Palo Alto Networks

Secure today, for a better tomorrow

paloalto® NETWORKS

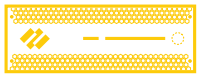
Palo Alto Networks is the only cybersecurity partner that frees digital enterprises from having to choose between the security they need today or being ready for what comes next. Our commitment is to deliver both, enabling security without compromise.

Here's how we protect you.

STRATA
BY PALO ALTO NETWORKS

Strata

Secure your enterprise against tomorrow's threats, today. Protect users, applications, and data anywhere with intelligent network security from Palo Alto Networks.



Next-Generation Firewall

PA-Series

VM-Series

CN-Series

App-ID

Content-ID

User-ID

Device-ID

Panorama

DNS Security

Enterprise DLP

Threat Prevention

URL Filtering

WildFire

IoT Security

GlobalProtect

5G Security

SD-WAN

Next-Generation Firewalls

Physical, Virtual, and Cloud-Delivered Protection

Confidently embrace digital transformation by consolidating multiple disconnected security products into a simple network security solution. Our ML-Powered Next-Generation Firewall (NGFW) is a consistent, integrated, and best-in-class network security solution delivered in physical, virtual, containerized, and cloud-based form factors—all managed centrally. The industry's first ML-Powered NGFW enables you to prevent unknown threats, see and secure everything—including IoT—and reduce errors with automatic policy recommendations. Secure your campus, hybrid cloud, branches, and mobile users with the nine-time Leader in the Gartner Magic Quadrant for Network Firewalls.

PA-Series

Physical Next-Generation Firewall

PA-Series Physical NGFWs are purpose-built for high-performance security processing with multiple high-speed interfaces for maximum throughput. PA-Series NGFWs provide visibility, security, and control of enterprise network traffic (including IoT and 5G traffic) for the data center, campus perimeter, branch offices, industrial installations, and mobile 5G infrastructure.

VM-Series

Virtual Next-Generation Firewall

VM-Series Virtual NGFWs are ideal for environments where it is difficult or impossible to deploy hardware firewalls. VM-Series firewalls provide all the capabilities of Palo Alto Networks NGFWs in a virtual form factor that delivers inline network security and protection against advanced threats to consistently safeguard public and private clouds, virtualized data centers, and branch locations.

CN-Series

Container Next-Generation Firewall

CN-Series Container NGFWs provide all the capabilities of Palo Alto Networks NGFWs in a container form factor to move security controls as close as possible to container workloads and gain critical container context for use in policy formulation. This allows the CN-Series firewall to enforce threat prevention and other advanced network security services, such as IPS and URL filtering, on allowed traffic—whether outbound, inbound, or lateral—between container pods as well as between container applications and legacy workloads, such as virtual machines and bare metal servers.

App-ID

Application Classification Feature

App-ID™ is a patented traffic classification technology only available on Palo Alto Networks firewalls. It determines an application's identity irrespective of port, protocol, TLS/SSL/SSH encryption (including TLS 1.3 and HTTP/2), or any other evasive tactic the application may use. It applies multiple classification mechanisms—including application signatures, application protocol decoding, and heuristics—to your network traffic stream to accurately identify applications. When an application is identified, a policy check lets you determine how to treat it. For example, you can block; allow and scan for threats; inspect for unauthorized file transfer and data patterns; or shape using QoS. Moving from port-based legacy firewall rules to App-ID-based rules dramatically reduces the opportunity for attack. Policy Optimizer, a feature within PAN-OS®, makes it easy by using simple workflows and intelligence gathered by PAN-OS to move from legacy rules to App-ID-based controls and strengthen your security.

Content-ID

Content Classification Feature

Content-ID™ technology employs multiple advanced threat prevention technologies to conduct a complete analysis of all allowed traffic in a single scan. With Content-ID, our Next-Generation Firewalls can block vulnerability exploits, buffer overflows, and port scans as well as protect against attackers' evasion and obfuscation methods. Our cloud-delivered security services such as Threat Prevention and URL Filtering leverage Content-ID to stop outbound malware communications, block access to known malware and phishing download sites, and reduce the risks associated with the transfer of unauthorized files and data. Content-ID enables comprehensive threat protection in a single scan of network traffic, optimizing your NGFW performance.

User-ID

User Classification Feature

User-ID™ technology helps define policies that safely enable applications based on users or groups of users in outbound or inbound directions. For example, you can allow only the IT department to use SSH, telnet, and FTP tools on standard ports. With User-ID, policy follows your users no matter where they go—headquarters, branch office, or home—and whichever devices they use. You can get visibility into application activity at the user level, not just by IP address, and generate informative reports on user activities. You can also enforce multi-factor authentication (MFA) for your users without any changes to your applications.

With User-ID, you can prevent corporate credentials from leaving your enterprise and stop attackers from using stolen credentials to move laterally in your network. Dynamic User Groups (DUGs) allow administrators to dynamically change user access or enforce MFA, whether due to new indicators of compromise or a business need, such as granting temporary access to a set of users.

Device-ID

Device Classification Feature

Device-ID™ is a new policy construct that allows administrators to write policies based on device characteristics. It enables security teams to understand how events relate to devices and write policies associated with devices instead of their IP addresses or locations, which can change over time. With Device-ID, our NGFWs can restrict IoT devices to known good behavior, block devices on the network with outdated OS, quickly trace threats back to individual devices, and use "device" as a dimension in other policy types. You can use Device-ID in security, decryption, quality of service (QoS), and authentication policies. Device-ID is available on Panorama and all ML-Powered NGFWs (except the VM-50 and CN-Series) running PAN-OS 10.0 or later.

Panorama

Management Solution

Panorama™ provides a centralized network security management solution for all your Palo Alto Networks firewalls irrespective of form factors and locations. It reduces complexity by simplifying the configuration, deployment, and management of your security policies. Panorama provides centralized visibility and comprehensive insights into your network traffic, logs, and threats. It reduces administrative workload by helping manage updates, automating threat responses through policy-based actions, and using API-based integrations with third-party systems.

Network security teams can regain visibility and control over their security posture, consolidate tooling, and automate network security. Panorama manages rules and dynamic security updates so you can keep up with ever-evolving network threats. You can simplify operations by effectively managing software updates and automate the scheduling of content updates that, in turn, help maintain the best possible overall security posture. With a single management solution, you can fully utilize all the capabilities of your security investments and attached subscriptions, all from one place.

DNS Security

Prevention of Attacks Using DNS

Eighty percent of malware uses DNS to establish a command-and-control (C2) channel. Attackers often hide in DNS because the traffic volume is so high that many organizations lack the tools to monitor it properly. To protect against threats over DNS, you need superior detection combined with analytics that empower security personnel with the context to craft policies and respond to threats quickly and effectively. Our DNS Security service applies predictive analytics, machine learning, and automation to block attacks that use DNS. Tight integration with our NGFWs gives you automated protection, prevents attackers from bypassing security measures, and eliminates the need for independent tools or changes to DNS routing. Rapidly predict and prevent malicious domains, neutralize threats hidden in DNS tunneling, and apply automation to quickly find and contain infected devices.

DNS Security reporting enables deeper insights into threats than ever, delivering full visibility into DNS traffic at macro, industry, and organizational levels. Cloud-based protections scale infinitely and are always up to date, giving your organization a critical new control point from which to stop attacks that use DNS. Palo Alto Networks combines best-in-class detection with the analytics and inline enforcement necessary to protect DNS in real time.

Enterprise Data Loss Prevention

Data Protection and Compliance

Palo Alto Networks Enterprise Data Loss Prevention (DLP) is the industry's first cloud-delivered security service that discovers, monitors, and protects sensitive data, such as personally identifiable information (PII) and intellectual property (IP), across every network, cloud, and user. A single cloud service and predefined policies deliver data privacy and compliance easily and consistently, whether on-premises, across remote workforces, or in the cloud. Natively integrated into existing Palo Alto Networks control points, our Enterprise DLP drastically lowers TCO by three times when compared to complex legacy DLP products, simplifying deployment and maintenance while eliminating the need for additional infrastructure.

Threat Prevention

Exploit, Malware, and C2 Prevention

Our Threat Prevention service automatically stops known client- and server-side vulnerability exploits with IPS capabilities, offers inline malware protection, and blocks outbound C2 traffic. Threat Prevention inspects all traffic for threats, regardless of port, protocol, or encryption, so nothing gets swept under the rug. The included IPS protections are based on signature matching and anomaly detection, with the ability to import and automatically apply signatures and rules in popular formats, such as Snort and Suricata®. By looking for threats at all points within the cyberattack lifecycle, not just when they first enter the network, Threat Prevention provides layered defense founded in the Zero Trust model.

A uniform signature format for all threats ensures speedy processing by enabling all analysis to be performed in one integrated scan, eliminating redundant processes common to offerings that use multiple scans. Threat Prevention combs through each packet as it passes through our NGFWs, looking closely at byte sequences within packet headers and payloads. From this analysis, we can identify important details about each packet, including the application used, its source and destination, whether the protocol is RFC-compliant, and whether the payload contains an exploit or malicious code. Beyond individual packets, we also analyze the context of the arrival order and sequence of multiple packets to catch and prevent evasive techniques. All this happens in one scan so your network traffic stays as fast as you need it to be.

URL Filtering

Malicious Site and Phishing Prevention

URL Filtering enables you to safely use the web for business needs. The cloud-delivered service goes beyond basic web filtering by identifying threats through a unique combination of static analysis and machine learning. Phishing pages and JavaScript-based attacks are identified in milliseconds. With thousands of new malicious URLs created every day, malicious webpages must be identified instantly to protect against web-borne attacks. Automated protections block access to malicious sites that deliver malware and steal credentials, stopping any data loss. Minimize your organization's exposure to attack by extending firewall policy and benefit from protections that are always up to date. Application- and user-based policies simplify complex web security rules, reducing operational overhead.

To accurately determine categories and risk ratings, URL Filtering scans websites and analyzes their content using machine learning with static and dynamic analysis. It classifies URLs into benign or malicious categories, which you can easily build into NGFW policy for total control of web traffic. Upon discovery of newly categorized malicious URLs, URL Filtering blocks them immediately, requiring no analyst intervention.

WildFire

Malware Prevention

WildFire® malware prevention service is the industry's most advanced cloud-based analysis and prevention engine for highly evasive zero-day exploits and malware. Going beyond traditional approaches used to detect unknown threats, WildFire brings together the benefits of multiple complementary techniques for high-fidelity and evasion-resistant discovery, including dynamic analysis, static analysis, machine learning, and bare metal analysis. WildFire continuously delivers innovative new detection engines with none of the operational impact common to traditional "hold and release" network sandboxing solutions. It saves time and resources for security teams by providing detailed insight into the behavior of identified threats, indicators of compromise, and how they were blocked.

Drawing on threat models continually honed in the cloud, WildFire also powers a revolutionary inline machine learning-based engine, delivered within physical and virtual NGFWs. This innovative signatureless capability prevents malicious content—such as unknown portable executable files and dangerous fileless attacks stemming from PowerShell—completely inline, with no cloud submission step.

The WildFire community serves as one of the industry's largest enterprise malware analysis networks, leveraging threat intelligence submitted from networks, endpoints, clouds, and third-party partners. When any WildFire subscriber discovers zero-day exploits or malware, the service automatically orchestrates enforcement of high-fidelity, evasion-resistant protections for all subscribers in seconds following first discovery anywhere in the world.

IoT Security

IoT Security for Enterprises and Healthcare

IoT Security is the industry's most comprehensive IoT security solution, delivering ML-powered visibility, prevention, and enforcement in a single platform. It is the only solution in the market that uses machine learning with our leading App-ID technology and crowdsourced telemetry to profile all devices—even those not seen before—for discovery, risk assessment, vulnerability analysis, anomaly detection, and trust-based policy recommendations. It also delivers built-in prevention instead of taking an alert-only approach, keeping all devices safe from all threats and vulnerabilities. Additionally for healthcare customers, the IoT Security solution enables maximum ROI and patient experience with deep visibility, focused operational device utilization insights, and enhanced security for medical devices.

IoT Security is effortless to deploy and provides seamless integration into existing workflows, reducing the burden on infrastructure, security, and network teams. For example, the subscription augments existing security teams with IoT intelligence, using a rich portfolio of native integrations across asset management (CMMS/ITSM), network access control (NAC), security information and event management (SIEM), and industry-specific device intelligence databases.

IoT Security supports use cases in the enterprise, medical, ICS/SCADA systems, building management systems, smart city infrastructure, oil and gas, utilities, and transportation verticals.

GlobalProtect

Mobile User Security

GlobalProtect™ network security for endpoints extends our market-leading threat prevention capabilities to mobile workers, regardless of their location. Prisma Access uses GlobalProtect to provide clientless and client-based encrypted access for remote users. This allows organizations to extend corporate access control policies to unmanaged devices as well as access to applications in the cloud and data centers. It enables support for per-app VPN using integrations with enterprise mobility management offerings, including AirWatch®, Microsoft Intune®, and MobileIron®.

Prisma Access provides Zero Trust network access for remote workers. It combines role-based access control (RBAC), digital experience monitoring (DEM), and threat detection into a single cloud-delivered platform that delivers massive scalability and consistent secure remote access to every remote user. With more than 100 service locations globally, Prisma Access offers industry-leading SLAs to guarantee availability as well as high-performance connectivity to applications and services from anywhere in the world. Prisma Access enables organizations to set and enforce granular policies restricting access to services and applications based on user identity, role, location, and connecting device posture through a single pane of glass. It consolidates more than 10 networking and security products into a single service with advanced security capabilities that include anti-malware, exploit detection, and credential abuse prevention by inspecting all application traffic—across all ports—at all times, allowing you to create and enforce more efficient security policies.

5G-Native Security

Security for 5G Networks

As today's enterprises undergo digital transformation, they'll be looking for 5G networks to drive true Industry 4.0 transformation, leveraging the cloud, automation, AI, and IoT. With 5G networks comes a greater reliance on cloud and edge compute, creating a highly distributed environment that spans multi-vendor and multi-cloud infrastructures. Palo Alto Networks 5G-native security offers the most granular security for your cloud native 5G core, distributed edge clouds, and Enterprise 5G networks. 5G-native security offers a simple, and tightly integrated 5G security platform that leverages automation, Kubernetes® native orchestration, and integration with open APIs for operational simplicity. Leverage automated, cloud-delivered threat intelligence powered by ML to defend against adversaries operating at 5G speeds as well as prevent known and unknown threats in real-time across 5G networks on a global scale. Unlock new revenue streams by offering secure "as a service" offerings for 5G slice security, enterprise 5G security, and multi-access edge computing (MEC) security.

5G-native security is supported on physical firewall appliances in our PA-7000 Series and PA-5200 Series NGFWs, in our VM-Series Virtual NGFWs for virtualized 5G deployments, and in our CN-Series for containerized cloud native 5G deployments. This means that if you already use our NGFWs, you can continue to use the same platform to secure service provider 5G infrastructure or enterprise 5G networks.

SD-WAN

Secure Branch Connectivity

The SD-WAN subscription on our NGFWs enables you to easily adopt an end-to-end SD-WAN architecture with natively integrated, world-class security and connectivity. Using Prisma Access as the SD-WAN hub, you can optimize the performance to enhance user experience. In addition, Prisma Access can be consumed as a service, eliminating the complexity of building the SD-WAN hub infrastructure. Alternatively, you can build the hub and interconnect infrastructure yourself using Palo Alto Networks NGFWs.

PRISMA®
BY PALO ALTO NETWORKS

Prisma

Prisma® is the industry's most comprehensive cloud security portfolio. Accelerate your digital transformation with a product suite designed to secure the clouds of today against the threats of tomorrow.


Prisma SaaS


Prisma SD-WAN


Prisma Access


Prisma Cloud

Prisma SaaS

SaaS Application Security and Compliance

Prisma SaaS enables safe cloud adoption by providing visibility, compliance controls, and security consistently across software-as-a-service (SaaS) applications and sensitive data in the cloud. It helps minimize the use of shadow IT; secure access to corporate SaaS applications like Microsoft 365™, Salesforce®, Google Workspace™, Slack®, and Box; and mitigate the risk of a data breach in the cloud.

Prisma SaaS helps safeguard your organization and your data against cloud cyber risks, enabling you to safely adopt SaaS applications and safely store sensitive data in the cloud. As an integrated functionality of Palo Alto Networks NGFWs, the service is tied tightly to the broad company-wide security, providing streamlined deployment that surpasses the piecemeal approach of point controls like a cloud access security broker (CASB).

Prisma SD-WAN

Secure Cloud-Delivered Branch

Prisma SD-WAN is the industry's first next-generation SD-WAN solution that makes the secure cloud-delivered branch possible, delivering an ROI of up to 243%. Unlike legacy SD-WAN solutions that introduce cost and complexity, Prisma SD-WAN ensures an exceptional user experience with application-defined policies and simplifies both network and security operations using machine learning and automation.

Prisma Access

Cloud-Delivered Mobile User Security

Prisma Access transforms network security with the industry's most complete cloud-delivered platform, allowing organizations to securely enable remote workforces. Legacy network security products do not provide access to and protection for all applications—instead, they leave significant gaps in security coverage and cannot enable the work-from-anywhere experience organizations demand. Only Prisma Access fully inspects all application traffic—including web-based, non-web-based, and SSL/TLS-encrypted apps—bidirectionally on all ports, whether communicating with the internet, the cloud, the data center, or between branches, decreasing the likelihood of a data breach by 45%.

Additionally, Prisma Access provides more security coverage than any other solution, consolidating multiple point products into a single platform that includes firewall as a service (FWaaS), Zero Trust network access (ZTNA), CASB, secure web gateway (SWG), and more, all managed through a single console. Prisma Access is built upon a massively scalable network leveraging the combined infrastructure of Amazon Web Services (AWS®) and Google Cloud, with more than 100 service access points across 76 countries. This allows Prisma Access to provide ultra-low latency backed by industry-leading SLAs to ensure a great digital experience for end users.

Prisma Cloud

Cloud Native Security Platform

Prisma Cloud is the comprehensive Cloud Native Security Platform (CNSP) with the industry's broadest security and compliance coverage for the entire cloud native technology stack, applications, and data across hybrid and multi-cloud environments. Prisma Cloud protects cloud native applications across hosts, containers, serverless, and other platform-as-a-service (PaaS) offerings across cloud platforms. It dynamically discovers resources as they are deployed and correlates data that cloud services provide (resource configurations, flow logs, audit logs, host and container logs, etc.) to deliver security and compliance insights for your cloud environments and applications. It uses machine learning to profile user, workload, and application behaviors to prevent advanced threats.

With the industry's most complete library of compliance frameworks, it vastly simplifies the task of maintaining compliance. Prisma Cloud provides this through deep context-sharing that spans infrastructure, PaaS, users, development platforms, data, and application workloads. Seamless integration with security orchestration tools ensures rapid remediation of vulnerabilities.

For full-lifecycle security, Prisma Cloud integrates across DevOps tool chains for vulnerability management and compliance. With a broad set of DevOps plugins, spanning IDEs, SCM, CI, and CD technologies, your security teams and DevOps can secure infrastructure and applications covering infrastructure as code (IaC) templates, hosts, images, and functions.

CORTEX®
BY PALO ALTO NETWORKS

Cortex

Cortex® is the industry's most comprehensive product portfolio for security operations, empowering enterprises with leading attack surface management along with best-in-class prevention, detection, automation, and response capabilities.

AutoFocus

Cortex XDR

Cortex XSOAR

CRYPSIS™
A PALO ALTO NETWORKS COMPANY

Crypsis

EXPANSE
A PALO ALTO NETWORKS COMPANY

Expanse

AutoFocus

Contextual Threat Intelligence

AutoFocus™ contextual threat intelligence service gives you instant access to our massive repository of high-fidelity threat intelligence so you can consume it as a feed. Crowdsourced from the industry's largest footprint of network, endpoint, and cloud intelligence sources, you get unique insight into real-world attacks. Every threat is enriched with the deepest context from world-renowned Unit 42 threat researchers. Your analysts save significant time with intelligence embedded in any tool through a custom threat feed and agile APIs.

Cortex XDR

Extended Detection and Response

Cortex XDR™ is the industry's first extended detection and response platform that spans key security data sources to stop modern attacks. With Cortex XDR, you can cut through the noise and focus on real threats using intelligent alert grouping and incident scoring. Your team can slash complexity and replace disjointed point products with a unified platform for prevention, detection, investigation, and response.

Cortex XDR automatically blocks attacks with ironclad endpoint protection and accurately detects threats across your environment by analyzing rich data with behavioral analytics. It provides a complete picture of each incident and reveals the root cause, allowing you to investigate threats up to eight times faster than before. The unique offering simplifies every stage of security operations, from alert triage to threat hunting, reducing the need for highly experienced security analysts and significantly lowering the time to detect and respond to threats. Tight integration with enforcement points accelerates containment, enabling you to stop the stealthiest attacks before the damage is done.

Cortex XSOAR

Extended Security Orchestration, Automation, and Response

Cortex XSOAR supercharges SOC efficiency with the industry's most comprehensive security orchestration, automation, and response (SOAR) platform. Security leaders can transform any aspect of their operations with a unified approach to case management, automation, real-time collaboration, and threat intelligence management. Teams can manage alerts across all sources, standardize processes with playbooks, take action on threat intelligence, and automate response for any security use case—resulting in 90% faster response times and a 95% reduction in alerts requiring human intervention.

Crypsis

Incident Response Services

The Crypsis Group, a Palo Alto Networks company, is a security advisory firm working to create a more secure digital world by providing the highest quality incident response, risk management, and digital forensic services. We help and protect our clients by defending against and responding to severe cyberthreats. Our global response capability, constant technological innovation, and elite cybersecurity expertise enable us to stay ahead of the rapidly evolving threat landscape.

Expanse

Attack Surface Management

Expanse is an automated attack surface management (ASM) platform that provides a complete and accurate inventory of an organization's global internet-facing assets and misconfigurations to continuously discover, evaluate, and mitigate an external attack surface; flag risky communications; evaluate supplier risk; or assess the security of M&A targets.

© 2021 PALO ALTO NETWORKS | 3000 Tannery Way | Santa Clara, CA 95054 | Support: +1.866.898.9087 | www.paloaltonetworks.com