paloalto NETWORKS

Securing Multi-Cloud Environments with VM-Series Virtual Firewalls

Cloud-agnostic network security boosts application threat prevention

Security in the Public Cloud

The journey to the cloud is not optional. Enterprises that hesitate or fail to execute are likely to be left behind as their competitors take advantage of the opportunities. Cloud delivers tangible business benefits, such as consumption-based IT spending, speed, agility, and improved user experience—all essential to survive and thrive in today's dynamic marketplace.

At the same time, cloud has challenges that include a lack of visibility, increased attack surface, and divided security responsibility. These challenges need not be obstacles, though. Your business can not only overcome them but even turn them into competitive advantages. This white paper shows how Palo Alto Networks VM-Series Virtual Next-Generation Firewalls can help your organization navigate the cloud journey.

The Multi-Cloud Explosion Can Add Cost and Complexity

In the enterprise space, multi-cloud deployments are now the norm. In a recent survey of public cloud users, 81% of respondents said they are working with two or more providers. This heterogeneous mix of clouds puts pressure on security architects to develop effective cybersecurity and compliance strategies.

They do not have to do it all by themselves. The five large cloud service providers (CSPs)—Amazon Web Services (AWS®), Microsoft Azure®, Google Cloud Platform (GCP®), Oracle Cloud®, and Alibaba Cloud—all provide their customers with a basic level of native security for their infrastructures. However, the responsibility for securing applications, data, runtimes, middleware, and operating systems in the cloud against network-borne threats falls to the user, not the CSP.

In a multi-cloud environment, multiple security solutions can create a complex, rigid system that leads to gaps in the security posture. This approach is also labor-intensive because network security teams must master multiple tools and policy models—a recipe for human error and lower productivity.

XaaS Shared Security

This white paper is primarily concerned with infrastructure as a service (IaaS); however, most organizations use a mix of XaaS cloud services, each of which has its own shared security model, as shown in figure 1.

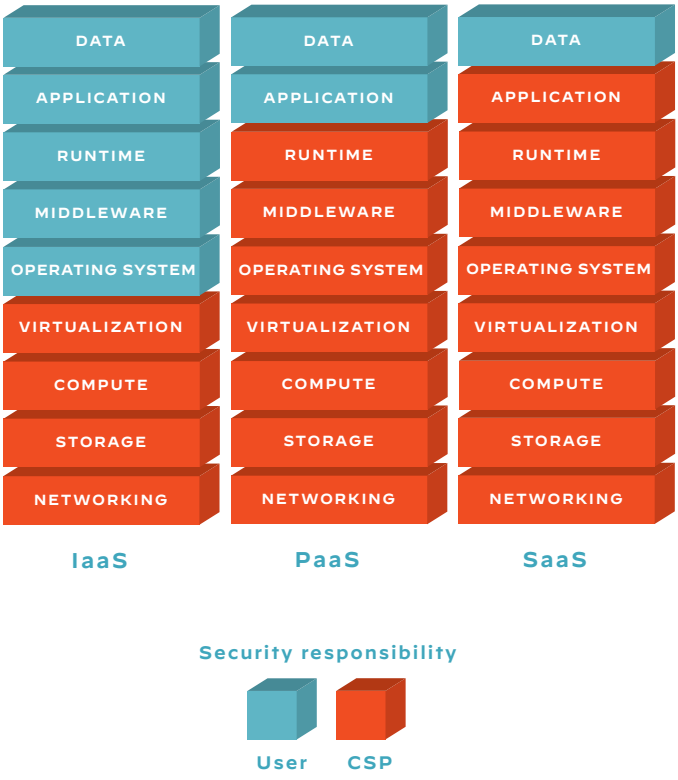

Figure 1: Shared responsibility in the public cloud

Understanding Shared Security Reduces Mutual Risks

CSPs make it clear that they are responsible for securing the global cloud platform—hardware, operating system, and network—but the customer must secure applications and ensure data integrity (see figure 2). As the company succinctly sums it up, AWS is responsible for security of the cloud while users are responsible for security in the cloud.

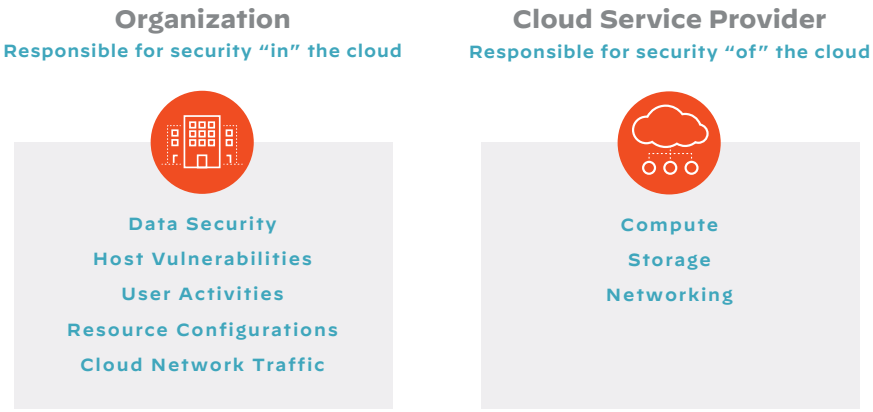

Figure 2: Shared security model for public cloud infrastructure

Within the customer organization, there is another kind of sharing. Security teams, developers, and DevOps teams have specific objectives and motivations for public cloud infrastructure that often differ from each other. Each of these groups influences—and shares—the organization's security model. Understanding the implications of shared security both internally and externally is a good first step toward reducing the risks associated with the cloud journey.

Platform Security Manages Part of the Equation

The CSP provides comprehensive native security for the cloud platform, including physical and environmental security, business continuity, access management, and network security. The baseline network security functionality typically includes the following components:

- **Security network architecture:** Monitor and control communications at the network's external boundary and key internal boundaries within the network using rule sets, access control lists (ACL), and configurations.
- **Secure access points:** Enable secure HTTPS communications between users and CSPs' resources.
- **Transmission protection:** Protect against eavesdropping, tampering, and message forgery using Secure Sockets Layer (SSL).
- **Account security:** Authenticate users and processes with passwords, cryptographic keys, digital signatures, certificates, and multi-factor authentication (MFA).

Service-Specific Security Comes with Conditions

Many organizations turn to the public cloud for IaaS offerings such as Azure Virtual Machines, Amazon S3 storage, and Amazon EC2 compute. For IaaS services, the CSP typically provides additional security appropriate for the service. For instance, Amazon Elastic Compute Cloud (EC2) offers instance isolation via hypervisor, MFA-protected access to the host OS, and Layer 4 firewall. The firewall is located within the hypervisor layer, between the physical network interface and each instance's virtual interface (see figure 3).

The seemingly clean division of shared responsibilities presented earlier is somewhat misleading for IaaS. While the CSP does provide the basic security tools described in the next section, the customer is required to perform all the necessary security configuration and management tasks for the IaaS services.

Conspicuously missing from the discussion of native security is anything to do with application (Layer 7) security, an obligation for which the customer is 100% responsible. As the closest layer to the end user, the application layer represents the largest threat surface. The need is for a comprehensive network security solution that complements and extends the native security provided by the CSP to detect Layer 7 threats that can evade other security measures. In addition, the security solution must augment CSP network security with threat protection features such as built-in threat prevention, malware detection, URL filtering, and exfiltration prevention.

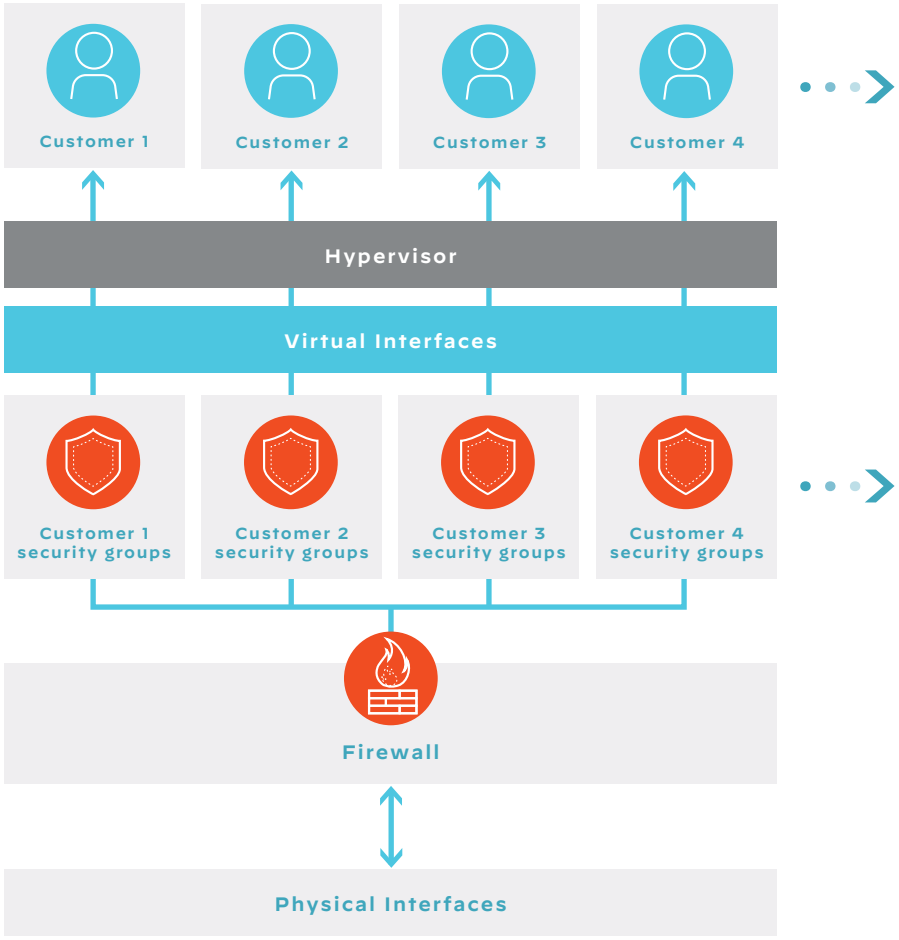

Figure 3: Security model for Amazon EC2 services

VM-Series Virtual Firewalls

Palo Alto Networks designed VM-Series Virtual Next-Generation Firewalls to meet the challenges outlined above. VM-Series firewalls provide consistent threat prevention and inline network security across cloud environments, helping network security teams regain visibility and control over traffic in their cloud networks. As part of the family of Palo Alto Networks ML-Powered NGFWs, the VM-Series offers all of the same capabilities as our industry-leading hardware firewalls in a VM form factor, making it highly scalable, a requisite for cloud environments. The key features of the VM-Series include Layer 7 firewall, cloud-delivered security subscriptions, and consolidated security management (see figure 4).

Layer 7 Firewall Secures Application-Layer Traffic

The heart of the VM-Series is our proprietary Layer 7 firewall, which can inspect traffic at the application layer and detect attacks that cannot be detected by the CSP's Layer 4 firewall. Using our patented App-ID™ features (see sidebar on following page), the VM-Series firewall can look within the application and make decisions about whether to allow a request based on the content, not just the port number. Typical attacks stopped by the VM-Series Layer 7 firewall include distributed denial-of-service (DDoS) attacks, HTTP floods, SQL injections, cross-site scripting, parameter tampering, and Slowloris attacks.

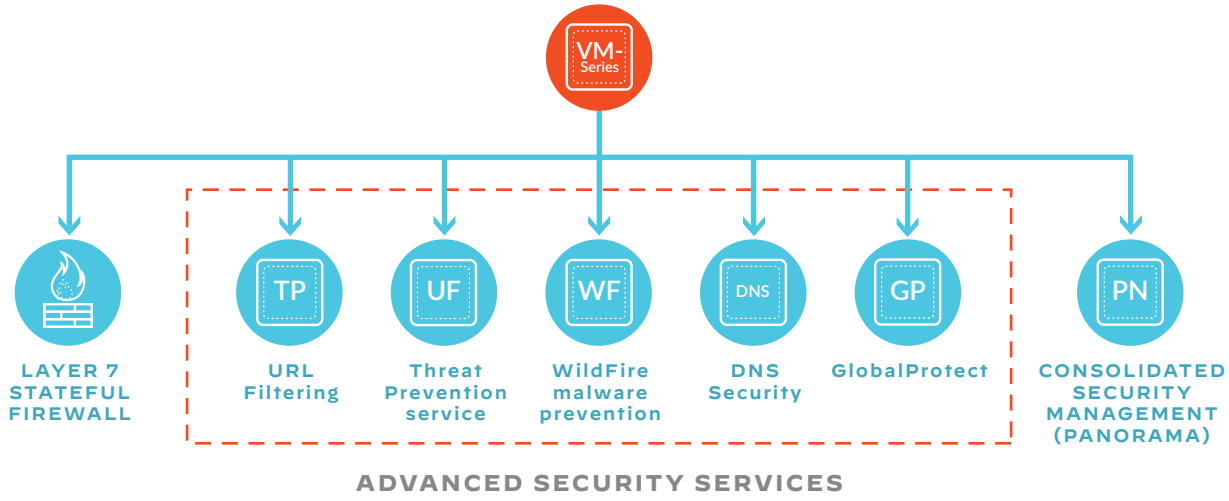

Figure 4: Features of VM-Series virtual firewalls

Proven Advanced Security Subscriptions Resolve Ongoing Threats

The VM-Series expands Layer 7 firewall capabilities by seamlessly integrating into our cloud-delivered security subscriptions just like our other Next-Generation Firewalls—CN-Series container firewalls and PA-Series physical firewalls—and Prisma™ Access. These cloud-delivered security subscriptions coordinate intelligence capabilities and provide protections across all attack vectors. This eliminates coverage gaps generated by disparate network security tools and provides a consistent platform experience to secure your organization against even the most advanced and evasive threats.

Threat Prevention

Threat Prevention works with the Layer 7 firewall to provide intrusion prevention system (IPS) capabilities that CSP native security lacks. By inspecting all traffic for known threats regardless of port, protocol, or encryption, Threat Prevention automatically blocks vulnerabilities, buffer overflows, spyware, malware, command and control (C2), and port scans. Customers can also leverage our leading threat intelligence based on local intelligence as well as import, sanitize, manage, and completely automate workflows to rapidly apply IPS signatures in popular formats such as Snort® and Suricata®.

URL Filtering

URL Filtering protects organizations against web-based threats such as phishing, malware, and C2. Inline machine learning identifies and prevents new and unknown malicious websites instantly, before they can be accessed by users. Unlike the fully qualified domain name (FQDN) filtering offered by CSPs, URL Filtering allows granular control of site access as an extension of your NGFW policy, reducing complexity by giving you a single policy set to manage. A typical use case involves developers requesting access to code repositories on GitHub. FQDN filtering can either grant or restrict access to the entire GitHub site. Doing so drastically increases the risk of a data breach and can easily inhibit productivity or force shadow IT practices. In contrast, URL Filtering can allow access to specific vetted code repositories within GitHub and block all others, aiding developer productivity while reducing threats.

Wildfire® Malware Prevention

WildFire® malware prevention uses multiple methods of analysis to detect and prevent unknown file-based threats, including static analysis with machine learning, dynamic analysis, and bare metal analysis. In an industry first, WildFire deploys inline machine learning modules to identify and prevent common and new unknown file-based threats, which protects users before a threat can even enter the network. Its cloud-based architecture scales to support real-time signature streaming, ensuring your networks, endpoints, and clouds are protected against all previously unknown threats in seconds after initial discovery.

DNS Security

DNS Security applies predictive analytics, machine learning, and automation to block attacks that use DNS. Tight integration gives you automated protections, prevents attackers from bypassing security measures, and eliminates the need for independent tools or changes to DNS routing. Comprehensive analytics allow deep insights into threats and empower security personnel with the context to optimize their security posture.

IoT Security

IoT Security is the industry's first complete IoT security solution, delivering a machine learning-based approach to discover all unmanaged devices, detect behavioral anomalies, provide risk-based policy recommendations, and automate enforcement without the need for additional sensors or infrastructure. This unique combination of IoT visibility and the VM-Series enables context-aware network segmentation to reduce risk exposure and applies our leading security subscriptions to keep IoT and operational technology (OT) devices secure from all threats.

GlobalProtect™

GlobalProtect™ safeguards the mobile workforce by using the capabilities of the VM-Series to inspect all mobile device traffic—incoming and outgoing. By leveraging the global presence of the CSP, security teams can quickly and easily deploy GlobalProtect gateways in any region without the expense or IT logistics that would be required to set up this infrastructure from scratch.

Consolidated Security Management Speeds Visibility, Cuts Effort

Panorama™ network security management centralizes administration for VM-Series firewalls across multiple cloud deployments alongside physical appliances, ensuring consistent and cohesive policy. Rich, centralized logging and reporting capabilities provide visibility into virtualized and containerized applications, users, and content. With Panorama, security managers can provision firewalls centrally and create effective security rules as well as gain insight into network traffic and threats.

App-ID: Foundation for Visibility and Control

App-ID™ technology is a primary capability of all Palo Alto Networks firewalls. App-ID identifies applications traversing the firewalls independently of port, protocol, and encryption method. As a key enabling technology in the VM-Series, App-ID provides visibility and control over applications—even those that try to evade detection by masquerading as legitimate traffic, hopping ports or sneaking through the firewall using encryption (TLS/SSL or SSH).

Key Benefits

VM-Series virtual firewalls offer the features that security teams need to secure multi-cloud environments, including full visibility and control, consistent policy enforcement, application security, exfiltration prevention, compliance and risk management, security automation, and cloud-agnostic management.

Full Visibility and Control Finds Threats Across Environments

The VM-Series helps security teams and others understand which applications—including those that are SSL-encrypted—are traversing the cloud deployment, where they are coming from and going to, and the user's identity. Rich centralized logging and reporting capabilities provide visibility into virtualized and containerized applications, users, and content.

The VM-Series integrates deeply into the public cloud environment to provide additional context such as tags and other metadata. A tag-based policy model, tight integration across all major CSPs, and a fully documented XML API allow network security teams to create flexible policies that can adapt to dynamic environments regardless of the underlying infrastructure.

Consistent Policy Enforcement Delivers Best-in-Class Security

Many organizations have critical applications hosted in on-premises data centers, private clouds, and multiple public clouds. To enforce consistent security policies across all three parts of this hybrid environment, the security team must duplicate policies across three clouds using the native controls in each—a labor-intensive and error-prone task. Managing the overall security posture requires the team to develop expertise in each cloud's controls and management interface.

VM-Series virtual firewalls deployed in multiple public and private cloud environments can all be managed from the same console. This capability lets security teams deliver the same best-in-class security to each environment and extend a uniform policy model across the entire ecosystem to ensure consistency and simplification of an organization's overall security posture (see figure 5).

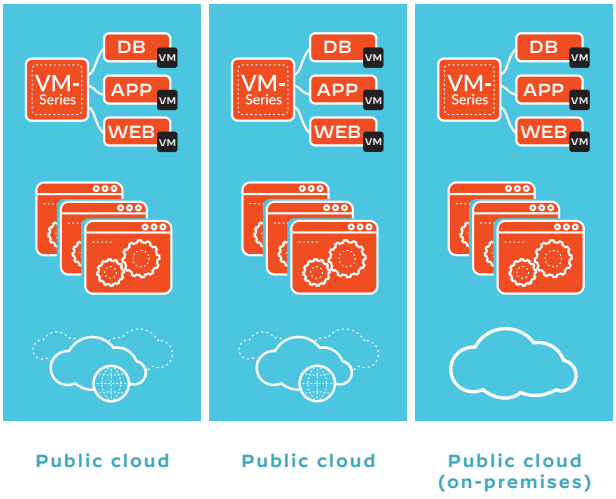

Figure 5: Consistent policy enforcement across public and private clouds

Compliance and Risk Management Become Easier

Risk management and compliance activities benefit from VM-Series features such as application allow listing, which reduces the attack surface by allowing specific applications and denying all else. Allow list policies also allow organizations to segment applications communicating with each other across different subnets and between virtual private clouds (VPCs) for regulatory compliance. For particularly stringent regulatory compliance standards, Threat Prevention can be turned on in allow list policies to add an extra layer of protection. Comprehensive reporting across decentralized environments streamlines audits and speeds compliance with government and industry regulations, including GDPR, PCI DSS, HIPAA, and SWIFT Standards.

By deploying the VM-Series, organizations can align application usage to business needs, control application functions—for example, allow SharePoint® documents for all but limit SharePoint administration access to the IT group—and stop threats from accessing and moving laterally across the public cloud deployment.

Security Automation Safeguards DevOps

The VM-Series includes management and automation features that enable developers to embed security in DevOps workflows and other application development processes. VM-Series firewalls can support cloud native, agile, and waterfall development methodologies. Developers can automatically provision a VM-Series firewall with a working configuration, complete with licenses and subscriptions, and then auto-register with Panorama. Auto-scale templates, bootstrapping, and other automated configuration capabilities ensure that VM-Series firewalls can be easily deployed to scale with increased demand. The VM-Series integrates with automation and orchestration platforms such as Jenkins®, Terraform®, Ansible®, and SaltStack® so developers can deploy firewalls as a routine task in application development to ensure security at DevOps speed.

Cloud-Agnostic Security Makes Multi-Cloud Deployments Real

The VM-Series supports all major CSPs, including AWS®, Azure®, GCP®, Oracle Cloud®, and Alibaba Cloud. Panorama, often deployed to manage multiple VM-Series firewalls, eliminates the need for multiple security toolsets by providing comprehensive visibility and control across multi-cloud and hybrid cloud environments from a single console. The advanced security subscriptions in VM-Series virtual firewalls eliminate the need for additional point security products, thereby reducing complexity and making it easy to deploy the right security controls wherever they are needed throughout your environment. Panorama provides centralized network security management for VM-Series firewalls across multiple cloud deployments alongside your physical appliances, ensuring consistent and cohesive policy.

Bringing Security to the Workload

One key guiding principle in the design of our firewalls is to move the security as close as possible to the workload. This strategy takes advantage of software constructs such as virtual machines, containers, and Kubernetes®, and helps provide additional context for creating and managing security policies.

In practice, our approach comes down to offering multiple form factors to integrate with different hosting environments. For workloads on physical machines, the PA-Series hardware solutions are often the right choice. Virtualized environments require VM-Series virtual firewalls that are deployed on virtual machines.

The recently released CN-Series targets cloud native development environments that rely on containers and orchestration (Kubernetes). The CN-Series Container NGFW is the first firewall in the industry to be designed with separate control and data planes, which are deployed inside separate containers to provide pod-level security. All three firewall form factors offer the same rich set of NGFW features and advanced security subscriptions, and they integrate seamlessly with Panorama for unified security management.

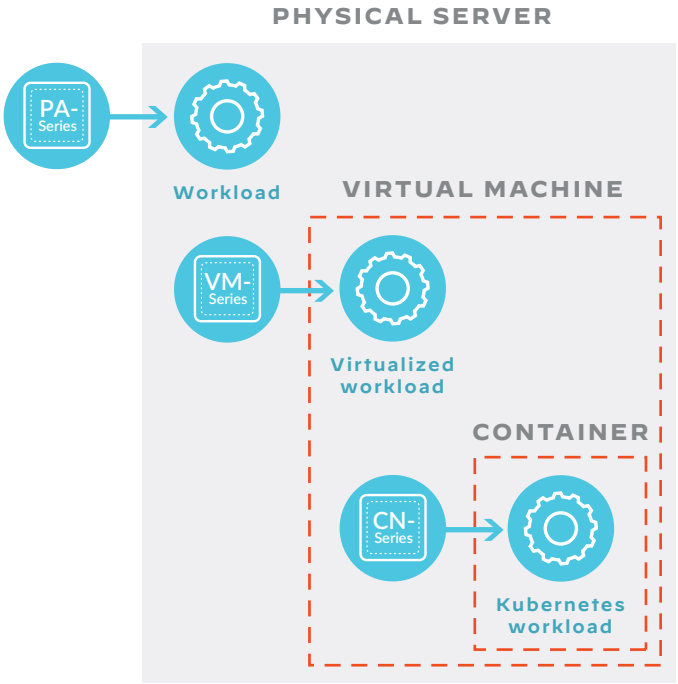

Figure 6: Palo Alto Networks Next-Generation Firewall form factors

Use Cases

Inbound Threat Prevention Stops Threats at the Edge

Port-based security groups implemented by CSPs lack application-level visibility into network traffic and have few integrated threat prevention capabilities. Most CSPs offer Layer 4 firewalls and web application firewalls (WAFs) as part of native security, but there are still gaps. Layer 4 firewalls will not discover threats that exploit open or nonstandard ports, while WAFs only protect web applications.

In contrast, VM-Series firewalls inspect every inbound packet and block suspicious traffic based on application type or user identity, going beyond simple port blocking to protect traffic over any open ports. The VM-Series also provides advanced security capabilities, such as intrusion prevention system (IPS) and sandboxing, to defend against both known and unknown vulnerabilities at the edge of a public cloud environment (see figure 7).

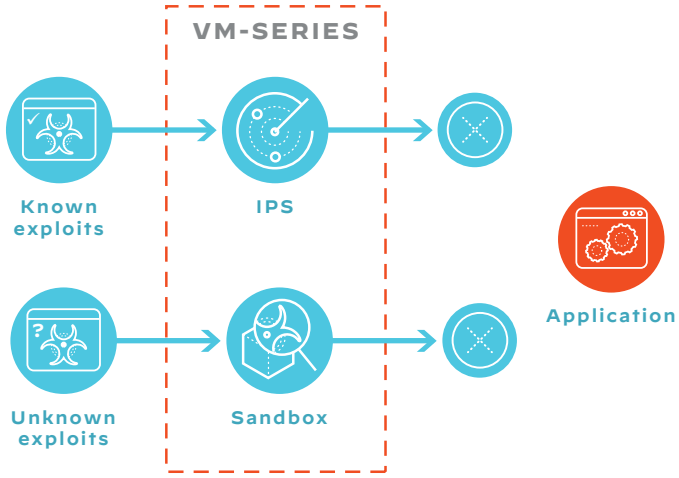

Figure 7: Inbound threat protection with VM-Series

Exfiltration Prevention Thwarts Data Theft

With the trend to more remote work—exacerbated by the COVID-19 pandemic—more employees, contractors, and others need to access critical data in the organization's clouds. With more data in motion, cyberattackers have more opportunities to steal valuable information.

The VM-Series prevents data exfiltration using a combination of application enablement, content inspection, and DNS Security features. The VM-Series looks inside files (as opposed to only at the file extension) to determine if the transfer action should be allowed. Executable files, found in drive-by downloads or secondary payloads, along with malware C2, can be blocked automatically. Data filtering features detect and control the outbound flow of confidential data patterns, such as credit card and Social Security numbers, as well as custom patterns.

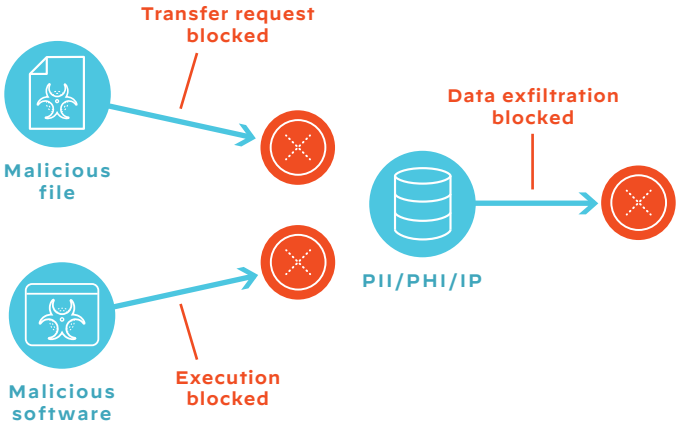

Figure 8: Exfiltration prevention with the VM-Series

Segmentation Augmentation Keeps Boundaries Solid

VPCs and VNets are emerging as the new trust boundaries in public cloud environments, and NGFWs are being deployed to protect all the traffic going in/out of these trust boundaries. Many organizations use VPCs to provide isolation and security boundaries for workloads. The VM-Series augments that separation through application-level segmentation policies to control traffic between VPCs and across subnets (see figure 9). Threat Prevention policies can be used to block suspicious interactions, for example, an accounting program trying to access source code.

The automation capabilities of the VM-Series make it easy to deploy and configure as part of an automated provisioning process, ensuring that any new infrastructure is automatically protected from the moment it is created. Autoscale templates ensure that VM-Series firewalls can be scaled elastically to respond to increased demand on the infrastructure during scale events like cloud bursting.

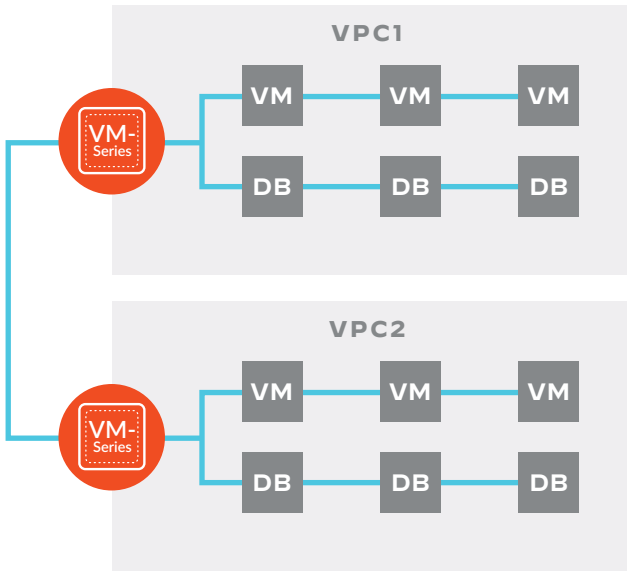

Figure 9: Segmentation with the VM-Series

Public Cloud Security Is Essential in Hybrid Cloud Environments

Every cloud has different security capabilities and policies. On-premises firewalls are managed separately from cloud security. The VM-Series provides consistent capabilities and policy models across all cloud and on-premises environments. VM-Series, PA-Series, and CN-Series firewalls are all managed from the same console (see figure 10).

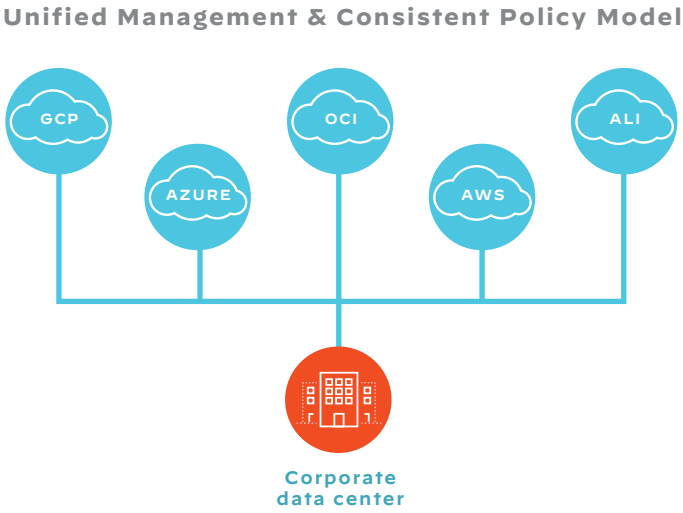

Figure 10: Hybrid cloud security with the VM-Series

Developer Protection Becomes Critical

Developers routinely use code repositories to shorten development cycles and reduce troubleshooting time. However, code repositories can hide a range of threats, including:

- Secrets inside committed code, such as private keys, API keys, or internal domains
- Regular expression plugins to find specific secrets, names, or PII inside code
- Internal project names that can result in the exposure of internal company information
- CI/CD integration that fails a build if something is found or a rule is fired

Native CSP firewalls often rely on FQDN filtering to prevent developers from accessing infected code repositories. However, FQDN filtering lacks the required granularity. For example, FQDN filtering can either grant or deny access to the entire GitHub domain but cannot discriminate between the URLs of individual code repositories within GitHub, some of which can be infected (see figure 11).

In contrast, URL Filtering in the VM-Series can grant access to company-sanctioned repositories in GitHub while blocking access to the rest. Now, developers can freely get resources from known secure repositories without the danger of accidentally downloading infected code that could compromise the entire network (see figure 12).

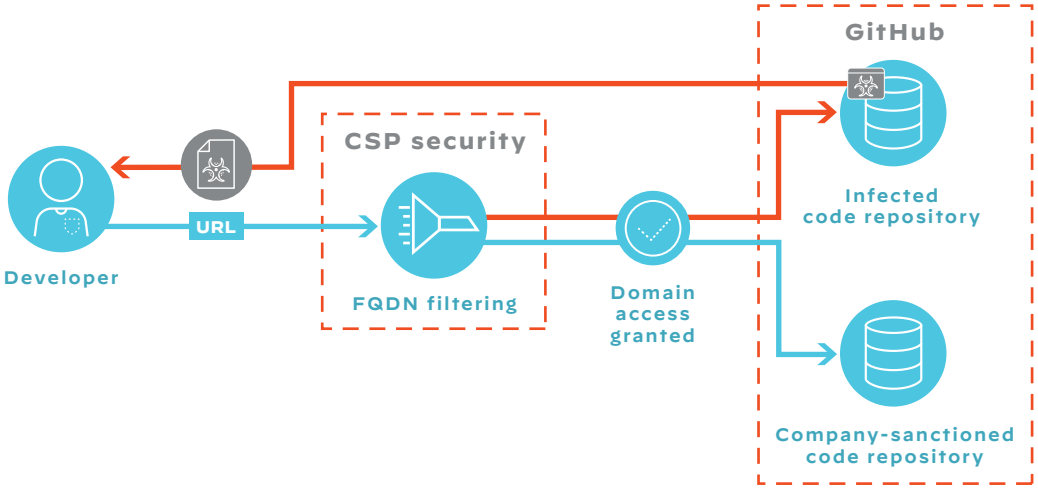

Figure 11: FQDN filtering to control GitHub access

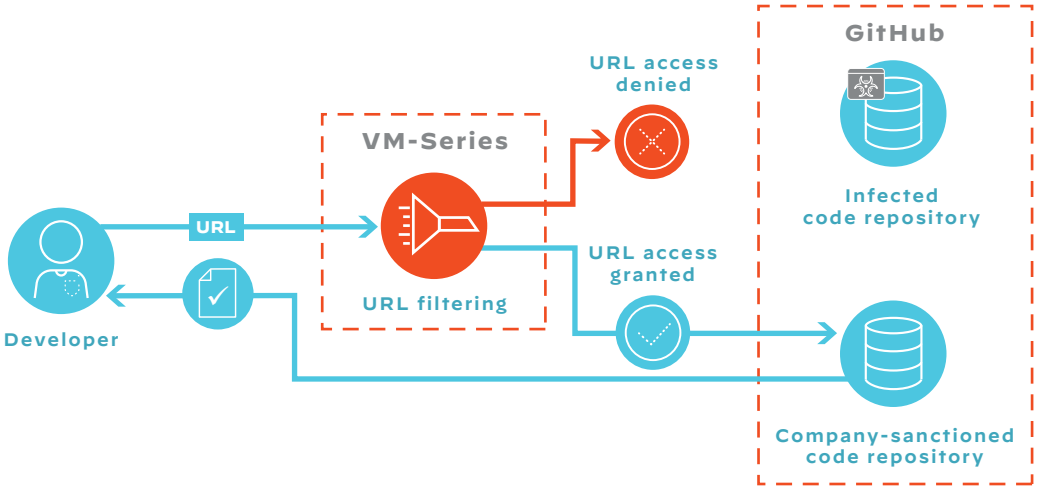

Figure 12: URL Filtering to control GitHub access

Palo Alto Networks Firewall Platform

The VM-Series is part of the family of Palo Alto Networks ML-Powered NGFWs. The industry-leading Strata™ network security suite, which includes the NGFW family, prevents attacks and consistently secures users, applications, and data, no matter where they reside (see figure 13). This comprehensive approach is vital for today's hybrid multi-cloud environments.

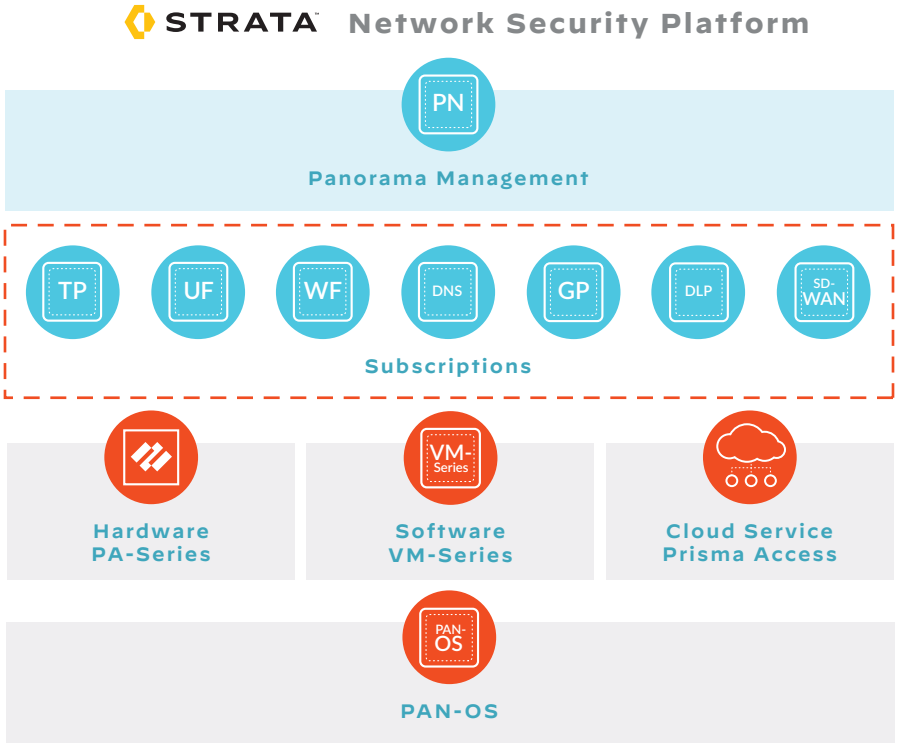

Figure 13: Strata network security suite

Summary

Multi-cloud deployments present significant challenges to security teams, especially the need to share security with the CSP. CSPs provide native security controls for the infrastructure, but the contracting organization must design and implement their own application security strategy. The overriding need is for a solution that integrates seamlessly with the CSP's native controls to amplify the overall network security posture and ensure network security for applications and data located in public clouds.

The VM-Series is designed for this particular purpose. The VM-Series has key features designed for securing public clouds to help organizations:

- Augment native network security with application enablement policies to detect and foil threats and prevent data loss.
- Allow developers to transparently embed network security and threat protection in the application development process through automation and centralized management.
- Enable network security to scale dynamically yet independently of workloads through deep integration with CSP autoscaling features.
- Drive high availability through active/passive firewall configurations integrated with native load balancing.

To learn more about the need for application-layer network security and threat protection in multi-cloud environments, read the e-book *Why Native Security Controls in Public Clouds Are Not Enough.*

For in-depth information tailored to your multi-cloud security issues, sign up for a personalized VM-Series demo.

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