McAfee Virtual Network Security Platform

Complete threat detection and intrusion prevention for cloud networks

McAfee® Virtual Network Security Platform (McAfee® vNSP) is a complete network threat detection and intrusion prevention system (IPS) built for the unique demands of private and public clouds. It quickly discovers and blocks sophisticated threats in cloud architectures with accuracy and simplicity, enabling organizations to protect workloads and restore compliance with confidence. Advanced technologies include signature-less detection, in-line emulation, and signature-based vulnerability patching. Streamlined workflows support for autoscaling, flexible integration options, and simplified licensing allow organizations to easily manage and scale their security to meet existing and future needs.

Complete Public Cloud Security

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 Amazon Web Services (AWS), Microsoft Azure, and Oracle Cloud Infrastructure (OCI)—today's leading public cloud services—delivering complete threat visibility and protection for data going through an internet gateway or server-to-server (east-west traffic).

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 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 inside private and public clouds, as well as software-defined data centers (SDDC). 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.

Key Advantages

- Complete protection for private and public clouds (AWS, Azure, and OCI)
- Inline IPS/intrusion detection system (IDS) mode of operation
- True east-west traffic protection
- Uniform policy and management workflow
- Advanced inspection technologies protect against known and unknown threats
- High availability, disaster recovery, and load balancing for performance
- Cloud license sharing for flexibility across private and public clouds
- Integrates with McAfee portfolio for device-to-cloud security
- Available at AWS Marketplace
- Available at Azure Marketplace

Connect With Us

Agility in Private Cloud

McAfee Virtual Network Security Platform can be deployed as a virtual appliance on VMware ESX server to protect virtual networks in a private cloud infrastructure. Available as an Open Virtualization Format (OVF) image, the virtual appliance can help inspect traffic between VMs on a particular ESX host, as well as across different ESX hosts and physical networks

Advanced 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 unknown 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 utilizes multiple inspection technologies, including in-line emulation of browsers, JavaScript, Adobe files, botnet, malware callback detection, behavior-based distributed denial-of-service (DDoS) detection, and protection from advanced cross-site scripting and SQL injection attacks.

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 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. McAfee also provides native support for Snort signatures to detect and protect against malware.

Flexible Cloud License Sharing

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

McAfee simplifies licensing and reduces costs through cloud license sharing, allowing organizations to share their McAfee Virtual Network Security Platform licenses across a combination of public and private cloud platforms. Cloud license sharing provides flexibility and improves security by enabling administrators to rapidly deliver east-west traffic protection and micro-segmentation to virtual workloads wherever they reside, without the hassles of complex licensing and time-consuming procurement processes.

Streamlined Workflows and Analytics

Modern threats can generate large volumes of alerts, quickly outpacing a security operator's ability to prioritize and track them. If the response is too slow, real

threats can slip by undetected. McAfee Virtual Network Security Platform includes advanced analytics and actionable workflows that correlate multiple IPS alerts into a single actionable event, enabling administrators to quickly identify relevant information. Also, integration with additional McAfee security solutions creates a truly comprehensive, connected network threat detection and mitigation platform.

Unified Policy and Management Workflow

McAfee® Network Security Manager can be deployed as a virtual instance on VMware ESX servers and in AWS/Azure/OCI environments. This helps security administrators to extend the on-premises security profile consistently across hybrid data centers as workloads shift to cloud platforms and manage them using uniform management console and workflows. McAfee Virtual Network Security Platform supports AWS Identity and Access Management (IAM), enabling administrators to easily and securely manage access to AWS services and resources based on permissions assigned to specific users and groups.

High Availability, Disaster Recovery, and Load Balancing

McAfee Virtual Network Security Platform automatically delivers uninterrupted control, protection, and performance via multiple methods. McAfee Network Security Manager provides high availability by proactively monitoring the environment. For instance, a new controller instance is launched when an active controller becomes unavailable. In addition, a standby McAfee Network Security Manager can be deployed for disaster recovery in AWS, Azure, and OCI environments.

McAfee Virtual Network Security Platform also provides high availability for IPS sensors. If a sensor becomes unavailable, the auto-scaling capability automatically creates a new virtual IPS sensor for seamless, uninterrupted protection. Also, if network traffic increases, automatic load balancing across sensors ensures that performance is optimized, and additional sensors can be deployed automatically to meet the required throughput performance.

Integrated Security

Sophisticated attacks do not respect product boundaries and will quickly take advantage of any infrastructure gaps, especially between security products. McAfee Virtual Network Security Platform is the only IPS to seamlessly integrate across multiple security products, efficiently leveraging data and workflows across solutions for superior security, protection, and an increased return on investment. Examples of McAfee security solution integration include:

- **McAfee® ePolicy Orchestrator® (McAfee ePO™) software:** Complete endpoint visibility for all IPS events and alerts
- **McAfee® Endpoint Intelligence Agent:** Combines network and endpoint perspectives 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 types 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:** Provides in-depth inspection to detect evasive threats
- **McAfee® Management for Optimized Virtual Environments (McAfee® MOVE):** An antivirus solution for virtual environments
- **Third-party vulnerability scanners:** Host and risk analysis for endpoints

Additional Features

Advanced threat prevention

- Advanced malware protection
- Native inbound SSL inspection
- Microsoft Office deep file inspection
- 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 distributed denial-of-service (DDoS) prevention
- Allow/block lists in support of Structured Threat Information eXpression (STIX)
- Threshold and heuristic-based detection
- Host-based connection limiting
- Native support for Snort signatures
- Self-learning, profile-based detection

McAfee Global Threat Intelligence

- File reputation
- IP reputation
- URL/domain reputation
- Geolocation-based restricted access
- IP address-based access control

	Sensor Type 1	Sensor Type 2
Platform	VMware ESX	AWS Azure OCI
Virtual IPS sensor model	**IPS-VM600**	**IPS-VM600-VSS**
Type of virtual IPS deployment	Stand-alone	Distributed
AWS support	No	Yes
Azure support	No	Yes
OCI support	No	Yes
Number of logical CPU	4	4
Memory required	8 GB	8 GB
Storage	40 GB	40 GB
Virtual Sensor Specifications		
Maximum throughput	Up to 1 Gbps	Up to 1 Gbps
Number of monitoring port pairs	3	1 (monitoring port, not a port pair)
Virtual interfaces (VIDS) per sensor	100	100
DoS profiles	300	300
Management port	Yes	Yes
Response port	No	No
Deployment modes	Inter-VM inspection, physical-to-VM inspection, physical-to-physical inspection, SPAN/inline port inspection	

Learn More

- Securing Your Amazon Web Services Virtual Networks
- Securing Your Microsoft Azure Virtual Networks

6220 America Center Drive
San Jose, CA 95002
888.847.8766
www.mcafee.com