Hackers Are Coming For Your Cloud-Based Applications

Software NGFWs and Prisma Cloud protect applications, minimize risk, and accelerate business value

Cloud Applications Face Unique Security Challenges

Virtually every modern enterprise now depends on cloud applications. To remain competitive in the market, businesses need agile development and deployment of cloud-native and lift-and-shift applications to accelerate migrations and to respond to competitive markets and business dynamics.

The cloud offers organizations a scalable, cost-effective platform for application deployment and management. Unlike legacy methodologies that heavily depended on writing most of the code from scratch, cloud-native development is frequently an assembly process that relies on code repositories, both in-house and external third party code.

In addition, the pace has picked up dramatically thanks to the CI/CD (continuous integration/continuous delivery) pipeline tools that allow applications to be developed, fixed, or enhanced at a rapid pace.

AI Supercharges Application Development

However, there's more to cloud-native application development than speed—and that's where artificial intelligence (AI) comes in. The synergy of cloud computing, data storage, and AI allows enterprises to sift through vast amounts of historical data, unearthing patterns and trends that are difficult or impossible to achieve through manual analysis. Those insights shine a spotlight on the company's customer preferences and pave the way for applications that meet those needs and resonate with the strategic objectives of the business.

Cloud-first strategies have reshaped application development, but security isn't always a priority for cloud developers. A survey highlighted that only 14% of cloud developers viewed application security as essential, with a significant proportion leaving known vulnerabilities unaddressed.[1]

Organizational challenges often relegate network security to later stages, limiting proactive measures. When network security teams suggest solutions like next-generation firewalls, they must prove these security products won't hinder business processes. This situation is exacerbated when developers mistakenly believe native cloud provider security is adequate for applications running "in the cloud."

The shift from centralized architectures to hyperconnected hybrid/multicloud environments increases vulnerability. Traditional centralized architectures had clear security boundaries, but with the rise of hybrid/multicloud strategies, defining the attack surface becomes more challenging due to interconnectedness.

[1] "Where does secure code sit on the list of development team priorities?" Secure Code Warrior, April 5, 2022.

Hackers Leverage Cloud and AI

The meteoric ascent of cloud applications has caught the attention of cybercriminals. With each technological leap, the most skilled among these adversaries are swiftly harnessing state-of-the-art tools such as AI to uncover security breaches, craft unique exploits, and refine their methods to bypass security protocols. Additionally, savvy hackers are pinpointing vulnerabilities within the public cloud awaiting exploitation. A common trait of many cloud services is their reliance on APIs for interfacing with apps. While these APIs may appear as straightforward solutions, they frequently become the most vulnerable point in terms of security. Ill-intentioned individuals can unleash DoS attacks and input harmful codes to infiltrate cloud servers, jeopardizing an organization's sensitive information.

Conversely, security professionals face challenges adapting to the relentless pace of technological advancement, which often surpasses their capability to fortify app security. Cyber threats are simultaneously morphing with unmatched intricacy, amplifying the challenge of safeguarding applications. For perspective, while security teams spend about 145 hours (nearly 6 days) addressing a single security warning, malicious actors can exploit a newly disclosed vulnerability in a mere 15 minutes.[2]

Cloud Developers, Security Managers See the World Differently

Shifting to cloud-first strategies has profound implications for security, starting with application development. Security is not always top of mind for cloud developers as they focus on tight deliverable schedules. Their mandate is to develop and release—as quickly as possible—applications that deliver business value. Yet it can be difficult to deliver value when applications are susceptible to attack.

To remedy these vulnerabilities, the network security group must have a seat at the table. However, organizational barriers and attitudes can get in the way. Network security often arrives late in the development lifecycle, limiting the range of available options. Furthermore, when the network security team recommends a security solution such as a next-generation firewall (NGFW), they bear the burden of proof to show that their recommendations will not slow the business down or delay time to value.

At the same time, the development group can be tempted into thinking the native "in cloud" security provided by cloud service providers is "good enough," so why bother adding more? This situation is particularly frustrating because the network security group is responsible for preventing breaches, compliance failures, and other security issues but does not have the authority—and sometimes knowledge—to implement necessary security changes to the cloud (or CI/CD) application development process. In addition, many of today's cloud developers lack the deep knowledge of modern sophisticated cyberattacks and their ability to morph and evade traditional security measures.

Cloud-Native Techniques Transform Application Development

The IT industry today is experiencing a profound shift in the way applications are developed, secured, and delivered. In the traditional on-premises data center environment, developers write the code for applications, IT teams build and maintain the underlying infrastructure that runs those applications, and then security teams apply the necessary security. In this siloed model, software engineers work within the constraints of infrastructure and operating systems. Security managers have the final word on what can and cannot be done in the application development process—they are the arbiters of application security.

[2] "Unit 42 Unveils Most 'Expansive' Cloud Threat Research Yet: Cloud Threat Report Volume 7 Examines the Expanding Attack Surface," Unit 42, April 18, 2023.

That model has been turned on its head with the advent of cloud-native development, a method of building applications that take full advantage of the unique characteristics of cloud platforms. Compared to traditional development methodologies, cloud-native development empowers software engineers to create highly scalable applications with unprecedented flexibility and resiliency that run on any cloud, public, private, or hybrid. Cloud-native technologies have transformed every aspect of application development, including the hosting platform, the code architecture, and the/integration/delivery methodology.

Hybrid Architectures Expand the Attack Surface

Why are cloud architectures so vulnerable to these kinds of attacks? One reason is the evolution of the infrastructure itself, from centralized data centers to dispersed, hyperconnected hybrid/multi-cloud environments, which makes it difficult to design an effective security strategy.

In the centralized model, a gateway firewall located at the data center edge secures north-south traffic for both local applications and software-as-a-service (SaaS) applications. Additional physical firewalls can be employed to enhance security for individual subnets and prevent east-west threat propagation. Network security teams have complete visibility into the network architecture and can ensure that firewall policies are consistent and effective using centralized tools.

However, this architecture is somewhat inefficient for remote workers and branch offices because SaaS traffic has to pass through the data center—a practice called hairpinning—thus introducing significant application latency and degrading performance. In response, many organizations have installed firewalls at remote locations, smaller physical appliances similar to the data center firewalls. Despite the use of remote firewalls, the attack surface is still relatively small and easily defined (see figure 1).

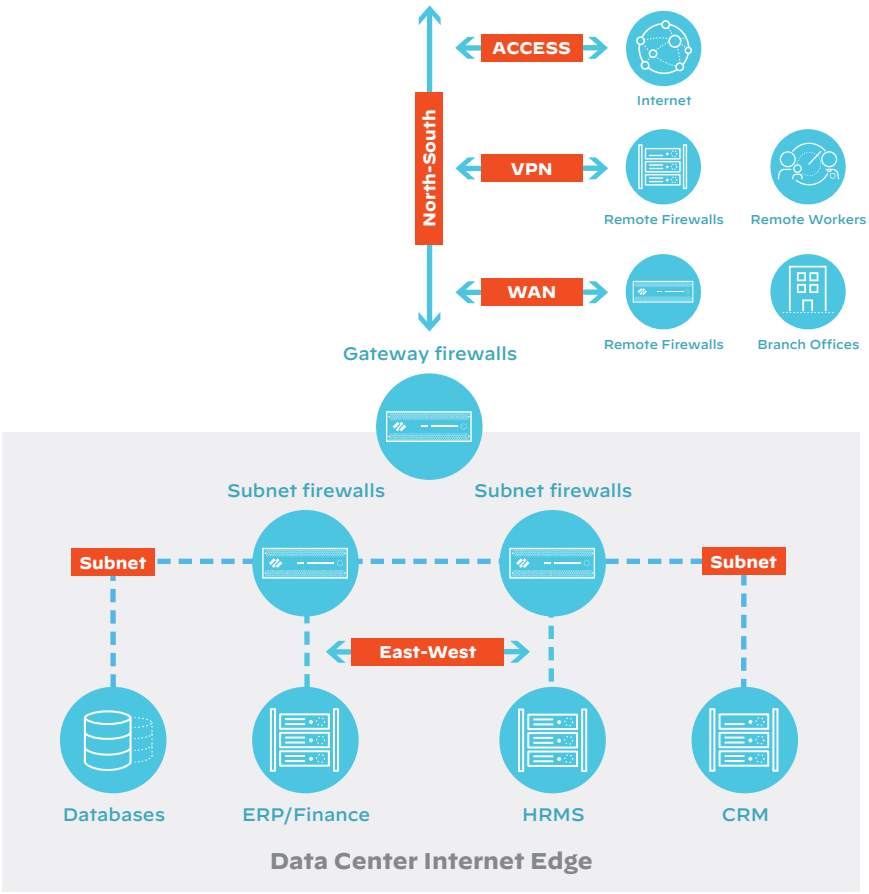

Figure 1: Firewall security in traditional data center architecture

The adoption of hybrid and multicloud architectures essentially explodes this model of security. For one thing, data centers are evolving into private clouds in which local applications are hosted on virtual machines, not directly on the physical servers. Other applications run in public clouds in virtualized environments, often using containers and Kubernetes orchestration. In this model, interconnections dominate the architecture, making the attack surface larger and more difficult to define.

Securing Modern Applications Requires Modern Thinking

Traditional approaches to application security cannot adequately address the challenges outlined in the previous section. Why? Because the network has changed and application development has accelerated, nothing short of a new way of thinking about application security will do. Instead of dividing the network into trusted and untrusted sections, now the need is to assume that every access is a potential threat until verified—the concept of zero trust. Instead of seeing application development and production as separate processes, the need today is to secure the entire lifecycle, one that reexamines the concept of trust and unifies security from development to runtime and runtime transactions and access—the concepts of code-to-cloud intelligence and Zero Trust: always verify in combination.

Code-to-Cloud Intelligence

The key innovation required for securing modern applications across the entire application development lifecycle is code-to-cloud intelligence. This revolutionary approach connects insights from the developer environment into the application runtime to reduce risk and prevent breaches. Code-to-cloud intelligence is more than just the latest jargon in cloud security—it signifies a revolutionary shift, offering a holistic strategy that aims to transform the way organizations safeguard their applications and cloud ecosystems. Code-to-cloud intelligence improves visibility, contextualizes alerts, prioritizes critical risks, and offers remediation guidance (see figure 2).

Figure 2: Code-to-Cloud Intelligence

Zero Trust: Verify Always

Zero Trust is the conceptual shift that makes it possible to secure today's complex hybrid and multicloud architectures. Zero Trust represents a shift in the way network and cloud security teams think of security. Zero Trust moves beyond this worldview by assuming that bad actors can be anywhere. Every person requesting network access is considered an unknown, and the security practice calls for a range of verified traffic identification to determine whether to grant access or not. Trust is not assumed but rather earned—literally every time a user, application, or device accesses a network service (see figure 3).

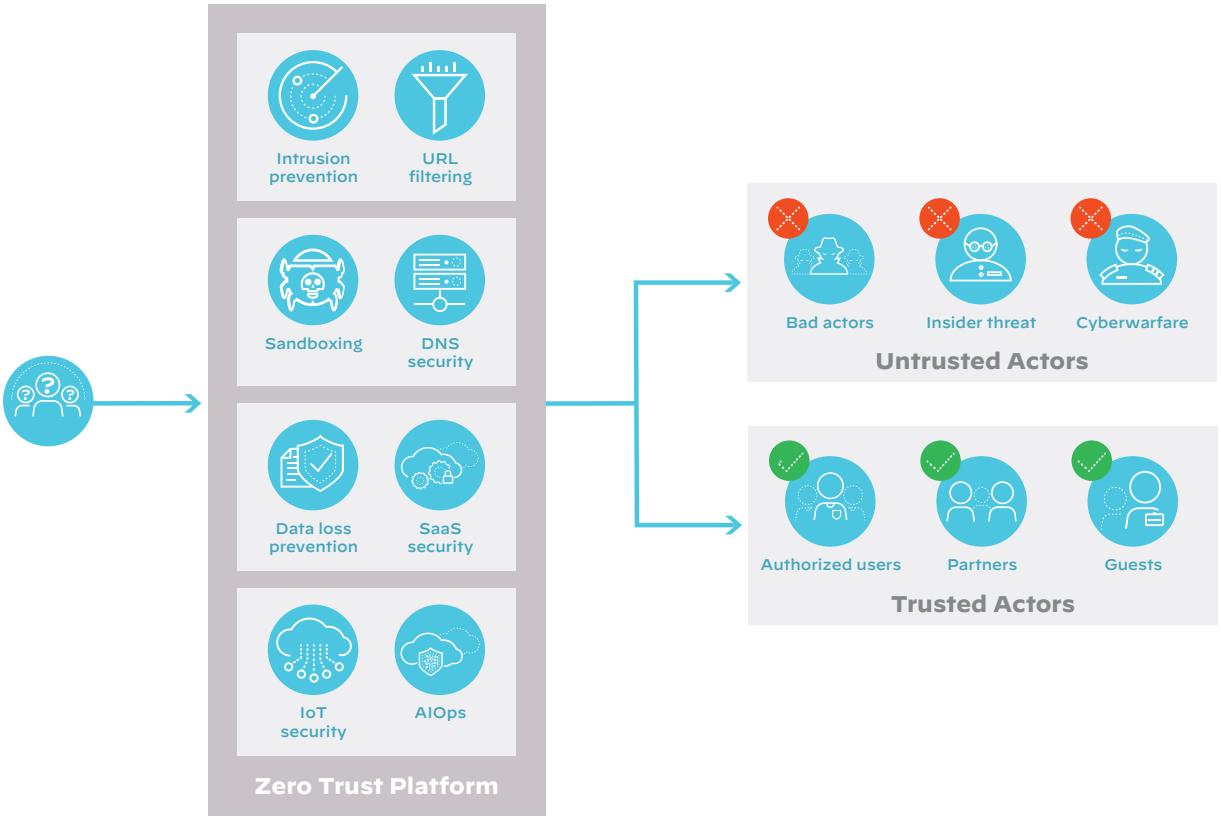

Figure 3: The Zero Trust approach to security

Keys to Highly Effective Application Security

To secure the organization's applications, security professionals must apply the insights presented in the previous section in two areas: the application development lifecycle and the application network transactions (see figure 4).

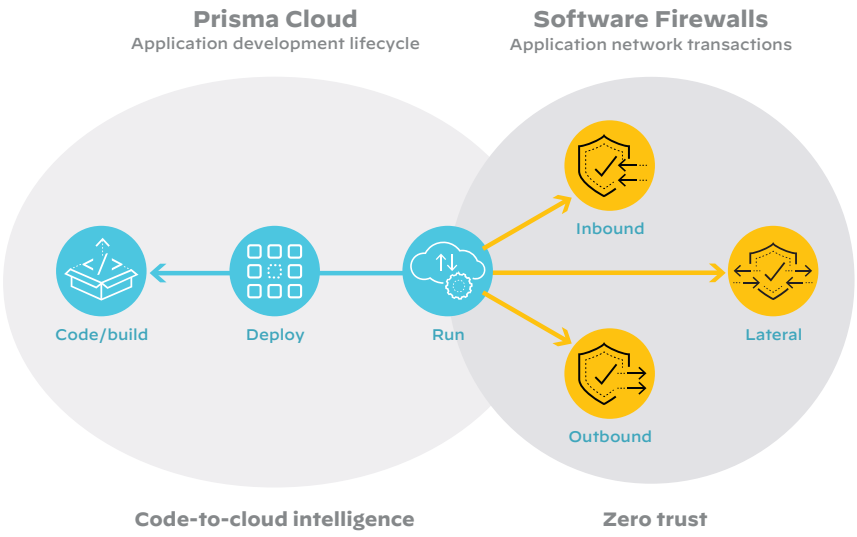

Figure 4: Securing application lifecycle and network transactions

Secure the Application Lifecycle

For effective security in a cloud-native world, you need the ability to protect applications through the complete application lifecycle, including initial code development, production deployment, application maintenance and update, and end-of-life decommissioning.

Palo Alto Networks addresses this need with **Prisma Cloud**, the industry's most complete Cloud Native Application Protection Platform (CNAPP). Built on the concept of code-to-cloud intelligence, Prisma Cloud bridges crucial connections between application vulnerabilities, security alerts, and operational environments throughout the application's life, providing insightful context. This intelligence from code to cloud marks a groundbreaking advancement in cloud security, establishing an unprecedented benchmark.

Protect Network Transactions

Applications engage in numerous network transactions as they communicate and exchange digital information with each other, in both development and production. All these transactions must be secured to prevent intrusions and malicious exploits. Software firewalls are the essential component for securing transactions.

Palo Alto Networks addresses this need with the **Network Security Platform**, which is based on VM-Series Virtual Next-Generation Firewalls (NGFWs), CN-Series Container Next-Generation Firewalls, and Cloud NGFW managed firewall services. Prisma Cloud also provide web application and API security on top of cloud workload protection to protect application's workloads, the APIs that connect them and the web interface from threats.

These software firewalls support Zero Trust principles, integrate with cloud platforms, and provide capabilities like advanced threat prevention, sandboxing, and continuous trust verification by, or in combinations of, users, applications, devices, and content. The result is to ensure consistent security across all environments and applications.

Prisma Cloud Protects Applications from Code to Cloud

Prisma Cloud is designed to protect applications across any public, private, hybrid, or multicloud environment. Unlike a collection of point products, Prisma Cloud integrates a broad set of security capabilities into a single platform to deliver unified, best-in-class security for three critical use cases: risk prevention, visibility and control, and runtime protection (see figure 5).

Figure 5: Prisma Cloud use cases

Risk Prevention

Prisma Cloud integrates with engineering ecosystems to prevent risks and misconfigurations from entering production. It identifies and fixes misconfiguration in popular Infrastructure-as-Code (IaC) offerings such as Terraform, CloudFormation, Azure Resource Manager, and Kubernetes. With Prisma Cloud you can find and secure exposed and vulnerable secrets across all files in repositories and CI/CD pipelines. Prisma Cloud helps you harden CI/CD pipelines, reduce the attack surface, and protect your application development environment.

Visibility and Control

WIth Prisma Cloud, you gain continuous visibility and control over cloud misconfigurations, identity and access, data, vulnerabilities, and API endpoints across your cloud environment. Prisma Cloud secures cloud infrastructures using cloud security posture management (CSPM), which monitors posture, detects and remediates risks, and maintains compliance. You can easily discover profiles, protect APIs across cloud-native applications, and scan hosts, containers, Kubernetes, and serverless assets for vulnerabilities and threats. Prisma Cloud can also detect sensitive data and scan for malware across public cloud storage. Prisma Cloud increases your visibility and control over unknown, unmanaged cloud assets exposed to the internet.

Runtime Prevention

Prisma Cloud also offers runtime protection to block breaches in runtime and protect applications against attacks. Prisma Cloud detects advanced threats, zero-day attacks, and anomalies across multicloud environments. With Prisma Cloud, you can secure cloud VMs, containers, Kubernetes platforms, serverless functions, web applications, and APIs across any public or private cloud.

Software Firewalls Secure Network Transactions

To secure today's complex hybrid and multicloud architectures, cloud architects and network security managers need an integrated solution that can secure any network based on any combination of public clouds, private clouds, virtualized data centers, and remote locations. As an integral part of Palo Alto Networks Network Security Platform there is just such a solution: Palo Alto Networks software firewalls (see figure 6).

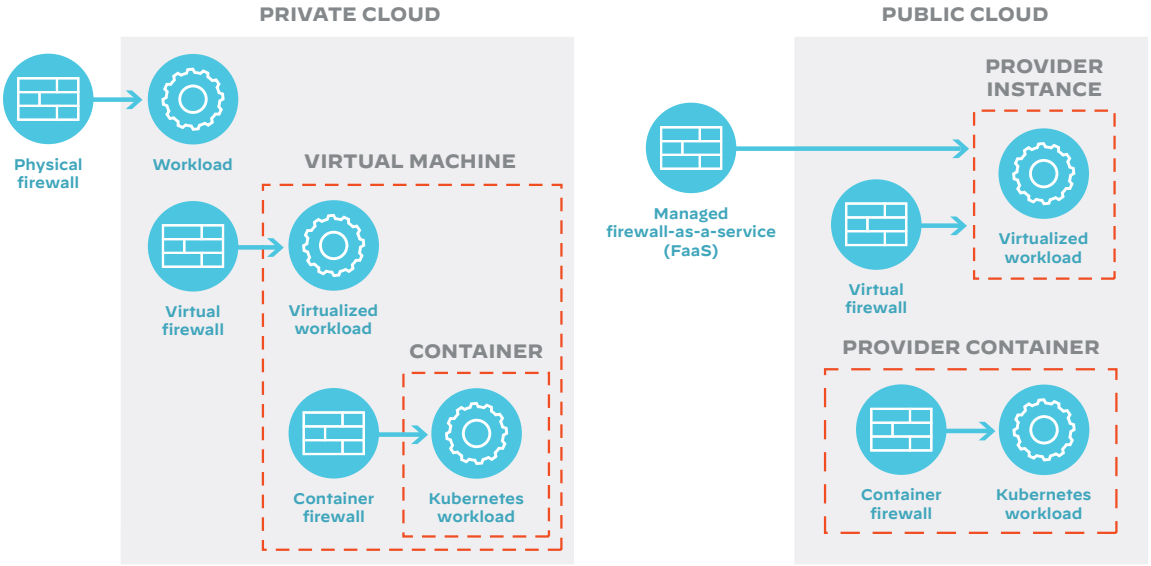

Figure 6: Software firewalls in hybrid/multicloud security

Palo Alto Networks software firewalls are built from the ground up to support Zero Trust. They combine artificial intelligence, machine learning, and software automation with threat research and intelligence from the Palo Alto Networks Unit 42 team to protect applications from cyberattacks with agile, best-in-class network security for all clouds—public, private, and hybrid. The platform features deep integration with clouds and virtualization technologies, automated DevOps deployment and scaling, and centralized management for all private, public, and hybrid and multiclouds (see figure 7). Palo Alto Networks software firewalls come in proven NGFW virtual and cloud form factors, each of which is described in more detail below.

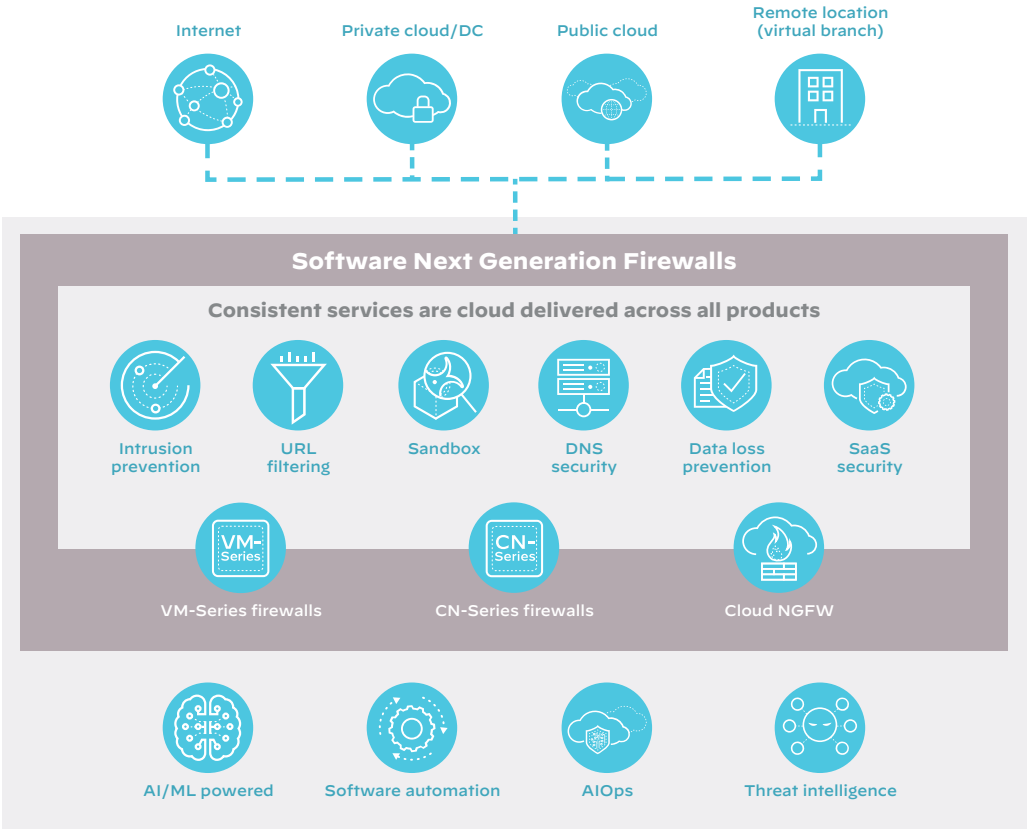

Figure 7: The Network Security Platform from Palo Alto Networks

VM-Series Virtual Next-Generation Firewall

The software firewall workhorse is the VM-Series virtual firewall, which secures workloads anywhere in the hybrid multicloud environment, including public and private clouds, virtualized data centers, and software-defined branch environments. The VM-Series virtual firewall features automated deployment, built-in scalability, and deep integrations with all major cloud hypervisors, and software-defined networks, protecting your applications wherever they reside. The VM-Series virtual firewall can be flexibly procured using Software NGFW Credits or directly from CSP marketplaces with pay-as-you-go usage.

CN-Series Container Next-Generation Firewall

Container workloads are difficult to secure with traditional firewalls because they are embedded in the Kubernetes environment. The Palo Alto Networks CN-Series container firewalls go where the need is. Deployed on Kubernetes clusters, the CN-Series container firewall protects against known and unknown threats seeking to move laterally between container workloads and other applications in the cloud environment. The CN-Series container firewall scales dynamically to extend protection as your infrastructure grows without compromising DevOps speed or agility. Like the VM-Series virtual firewall, the CN-Series container firewall can be procured using Software NGFW Credits and from integrated CSP marketplaces.

Cloud NGFW Managed Firewall Service

The newest member of the Palo Alto Networks of software firewalls is the Cloud NGFW managed firewall service. Cloud NGFW provides a flexible option for deploying application-level (Layer 7) security as a managed service. This versatile NGFW offers cloud-native ease of deployment with the security of a modern NGFW. It integrates with a CSP's native user experience and can be deployed in just a few clicks. Cloud NGFW is available on the AWS marketplace, Azure marketplace, and as a white-labeled service offered by Google Cloud Platform (Google Firewall Plus) and Oracle Cloud Infrastructure (OCI Network Firewall).

Panorama Network Security Management

Panorama network security management streamlines firewall management with easy-to- implement, consolidated policy creation and centralized management features. Now you can easily set up and control firewalls centrally with industry-leading functionality and an efficient rule base, and gain insight into network-wide traffic and threats. These policies provide consistent security across all clouds with no gaps in environments or applications—policies follow applications, while centralized log collection provides easy reviews, audits, and security history.

Key Benefits of Palo Alto Networks

Taken together, Prisma Cloud and Palo Alto Networks NGFWs offer an unparalleled array of benefits that deliver tangible business value.

Secure Applications Across the Entire Lifecycle

Our unique approach is powered by Code to Cloud™ Intelligence, connecting insights from the developer environment through application runtime to reduce risk and prevent breaches. Prisma Cloud contextualizes alerts, prioritizes critical risks, and offers remediation guidance. Now you can achieve comprehensive security across engineering and cloud environments. Prisma Cloud can create a complete application inventory to aid risk prioritization and perform attack path analysis to find interrelated weaknesses and isolate exploitable attack vectors. Most importantly, Prisma Cloud offers code-to-cloud remediation, meaning that you can fix issues wherever they occur from a single dashboard.

Stop Even The Most Sophisticated Threats In Real Time

Palo Alto Networks NGFWs provide the Zero Trust baseline capabilities to fully identify application traffic using built-in identification features such as App-ID™, User-ID, Device-ID, and Content-ID. Zero Trust enforcement can be delivered for inbound, outbound, lateral (East-West), and segmented/microsegmented traffic.

Prevent Known and Unknown Threats: Cloud Delivered Security Services (CDSS), including Advanced Threat Prevention, Advanced WildFire® (sandboxing), Advanced URL Filtering, DNS Security, Enterprise Data lLoss Prevention, and IoT Security, offer agile protection for business-critical applications and databases while meeting compliance requirements.

Industry's First ML-Powered NGFW: ML-Powered NGFWs identify variants of known attacks as well as unknown cyberthreats using ML models, defending against up to 95% of unknown inline threats.

Least Privilege Access and Continuous Trust Verification: Palo Alto Networks' components App-ID, User-ID, and Device-ID massively reduce risk of attack, decrypt SSL/TLS traffic, and prevent malware from entering the cloud in disguise.

Protect All Clouds with Agility—Private, Public, Hybrid

With Palo Alto Networks software firewalls, your staff now has the ability to truly protect any network, all clouds, and any virtualized environment with deep integrations that accelerate deployments and shorten the time for consistent hybrid/multicloud security posture. Now you can have the security foundation to protect any application and workload running anywhere your business needs across the enterprise. Palo Alto Networks software firewalls include deep integrations with all major CSPs, Kubernetes containers, SDN networks, and virtualization hypervisors (see table 1).

Table 1: The Network Security Platform Support for Vendor Offerings

Category	Premium
Cloud Service Providers	Amazon Web Services, Microsoft Azure, Google Cloud Platform, Oracle Cloud, Alibaba Cloud, IBM Cloud
Containers	VMware Tanzu, Rancher, Amazon EKS, Azure Kubernetes Services (AKS), Google Kubernetes Engine, OpenShift
Hypervisors	VMware ESXi, Linux KVM, Microsoft Hyper-V, Nutanix AHV
SDN Networks	Nutanix Flow, VMware NSX, OpenStack, Cisco ACI

Get Automated Best-In-Class Security With Agility

Palo Alto Networks software firewalls automate key processes such as deployment, scaling, and policy changes, so your staff does not have to spend hours and hours doing routine manual operations. Now your DevOps team can securely accelerate cloud migrations with familiar cloud automation and orchestration tools, including AWS CloudFormation, Azure Resource Manager templates, Terraform, Ansible, and Helm Charts. Core network security platform features automate policy changes with Dynamic Address Groups (DAG) and Application Tagging that enable policy migration and policy enforcement as cloud applications dynamically scale up and down within your cloud environments.

Why Palo Alto Networks?

The world of network security has changed for good, and, ready or not, your security strategy has to change, too. Who can you turn to help you navigate this new and challenging landscape?

Palo Alto Networks sets the gold standard for CNAPP with Prisma Cloud. Incorporating all aspects of cloud-native application defense, it grants unmatched insights throughout the application journey. With Prisma Cloud, an intelligence-infused methodology ensures that security is intricately integrated into your digital endeavors.

A recent study by Forrester Consulting shows how Palo Alto Networks software firewalls pay for themselves. Based on interviews and extensive surveying, companies in the study obtained a significant 163% return on investment (ROI) over three years. The Forrester study calculates that a composite organization experiences benefits of $5.98 million over three years versus costs of $2.28 million, adding up to a net present value (NPV) of $3.70 million.

Take the Next Step Toward Securing Your Future

Securing hybrid/multicloud architectures and applications from code to cloud poses challenges that traditional security solutions are not designed to overcome. Prisma Cloud and Palo Alto Networks software firewalls go where the applications and workloads are—on virtual machines, containers, and service provider instances in the cloud—as well as every point in the application development process. To learn more, get a personalized demo and discover how to securely make the most of cloud applications vital for competitive organizations.

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

hackers-are-coming-for-your-cloud-based-applications-wp-111523