Five Key Challenges in Private Cloud Security

Network Security Platform Overcomes Obstacles Delivering Zero Trust

paloalto® NETWORKS | STRATA™ BY PALO ALTO NETWORKS

Table of Contents

Private Clouds—Coming On Strong

The cloud comes in two flavors—public and private—and the distinction between the two is critically important. Public cloud providers sell resources such as computing cycles and storage bytes on a pay-as-you-go basis. The hardware and software that make up the platform are invisible—your team only sees a black-box abstraction that supports your applications and data. The benefits are substantial: You avoid capital investment and costly refresh cycles and gain virtually unlimited scalability, high reliability, dependable data backup, and business agility.

However, the public cloud also takes away control. Your applications and data share infrastructure with other companies, an uncomfortable arrangement for some companies in security-conscious industries such as healthcare and financial services. In addition, abstracting the platform creates problems for highly regulated industries that require validation whenever the system changes in any way that impacts workflows, data, or business logic—examples include medical devices and pharmaceuticals. For these and other reasons, many companies host their sensitive data and core business applications in private clouds and use public clouds to provide scalability and move services closer to their customers.

Public clouds seem to get all the attention, but private clouds have been quietly gaining ground and the pace is accelerating. The average enterprise uses 2.6 public clouds and 2.7 private clouds (see table below). Looking to the future, enterprises are experimenting with twice as many private clouds (2.2) compared to public clouds (1.1). This data clearly shows that most organizations find the best value in a mix of public and private clouds, in other words, a hybrid cloud environment.

	Public	Private
Currently using	2.6	2.7
Experimenting with	1.1	2.2
Total	**3.7**	**4.9**

Number of clouds used on average by enterprises

Private clouds have unique security challenges, as the next section explains.

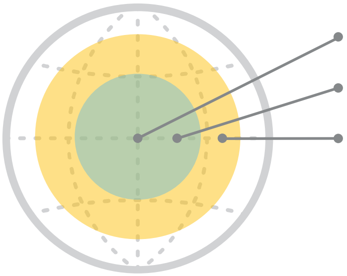
The Growing Challenges of Private Cloud Security

No one would argue that security is ever easy, but there is no doubt private cloud security is becoming progressively more difficult due to a number of factors.

Expanding Attack Surface—The trend to at-home and mobile work creates more and more possible entry points to attack the private cloud. In addition, the growth of the integrated supply chain creates additional risk because vendors and partners may not enforce an adequate level of security at their endpoints. As many as four in ten cyberattacks are now thought to originate in the extended supply chain, not the enterprise itself.

More Sophisticated Threats—Today's advanced threats evade security systems with techniques such as morphing into variants and encrypting traffic between the malware and the external attacker. These attacks either exploit undisclosed vulnerabilities or use of polymorphic malware variants that signature-based detection solutions do not recognize.

Shorter Action Windows—Not only are threats getting better at avoiding defenses, they also do damage much faster than in the past. Malware can begin to encrypt your data in just minutes after gaining entry to the network. Threats proliferate rapidly across networks that lack segmentation security. In a recent Palo Alto Networks Unit 42 internal study, an advanced threat replicated itself into more than 45,000 instances in 30 minutes (see diagram).



5 minutes = 9,864 instances

15 minutes = 27,492 instances

30 minutes = 45,457 instances

Now we look at the challenges of private cloud security, starting with the changing perimeter.

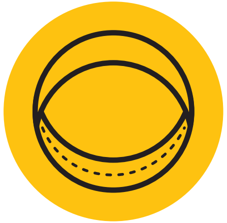
Challenge 1: Cloud Architectures Blur the Concepts of Inside and Outside

The traditional security model assumes there is a distinct boundary between you and the outside world—the security perimeter— that delineates the trusted world (inside) from the untrusted world (the outside). As long as you have good defenses at all the possible entry points, your valuable information should be safe on the inside.

Cloud-based architectures blur the distinction between inside and outside. Now users can be anywhere, not just seated at headquarters within the security perimeter. An application in the local data center may work with data in the cloud, causing traffic flows that continually enter and leave the perimeter.

Here is a helpful analogy: Think of the traditional security model as a simple loop of paper. The loop has two sides—inside and outside—clearly separated from each other. You can prove this by drawing a line lengthwise until you reach the starting point—only one side is marked.

In contrast, the cloud-based architecture is like a mobius strip, a loop with a half twist. Unlike the simple loop, the mobius strip only has one side. No matter where you start, your line will cover the entire surface before returning to the start. In the same way, cloud-based security makes no distinction between inside and outside. No device, user, or application can be trusted until proved to be trustworthy.



The simple loop has two sides, inside and outside.

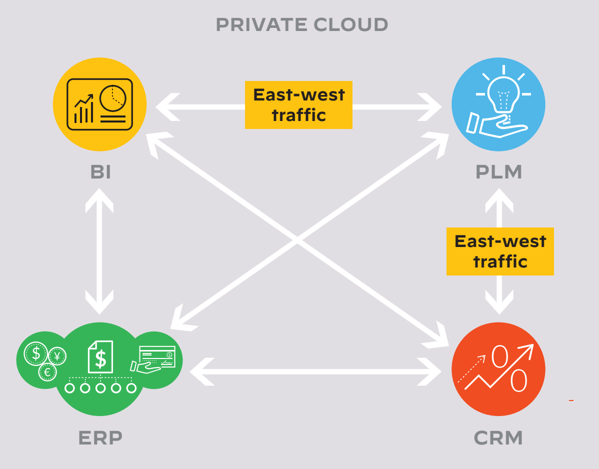
The Mobius strip has only one side—the concepts of inside and outside are meaningless.

Next: Integrated business applications up the ante on private cloud security.

Challenge 2: Integrated Business Applications Strain Legacy Security

Every business is a digital business, relying on a set of core business applications to operate. Product Lifecycle Management (PLM) systems manage the entire lifecycle of a product from inception through engineering, design, and manufacture and serve as a critical business repository for intellectual property. Enterprise Resource Planning (ERP) systems manage key financial business processes from procurement and production planning to manufacturing finished products and order fulfillment. Sales and marketing teams rely on Customer Relationship Management (CRM) and Business Intelligence (BI) to target and engage potential and current customers. The list goes on.

Core business applications do not exist in a vacuum— they are integrated in an interconnected matrix that facilitates collaboration, shortens time to market, and extracts value from the organization's massive amounts of data. These system data integrations generate a significant amount of traffic between the applications—often called east-west traffic—that must be safeguarded against malware, targeted threats, phishing campaigns and other advanced exploits. Legacy security strategies are neither flexible nor powerful enough to meet these challenges.

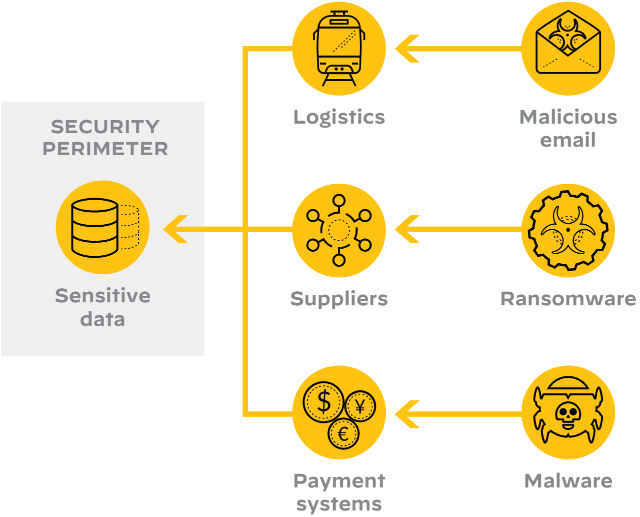


Next: Integrated supply chains create vulnerabilities.

Challenge 3: External Integrations Poke Holes in Private Cloud Perimeter

To meet growing customer and market expectations, traditional linear supply chains are morphing into interconnected supply chain networks. In many cases, suppliers can access portions of the enterprise network directly. These suppliers in turn have their own tightly integrated supply chains, which effectively function as extensions of the parent corporate network. There are other vulnerabilities associated with external integrations, including payment systems and logistics.

These third-party integrations greatly increase the number of nodes that must be secured—a huge expansion of the attack surface and a further blurring of the peripheral boundaries. The result is increased risk of data breaches: According to Accenture, as many as four in ten cyberattacks are now thought to originate in the extended supply chain, not the enterprise itself.



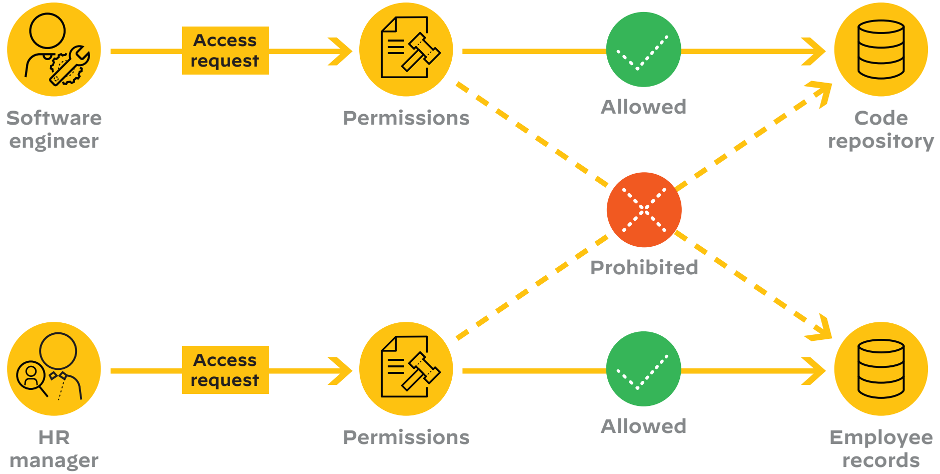
Next: Compliance challenges in private clouds.

Challenge 4: Cloud Environments Strain Existing Compliance Frameworks

All public companies must comply with SOX on both the financial and IT side. Companies in highly regulated industries face considerable risk exposure if they fail to comply with stringent regulations and standards such as HIPAA[1] in healthcare, PCI DSS[2] in retail, and ACH[3] in banking. Moving appliances and data from an on-premises data center to a private cloud can significantly impact compliance strategies.

Developing an effective strategy for compliance in cloud environments requires changes to the security system. A key need is centralized security management to ensure that security managers can harmonize policies across the entire hybrid environment. Another aspect to the compliance challenge is the rising use of Kubernetes containers in cloud application development, which limits the effectiveness of legacy firewalls because they cannot access the containers themselves. Finally, access control needs to be tightened with policies such as least privilege access and multi-factor authentication.

In least privilege access, users are assigned only the permissions needed to fulfill the job duties of their organizational roles. For example, a software engineer needs access to the code repository but is prohibited from accessing employee records.



[1] Health Insurance Portability and Accountability Act.
[2] Payment Card Industry Data Security Standard.
[3] Automated Clearing House.

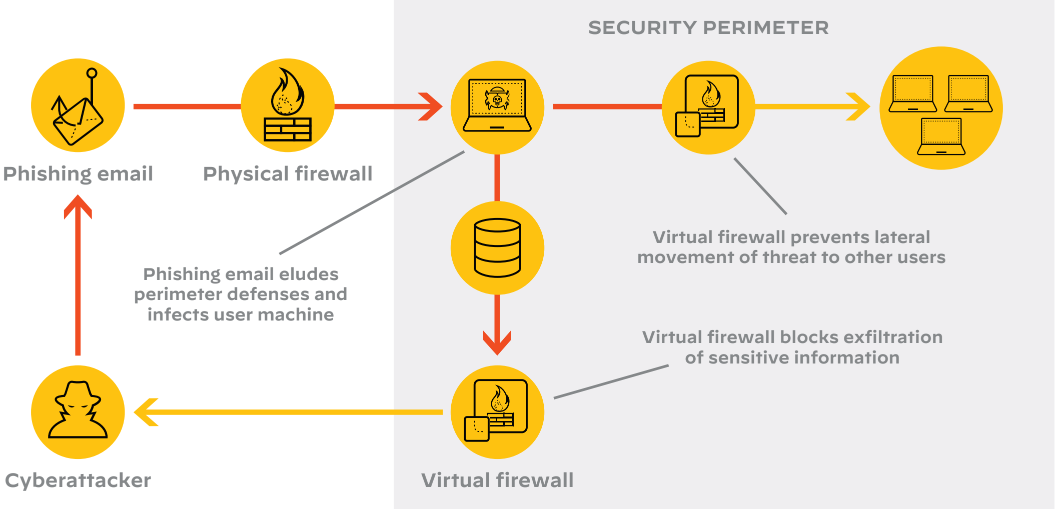
Today's virtualized environments create unique challenges for firewalls, as shown next.

Challenge 5: Virtualized Environments Require Virtual Firewalls

The next-generation firewall (NGFW) serves as the cornerstone of modern network security, guarding against network and transport level threats (layers 3 and 4 of the OSI model) and application level (layer 7) attacks such as distributed denial of service (DDoS), HTTP floods, and SQL injections. Until recently, NGFWs were deployed as physical appliances that were difficult to relocate in the network architecture. That approach works well in static data centers but has limitations in today's dynamic virtualized environments.

Enter the virtual firewall. These versatile software NGFWs have all the capabilities of their physical cousins with the added benefit that they automatically follow applications and workloads within the virtualized environment. Now physical firewalls protect data and applications from external threats at the security perimeter, while virtual firewalls help secure traffic between devices and workloads within the perimeter.

For example, phishing emails often elude perimeter defenses and reach unsuspecting users who accidentally launch the attached malware threats.

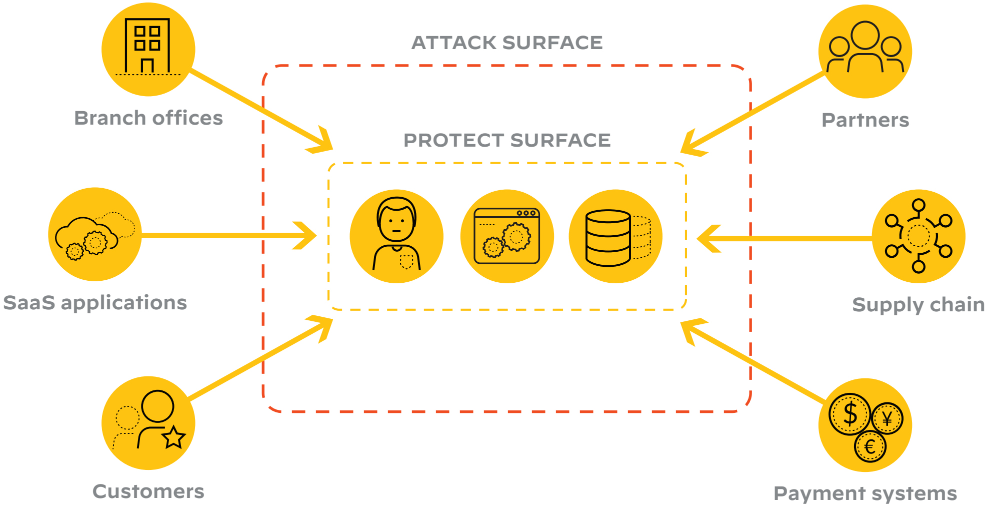

SECURITY PERIMETER
Phishing email
Physical firewall
Phishing email eludes perimeter defenses and infects user machine
Virtual firewall prevents lateral movement of threat to other users
Virtual firewall blocks exfiltration of sensitive information
Cyberattacker
Virtual firewall

Private cloud security requires a Zero Trust approach as discussed on the next page.

The Zero Trust Principle: Never Trust, Always Verify

Zero Trust is a set of best practices that help prevent successful data breaches in virtualized environments by eliminating the concept of trust. Rooted in the principle of "never trust, always verify," implementing a Zero Trust Enterprise Architecture protects modern digital environments by leveraging network segmentation, preventing lateral movement, providing Layer 7 threat prevention, and simplifying granular user-access control.

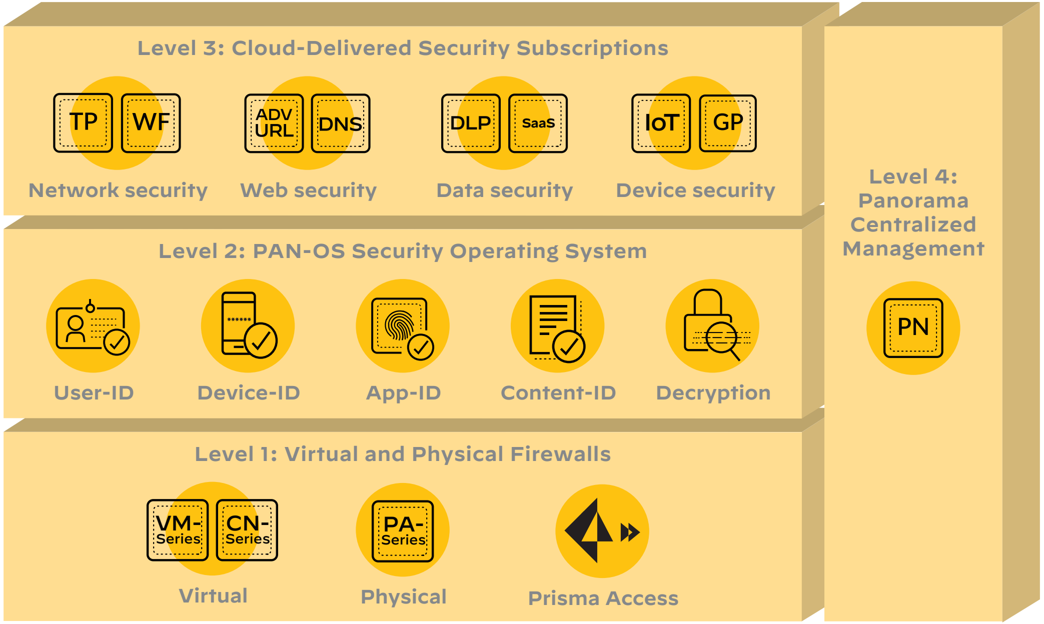
Zero Trust principles start with a fundamental paradigm change. Legacy security revolves around the concept of the attack surface—the sum total of the devices and connections hackers could potentially use to penetrate network defenses. Zero Trust turns that perimeter paradigm on its head by shifting the emphasis from the attack surface to the protect surface, which consists of the data, applications, assets, and services that must be protected. The protect surface is orders of magnitude smaller than the attack surface and is always knowable.



Implementing Zero Trust requires a purpose-built Network Security Platform—our next topic.

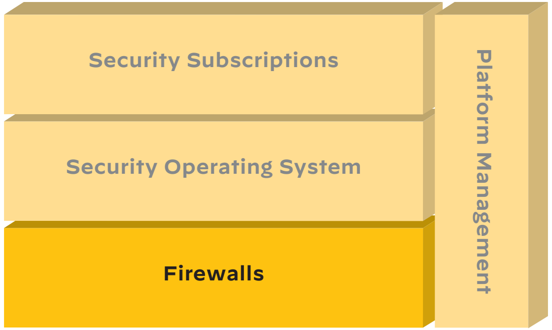
The Network Security Platform—Purpose-Built for Zero Trust

As organizations move to hybrid cloud architectures and decentralize the workforce (branches, home offices, and mobile users), legacy solutions and discrete point products simply cannot do the job. To implement a Zero Trust Enterprise Architecture strategy, you need an integrated offering consisting of NGFWs, firewall operating system, security subscriptions, and centralized management—just what Palo Alto Networks offers in the Network Security Platform.



Now let's break down each level of the platform, starting with firewalls on the next page.

Level 1: Physical and Virtual Firewalls



Our innovation in NGFWs has helped customers around the world secure their businesses against sophisticated attacks. Our focus is to make each day safer for our customers than the one before, with the most intelligent network security solutions that protect your organization from ever-emerging threats. Customers have a choice of robust NGFWs, available in physical, virtual, containerized, and cloud-delivered form factors.

But you need not take our word for it. For the 10th time in a row, Palo Alto Networks has been recognized as a leader in the Gartner® Magic Quadrant™ for Network Firewalls for 2021, ranked highest in Ability to Execute and Completeness of Vision.

VM-Series virtual firewalls flexibly scale to secure deployments in public clouds, private clouds, and SDN environments.

CN-Series is the container-native version of the ML-powered NGFW, designed specifically for Kubernetes environments.

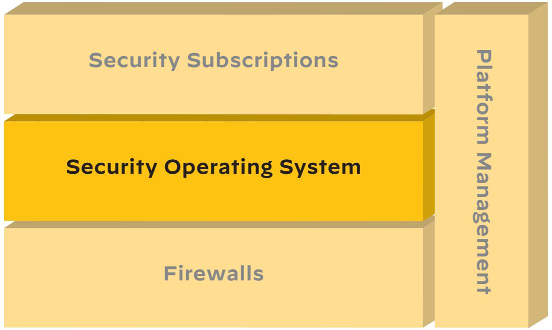
PA-Series phyical firewalls secure high-volume traffic and serve as segmentation gateways for Internet traffic.

Prisma Access consistently secures all apps for remote or mobile users and those located in branch offices.

VM-Series
CN-Series
PA-Series

Next: The firewall operating system plays a pivotal role in Zero Trust security.

Level 2: PAN-OS Firewall Operating System



PAN-OS is our best-in-class firewall operating system that uses machine learning and analytics to uniquely identify users, applications, devices, and content and address new threats that rely on fingerprinting and signatures. PAN-OS continuously updates the machine learning models, particularly helpful for detecting phishing attacks. PAN-OS also collects telemetry, recommends policy and configuration changes to reduce risk, and lessen the chances of human error. The key features of PAN-OS that contribute to Zero Trust private cloud security are described below.

PAN-OS

PAN-OS FEATURES

User-ID

Validate users to make sure they are who they say they are via strong authentication.

Device-ID

Ensure the integrity of every workload and device in the network, including IoT.

App-ID

Use least-privilege access policies to prevent unauthorized access.

Content-ID

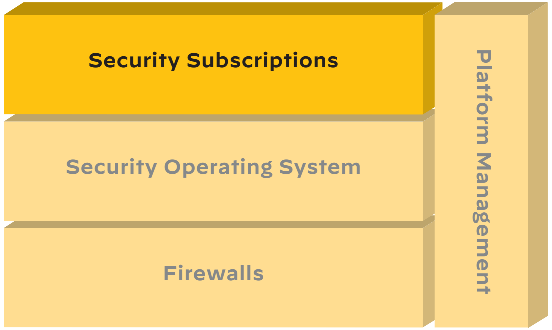
Limit unauthorized transfer of files and sensitive data such as credit cards and SSNs.

Decryption

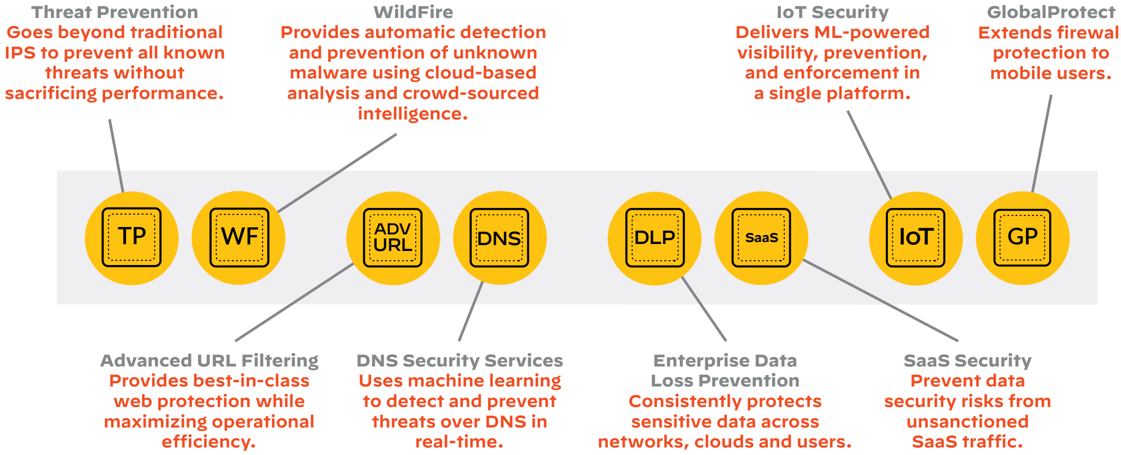
Scan all traffic on the network for malicious activity and data theft.

Next: Cloud Delivered Security Services—flexible and cost-effective way to meet security needs.

Level 3: Cloud Delivered Security Subscriptions



A unique and powerful feature of the Software Virtual NGFWs from Palo Alto Networks is our approach to Cloud Delivered Security Services (CDSS). With Palo Alto Networks, you can choose just the services you require and modify those choices on the fly as your security requirements evolve and change. Now you can have maximum cloud-like control over your security posture and unparalleled flexibility to respond to changes in the threat environment.



Threat Prevention
Goes beyond traditional IPS to prevent all known threats without sacrificing performance.

WildFire
Provides automatic detection and prevention of unknown malware using cloud-based analysis and crowd-sourced intelligence.

IoT Security
Delivers ML-powered visibility, prevention, and enforcement in a single platform.

GlobalProtect
Extends firewall protection to mobile users.

Advanced URL Filtering
Provides best-in-class web protection while maximizing operational efficiency.

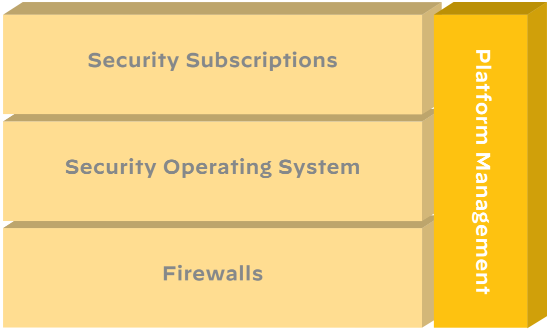
DNS Security Services
Uses machine learning to detect and prevent threats over DNS in real-time.

Enterprise Data Loss Prevention
Consistently protects sensitive data across networks, clouds and users.

SaaS Security
Prevent data security risks from unsanctioned SaaS traffic.

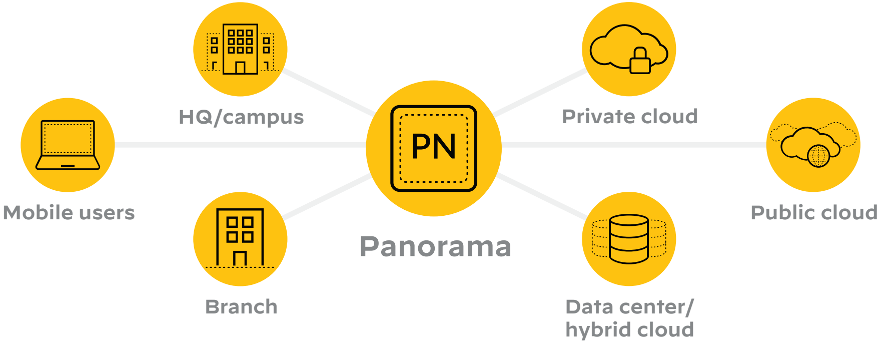
Next: Centralized management—critical for today's complex cloud architectures.

Level 4: Panorama Centralized Management



Large organizations commonly have multiple NGFWs deployed throughout their networks and more often than not, the process of managing and controlling them is cumbersome due to complex configurations and inconsistent management consoles. This situation increases administrative costs and degrades the security posture.

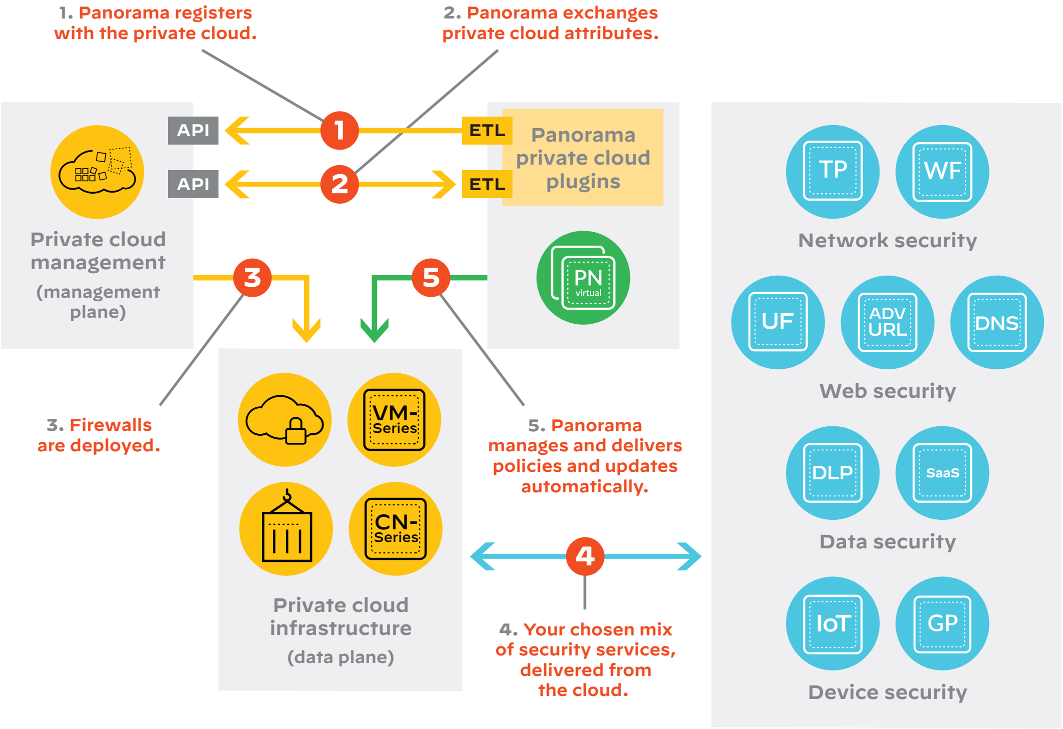
Panorama™ provides centralized management and visibility for all Palo Alto Networks firewalls irrespective of form factor or location, from perimeter firewalls and branch offices to cloud environments and the data center. Using Panorama, administrators can gain insights into applications, users, devices, and content across all network traffic and threats. By centralizing firewall management across the entire network, Panorama reduces the time needed to manage the firewall deployment and allows administrators to efficiently protect their network.



See how the Network Security Platform works in real life on the following page.

The Platform In Action

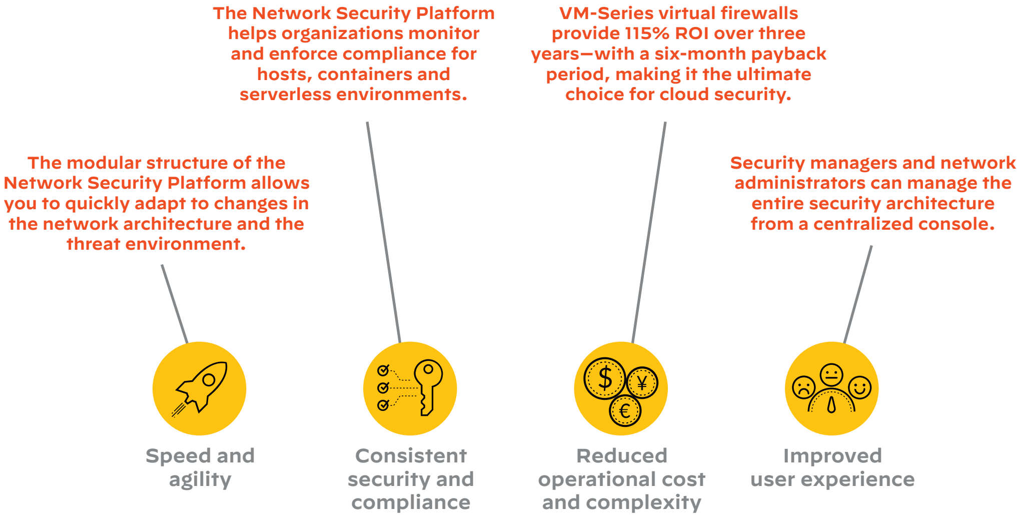
Virtual firewalls from Palo Alto Networks integrate seamlessly with the private cloud controller or SDN orchestrator to automate the process of deploying, managing, and updating your population of Palo Alto Networks virtual firewalls (VM-Series and CN-Series). You benefit by spending less time managing firewalls and maintaining consistent, up-to-date policies in the network.


1. Panorama registers with the private cloud.
2. Panorama exchanges private cloud attributes.
API
API
1
2
ETL
ETL
Panorama private cloud plugins
Private cloud management
(management plane)
3
5
PN
virtual
3. Firewalls are deployed.
VM-Series
CN-Series
Private cloud infrastructure
(data plane)
5. Panorama manages and delivers policies and updates automatically.
4
4. Your chosen mix of security services, delivered from the cloud.
TP
WF
Network security
UF
ADV URL
DNS
Web security
DLP
SaaS
Data security
IoT
GP
Device security

The Network Security Platform delivers real-world benefits—keep going.

The Platform Delivers Tangible Value

This document makes the case for the Network Security Platform as the cornerstone of your *private* cloud security, but the platform is equally well suited for public and hybrid clouds too. Across a broad spectrum of cloud use cases, the Network Security Platform delivers speed and agility, consistent security and compliance, reduced operational cost and complexity, and a better user experience.



Speed and agility

The modular structure of the Network Security Platform allows you to quickly adapt to changes in the network architecture and the threat environment.

Consistent security and compliance

The Network Security Platform helps organizations monitor and enforce compliance for hosts, containers and serverless environments.

Reduced operational cost and complexity

VM-Series virtual firewalls provide 115% ROI over three years—with a six-month payback period, making it the ultimate choice for cloud security.

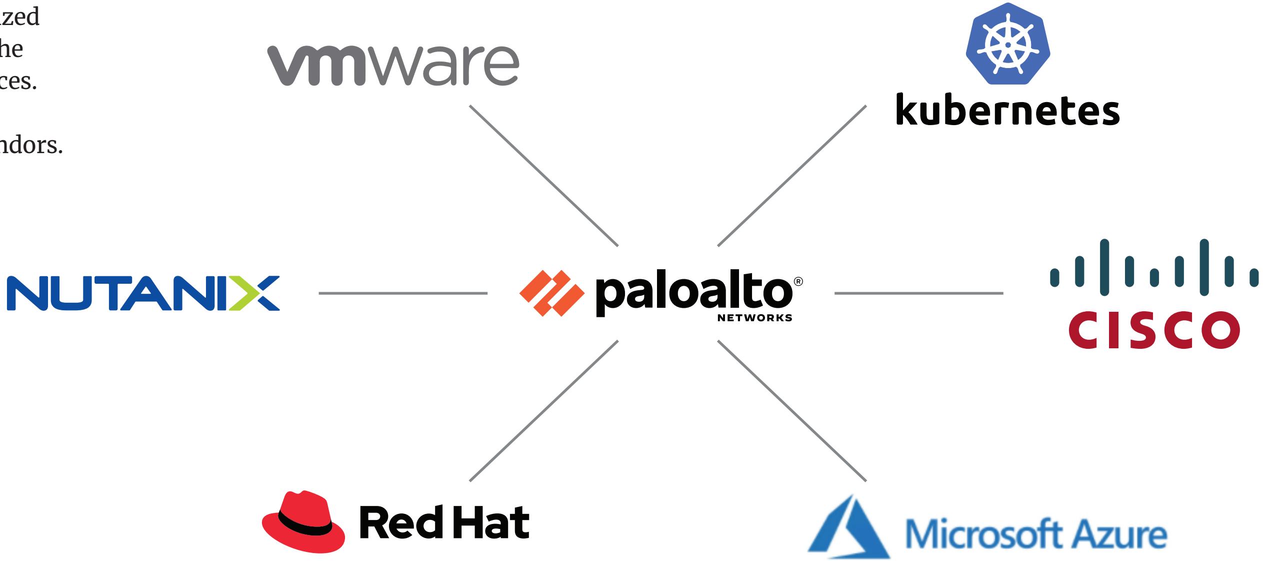
Improved user experience

Security managers and network administrators can manage the entire security architecture from a centralized console.

Our virtual firewalls support a range of virtualization systems, as shown next.

The Platform Integrates with Top Virtualization Systems

Private cloud of necessity implies a virtualized environment. When it comes to choosing the virtualization system, you have many choices. The Network Security Platform supports virtualization offerings from all the top vendors.



Ready to take the next step? See options on the next page.

Take the Next Step Today

The threats to private clouds are accelerating in virulence, volume, and sophistication. The traditional approach of relying on a security perimeter to divide the world neatly into trusted and untrusted zones simply does not fit today's hybrid cloud architectures and cloud-native development strategies. Instead, effective cloud security requires multiple smaller perimeters as well as a shift to Zero Trust principles.

In response to the challenges of distributed architectures, more virulent threats, and shorter time windows for detection and mitigation, Palo Alto Networks has created the VM-Series virtual NGFW and the CN-Series container NGFW, breakthrough products that enable effective security for private, public, and hybrid clouds. Together with the PA-Series physical firewalls, they constitute the foundation of the Network Security Platform, our innovative and flexible framework for cloud security.

You can learn more about how Palo Alto Networks can benefit your organization, there are no-obligation steps you can take right now—just click on the boxes below. Private clouds are coming on strong—and for competitive organizations ready to secure them, the future looks bright for more competitiveness and innovation. Palo Alto Networks looks forward to winning your trust so we can be your security partner of choice.

Take an ultimate test drive

Request a personalized DEMO

Use VM-Series free for 30 days

Try CN-Series QuikLabs

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