

Symantec Data Center Security for SDDC

Leveraging VMware NSX™ for Anti-Malware and Guest Network Threat Protection

Overview

Symantec and VMware have been building joint solutions to help our mutual customers provide more agile and secure data centers that enable them to deliver better service to their businesses. An agile and secure data center requires a software-based architectural approach with complete abstraction and programmatic control of infrastructure resources. Security, a key data center service, requires a fundamentally different architecture that leverages the native position of the hypervisor at the virtual layer to maximize security. For VMware ESXi, security services can leverage guest introspection to optimize file scanning. With VMware NSX, security services can leverage the platform's inherent isolation, segmentation and micro-segmentation capabilities and provide deep packet inspection, intrusion detection and prevention, and application-level network security. NSX extensibility and distributed services framework can also be leveraged to dynamically insert and deploy these services, and standard tagging capability allows unified workflows and interoperability between security services from ecosystem partners.

Solution Description

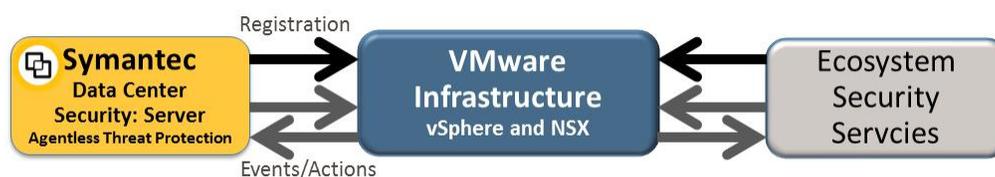
Symantec and VMware collaboration delivers threat protection for trusted workloads in the enterprise virtualized network based on the VMware NSX platform. Symantec protection is delivered as a security virtual appliance, on the NSX platform, managed cooperatively in the NSX ecosystem. The VMware NSX networking and security platform is a key element of VMware's vision for virtualized networks in the Software Defined Data Center (SDDC).

Symantec Data Center Security: Server

Symantec Data Center Security: Server is a purpose-built solution for VMware NSX and the new SDDC architectures, and allows our customers to automatically provision security controls and orchestrate policy across a fully abstracted resource pool.

The Symantec Data Center Security: Server solution includes:

- Virtual Machine security via agentless anti-virus/anti-malware, Symantec Insight™ reputation, and guest network threat protection services deployed as virtual appliances (SVA) across the virtualized network, via NSX.
- Security as a Service provisioning via VMware NSX Service Composer.
 - Supports automation for security service registration and deployment to the VMware infrastructure.
 - Protection follows workload across virtualized networks.
 - Automated, cooperative NSX security ecosystem workflows supported via Service Composer.
- Protections for ESXi monitoring and vCenter Server hardening automate VMware vSphere® best practices to secure the infrastructure.



Infrastructure Benefits

- Provides single instance security service per host integrated with the security ecosystem.
- Reduces resource impact (i.e. scan/update storms) associated with scanning and definition file updates.
- Provides scale out security to meet elasticity demands for new services, ensuring the business is compliant.

Security Benefits

- Increases security postures by centralizing multiple security profiles into a unified policy, leveraging the full contextual power of the virtual infrastructure itself.
- Improves security response across security ecosystem by leveraging standard tagging capability and unified workflows.
- Reduces security risks associated by rogue virtual machines by delivering threat protections from the hypervisor.

Operational Benefits

- Accelerates security provisioning time by facilitating deployment from within the VI Admin's consoles.
- Reduces management overhead by providing file scanning services and definition-file management at the per-host level, versus per guest VM.
- Reduces manual errors and RACE conditions thereby minimizing risk associated with misconfigurations and out-of-date information.

Summary

Symantec Data Center Security: Server provides a security system built on VMware hypervisors. With software defined security perspective, and focusing on an architecture that supports the basic premise of virtualization (i.e. agility, elasticity, movement, etc). Symantec is leading the security industry in delivering innovative architectures, along with a breadth of security intelligence and policy orchestration to ensure customers of Symantec and VMware have the confidence to advance their journey to the software defined data center.

Symantec continues to innovate with VMware and security ecosystem partners such as Palo Alto Networks and Rapid7 through a project called "Wonderland" to automate the orchestration of security policies using built in NSX platform mechanisms of security groups and security tags. This project includes automation of vulnerability management, threat protection and network security into one seamless workflow to provide micro-segmentation. These efforts result in customers being able to deploy SDDC architectures that maximize security, compliance, and responsiveness to the businesses they serve.

Look for more Data Center Security solutions from Symantec to include protection for VDI infrastructures and data stores.