Solution Brief

Next-Generation IPS Integrated with VMware NSX™ for Software-Defined Data Centers

The integration of McAfee® Network Security Platform into VMware NSX allows you to dynamically protect, manage, remediate, and support compliance in your Software-Defined Data Center with next-generation intrusion prevention system (IPS) services.

VMware NSX Software-Defined Data Centers (SDDC) Enable Better Security

The Software-Defined Data Center (SDDC) approach inherently builds security and agility into the data center construct. The foundation of an SDDC approach is automated provisioning and scale-out performance distributed across hypervisors in the data center. It leverages the position of the hypervisor to securely acquire and share application context, the basis for distributed enforcement at each virtual interface.

VMware NSX provides the network virtualization and automation pillar of the SDDC. It uses network isolation, segmentation with firewalling, and advanced security services from ecosystem partners like Intel Security for micro-segmentation to help the SDDC implement unit level trust and reduce the attack surface. The VMware NSX controller consolidates all configuration and state information for all network connections and services and enables it to be consumable by services like IPS.

McAfee Network Security Platform and Next-Generation IPS

McAfee Network Security Platform is an intelligent security solution that discovers and blocks sophisticated threats in the network. Using multiple, advanced signature-less detection techniques (such as McAfee Advanced Threat Defense), real-time emulation, and endpoint integration, it moves beyond mere pattern matching to defend against unknown stealthy attacks with extreme accuracy.

McAfee Network Security Platform consists of two primary components: sensors and a management application, McAfee Network Security Manager, which configures the IPS policies and sensors, analyzes data into actionable information, provides reporting, and takes steps for remediation. Available as both physical and virtual appliances, it has been optimized to run on Intel architecture, using Intel® Xeon™ technology like Intel® HyperScan and Intel® Data Plane Development Kit (Intel DPDK) for maximum performance in virtualization solutions such as VMware ESX.

Key Advantages

Next-Generation IPS Protection
Adaptive, intelligent IPS rated "Recommend" by NSS Labs and a Gartner Magic Quadrant Leader for seven consecutive times, now integrated with VMware NSX.

Comprehensive Security for Software-Defined Data Centers
Deployment is automated, and IPS security policies are automatically synchronized with VMware NSX and applied to groups of virtual workloads.

intel Security

Integration Using the Intel® Security Controller

Intel Security and VMware have collaborated on an integrated solution that leverages VMware NSX automation, platform extensibility, micro-segmentation, and traffic steering capability to dynamically secure workloads using next-generation IPS services, and allows infrastructure and security administrators to continue to use the tools they have for best leverage of skills and duty separation.

The integration is achieved via the Intel® Security Controller, which is deployed as an application within a virtual machine. It runs transparently to broker between the VMware NSX infrastructure and the McAfee Network Security Platform (Figure 1). Next-generation IPS services from the McAfee Virtual Network Security Platform are contained within its security function catalog, deployable as a distributed appliance on demand on VMware vSphere infrastructure and the VMware NSX manager.

Working in conjunction with the VMware NSX Manager, it enables network IPS protection to be dynamically and automatically provisioned to protect intra-VM traffic, according to the policies and requirements defined within VMware NSX and configured by McAfee Network Security Manager. It leverages the VMware NSX distributed service framework for dynamic service insertion at multiple points in the logical service pipeline.

By performing dynamic, bi-directional synchronization between essentially unlimited deployments of McAfee Network Security Manager and VMware NSX, administrators experience a "plug-in" like environment that enables support for micro-segmentation, security profiles, workflows, policies, and groups.

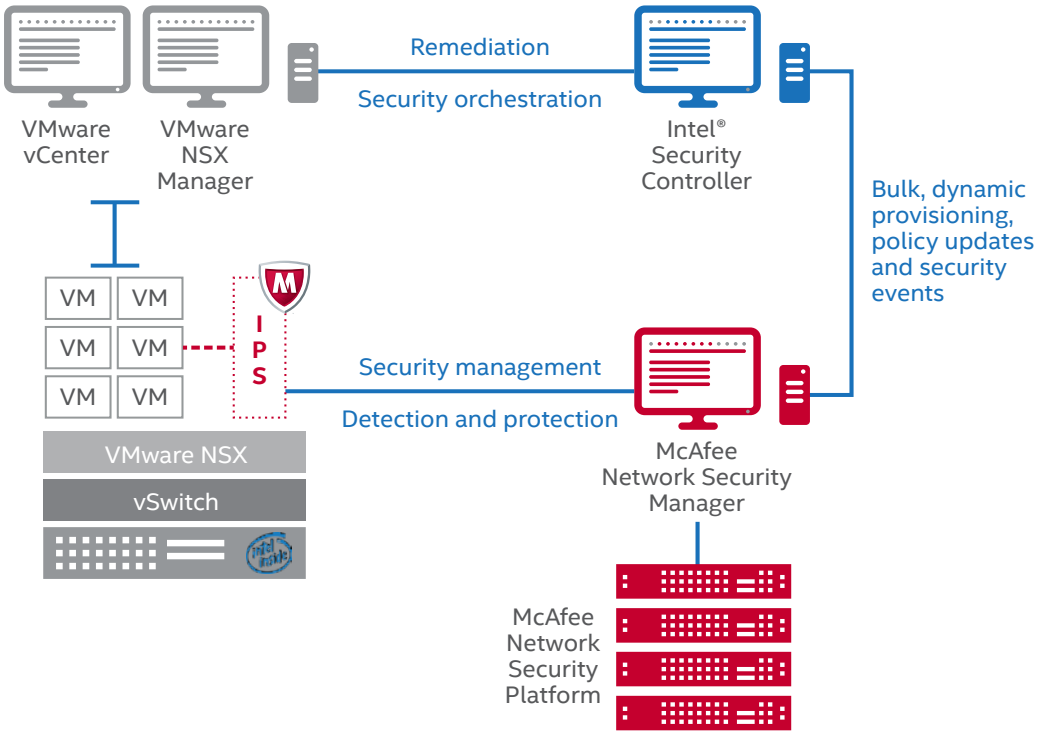

Figure 1. Integration architecture.

Key Advantages continued

Efficient Management
Infrastructure and security administrators continue to use the same tools to manage the data center, supporting separation of duties, consistent policy management across the infrastructure, automation of manual tasks, and investment protection.

Benefits

- **High performance protection and compliance**—Uses intelligent, multiple signature-less engines from McAfee Network Security Platform and visibility from VMware NSX. The McAfee Virtual Network Security Platform uses rich contextual data about users, devices, and applications provided by the VMware NSX controller for fast and accurate response to network-borne, signature-less attacks.
- **Reduction in management costs and time-to-service, with consistent policy enforcement**—Automation of typically manual security tasks for provisioning and reconfiguration of traditional appliances saves costs and speeds delivery. Intel® Security Controller, VMware NSX, and the McAfee Network Security Manager enable consistent policy enforcement for both physical and virtual appliances and protect your investment in high-performing, dedicated physical appliances at the high-traffic perimeter.
- **Security intelligence as part of Security Connected from McAfee**—The Intel® Security Controller works in conjunction with McAfee Network Security Manager and other Security Connected solutions, so that attacks within the VMware NSX virtual infrastructure are not only detected, but also blocked and quarantined, and may be forwarded to other McAfee server, endpoint, and management solutions for remediation.

Compatibility

The Intel® Security Controller is available to customers of the McAfee Virtual Network Security Platform sensor. Please refer to Table 1 for supported environments.

Table 1. Solution Compatibility

Products	Configurations
VMware	• VMware ESXi v5.5 • VMware vCenter Server v5.5 • VMware vSphere Web Client v5.5 or above • VMware NSX Manager v6.1 • IPv4 environments only
McAfee Network Security Platform	• McAfee Network Security Manager 8.2 • McAfee Virtual Network Security Platform 8.1

For More Information

To get detailed information on each component of this solution, please review these data sheets:

- **McAfee Virtual Network Security Platform**
- **Intel® Security Controller**
- **VMware NSX**

To learn more about Intel Security's strategy for Software Defined Security and about this solution, or to request a demonstration or participation in our evaluation program, contact your local sales representative or visit **www.intelsecurity.com/sdi**.

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com