Solution Brief

Securing the Software-Defined Data Center

The future of the data center is software defined

With the advent of proven solutions for network virtualization and their integration into comprehensive cloud management stacks, the software-defined data center (SDDC) has become a realistic infrastructure model for both private and public clouds. SDDCs offer compelling advantages for enterprise IT departments and the organizations they serve including:

- Better support for business innovation through an IT infrastructure that is more flexible, available, scalable, and reliable.
- Greater business agility through faster delivery of new services.
- Lower capital and operating costs through more efficient resource utilization.
- Streamlined auditing and compliance through policy-based automation and reporting.
- Simpler integration of new technologies and legacy resources.
- A data center infrastructure that intrinsically supports the development of hybrid private and public cloud environments.

The Sinkhole in the SDDC Roadmap: Network Security

The virtualization of network infrastructure—the routers, switches, servers, load balancers, and other functionalities that enable modern digital communications—has progressed rapidly in recent years. Virtual network function (VNF) equivalents for most traditional network components are now available from established vendors, making it easy for organizations to realize the benefits of a more flexible and scalable IT infrastructure, especially within the data center.

Network security virtualization, unfortunately, has not kept pace, making it difficult to implement best practice protection for software-defined infrastructure. Intrusion prevention systems (IPS) and other essential security controls have been stranded at the SDDC perimeter, blind to the internal east-west flows that make up more than three quarters of today's SDDC traffic. Without fully functional security VNFs to segment networks and isolate virtualized workloads, attacks that successfully bypass perimeter security are free to propagate undetected.

Key Advantages

McAfee® Network Security Platform 8.4

- Delivers best-in-class IPS security across physical and software-defined infrastructure.
- Secures private, public, and hybrid clouds with single-pane-of-glass management of advanced threats.
- Provides micro-segmentation and deep inspection of east-west traffic in the SDDC
- Integrates with leading private and public cloud platforms for seamless security orchestration.
- Simplified licensing with throughput sharing across multiple clouds and platforms.

intel Security

To fully protect private cloud SDDCs, security VNFs must not only replicate all of the capabilities of their physical instances, they must also provide seamless integration with cloud management stacks, especially their provisioning and orchestration controllers. Until recently, few third-party security solutions were integrated with software-defined networking (SDN) controllers, and almost none were able to operate across heterogeneous, hybrid clouds. So as virtual networks became ever easier to orchestrate, automate, and manage, virtual security management remained manual, labor-intensive, and error-prone.

Most public cloud service providers take responsibility for securing basic underlying infrastructure, but they place responsibility for securing everything else, including operating systems, applications, and data, on the customer. Public cloud service providers typically offer catalogs of basic homegrown security controls, along with some third-party security solutions, such as segmentation firewalls. While useful, these firewalls offer little visibility into traffic payloads and practically no ability to detect and block advanced threats and malware.

The maturity gap between virtual infrastructure and available virtual security solutions has forced IT organizations to choose between implementing an SDDC with perimeter-only security, or relying on basic built-in security functions offered with some SDN controllers and public cloud providers. Further complicating security, many enterprises are moving to a hybrid cloud model, which means they have little choice but to deploy separate security solutions with separate management consoles for their private and public clouds. Thus, the SDDC has remained, for some organizations, a risky proposition.

What's Still Needed: Software-Defined Security as Agile and Automated as the SDDC Itself

To adequately secure the SDDC, IT departments need software-defined security controls that can:

- Deploy inside virtualized environments to inspect east-west traffic flows between virtual machines.
- Find, block, and remediate advanced threats capable of evading access controls and firewalls.
- Be managed seamlessly across physical, virtual, and cloud-based environments, including private, public, and hybrid clouds.
- Be provisioned as policy-defined workload attributes that deploy, scale, migrate, and decommission automatically, in tandem with the workloads they protect and throughout their lifecycles.
- Integrate and orchestrate seamlessly with major cloud platforms.

The SDDC Security Solution: McAfee Virtual Network Security Platform

The virtual version of the McAfee award-winning intrusion prevention systems (IPS), McAfee Virtual Network Security Platform, fulfills all of these requirements with a solution stack that redefines how organizations block advanced threats in private and public cloud environments. Unlike traditional IPS solutions, it extends beyond signature matching, instead providing layered, signature-less technologies that defend against never-before-seen threats. Intelligent workflows save time by isolating threat patterns, enabling security administrators to provide fast and accurate responses to network threats and breaches.

McAfee IPS solutions unify threat defense across both physical data centers and SDDCs and into private, public, and hybrid clouds, all with orchestrated security provisioning, single-pane-of-glass visibility, correlated threat intelligence, and integrated attack response. Solutions include:

- **McAfee Virtual Network Security Platform:** A software-only sensor that deploys on major public and private cloud platforms as a native security VNF to inspect traffic at the SDDC perimeter, between VMs, or across hybrid cloud environments.
- **McAfee Network Security Platform appliances**: Hardware-based sensors with throughput capacities to 40 Gbps that are ideal for large data center perimeter applications.
- **McAfee Network Security Manager**: A management console application providing centralized administration, logging, correlation, analytics, and remediation workflows for both virtual and physical sensors.

Future-Proof Virtual Security for Private, Public, and Hybrid Clouds

McAfee provides your organization with peace of mind. You know that your IT department can seamlessly deploy the same strong security enjoyed in physical data centers today across your private and public cloud environments tomorrow. Even if you start small, McAfee Virtual Network Security Platform scales effortlessly with your business to support your most ambitious growth plans. Advanced features include:

Amazon Web Services (AWS) support: Available as a lightweight AWS machine image that delivers true visibility across the AWS gateway and east-west traffic within an Amazon virtual private cloud (VPC) environment. With an innovative approach to network inspection, McAfee Virtual Network Security Platform can deliver complete visibility to east-west traffic between AWS workloads, as well as at the gateway.

VMware NSX integration: Certified with native support to provide automated micro-segmentation and deep inspection of east-west traffic between virtualized workloads and VMs, managed from within the familiar NSX console.

OpenStack deployments: Support for orchestration of OpenStack-based SDN environments enables automated micro-segmentation and inspection of traffic between private cloud workloads.

Open Security Controller: Introduces a new way to enable software-defined security within a virtual infrastructure. It uses bi-directional, notification-based application programming interfaces (APIs) and provides a continuous brokering service between security VNFs and virtual networking SDN controllers.

Flexible licensing: Cloud sharing allows you to cost effectively share throughput from a single license across any number of McAfee Network Security Platform virtual sensor instances deployed in public and private clouds. Cloud sharing also improves security by enabling administrators to rapidly deliver east-west traffic protection and micro-segmentation to virtual workloads wherever they are, without having to wade through the time-consuming procurement process.

Cloud sandboxing: Integration with McAfee Cloud Threat Defense enables McAfee Virtual Network Security Platform to submit file content to cloud-based analysis and sandboxing and take action when a file is convicted as malicious. Additional copies of the file are blocked with no need for further analysis.

A Fully Integrated Security Solution

McAfee Virtual Network Security Platform also extends its functionality and your threat visibility through seamless integration with other McAfee solutions. This enables a complete picture of activity across both traditional and virtualized network environments, including the SDDC. Integrations include:

- **McAfee Advanced Threat Defense**: This malware sandbox detects today's stealthiest zero-day attacks with an innovative, layered approach. It combines low-touch antivirus signatures, reputation intelligence, and real-time emulation defenses with in-depth static code and dynamic analysis of actual behavior. When McAfee Advanced Threat Defense convicts a file as malicious, McAfee Virtual Network Security Platform can immediately quarantine the infected host and block other copies of the file, halting the spread of malicious activity in the network.
- **McAfee MOVE AntiVirus**: McAfee Management for Optimized Environments AntiVirus (McAfee MOVE AntiVirus) brings optimized, advanced malware protection to virtualized desktops and servers. It offloads malware scanning to free up hypervisor resources and to eliminate bottlenecks, delays, and antivirus storms. Implement it across multiple hypervisors, or choose an agentless, tuned option for VMware NSX or VMware CNS. Either way, you get top-rated security for swift threat detection and containment with minimal impact on virtual machine performance.
- **McAfee Threat Intelligence Exchange**: This collaborative system closes the gap between malware encounter and containment from days, weeks, and months down to milliseconds. It leverages the McAfee Data Exchange Layer to combine and instantly operationalize multiple threat information sources, sharing data with all connected security solutions, including third-party solutions.

Software-Defined Security in the SDDC: Three Use Cases

To better appreciate how McAfee Virtual Network Security Platform strengthens SDDC security while simplifying security management, let's review three typical use cases.

Unified cloud visibility

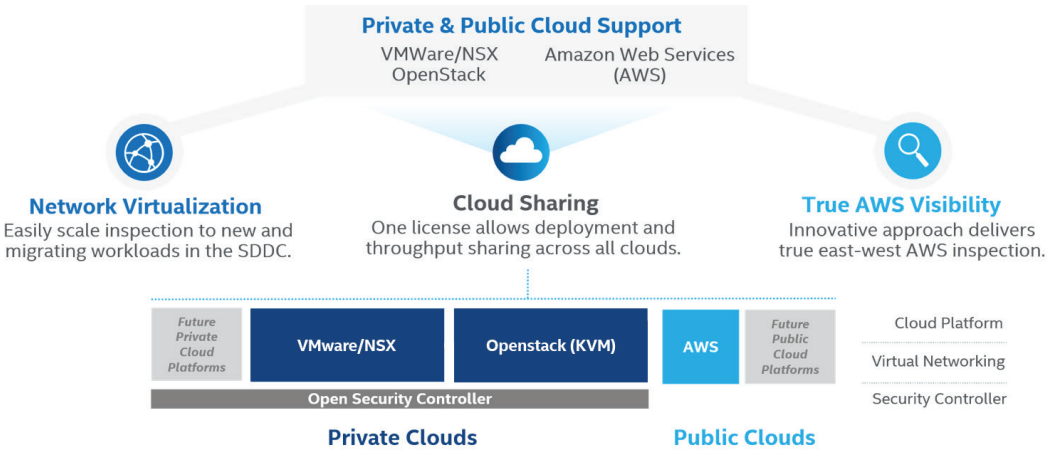

Figure 1. Extending threat visibility across AWS and private clouds with a new streamlined orchestration model.

The illustration above shows workloads being provisioned into both private cloud and public cloud environments. With cloud sharing, McAfee Virtual Network Security Platform gives you an easy way to deliver threat visibility across their cloud architectures. With one license, administrators can share throughput across any combination of supported public and private clouds. McAfee Virtual Network Security Platform provides full inspection of both north-south and east-west traffic flows, even within the AWS environment, which can be a challenge for other vendors. With the ability to easily deliver a unified policy across an organization's complete cloud footprint, McAfee Network Security Manager provides administrators with complete, integrated security management.

Dual-layer workload security: micro-segmentation plus automated IPS provisioning

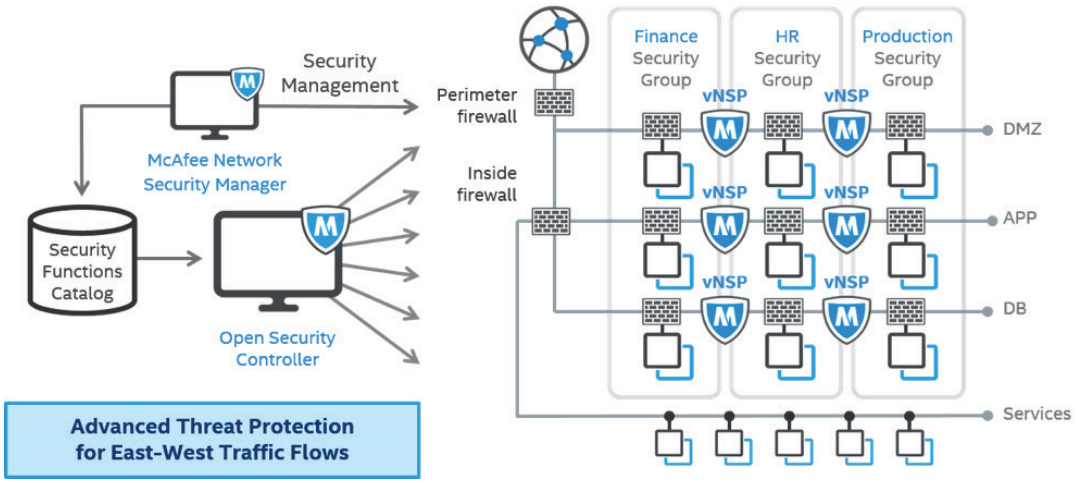

Figure 2. Workload micro-segmentation and deep threat inspection in the SDDC with McAfee Virtual Network Security Platform.

Figure 2 shows an SDDC in which McAfee Virtual Network Security Platform instances are automatically provisioned as policy-defined security attributes of newly instantiated workloads. Open Security Controller provides security policy management, a virtual sensor system image, and brokering services to integrate security infrastructure orchestration with the SDN controller.

The result? Every workload in the SDDC is automatically instantiated with network isolation (or micro-segmentation) and IPS protection pre-configured for the unique security requirements of its application, data, and user roles. In this example, unique security policies have been defined for finance, human resource, and production workloads. Traffic to each workload is allowed only from approved sources, and all permitted traffic is inspected and analyzed for indicators of compromise (IoCs), which trigger policy-defined blocking and remediation activities.

Manage on Your Terms

McAfee Endpoint Security keeps management simple and flexible.

- **McAfee® ePO™, on premises (5.1 and higher)**: It's easy to deploy one product that includes all of the recommended baseline protection technologies.
- **Unmanaged/standalone**: Those who don't use a McAfee management system will find it easy to install the new endpoint security client using the integrated installer. This can also be used for deploying the product using third-party deployment tools.
- **Cross-platform support:** Protection for desktops and servers across Windows, Macs, and Linux. Windows and Mac systems can be managed with common policies, with the data gathered by endpoints of either operating system that shares insights with McAfee ePO software.

Ensuring separation of duties for security and systems administrators

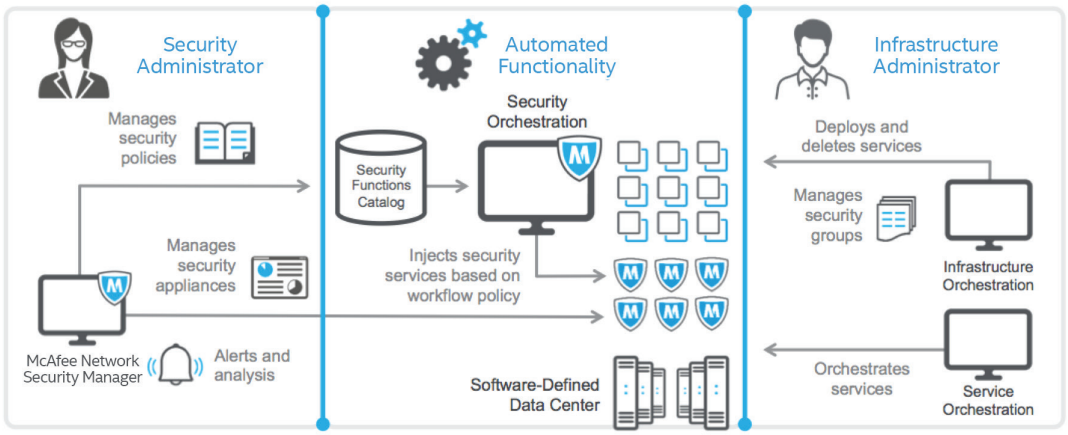

Figure 3. McAfee Virtual Network Security Platform segmenting administrative duties in a virtual environment.

With a software-defined security infrastructure based on McAfee Virtual Network Security Platform and Open Security Controller, IT organizations can also enforce strict separation of duties between security and infrastructure administrators. Security team members set security policy, monitor alerts, and analyze events in McAfee Network Security Manager, eliminating the need for direct access to production systems. Infrastructure administrators can focus on managing the virtual infrastructure through the cloud platform's provisioning and orchestrating controller without worrying about security. Open Security Controller ensures continuous synchronization between visualized infrastructure and security policy changes in the SDDC by brokering between security and cloud management stacks.

A Complete Software-Defined Security Solution for the SDDC

McAfee Virtual Network Security Platform provides a unique combination of deep visibility into SDDC traffic flows with automated security management. Tight integration with both private and public cloud management platforms ensures that your security infrastructure is dynamic and as easy to manage as the rest of your virtualized infrastructure. Finally, the SDDC is as appealing to data center operations teams risk managers as it is to business planners.

intel Security

McAfee
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com