VM-SERIES FOR VMWARE

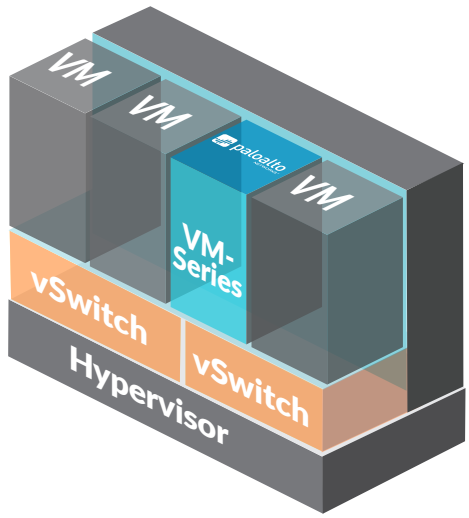
Virtualization technology from VMware is fueling a significant change in today's modern data centers, resulting in architectures that are commonly a mix of private, public or hybrid cloud computing environments. The benefits of cloud computing are well-known and significant. However, so too are the security challenges, exemplified by the many recent high-profile data breaches. Whether stored in a physical data center or in a public, private or hybrid cloud, your data is the cybercriminal's target.

The VM-Series for VMware® supports VMware NSX®, ESXi™ stand-alone and vCloud® Air™, allowing you to deploy next-generation firewall security and advanced threat prevention within your VMware-based private, public and hybrid cloud computing environments.

- Identify and control applications within your virtualized environments; limit access based on users; prevent known and unknown threats
- Isolate and segment mission-critical applications and data using Zero Trust principles
- Streamline policy deployment so that security keeps pace with the rate of change within your private, public or hybrid cloud.

Organizations are expanding their virtualization and cloud initiatives in a variety of ways with security remaining top of mind. Increased use dictates an effort for more-streamlined security workflows and an eye towards cloud-centric architectures that are scalable and resilient.

- More workloads are now virtualized on-premise (private cloud) than ever before, and the use of the public cloud is increasing dramatically, leading to multi-vendor (private and public) environments, along with increased demands on capacities. Additional examples include security deployed as an NFV component for a more cost-effective alternative to securing branch offices and data center/private cloud workloads, as well as an uptick in virtualization to address demands for (more) complete tenant isolation in multi-tenancy environments.
- Cloud security automation workflows have streamlined deployments, but they can still be complex and involve many carefully orchestrated steps.
- Security, traditionally viewed as a bottleneck that slows deployment, must more readily support the move toward cloud-centric architectures.



Securing your VMware-based cloud introduces a range of challenges, including a lack of application visibility, inconsistent security functionality, and difficulty keeping pace with the rate of change commonly found in cloud computing environments. To be successful, organizations need a cloud security solution that:

- Has the ability to identify and control applications within the cloud, based on the identity, not the port and protocols it may use.
- Stops malware from gaining access to and moving laterally (east-west) within the cloud.
- Determines who should be allowed to use the applications and grant access based on need and their credentials.
- Simplifies management and minimizes the security policy lag as VMs are added, removed or moved within the cloud environment.

The Palo Alto Networks VM-Series for VMware allows you to protect your data that resides in NSX, ESXi, and vCloud Air environments from cyberthreats with our next-generation firewall security and advanced threat prevention features. Panorama™ network security management, combined with native automation features, allows you to streamline policy management in a manner that minimizes the policy time gap that may occur as virtual machines are added, moved or removed.

Virtualized Next-Generation Security at High Performance and Scale

The VM-Series virtualized next-generation firewall has been optimized and expanded to deliver App-ID™ enabled throughput that ranges from 200 Mbps to 16 Gbps across five models, both of which are industry-leading metrics. The VM-Series models include:

- The VM-50 is optimized to consume minimal resources and support CPU oversubscription, yet deliver up to 200 Mbps of App-ID enabled firewall performance, for customer scenarios that range from virtual branch office/customer premise equipment (CPE) to high-density, multi-tenancy environments.
- The VM-100 and VM-300 have been optimized to deliver performance at 2 Gbps and 4 Gbps of App-ID enabled firewall performance for hybrid cloud, segmentation, and internet gateway use cases.
- The VM-500 and VM-700 deliver an industry-leading 8 Gbps to 16 Gbps of App-ID enabled firewall performance, respectively, and can be deployed as NFV security components in fully virtualized data center and service provider environments.

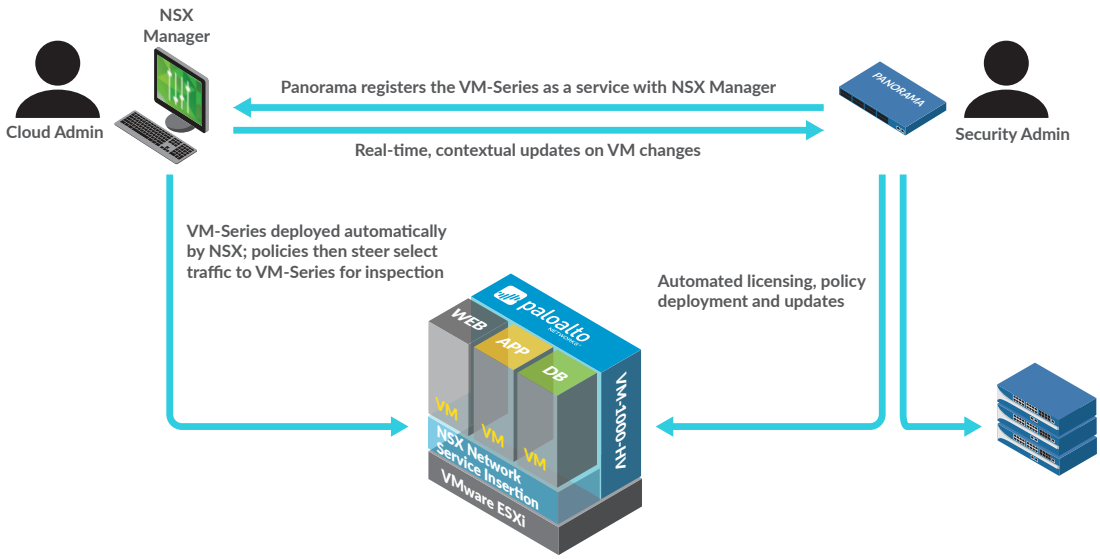
Intel® Data Plane Development Kit (DPDK) has been integrated with the VM-Series for VMware for enhanced packet-processing performance on x86 infrastructure. Network I/O options, such as PCI passthrough and single-root I/O virtualization (SR-IOV), are supported for enhanced performance.

Applying Next-Generation Security to Virtualized Environments

The VM-Series virtualized firewall is based on the same full-stack traffic classification engine that can be found in our physical form factor firewalls. The VM-Series natively classifies all traffic, inclusive of applications, threats and content and then ties that traffic to the user. The application, content and user – the elements that run your business – are then used as the basis of your virtualized security policies, resulting in an improved security posture and a reduction in incident response time.

Isolate Mission-Critical applications and Data Using Zero Trust Principles

Security best practices dictate that your mission-critical applications and data should be isolated in secure segments using Zero Trust (never trust, always verify) principles at each segmentation point. The VM-Series can be deployed throughout your virtualized environment, residing as a gateway within your virtual network or in between the VMs running in different tiers, thereby protecting east-west traffic, by exerting control based on application and user identity.



Block Lateral Movement of Cyberthreats

Today's cyberthreats will commonly compromise an individual workstation or user and then move across the network, looking for a target. Within your virtual network, cyberthreats will move laterally and rapidly from VM to VM, in an east-west manner, placing your mission-critical applications and data at risk. Exerting application-level control using Zero Trust principles in between VMs will reduce the threat footprint while applying policies to block both known and unknown threats

Automated, Transparent Deployment and Provisioning

A rich set of APIs can be used to integrate with external orchestration and management tools, collecting information related to workload changes, which can then be used to dynamically drive policy updates via VM Monitoring and Dynamic Address Groups.

- **RESTful APIs:** A flexible REST-based API allows you to integrate with third-party or custom cloud orchestration solutions. This enables the VM-Series to be deployed and configured in lockstep with virtualized workloads.
- **VM Monitoring:** Security policies must be able to monitor and keep up with changes in virtualization environments, including VM attributes and the addition or removal of VMs. Virtual machine monitoring (VM Monitoring) automatically polls your virtualization environments, such as vCenter for virtual machine inventory and changes, collecting this data in the form of tags that can then be used in Dynamic Address Groups to keep policies up to date.
- **Dynamic Address Groups:** As your virtual machines change functions or move from server to server, building security policies based on static data, such as IP address, delivers limited value and can contain outdated information. Dynamic Address Groups allow you to create policies using tags (from VM monitoring) as identifiers for virtual machines instead of a static object definition. Multiple tags representing virtual machine attributes, such as IP address and operating system, can be resolved within a Dynamic Address Group, allowing you to easily apply policies to virtual machines as they are created or travel across the network without administrative intervention.

Centrally Manage Virtualized and Physical Form Factor Firewalls

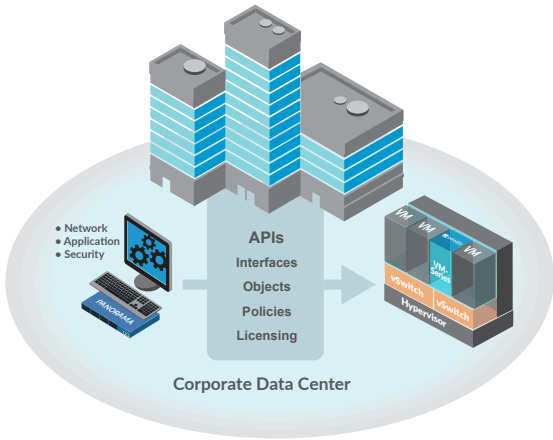
Panorama allows you to manage your VM-Series deployments along with your physical security appliances, thereby ensuring policy consistency and cohesiveness. Rich centralized logging and reporting capabilities provide visibility into virtualized applications, users and content.

Deployment Flexibility

The VM-Series for VMware supports NSX, ESXi and vCloud Air environments.

VM-Series for VMware NSX

The VM-Series for NSX is a tightly integrated solution that ties together the VM-Series virtualized next-generation



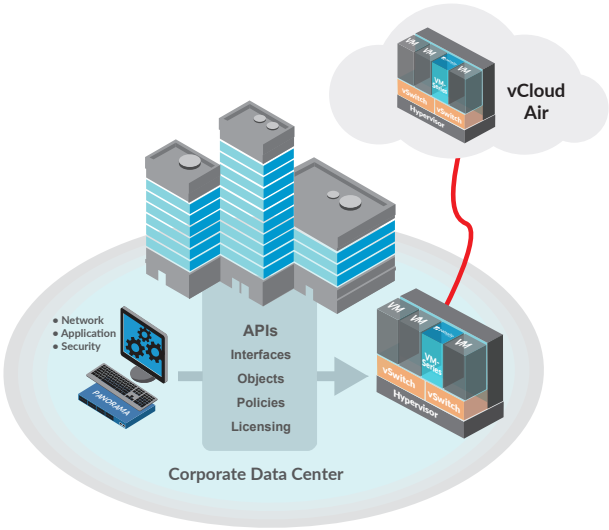
firewall, Panorama for centralized management, and VMware NSX to deliver on the promise of a software-defined data center. As new virtual workloads are deployed, NSX Manager simultaneously installs a VM-Series next-generation firewall on each ESXi server. Once deployed on the ESXi server, safe application enablement policies that identify, control, and protect your virtualized applications and data can be deployed to each VM-Series virtual appliance in an automated manner by Panorama. NSX will then begin steering select application traffic to the VM-Series for more granular application-level security. As new workloads are added, moved or removed, NSX feeds those attribute changes to Panorama where they are translated into dynamic security policy updates to the virtual and perimeter gateway firewalls. The VM-Series for NSX supports virtual wire network interface mode, which requires minimal network configuration and simplifies network integration. Please see the VM-Series for VMware NSX datasheet for more information on this integration.

VM-Series for ESXi (Standalone)

The VM-Series on ESXi servers is ideal for networks where the virtual form factor may simplify deployment and provide more flexibility. Common deployment scenarios include:

- Private or public cloud computing environments where virtualization is prevalent.
- Environments where physical space is restricted and at a premium.
- Remote locations where shipping hardware is not practical.

The VM-Series for ESXi allows you to deploy safe application enablement policies that identify, control and protect your virtualized applications and data. Panorama and a rich set of APIs can be used to integrate with external orchestration and management tools to collect information related to workload changes, which can then be used to dynamically drive policy updates via Dynamic Address Groups and VM Monitoring. A range of interface types, including L2, L3 and virtual wire, allow you to deploy the VM-Series for ESXi in a different interface mode for each virtualized server, depending on your needs.



VM-Series for vCloud Air

The VM-Series for vCloud Air allows you to protect your VMware-based public cloud with the same safe application enablement policies that are used to protect your ESXi-based private cloud. Common use cases include:

Perimeter gateway: In this use case, the VM-Series is deployed as your gateway firewall, securing your vCloud Air environment based on application, regardless of port and protocol, while preventing known and unknown threats and controlling access based on user identity.

- **Hybrid cloud security:** In this use case, the VM-Series is configured to establish a secure, standards-based IPsec connection between your private, VMware-based cloud and your vCloud Air-based public cloud. Access to the vCloud Air environment can then be controlled based on application and user identity.

Panorama and a rich set of APIs can be used to integrate with external orchestration and management tools to collect information related to workload changes, which can then be used to dynamically drive policy updates via Dynamic Address Groups and VM-Monitoring. A range of interface types, including L2, L3 and virtual wire, allow you to deploy the VM-Series for ESXi in a different interface mode for each virtualized server, depending on your needs.

Performance and Capacities Summary

The security performance table listed below is tested under controlled lab conditions using PAN-OS® 8.0. In virtualized and cloud environments, many factors, such as the type of CPU, hypervisor version, number of cores assigned, memory, and network I/O options, can impact your performance. We recommend additional testing within your environment to ensure your performance and capacity requirements are met.

Performance and Capacities	VM-50 (0.4 core)	VM-100/ VM200 (2 Cores)	VM-300/ VM-1000-HV (4 Cores)	VM-500 (8 Cores)	VM-700 (16 cores)
With Single Root I/O Virtualization (SR-IOV)/PCI Passthrough of I/O enabled					
Firewall throughput (App-ID enabled)	200 Mbps	2 Gbps	4 Gbps	8 Gbps	16 Gbps
Threat prevention throughput	100 Mbps	1 Gbps	2 Gbps	4 Gbps	8 Gbps
IPsec VPN throughput*	In process	In process	In process	In process	In process
With VMware Distributed Virtual Switch (VMXNET3)					
Firewall throughput (App-ID enabled)	100 Mbps	1 Gbps	2 Gbps	4 Gbps	8 Gbps
Threat prevention throughput	50 Mbps	500 Mbps	1 Gbps	2 Gbps	4 Gbps
IPsec VPN throughput*	In process	In process	In process	In process	In process
Capacities					
New sessions per second	1,000	8,000	15,000	30,000	60,000
Max sessions	50,000	250,000	800,000	2,000,000	10,000,000

*IPsec VPN throughput data will be published upon completion of the test suite

The performance and capacities results shown above were tested under the following conditions:

- Firewall and IPsec VPN throughput are measured with App-ID and User-ID features enabled.
- Threat prevention throughput is measured with App-ID, User-ID, IPS, antivirus and anti-spyware features enabled.
- Throughput is measured with 64KB HTTP transactions.
- Connections per second is measured with 4KB HTTP transactions.

VM-Series Specifications and Features

The tables below list all supported specifications, resource requirements and networking features on the VM-Series for VMware.

Virtualization Specifications	
Image formats supported	OVA
Hypervisors supported	VMware ESXi 5.1, 5.5 and 6.0 VMware NSX Manager 6.0, 6.1 and 6.2
Network I/O options	• VMware paravirtual drivers (vmxnet3, e1000) • PCI pass-through • Single-root I/O Virtualization (SR-IOV)

System Requirements	VM-50 (0.4 Core)	VM-100/ VM-200 (2 Cores)	VM-300/ VM-1000-HV (4 Cores)	VM-500 (8 Cores)	VM-700 (16 Cores)
vCPU configurations supported	2[1]	2	2,4	2,4 and 8	2,4,8 and 16
Memory (minimum)	4.5GB	6.5GB	9GB	16GB	56GB
Disk drive capacity (min/max)	32GB[2]/2TB	60GB/2TB	60GB/2TB	60GB/2TB	60GB/2TB

1. CPU oversubscription is supported with up to 5 instances running on a 2 CPU core configuration
2. 60GB drive capacity is needed on initial boot. VM-Series instance will use 32GB drive capacity after license activation.

Networking Features	
Interface Modes:	**VLANs**

• L2, L3, tap, virtual wire (transparent mode): VM-Series for ESXi
• **L3:** vCloud Air
• **Virtual wire (transparent mode):** VM-Series for NSX
	• **802.1q VLAN tags per device/per interface:** 4,094/4,094
	• **Max interfaces:**
	  • 4096 (VM-500/VM-700)
	  • 2048 (VM-100/VM-300)
	  • 512 (VM-50)

Routing	**Network Address Translation (NAT)**
• **Modes:** OSPF, RIP, BGP, Static • Policy-based forwarding • **Multicast:** PIM-SM, PIM-SSM, IGMP v1, v2, and v3	• **NAT modes (IPv4):** static IP, dynamic IP, dynamic IP and port (port address translation) • NAT64 • **Additional NAT features**: dynamic IP reservation, dynamic IP and port oversubscription
High Availability	**IPv6**
• **Modes**: active/passive with session synchronization • **Failure detection:** path monitoring, interface monitoring	• L2, L3, tap, virtual wire (transparent mode) • Features: App-ID™, User-ID™, Content-ID™, WildFire™ and SSL decryption

To view additional information on the VM-Series security features and associated capacities, please visit www.paloaltonetworks.com/products.

4401 Great America Parkway
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

vm-series-for-vmware-ds-020617