to roll-out for new deployments and upgrades for DCS: Server and DCS: Server Advanced
- High availability and scalability
- Agentless anti-malware protection for workloads running on a VMware NSX platform
- DCS:S continues to deliver an agentless anti-malware solution by integrating directly at the hypervisor, thus offloading anti-malware scanning to a Security Virtual Appliance (SVA), which delivers higher performance and a greater density of Guest Virtual Machines.
- Automatic deployment of Security Virtual Appliance: DCS:S leverages a single SVA to deliver threat protection for VMware NSX by automatically deploying to VMware ESX, which allows it to scale to the size of the data center.

DCS:S Standard Features

The following features are standard in DCS:S:

- A single Security Virtual Appliance (SVA) for each ESX host
- A simplified UI with a rich user experience and simplified policy and asset management for VMware NSX
- Agentless anti-malware threat protection:
  - Supports VMware NSX, delivering agentless threat protection for workloads running on virtual environments
  - Anti-malware combined with Insight Reputation
  - Automatic deployment of the Security Virtual Appliance (SVA) in NSX environments (SVA), which allows you to scale out infrastructure
  - Group asset and protection policy
- Integration with DEEPSIGHT® provides reputation security technology to files and URLs:
  - Automatic deployment and provision of Security Virtual Appliance to an ESX host in a cluster
  - Integration at the hypervisor, providing real-time detection and remediation of malware infection
  - Always-on security with best-in-class security protection technology
  - Part of an extensive telemetry collection network

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 apply application-centric security across their public, private, and private-cloud environments.

The Data Center Security product family includes:

Data Center Security: Server (DCS:S)

DCS:S delivers frictionless threat protection with agentless anti-malware, network based IPS, and file reputation services for VMware environments.

DCS:S supports an in-guest quarantine feature to isolate suspected malware files and remediate them based on policy. DCS:S automatically delivers Security Virtual Appliances (SVA) that scale out, resulting in huge savings in OpEx costs.

Data Center Security: Server Advanced (DCS:SA)

DCS:SA offers security detection, monitoring, and prevention capabilities for both physical and virtual server infrastructures. Delivering agentless anti-malware protection and security monitoring for virtual and physical infrastructures and across the AWS and OpenStack clouds, DCS:SA protects both physical and virtual servers by delivering applications and protected white-listing, fine-grained intrusion detection and prevention; file, system, and administrative lockdown; and file integrity and configuration monitoring. DCS:SA also supports Docker Containers and full hardening of OpenStack Keystone.

For more information, please visit:
www.broadcom.com/products/cybersecurity/endpoint/hybrid-cloud/data-center-security

BROADCOM®
connecting everything®

For more information, visit our website at: www.broadcom.com

SED-DCS-PB102 December 14, 2023