Trend Micro™

Deep Security and VMware NSX

Advanced security framework for the Software-Defined Data Center

MORE SECURITY SPEND ≠ MORE SECURE

Even with over $70B in 2014 global information security spend and a 46% increase in 2015 security technology spend, the cost of security breaches far surpasses the amount spent on security.

Traditional perimeter-based security models severely lack the capability to extend unit level protection to data center workloads and keep up with the dynamic nature of the cloud. This results in insufficient visibility into east-west traffic, and when malware makes its way into the data center, there is little control to block and isolate the attack inside the data center. Additionally, manual security configuration and patching remains one of the biggest areas of exposure for corporations as hackers are quick to exploit any holes they can find. And the dynamic nature of today's data centers makes keeping up with basic security even more difficult as workloads are spun up and down and security policies have to be moved or reconfigured with the workloads.

As more and more workloads transition from physical infrastructure to the cloud (private and public), the Software-Defined Data Center brings new opportunities for security and automation.

RIGHT TOOLS FOR THE RIGHT JOB

The VMware NSX networking and security platform combined with Trend Micro's Deep Security builds on security in the Software-Defined Data Center to deliver a new level of data center security. The integration of Deep Security and VMware NSX focuses on three key aspects:

SECURITY: Providing elastic protection and scalability

The joint solution extends *micro-segmentation*—isolation of virtual clusters of workloads, even to the individual VM level, via distributed firewalling made possible by NSX. Deep Security extends micro-segmentation via multiple security controls including IDS/IPS, anti-malware, virtual patching, URL filtering, file integrity monitoring, and log inspection. This means not only can the workloads be locked down, but they can be locked down multiple ways from a single platform, achieving a layered security approach that's flexible depending on the needs of a given workload. This approach reduces the attack surface within the data center vs. perimeter security

SPEED AND AGILITY: Automated deployment and provisioning

Deep Security has long offered network and endpoint introspection through vSphere with the ability to easily provision existing and new virtual machines (VMs). New integration capabilities delivered through NSX automation and Service Composer will further streamline the provisioning and deployment processes, making insertion, orchestration, and scaling of Deep Security significantly faster and easier across your data center.

OPERATIONAL EFFICIENCY: Automating workflow across protection layers

Through the use of a new common NSX tagging and orchestration framework, Deep Security services can be inserted as part of an automated, defined workflow for each security group, which is configured in NSX. The user can then decide to create an automated remediation process for each workload or group. This could be used to automate real-time remediation and incident response during attacks. The degree of automation reduces risk of human error in the configuration process and also prevents proliferation of threats that do appear in the data center by isolating them and removing them once detected.

A history of joint innovation

2009: Trend Micro Deep Security 7.0 was the first solution supporting introspection of network traffic through the hypervisor.

2010: VMware vShield launched with Deep Security 7.5, the first and only partner solution to support VMware vShield—establishing the first fully "agent-less" anti-malware.

2011: Trend Micro announced Deep Security 8.0, supporting the latest vShield security ecosystem, and offered the only fully agentless security platform to include anti-malware, intrusion prevention, and integrity monitoring.

2012: Trend Micro announced Deep Security 9.0 supporting the latest vSphere 5.1 platform, and providing security for hybrid clouds and vCloud-based service providers via vCloud Director integration.

2013: Trend Micro demonstrated a prototype of Deep Security with NSX integration at VMworld. Trend Micro supports the VMware Hybrid Cloud Service.

2014: Trend Micro Deep Security validated on vCloud Air and plugin released for vRealize Operations Manager.

2015: Trend Micro announced support for vRealize 6.0 and also supports Log Insight.

TREND MICRO DEEP SECURITY SOLUTION COMPONENTS

The following are the key components from Trend Micro for this integrated solution:

Deep Security Manager: This is the management component of the system and is responsible for sending rules and security settings to the Deep Security Virtual Appliance (DSVA). The Deep Security Manager is controlled using the web-based management console. From this interface, the administrator can define security policies, integrate VMware solution components (such as NSX manager), and query status of various managed instances.

Deep Security Virtual Appliance: This is a security virtual machine built for VMware vSphere environments that agentlessly provides anti-malware, web reputation, host firewall, intrusion prevention, and integrity monitoring to virtual machines. It's a single virtual appliance that provides both Guest Introspection Services and Network Introspection Services by integrating with the VMware NSX platform.

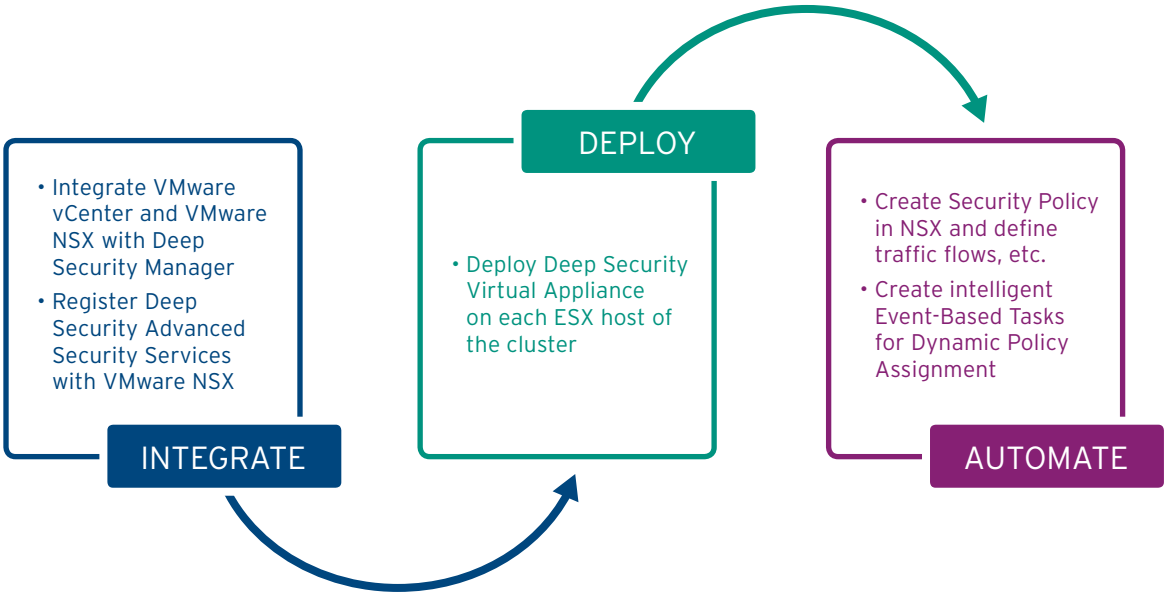
VMware NSX Security Solution Components:

- NSX Manager
- Service Composer
- NSX Controller
- Distributed Services

For more details on VMware NSX components, please see this guide:
http://www.vmware.com/files/pdf/products/nsx/vmw-nsx-network-virtualization-design-guide.pdf

HOW THE INTEGRATED SOLUTION WORKS

The Trend Micro Deep Security solution builds on the VMware NSX distributed service platform for automated insertion, deployment, and orchestration of security services in the Software-Defined Data Center. On NSX, Deep Security benefits from VMware's advanced security automation for deployment and provisioning—protecting applications with agentless security services inside the guest VM and attached to the virtual network. The NSX service composer allows Deep Security protections to be applied when and where they are needed for virtual machines and applications. NSX workflow automation allows Deep Security to scale on demand and manage dynamic responses to emerging threats. Integration with the NSX Service Composer simplifies security operations while improving visibility and coordinating activity with data center operations teams and application owners.



INTEGRATE: Trend Micro Deep Security integrates with VMware vCenter and VMware NSX manager with a "wizard application" to collect connection information and authentication credentials. As an extension of NSX advanced security services, Deep Security is now a service, available to all ESX hosts, applicable to every virtual machine and virtual network segment.

NSX integration registers Deep Security for advanced security services providing both NSX Guest Introspection and Network Introspection Services from the same security virtual appliance (SVA).

All necessary information is automatically defined for the NSX manager (Service Composer) to retrieve and seamlessly deploy the Deep Security Virtual Appliance package as an OVF.

DEPLOY: Deployment of Deep Security is automated by NSX for each ESXi host of the cluster. As new hosts are added, NSX will automatically load the Deep Security Virtual Appliance on each new host—ready to provide protection to the virtual system and enforce defined security policy.

AUTOMATE: Deep Security services use VMware's NSX (Service Composer) security groups for automatic workflow capabilities using Event-Based Tasks and service chaining. Deep Security Manager and NSX share the dynamic security description of the protected policy objects. For example, the capability allows adding new virtual machines to an NSX Security Group for web servers and the Trend Micro Deep Security Manager applies appropriate existing policy individually for these new web servers, regardless of which ESXi hosts or physical networks they are attached to.

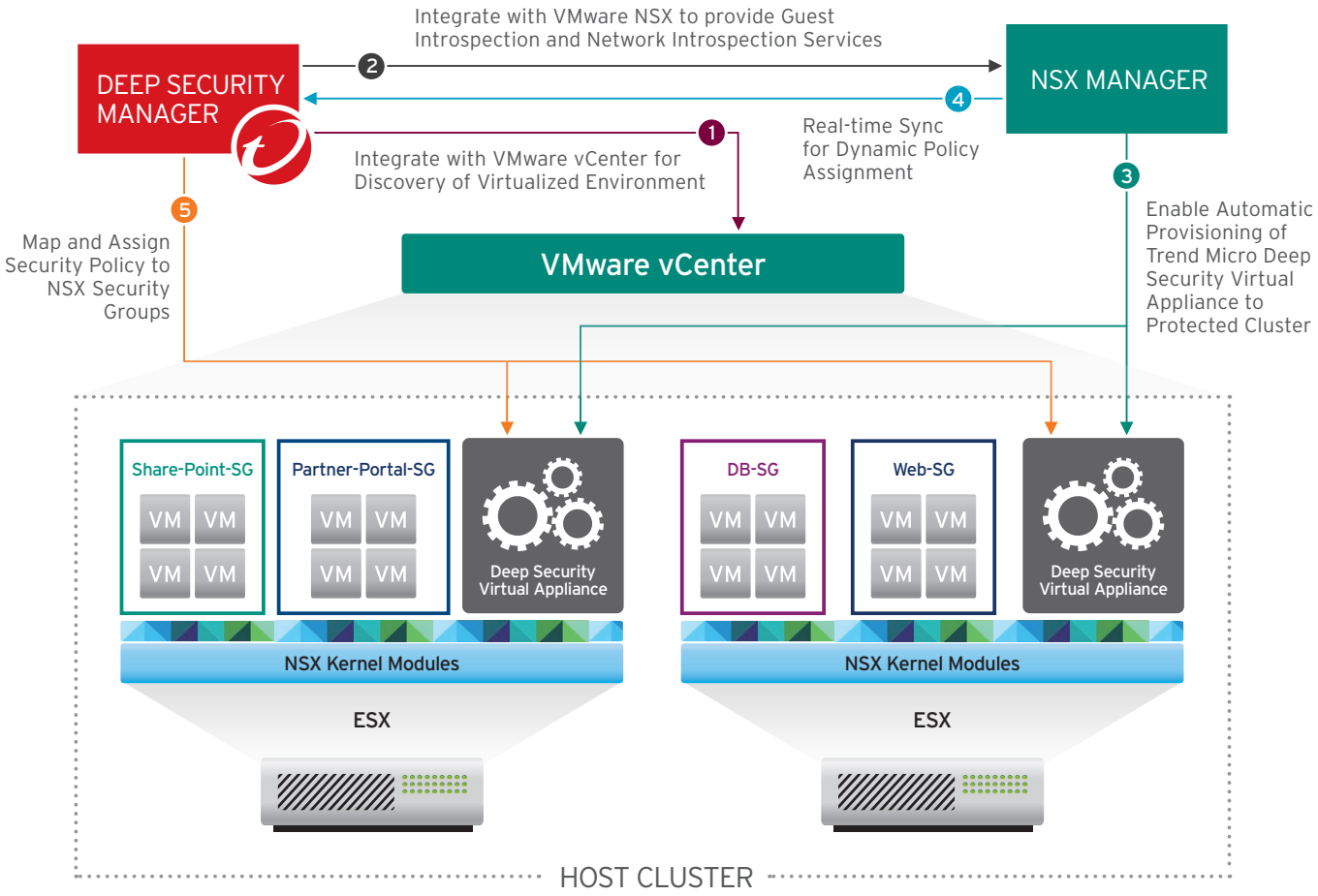


Figure 1: Trend Micro Deep Security and NSX Solution Components Integrated View

UNLOCKING THE POWER TO DO MORE

The joint VMWare NSX and Trend Micro Deep Security solution enables various infrastructure use cases, some of which are captured below:

Secure End User: Trend Micro™ **Deep Security™** offers optimized, VDI-centric security for virtualized computers that can help improve the security and performance of VDI servers. The agentless security model helps maximize consolidation ratios with security solutions designed specifically to handle the rigors of desktop virtualization. VMware NSX simplifies VDI. NSX micro-segmentation provides isolation and segmentation of data center traffic to allow desktops to share infrastructure. NSX enables Deep Security services to be based on logical groupings and automates the application of Deep Security policy to desktop users and pools. NSX service chaining allows advanced services to be adaptively inserted.

Compliance: Trend Micro Deep Security is a comprehensive security platform that packs in key compliance requirements including web application security, integrity monitoring, and log collection along with a wide range of other compliance requirements for PCI DSS, as well as HIPAA, NIST, SAS 70, and others. VMware NSX micro-segmentation and Distributed Firewall provide network isolation and segmentation to allow compliance zones to be set up on the same underlying infrastructure. NSX provides unit-level threat protection to prevent threats in one trust zone from being propagated to others.

Multi-tenant Infrastructure and Multi-vCenter deployments: Deep Security has an agile multi-tenant architecture for software-defined data centers and providers that enables logical separation of tenant policies and data, allows delegation and self-service for tenants, and supports elastic cloud-scaling with automated deployment and provisioning of Deep Security components. RESTful management APIs also facilitates extensibility and integration into modern cloud infrastructure. NSX micro-segmentation enables complete separation of unrelated networks and allows fully automated deployment of Deep Security multi-tenant services based on virtual networks, network segments, or security groups.

SECURITY OPTIMIZED FOR VIRTUAL AND CLOUD ENVIRONMENTS

With thousands of successful customer deployments worldwide, Trend Micro Deep Security has proven it improves security, manageability, scalability, and VM density. Trend Micro has received numerous accolades and recognition for virtualization security, including IDC's #1 ranking[1] in market share for server security (which includes virtualization and cloud security) since 2009.

Trend Micro has led the market with several significant "firsts":

- *First* agentless security suite for the VMware hypervisor
- *First and only* security solution to integrate with cloud platforms including Amazon EC2, VMware vCloud, and Microsoft Azure
- *First and only* security architecture designed for service providers and enterprises with software-defined data centers; with support for multi-tenancy, auto-scaling, utility computing, and self-service

The VMware NSX platform represents the latest step forward, demonstrating VMware and Trend Micro's commitment to design the ideal next-gen security framework for today's virtualized and cloud environments.

CONTACT AND AVAILABILITY

If you are a VMware vSphere customer interested in learning more about Trend Micro integrated solutions with NSX, please contact us at 1-877-218-7363 or visit **trendmicro.com/virtualization**.

vmware®

TREND MICRO™

[1] IDC Worldwide Endpoint Security 2014-2018 Forecast and 2013 Vendor Shares, Figure 2, doc #250210, August 2014