Cloud-first development initiatives and an insatiable appetite for compute and storage resources are transforming today’s data centers into hybrid clouds. Palo Alto Networks® VM-Series on Azure® securely enables this transformation with a full suite of next-generation firewall and advanced threat prevention features.

<table>
<thead>
<tr>
<th>VM-Series on Azure Use Cases</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hybrid Cloud</td>
</tr>
<tr>
<td>• Securely extend your application development and testing environment onto Azure across a site-to-site IPsec VPN or Express Route.</td>
</tr>
<tr>
<td>Segmentation Gateway</td>
</tr>
<tr>
<td>• Maintain separation of confidential data from other traffic for security and compliance purposes by controlling applications across VNETs and subnets while blocking threats.</td>
</tr>
<tr>
<td>Internet Gateway</td>
</tr>
<tr>
<td>• Protect web-facing applications from advanced threats while securely enabling direct access to web-based developer tools and resources.</td>
</tr>
<tr>
<td>GlobalProtect</td>
</tr>
<tr>
<td>• Extend perimeter firewall and threat prevention policies to remote users and mobile devices with GlobalProtect.</td>
</tr>
</tbody>
</table>

Security Challenges in the Public Cloud
Organizations worldwide are expanding their use of Azure® at an unprecedented pace. However, security, workflow automation and how to build scalable, resilient cloud-centric architectures are key challenges that must be addressed.

The VM-Series on Azure solves these challenges, enabling you to:
- Protect your Azure workloads through unmatched application visibility, control and advanced threat prevention.
- Simplify management and automate security policy updates as your workloads change.
- Build secure, cloud-centric architectures that are scalable and highly available.

The Palo Alto Networks VM-Series allows new cloud customers to protect their workloads with next-generation security features that deliver superior visibility, control and threat prevention at the application level when compared to other cloud-oriented security solutions. Existing customers will reap the benefits of a security feature set that mirrors those protecting their physical networks and delivers a consistent security posture from the network to the cloud.
Are Native Security Features Sufficient?
As part of their security offering, Azure provides users with some basic security features, such as Network Security Groups. These features will help you protect your Azure deployment; however, they look at traffic from a ports-only perspective and cannot identify and control it at the application level. This only provides a base level of security to reduce your attack surface; it does not protect against external or lateral threats. As Azure becomes an extension of your data center, advanced security features such as those available from a next-generation firewall should become a requirement.

VM-Series on Azure
The VM-Series on Azure enables you to securely implement a cloud-first methodology while transforming your data center to a hybrid architecture that combines the scalability and agility of the Azure public cloud with your on-premise resources. This allows you to move your applications and data to Azure while maintaining a security posture that is consistent with the one you may have established on your physical network.

The VM-Series on Azure natively analyzes all traffic in a single pass to determine the application, content and user identity. The application, content and user are used as core elements of your security policy and for visibility, reporting and incident investigation.

Application Visibility for Better Security Decisions
The VM-Series on Azure provides you with application visibility across all ports, which means you have far more relevant information about your Azure environment, which, in turn, means you can make more informed security policy decisions.

Exert Greater Control With Whitelisting Policies
With the VM-Series on Azure, you can extend your firewall access control policies to the application level, forcing them to operate on specific ports, while leveraging the "deny all else" premise that a firewall is based on to block all others. The level of control becomes critically important as you deploy more of your data center assets in the public cloud.

User-Based Policies Improve Security Posture
Integration with a wide range of user repositories, such as Microsoft Active Directory®, LDAP and Microsoft Exchange, introduces the user identity as a policy element, complementing application whitelisting with an added access control component. User-based policies mean you can grant access to critical applications and data based on user credentials and respective need. For example, the development group has full access to the development VNET, while only IT admins have RDP/SSH access to the production VNET. When deployed in conjunction with GlobalProtect™ network security for endpoints, the VM-Series on Azure enables you to extend your corporate security policies to mobile devices and users regardless of their location.

Prevent Advanced Attacks at the Application Level
Attacks, much like many applications, are capable of using any port, rendering traditional prevention mechanisms ineffective. The VM-Series on Azure allows you to use Threat Prevention and the WildFire™ cloud-based threat analysis service to apply application-specific threat prevention policies that block exploits, malware and previously unknown threats from infecting your cloud.

Segmentation for Data Security and Compliance
Today’s cyberthreats commonly compromise an individual workstation or user and then move laterally across your physical or virtualized network, placing your mission-critical applications and data at risk. Using whitelisting policies allows you to segment applications communicating across different subnets and between VNETs for regulatory compliance. Enabling Threat Prevention and WildFire to complement your segmentation policies will block both known and unknown threats and stop them from moving laterally from workload to workload.

Centralized Management Delivers Policy Consistency
Panorama™ network security management enables you to manage your VM-Series deployments across multiple cloud 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.

Automation Features to Support Cloud-First Initiatives
The VM-Series on Azure includes management features that enable you to integrate security into your cloud-first development projects. Bootstrapping can be used to automatically provision a firewall with a working configuration, complete with licenses and subscriptions, and then auto-register itself with Panorama. To automate policy updates as workloads change, a fully documented XML API and Dynamic Address Groups allow the VM-Series to consume external data in the form of tags that can drive policy updates dynamically. The result is that new applications and next-generation security can be deployed simultaneously in an automated manner.
VM-Series on Azure Scalability and Availability

The VM-Series on Azure enables you to deploy a managed scale-out solution for your inbound web application workload traffic using a load balancer “sandwich.” The Application Gateway acts as the external load balancer, front-ending the web application, and serving as an internet gateway for the entire service. The Application Gateway provides application delivery controller as a service and includes Layer 7 load balancing for HTTP and HTTPS, along with features such as SSL offload and content-based routing. The Application Gateway distributes traffic across multiple VM-Series firewalls deployed to protect Azure deployments from known and unknown threats. After security inspection by the VM-Series firewalls, traffic is sent to the Azure Load Balancer acting as the internal load balancer, which distributes traffic to your web applications.

The VM-Series on Azure scalability and availability solution provides the following benefits:

- **Scalability:** VM-Series firewalls can be added or removed from the Application Gateway load balancing pool as demand for the web application grows or shrinks. Similarly, the front-end web tier of the application can be scaled out or scaled in behind the Azure Load Balancer.

- **Resiliency and High Availability:** Support for Azure availability sets provides protection against planned and unplanned maintenance of the Azure infrastructure. This addresses the need for resiliency and availability by minimizing or eliminating the negative impact that Azure infrastructure maintenance or system faults may have on your business by distributing the workloads across different hosts.

- **Flexible Architecture:** You can also enable HTTPS load balancing on the Application Gateway for applications that use secure connections and enable SSL offload on the Application Gateway. Application Gateway also allows using separate backend pools of VM-Series firewalls based on URL-based content routing.

Deploying business critical applications in Azure dictates the need for a security solution that scales in a managed manner and is resilient. Utilizing cloud services supported and maintained by Microsoft Azure, combined with the VM-Series, allows you to build secure, cloud-centric architectures.
VM-Series on Azure Use Cases
The VM-Series can be deployed on Azure to address several different use cases.

Hybrid Cloud: Securely Enable App Development and Testing
Securely migrate application development and testing onto Azure through a hybrid deployment that integrates your existing development environment with Azure via a secure connection. This approach allows your application development and testing team to get started while maintaining a strong security posture. When deployed on Azure, the VM-Series can act as an IPsec VPN termination point to enable the secure communications to and from Azure. Application control and threat prevention policies can be layered atop the IPsec VPN tunnel or Azure Express Route as added security elements.

Segmentation Gateway: Separation for Security and Compliance
High-profile breaches have shown that cybercriminals are adept at hiding in plain sight, bypassing perimeter controls and moving at will across networks – both physical and virtualized. An Azure VNET provides an isolation and security boundary for your workloads. The VM-Series can augment that separation through application-level segmentation policies to control traffic between the VNETs and across subnets. With application-level policies, you have greater control over application traffic moving laterally, and you can apply threat prevention policies to block their movement as well.

Internet Gateway: Protect Production Workloads
As your Azure deployment expands to include public facing workloads, you can use the VM-Series on Azure as an internet gateway to protect web-facing applications from known and unknown threats. Additionally, you can enable direct access to web-based developer resources, tools and software updates, thereby minimizing the traffic that flows back to corporate and out to the web.

GlobalProtect: Extend Security to Users and Devices
GlobalProtect network security for endpoints will enable you to extend perimeter security to your remote users and mobile devices regardless of their location. GlobalProtect establishes a secure connection to protect the user from internet threats and enforces application-based access control policies. Whether the need is for access to the internet, data center or SaaS applications, the user will enjoy the full protection provided by the platform.

VM-Series on Azure for Government
The VM-Series can be deployed on Azure for Government to support any of the uses cases described previously. Learn more about Azure for Government.
Performance and Capacities

Many factors such as the Azure Virtual Machine size, the maximum packets per second supported, and the number of cores used, can impact VM-Series performance. The performance and capacities listed below have been generated under controlled lab conditions using recommended Azure Virtual Machine size and the following test conditions:

- Firewall throughput and IPsec VPN are measured with App-ID™ and User-ID™ features enabled, utilizing 64K HTTP transactions.
- Threat prevention throughput is measured with App-ID, User-ID, IPS, antivirus and anti-spyware features enabled, utilizing 64K HTTP transactions.
- IPsec VPN performance is tested between two VM-Series in the same region. Performance will depend on Azure VM size and network topology, that is, whether connecting on-premise hardware to VM-Series on Azure; from VM-Series on an Azure VNET to an Azure VPN Gateway in another VNET; or VM-Series to VM-Series between regions.
- Connections per second is measured with 0K HTTP transactions.

We recommend additional testing within your environment to ensure your performance and capacity requirements are met. For a complete listing of all VM-Series features and capacities, please visit www.paloaltonetworks.com/comparefirewalls.

<table>
<thead>
<tr>
<th>Model</th>
<th>VM-50 (0.4 Cores)</th>
<th>VM-100/ VM-200 (2 Cores)</th>
<th>VM-300/ VM-1000-HV (4 Cores)</th>
<th>VM-500 (8 Cores)</th>
<th>VM-700 (16 Cores)</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM size used</td>
<td>D3_v2</td>
<td>D3_v2</td>
<td>D4_v2</td>
<td>D5_v2</td>
<td></td>
</tr>
<tr>
<td>Firewall throughput (App-ID enabled)</td>
<td>N/A</td>
<td>1 Gbps</td>
<td>1 Gbps</td>
<td>1 Gbps</td>
<td>1 Gbps</td>
</tr>
<tr>
<td>Threat Prevention throughput</td>
<td>N/A</td>
<td>1 Gbps</td>
<td>1 Gbps</td>
<td>1 Gbps</td>
<td>1 Gbps</td>
</tr>
<tr>
<td>IPsec VPN throughput</td>
<td>N/A</td>
<td>700 Mbps</td>
<td>900 Mbps</td>
<td>900 Mbps</td>
<td>1 Gbps</td>
</tr>
<tr>
<td>New sessions per second</td>
<td>N/A</td>
<td>8K</td>
<td>11K</td>
<td>11K</td>
<td>11K</td>
</tr>
<tr>
<td>Max sessions</td>
<td>N/A</td>
<td>250K</td>
<td>800K</td>
<td>2M</td>
<td>10M</td>
</tr>
</tbody>
</table>

**System Requirements**

<table>
<thead>
<tr>
<th>Cores supported (Min/Max)</th>
<th>N/A</th>
<th>0.4/2</th>
<th>2/4</th>
<th>2/8</th>
<th>2/16</th>
</tr>
</thead>
<tbody>
<tr>
<td>Memory (Minimum)</td>
<td>N/A</td>
<td>6.5GB</td>
<td>9GB</td>
<td>16GB</td>
<td>56GB</td>
</tr>
<tr>
<td>Disk drive capacity (Minimum)</td>
<td>N/A</td>
<td>60GB</td>
<td>60GB</td>
<td>60GB</td>
<td>60GB</td>
</tr>
<tr>
<td>Azure VM sizes supported (Only standard Azure VM sizes are supported)</td>
<td>N/A</td>
<td>D3_v2*, D3</td>
<td>D3_v2*, D3</td>
<td>D4_v2*, D4, A4</td>
<td>D5_v2*, D55_v2</td>
</tr>
<tr>
<td>Licensing options</td>
<td>N/A</td>
<td>BYOL only</td>
<td>BYOL or Marketplace</td>
<td>BYOL only</td>
<td>BYOL only</td>
</tr>
</tbody>
</table>

* Refers to recommended VM size based on CPU cores, memory and Azure prices for VMs.
N/A: The VM-50 is not available on Azure.
Flexible Licensing Options

The VM-Series on Azure supports several licensing options including consumption-based licensing via the Azure Marketplace, bring-your-own-license and the VM-Series Enterprise Licensing Agreement (VM-Series ELA).

- **Consumption-based licensing**: Use your Azure Management Console to purchase and deploy VM-Series hourly subscription bundles directly from the Azure Marketplace.
  
  **Bundle 1 contents**: VM-300 firewall license, Threat Prevention (inclusive of IPS, AV, malware prevention) and Premium Support (written and spoken English only).
  
  **Bundle 2 contents**: VM-300 firewall license, Threat Prevention (inclusive of IPS, AV, malware prevention), WildFire, URL Filtering and GlobalProtect subscriptions and Premium Support (written and spoken English only).

- **Bring-your-own-license**: Any one of the VM-Series models, along with the associated subscriptions and support, are purchased via normal Palo Alto Networks channels and then deployed via a license authorization code through your Azure Management Console.

- **VM-Series Enterprise Licensing Agreement**: Allows you to forecast your VM-Series firewall consumption over a 1- or 3-year period and purchase a VM-Series ELA based on that projected usage. Included in each VM-Series ELA is a VM-Series firewall license, subscriptions for Threat Prevention, URL Filtering, WildFire, GlobalProtect Gateway, unlimited Panorama Virtual Machine licenses and Support. The VM-Series ELA provides you with a single license authorization code across all of virtualization environments supported by the VM-Series and is ideally suited for customers with large-scale, expanding virtualized environments who want the ability to deploy the VM-Series next generation firewalls and associated subscriptions wherever security needs dictate. The VM-Series ELA simplifies the licensing process and provides a more predictable cost structure by establishing a single start and end date for all VM-Series licenses and subscriptions.