DATA SHEET

McAfee Virtual Network Security Platform

Complete threat detection for cloud networks

McAfee® Virtual Network Security Platform is a complete network threat and intrusion prevention system (IPS) solution built for the unique demands of private and public clouds. It discovers and blocks sophisticated threats in cloud architectures with accuracy and simplicity, enabling organizations to restore compliance and embrace cloud security with confidence. Advanced technologies include signature-less detection, in-line emulation, signature-based vulnerability patching, and support for Amazon Web Services (AWS) and network virtualization. With streamlined workflows, multiple integration options, and simplified licensing, organizations can easily manage and scale their security in the most complex cloud architectures.

Complete Public Cloud Security with Advanced Security Technology

Public clouds offer convenience, cost savings, and the opportunity to shift infrastructure spending to an operational expense model. They also introduce a new level of risk, where a vulnerability in publicly accessible software could enable an attacker to puncture the cloud and exfiltrate sensitive information or accidentally expose customer data to other tenants using the same service. McAfee Virtual Network Security Platform supports AWS—today's leading public cloud service—delivering complete threat visibility of data going through an internet gateway and also into east-west traffic. With it, you can restore threat visibility and security compliance into public cloud architectures with an intrusion prevention system (IPS) platform that delivers true east-west traffic inspection.

Securing Virtualized Environments

Enterprises are rapidly adopting virtualized IT infrastructures—such as private and public clouds—where physical servers can simultaneously host multiple virtual machines (VMs) and even entire virtualized workloads. The resulting inter-VM communication, along with instant migration, replication, and backup of these workloads, have combined to dramatically increase east-west traffic

Key Advantages

Unparalleled advanced threat prevention

- Signature-less, advanced malware analysis.
- Protect against cross-site scripting and SQL injection.
- Advanced botnet callback and malware detection.
- Behavior-based analysis and distributed denial-of-service (DDoS) protection.
- Integration with McAfee Advanced Threat Defense.
- IPS and intrusion detection system (IDS) deployment.
- Always-on VMware ESX-McAfee Virtual Network Security Platform solution.

Cloud-ready architecture

- One license allows throughput sharing across any combination of public and private clouds.

inside private and public cloud as well as SDDCs. Adding to the chaos, the flexibility provided by network virtualization makes these escalating traffic flows dynamic and unpredictable. To keep up, virtualized security solutions must be flexible and scalable, and, even more importantly, they must function seamlessly with software-defined networking (SDN) platforms that orchestrate these often short-lived VMs and workloads.

Drive Agility in Private Clouds

Designed to meet the demands of securing virtualized environments, McAfee Virtual Network Security Platform integrates seamlessly with popular private cloud platforms including VMware NSX and OpenStack-based SDN environments. In fact, McAfee Virtual Network Security Platform is the only dedicated virtual IPS solution certified to work with VMware NSX. Micro-segmentation of VMs and deep inspection of east-west traffic is maintained automatically in virtualized environments, even as workloads are rapidly born, migrated, and retired.

Unparalleled Threat Prevention

McAfee Virtual Network Security Platform is based on a next-generation inspection architecture designed to deliver deep inspection of virtual network traffic. It uses a combination of advanced inspection technologies—including full protocol analysis, threat reputation, behavior analysis, and advanced malware analysis—to detect and prevent both known and zero-day attacks on the network.

No single malware detection technology can prevent all attacks, which is why McAfee Virtual Network Security Platform layers multiple signature and signature-less detection engines to help prevent unwanted malware from wreaking havoc in your clouds. It delivers numerous inspection technologies, like in-line emulation of browser, JavaScript, and Adobe files, botnet, and malware callback detection, behavior-based DDoS detection, and protection from advanced attacks like cross-site scripting and SQL injection. McAfee Virtual Network Security Platform can also identify and block the stealthiest of files via integration with McAfee Advanced Threat Defense, where files are submitted for in-depth behavior analysis. McAfee Advanced Threat Defense combines in-depth static code analysis, dynamic analysis (malware sandboxing), and machine learning to increase zero-day threat detection, including threats that use evasion techniques and ransomware.

Simplify with Cloud License Sharing

Today, many enterprises spread their IT resources and infrastructure across multiple clouds and platforms—whether to support legacy applications, reduce dependency on a single vendor, system redundancy, or for cost savings. Licensing security solutions for virtualized environments can be complicated and expensive, as most vendors require the purchase of separate licenses across private and public clouds and for different SDN platforms.

McAfee simplifies licensing and reduces costs through cloud license sharing, a new concept that allows customers to share their McAfee Virtual Network Security Platform throughput and license across any combination of public and private cloud platforms. Cloud license sharing also improves security by

- Innovative AWS inspection approach provides true east-west traffic protection in the public cloud.
- Support for orchestration with VMware NSX and OpenStack-based SDN environments enables automated micro-segmentation and inspection of traffic between private cloud workloads.
- VM-aware dashboard with quarantine enforcement capability available with VMware integration.
- Single centralized management console for the physical and virtual Sensors, on premises and in the cloud.

Intelligent security management

- Single console manages the on-premises and cloud Sensors.
- Intelligent alert correlation and prioritization.
- Robust malware investigation dashboards.
- Preconfigured investigation workflows.
- Scalable web-based management.

Visibility and control

- Application identification.
- User identification.
- Device identification.
- Security status of all VMs in AWS.

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.

Streamline Workflows and Analytics

Discover and block the most sophisticated threats with ease. McAfee Virtual Network Security Platform includes advanced analytics and integrations with additional security solutions to create a truly comprehensive and connected network threat detection and mitigation platform.

Modern threats can generate large volumes of alerts, quickly outpacing a security operator's ability to prioritize and track them. If the dots are not connected in time, real threats can slip by undetected. McAfee Virtual Network Security Platform's out-of-the-box advanced analytics and actionable workflows correlate multiple IPS alerts into a single, actionable event, helping administrators rapidly cut through the noise and get to relevant, actionable information.

Centralized Management with Real-Time Control of Real-Time Data

A single McAfee Network Security Manager appliance delivers centralized, web-based management and unrivaled ease of use. The state-of-the-art console and enhanced graphical user interface put you in control of real-time data. You can easily manage, configure, and monitor all McAfee Network Security Platform appliances, virtual or physical, as well as McAfee Network Threat Behavior Analysis appliances across your traditional, private, and public cloud resources from a single console. The intuitive web-based management interface handles any deployment—from single devices on up to widely distributed, mission-critical clusters. McAfee Network Security Manager can also be deployed as a virtual instance on VMware ESX servers and in AWS.

High Availability and Disaster Recovery

McAfee Network Security Manager arbitrates among controllers and determines one as the active and the other as standby. When the active controller becomes unavailable, the standby controller become active. As such, controller high availability (HA) is provided for AWS deployments, providing a failover mechanism where one controller is always active and reachable. In addition, a standby McAfee Network Security Manager provides disaster recovery for AWS environments.

The McAfee Virtual Network Security Platform provides high availability with the manager disaster recovery (MDR), controller high availability (HA), and the virtual IPS Sensor auto-scaling features. This enables McAfee Virtual Network Security Platform to work seamlessly without interruption. The MDR solution provides a secondary Manager, which takes over when the primary Manager is down. In the controller HA pair, one of the controllers is always active and reachable so that there is no downtime in the network. The auto-scaling feature for virtual IPS Sensors creates a new virtual IPS Sensor when an instance of the Sensor is down. This performs a load balancing function whenever there is an increase in network traffic.

Unified Defense Architecture

Sophisticated attacks do not respect product boundaries, taking advantage of any infrastructure gaps, especially between security products. McAfee Virtual Network Security Platform is the only IPS to integrate across multiple security products, leveraging data and workflows to plug these gaps resulting in increased return on investment and reduced total cost of ownership. Additional security product integrations include:

- **McAfee ePolicy Orchestrator® (McAfee ePO™) software:** Complete endpoint visibility for all IPS events and alerts.
- **McAfee Endpoint Intelligence Agent:** Combines network and endpoint perspective to stop data leaks.
- **McAfee Enterprise Security Manager:** Rich data sharing and IPS quarantining for IPS alerts.
- **McAfee Threat Intelligence Exchange:** Shared learning across different kinds of devices.
- **McAfee Global Threat Intelligence:** Largest and most active reputation service in the world.
- **McAfee Network Threat Behavior Analysis:** Extend visibility across the network.
- **McAfee Virtual Advanced Threat Defense**
- **McAfee Cloud Threat Detection**
- **McAfee Management for Optimized Virtual Environments (McAfee MOVE)**
- **Third-Party vulnerability scanners:** Host and risk analysis for endpoints.

Additional Features

Advanced threat prevention

- McAfee Gateway Anti-Malware emulation engine.
- PDF JavaScript emulation engine (lightweight sandbox).
- Adobe Flash behavioral analysis engine.
- Advanced evasion protection.

Botnet and malware callback protection

- Domain name servers (DNS)/domain generation algorithms (DGA) fast flux callback detection.
- DNS sinkholing.
- Heuristic bot detection.
- Multiple attack correlation.
- Command and control database.

Advanced intrusion prevention

- IP defragmentation and TCP stream reassembly.
- McAfee, user-defined, and open-source signatures.
- Host quarantine and rate limiting.
- Inspection of virtual environments.
- Denial-of-service (DoS) and DDoS prevention.
- Threshold and heuristic-based detection.
- Host-based connection limiting.
- Self-learning, profile-based detection.

McAfee Global Threat Intelligence

- File reputation.
- IP reputation.
- Geolocation-based restricted access.
- IP address-based access control.

	Sensor Type 1	Sensor Type 2	Sensor Type 3
Platform	VMware ESX 5.5/6.0/6.5 KVM/OpenStack	VMware ESX 5.5/6.0/6.5 KVM/OpenStack	VMware ESX 5.5/6.0/6.5 NSX 6.3 AWS
Virtual IPS Sensor model	**IPS-VM100**	**IPS-VM600**	**IPS-VM100-VSS**[1]
Type of virtual IPS deployment	Stand-alone	Stand-alone	Distributed
VMware NSX support	No	No	Yes
AWS support	No	No	Yes
Number of logical CPU cores[2]	3	4	3
Memory required[3]	4 GB	6 GB	5 GB
Virtual Sensor Specifications			
Maximum throughput[4]	Up to 500 Mbps	Up to 1 Gbps	Up to 500 Mbps
Concurrent connections	200,000	600,000	200,000
Connections established per second	6,000	20,000	6,000
Supported UDP flows	39,168	254,208	39,168
Number of monitoring port pairs	2	3	1[5]
Virtual interfaces (VIDS) per Sensor	32	100	32
DoS profiles	100	300	100
Management port	Yes	Yes	Yes
Response port	Yes	Yes	No
Deployment modes	Inter-VM inspection, physical-to-VM inspection, physical-to-physical inspection, SPAN port inspection		VMware NSX inline inspection

[1] For use only in VMware NSX environments as an inserted service.

[2] The VM resource requirements may change for releases. Please refer to release specific documentation.

[3] Ibid.

[4] Measured with 1518 bytes UDP packets under ideal testing conditions.

[5] Ingress and egress virtual representation. Inspection is closely tied to VMware NSX at the kernel layer.

McAfee™
Together is power.

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