Symantec
A Division of Broadcom

Product Brief

Symantec™ Data Center Security: Server

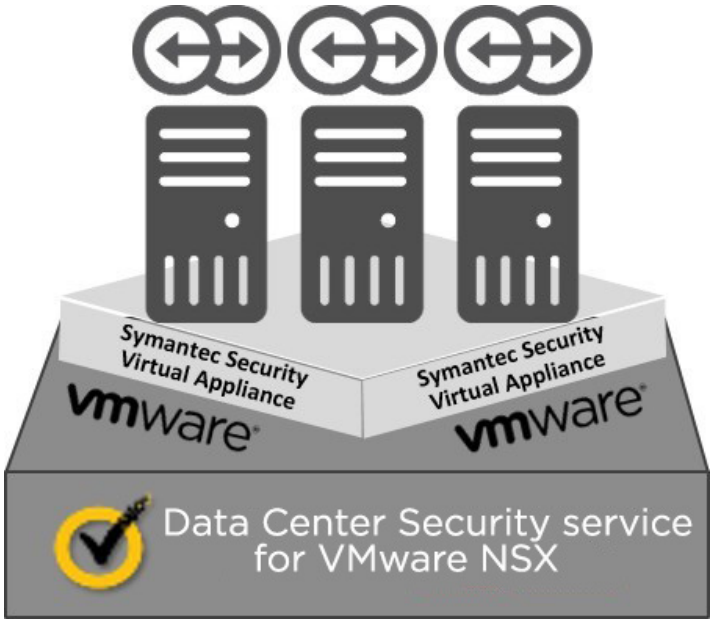
Threat Landscape Overview

Hundreds of million 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.

Solution Overview

Symantec™ Data Center Security Server (DCS:S) delivers agentless anti-malware protection, agentless network IPS, and file reputation services for workloads running on VMware NSX platform. 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.

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 my infrastructure and applications?

Why DCS:S? (cont.)

- How can I manage and secure my assets in my data center with minimal training to my admins?
- 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 that is associated with scanning and updating definition files, such as in scan and update storms?

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 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 datacenter.

Symantec Data Center Security: Server 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 agent-less threat protection for workloads running on virtual environments
  - Anti-Malware combined with Insight Reputation from Symantec
  - 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 Symantec 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 the best-of-breed security protection technology
  - Part of the extensive telemetry collection network from Symantec

Customer Benefits

DCS:S provides the following 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 you to optimize the performance of your network 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 level of the hypervisor eliminates the need for virus scanning on each virtual machine.
- The centralized management of virus definitions eliminates the need for virus updates to each and every guest VM.
- The ability to enable always-on security during new workload provisioning reduces 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 (DCS:S)
DCS:S delivers friction- less threat protection with agentless anti-malware, network based IPS and file reputation services for the VMware environments.

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

Symantec 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.

Symantec Cloud Workload Protection (CWP)
CWP allows enterprises to secure their critical workloads wherever they are – public clouds, private clouds, and physical on-premises data centers – all from a single centralized console. CWP is a native cloud SaaS offering that automates workload security, providing discovery, visibility, and protection against advanced malware and threats across multiple cloud service providers (AWS, Azure, GCP, OCI).

Automatic identification of the workload security posture and of software services, including visibility into infrastructure changes and flow logs, enables automatic policy recommendations and deployment. CWP provides multi-layered protection for cloud computing instances, including anti-malware scanning, application control, and isolation to help block exploits that target known and unknown vulnerabilities, OS hardening that helps to stop zero-day threats, and real-time file integrity monitoring (RT-FIM) that helps to prevent unauthorized system changes. CWP also supports Docker containers and orchestration applications.

Cloud-native integration with APIs for a public cloud platform, allows CWP to share and consume information in real-time, including any changes to the cloud infrastructure and to the security settings. Public cloud API integration also enables DevOps practitioners to build security directly into service deployment workflows, ensuring that workloads are protected, and that security scales automatically with dynamic cloud infrastructure.

The CWP cloud console can also be used to manage Symantec Data Center Security (DCS) agents on virtualized and physical on-premises servers.

For more information, visit our site at broadcom.com/data-center-security.

Symantec™
A Division of Broadcom

For product information and a complete list of distributors, visit our website at: broadcom.com

SED-DCS-PB100 November 17, 2020