STRATA™
BY PALO ALTO NETWORKS

VM-Series on Oracle Cloud

Palo Alto Networks VM-Series Virtual Next-Generation Firewalls protect your workloads with security features that allow you to confidently, quickly migrate your business-critical applications to the cloud. Templates and third-party tools allow you to embed the VM-Series in your application development lifecycle to prevent data loss and business disruption.

VM-Series on Oracle Cloud

- Complements native Oracle Cloud security with deep visibility, granular control, and segmentation of applications.
- Prevents threats and data loss within allowed application flows.
- Enables policies to be updated at the speed of the cloud.
- Ensures consistent policy enforcement with centralized management.

Oracle Cloud® enables you to rapidly move your database and high-performance computing applications to global cloud infrastructure. However, risks of data loss and business disruption potentially slow these initiatives. The VM-Series on Oracle Cloud enables you to:

- Protect workloads deployed on Oracle Cloud through unmatched visibility and precise control of applications.
- Prevent threats from moving laterally between workloads and stop data exfiltration.
- Eliminate security-induced development bottlenecks with automation and centralized management.

Native Oracle Cloud Security vs. VM-Series

Public cloud security posture best practices dictate that you should understand your threat exposure through application visibility, use policies to reduce your attack surface area, and prevent threats and data exfiltration within allowed traffic. Native Oracle Cloud security lets you establish baseline protection and control, but today's attackers are adept at hiding in plain sight, bypassing these controls. The VM-Series complements this native security by reducing your attack surface through enabling applications, blocking threats, and stopping data exfiltration.

VM-Series on Oracle Cloud

The VM-Series allows you to embrace a prevention-based approach to protecting your applications and data on Oracle Cloud:

- **Complete visibility improves security decisions.** Understanding the applications in use on your network, including those that may be encrypted, helps you make informed security policy decisions.
- **Segmentation and application whitelisting aid data security and compliance.** Enforcing a positive security model through application whitelisting reduces your attack surface. Whitelisting policies also let you segment applications that communicate across subnets and between virtual cloud networks (VCNs) to stop lateral threat movement and meet compliance requirements.
- **User-based policies improve security posture.** Integration with on-premises user repositories, such as Microsoft Exchange, Active Directory®, and LDAP, lets you grant access to applications and data based on user credentials and needs. For example, your developer group can have full access to the developer VCN while only IT administrators have RDP/SSH access to the production VCN. In conjunction with Palo Alto Networks GlobalProtect™ network security for endpoints, the VM-Series on Oracle Cloud can extend your corporate security policies to mobile devices and users wherever they are.
- **Applications and data are protected from known and unknown threats.** Attacks, like many applications, can use any port, rendering traditional prevention mechanisms ineffective. Threat Prevention and DNS Security, along with Palo Alto Networks WildFire® malware prevention service, will serve as segmentation policy elements to protect you against exploits, malware, and previously unknown threats from both inbound and lateral movement perspectives.
- **Multiple defenses block data exfiltration and unauthorized file transfers.** A combination of application enablement and Threat Prevention features can prevent data exfiltration. File transfers can be controlled by looking inside files, not only at file extensions, to determine whether transfer actions should be allowed. Command and control, associated data theft, and executable files found in drive-by downloads or secondary payloads can also be blocked. Data filtering features can detect and control the flow of confidential data patterns, such as credit card and Social Security numbers, in addition to custom patterns.

Centralized Management for Policy Consistency

Panorama™ network security management provides a single pane of glass for your VM-Series firewalls across multiple cloud deployments alongside your physical appliances, ensuring consistent and cohesive policy. Rich, centralized logging and reporting capabilities provide deep visibility into virtualized applications, users, and content.

Automation to Support Developer Workflows

The VM-Series on Oracle Cloud includes management and automation features that enable you to embed security in your application development workflows:

- Bootstrapping allows you to create a working VM-Series configuration, complete with licenses and subscriptions, that can be deployed in an automated, scalable manner.
- A fully documented API, Dynamic Address Groups, and External Dynamic Lists allow you to automate VM-Series configuration changes and consume external data to dynamically drive security policy updates.
- Action-Oriented Log Forwarding lets you drive actions based on observed incidents in the logs.

Automating Deployments with Terraform and Ansible

If your organization uses multiple public and private cloud platforms, or you want to embed VM-Series deployments in your application development processes, you can deploy and configure the VM-Series using third-party toolsets, such as Terraform® and Ansible®. The combination of these tools and VM-Series automation features enables you to deploy and configure heterogeneous environments at scale with great agility.

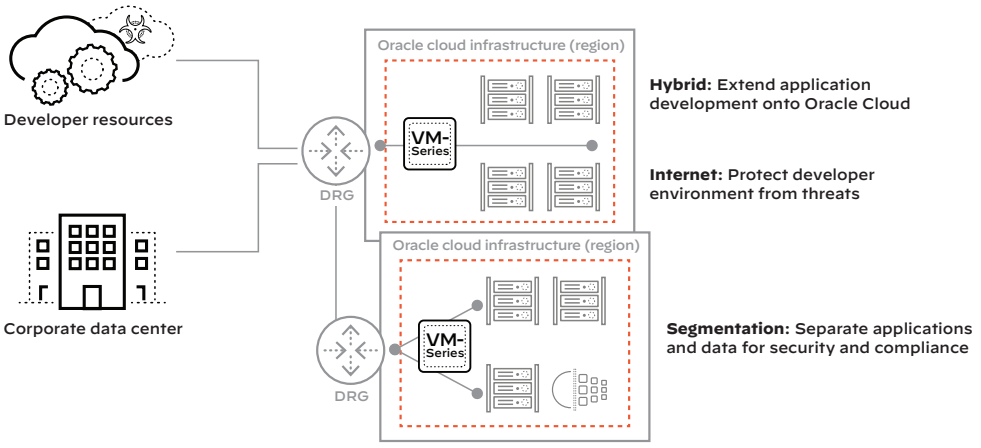

Figure 1: VM-Series on Oracle Cloud use cases

VM-Series on Oracle Cloud Use Cases

The VM-Series can be deployed on Oracle Cloud to address several different use cases.

Hybrid Cloud: Securely Enable App Dev and Test

Securely migrate application development and testing to Oracle Cloud through a hybrid deployment that integrates your existing development environment with Oracle Cloud via a secure connection. This allows your development and testing teams to get started while maintaining a strong security posture. Deployed on Oracle Cloud, the VM-Series can act as an IPsec virtual private network (VPN) termination point to enable secure communications to and from Oracle Cloud.

Internet Gateway: Protect Production Workloads

As your Oracle Cloud deployment expands to include public-facing workloads, you can use the VM-Series 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.

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 physical or virtualized networks. An Oracle Cloud VCN 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 VCNs 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. If traffic is flowing between VCNs in different regions across the internet, you can enable encryption for added protection.

Licensing and Deployment

The VM-Series on Oracle Cloud supports a bring-your-own-license (BYOL) model via Oracle Cloud Marketplace. We also offer a VM-Series enterprise license agreement (ELA).

BYOL

You can purchase your VM-Series license Basic, Bundle 1, or Bundle 2 through normal Palo Alto Networks channels, and then deploy the VM-Series via your Oracle Cloud Management Console using the license authorization code you received.

VM-Series ELA

For large-scale and/or multi-cloud deployments or across multiple virtualization environments, the VM-Series ELA allows you to forecast, and purchase upfront, VM-Series firewalls to be deployed over a one- or three-year period. The VM-Series ELA gives you a single license authorization code to use for the life of the term, providing predictable security spend and simplifying the licensing process with a single start and end date for all VM-Series licenses and subscriptions. Each VM-Series ELA includes a VM-Series firewall, subscriptions for Threat Prevention, DNS Security, WildFire, and GlobalProtect Gateway, plus unlimited Panorama virtual machine licenses and Premium Support (written and spoken English only).

Performance and Capacities

For a complete listing of all VM-Series features and capacities, please visit paloaltonetworks.com/comparefirewalls.

Please refer to the latest information on VM-Series performance on Oracle instances here.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

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

www.paloaltonetworks.com