

Protect Hybrid Cloud Infrastructure with Our Firewall Platform Approach



Hybrid is for real—organizations of all sizes and across all industries are migrating to hybrid cloud architectures.

Legacy solutions simply cannot address challenges such as limited visibility, increased complexity and more virulent threats.

85% of IT professionals see hybrid cloud as the ideal IT operating model.

Source: [Nutanix Enterprise Cloud Index, Nutanix, 2019.](#)

Now, organizations of all sizes can automatically deploy security across any combination of on-premises and cloud resources, no matter how complex. Our platform incorporates machine learning (ML) and automation to consistently and effectively protect against known and unknown threats, including ransomware, cryptoworms, cryptojacking and more.

The Palo Alto Networks Firewall Platform Approach

Centralized Management



Panorama Management

Panorama™ reduces complexity with centralized management to gain insight into network-wide traffic, logs and threats.

Cloud-Delivered Security Services



Threat Prevention

prevents known threats and zero-day exploits.



WildFire® malware prevention

cloud-based threat analysis service detects and prevents highly evasive threats and malware.



URL Filtering

enables safe access to the internet.



DNS security disrupts command-and-control (C2) activity and other DNS-based attacks.



IoT Security offers visibility, prevention and enforcement for IoT and OT devices.



Enterprise Data Loss Prevention protects sensitive data and streamlines compliance.



Prisma® SaaS delivers complete visibility and granular enforcement for SaaS applications.



GlobalProtect™ extends NGFW protection to all end user devices.



SD-WAN enables secure, cloud-delivered branches.

Firewall Form Factors



Hardware PA-Series

PA-Series Next-Generation Firewalls (NGFWs) protect the entire network perimeter, from headquarters to branch offices, data centers, and your mobile and remote workforce.



Software VM-Series | CN-Series

VM-Series Virtual NGFWs provide all the ML-powered capabilities of the PA-Series in a virtual machine form factor.
CN-Series Container NGFWs implement threat prevention in Kubernetes®/container environments.



Cloud Service Prisma Access

Prisma Access delivers the coverage of our ML-Powered NGFWs to maintain traffic visibility and policy enforcement from a cloud-based security infrastructure.

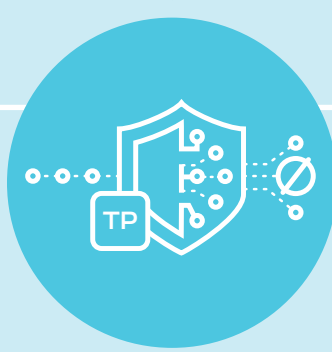
Addresses Hybrid Cloud Security Challenges



See your infrastructure clearly, end to end

Eliminate blind spots through consistent visibility across on-premises, virtualized and multi-cloud environments
Enforce security policies uniformly across the hybrid environment
Define security policies based on application context, not IP address or port number

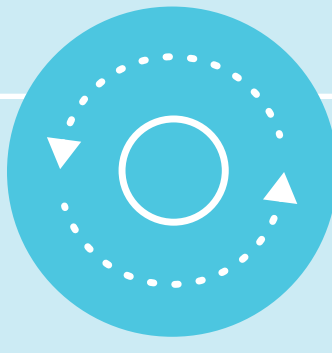
Enabling technology: Layer 7 (application) visibility



Outsmart even the smartest threats

Identify both known and unknown threats with a high rate of accuracy
Intervene at key stages in the attack lifecycle to prevent infiltration, stop C2 communication, block evasion techniques, and stop exfiltration
Stay ahead of increasingly sophisticated attacks using automation and AI

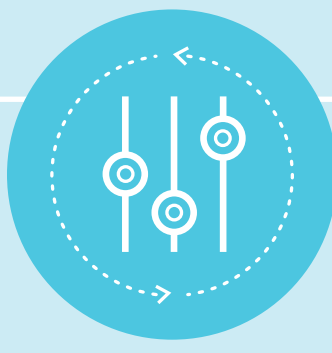
Enabling technology: ML-powered intelligent threat prevention



Respond quickly and effectively at cloud speed

Dynamically auto scale firewalls according to meet resource demands
Apply security policies automatically to new workloads
Incorporate security deployment into existing DevOps and infrastructure provisioning processes

Enabling technologies: Automation and scalability



Manage complexity down to size

Manage security across discrete clouds and on-premises environments from a single location
Simplify day-to-day operations and troubleshooting
Eliminate the need to manage different policy sets for different parts of the environment

Enabling technology: Centralized security management

Get started securing your hybrid infrastructure. Sign up for your personalized demo today.