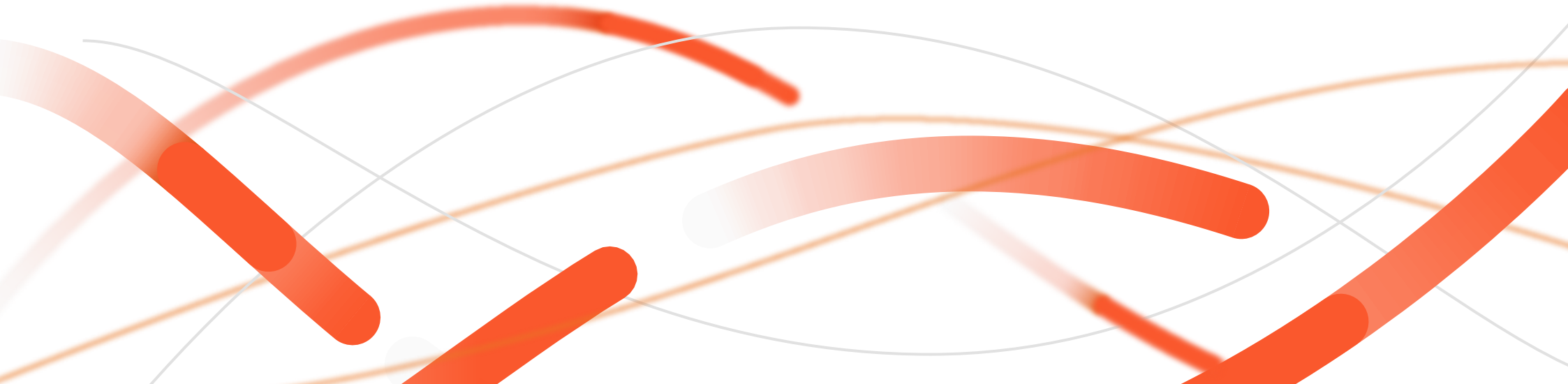
paloalto NETWORKS

Palo Alto Networks

Making Each Day Safer and More Secure than the One Before



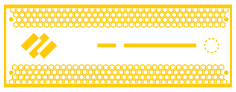
Palo Alto Networks, the global cybersecurity leader, is shaping the future with technology that is transforming the way people and organizations operate. Our mission is to be the cybersecurity partner of choice, protecting our digital way of life. We help address the world's greatest security challenges with continuous innovation that seizes the latest breakthroughs in artificial intelligence, analytics, automation, and orchestration. By delivering an integrated platform and empowering a growing ecosystem of partners, we are at the forefront of security, protecting tens of thousands of organizations across clouds, networks, and mobile devices.

Here's how we protect you …

STRATA™
BY PALO ALTO NETWORKS

Secure the Enterprise

Palo Alto Networks Strata™ Firewall Platform is a consistent, integrated, and effective network security solution delivered in physical, virtual, and cloud-based form factors.


Next-Generation Firewall


App-ID


Content-ID


User-ID

Panorama

DNS Security

Threat Prevention

URL Filtering

WildFire


Zingbox

GlobalProtect

SD-WAN

Next-Generation Firewalls

Physical, Virtual, and Cloud-Delivered Protection

Palo Alto Networks Next-Generation Firewalls stop cyberattacks while simplifying security. Innovations are tightly integrated into the Strata™ Firewall Platform, replacing disconnected point products. Physical, virtual, and cloud-delivered deployment options provide consistent protection wherever your data and apps reside. Securely transform your network while protecting against the most sophisticated attackers with the world's best cybersecurity.

App-ID

Application Classification Technology

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, SSH/SSL encryption, 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™ technology-based ones greatly reduces the opportunity for attack. Policy Optimizer, a feature within PAN-OS, makes it easy. It uses 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 Technology

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, protect against attackers' evasion and obfuscation methods, 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.

User-ID

User Classification Technology

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 tools such as SSH, telnet, and FTP on standard ports. With User-ID, policy follows your users no matter where they go—headquarters, branch office, or home—and what device they may use. You can generate informative reports on user activities using custom or predefined templates.

Visibility into application activity at the user level, not just by IP address, lets you more effectively enable the applications traversing your network. You can align application usage with business requirements and, if appropriate, inform users they are violating policy or block their application usage outright. Dynamic User Groups (DUGs) allow admins to dynamically change user access based on changes in circumstances, whether the change is due to new indicators of compromise or due to a business need, such as granting temporary access to a set of users.

Panorama

Management Solution

Panorama™ network security management provides a centralized administration solution for all your Palo Alto Networks firewalls irrespective of their form factors and locations. It reduces complexity by simplifying the configuration, deployment, and management of your entire firewall estate—from onboarding firewalls to provisioning them in your network and setting up security policies that fully utilize all capabilities. Panorama also provides centralized visibility and comprehensive insights into your network traffic, logs, and threats. It reduces administrative workload by helping manage software updates and automate the scheduling of content updates that, in turn, help maintain the best possible overall security posture.

Panorama can manage all your firewalls wherever they are: your perimeter, branches, data center, mobile users, or the cloud. APIs allow easy integrations with third-party systems and your existing operational tools. The fully customizable Application Command Center offers comprehensive, correlated insight into current and historical network and threat data. Coupled with API-based integrations, Panorama also helps you automate threat responses through policy-based actions that simplify operations.

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 traffic volume is so high that many organizations lack the tools to monitor it properly. Our DNS Security service applies predictive analytics, machine learning, and automation to block attacks that use DNS. Tight integration with the Next-Generation Firewall gives you automated protections, 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. 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.

Threat Prevention

Exploit, Malware, and C2 Prevention

Our Threat Prevention service automatically stops known client- and server-side vulnerability exploits with IPS capabilities, offers in-line 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. By looking for threats at all points within the cyberattack lifecycle, not just when they first enter the network, Threat Prevention provides layered defense as founded in the Zero Trust model.

A uniform signature format for all threats ensures speedy processing by enabling all analysis to be performed in a single, integrated scan, eliminating

redundant processes common to offerings that use multiple scans. Threat Prevention combs through each packet as it passes through our Next-Generation Firewalls, 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 Sites 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 augmented with machine learning. Automated protections block access to malicious sites that deliver malware and steal credentials, stopping any data loss. Organizations can minimize 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 both static and dynamic analysis. It classifies URLs into benign or malicious categories, which you can easily build into Next-Generation Firewall 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 automatically detects and stops unknown threats. Going beyond traditional sandboxing, WildFire helps security teams stay ahead of the latest attack techniques with complementary engines, including machine learning, static analysis, dynamic analysis, and network profiling. WildFire stops even the most advanced threats with built-in evasion prevention using a custom hypervisor and the industry's first bare-metal analysis engine. With its cloud-delivered, modular architecture, WildFire continuously delivers innovative new detection engines with none of the operational impact common to traditional "hold and release" sandboxing solutions.

WildFire detects unknown threats with data from a growing global community in the tens of thousands. By using shared data, WildFire quickly identifies and prevents advanced attacks. It is the industry's largest enterprise malware analysis community, leveraging threat intelligence submitted from networks, endpoints, clouds, and third-party partners.

WildFire automates prevention and gains threat intelligence for advanced attacks. Within seconds, clients can get immediate automated protections across their entire platform, stopping malware, malicious URLs, DNS-based attacks, and command and control. WildFire seamlessly integrates with our AutoFocus service to provide rich context and attribution information on all data WildFire collects and processes. Security teams save time with detailed insight into the behavior of identified threats, indicators of compromise, and how they were blocked.

Zingbox

Enterprise IoT Security and OT Intelligence

Zingbox® delivers industry-leading security for the internet of things (IoT), empowering organizations to discover, secure, and optimize unmanaged devices. An agentless approach, powered by machine learning and industry-specific intelligence, protects enterprises from IoT device-targeted threats across IT, healthcare, oil and gas, manufacturing, smart city, and ICS/SCADA environments.

A combination of AI, machine learning, and integrated intelligence discerns each device's behaviors, automatically detects suspicious activities, and enforces trust in all network-connected IoT assets. Zingbox enables organizations to orchestrate the entire IoT and OT infrastructure lifecycle, including in-depth operational insights to optimize (e.g., X-ray machines, smart cameras, smart printers) for better business outcomes.

The product augments every key IT system with IoT intelligence, using the broadest portfolio of native integrations across asset management; network access control (NAC); security information and event management (SIEM); security orchestration, automation, and response (SOAR); wireless LAN controllers; network management; vulnerability scanners; and industry-specific device intelligence databases.

GlobalProtect

Mobile User Security

GlobalProtect™ network security for endpoints enables you to protect your mobile workforce by extending Next-Generation Firewall features to all users, regardless of their device or location. It safeguards users with unmatched threat prevention capabilities to protect against evasive application traffic, phishing and credential theft, and more. In addition, GlobalProtect provides granular visibility by inspecting all application traffic—across all ports—at all times, allowing you to create and enforce more efficient security policies.

With clientless VPN, GlobalProtect provides secure options for bring-your-own-device (BYOD) initiatives 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®.

SD-WAN

Secure Branch Connectivity

Palo Alto Networks SD-WAN solution 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, our secure Prisma Access SD-WAN hub 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 Next-Generation Firewalls. Regardless of the deployment model, this tight integration will allow you to manage security and SD-WAN on a single, intuitive interface.

PRISMA™
BY PALO ALTO NETWORKS

Secure the Cloud

Prisma™ is the industry's most complete cloud security offering. Accelerate your cloud journey with a product suite designed to secure today's complex IT environments.


Prisma Access


Prisma Cloud


Prisma SaaS

Data Loss Prevention

Prisma Access

Cloud-Delivered Mobile User Security

Prisma™ Access is a secure access service edge (SASE) that helps your organization deliver consistent security to your remote networks and mobile users. It's a generational step forward in cloud security, using a common cloud-based infrastructure to connect all users to all applications. All your users, whether at your headquarters, in branch offices, or on the road, connect to Prisma Access to safely use cloud and data center applications as well as the internet. Located in more than 100 locations around the world in 76 countries, Prisma Access consistently inspects all traffic across all ports and provides bidirectional networking to enable branch-to-branch and branch-to-HQ traffic.

Delivering protection at scale, Prisma Access provides global coverage so you don't have to worry about sizing and deploying hardware firewalls at the branch. Prisma Access uses Cortex Data Lake for centralized analysis, reporting, and forensics.

Prisma Cloud

Cloud Native Security Platform

Prisma™ Cloud is the unified cloud native security platform 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 and data spanning hosts, containers, serverless deployments, storage, and other platform-as-a-service (PaaS) offerings across cloud platforms. It dynamically discovers resources as they are deployed and correlates data cloud services provide (resource configurations, flow logs, audit logs, host and container logs, etc.) to provide security and compliance insights for your cloud applications. It uses machine learning to profile user, workload, and app behaviors to prevent advanced threats.

Prisma Cloud integrates with CI/CD tool chains to provide full lifecycle vulnerability management, infrastructure-as-code (IaC) scanning, runtime defense, and cloud native firewalling. 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.

Prisma SaaS

Secure SaaS Access

Prisma™ SaaS enables safe cloud adoption by providing visibility, compliance controls, and security for cloud applications and sensitive data. It helps minimize the use of shadow IT, secure access to corporate SaaS applications like Office 365®, Salesforce®, G-Suite®, Slack®, and Box, and mitigate the risk of a data breach in the cloud.

Prisma SaaS is a cloud service that consistently provides visibility, compliance controls, and protection across multiple SaaS applications. It safeguards organizations and their data against cloud cyber risks, helping them safely adopt SaaS applications and safely store their sensitive data in the cloud. As an integrated functionality of Palo Alto Networks firewalls, Prisma SaaS delivers its functions across all internet traffic and all applications for in-line inspection of all network traffic and API-based (or introspection-based) security for SaaS applications. It extends visibility, corporate security postures, control and compliance, and data protection into SaaS applications in a consistent way, so SaaS security is tight to—never disjointed from—company-wide security initiatives.

Data Loss Prevention

Data Protection and Compliance

Palo Alto Networks Enterprise Data Loss Prevention is a cloud service that provides consistent, reliable protection of sensitive data, such as personally identifiable information (PII) and intellectual property, for all traffic, all applications, and all users. Native integration with existing Palo Alto Networks products makes it simple to adopt, and advanced machine learning minimizes management complexity. Enterprise DLP allows organizations to discover, monitor, govern, and protect sensitive data, everywhere it resides and moves. It enables safe cloud adoption by minimizing the risk of a data breach in cloud applications, such as Office 365 and Box, and verifiably assists in meeting data privacy and regulatory compliance, including stringent regulations such as the GDPR, CCPA, PCI DSS, HIPAA, and others.

CORTEX™
BY PALO ALTO NETWORKS

Secure the Future

Cortex™ is the industry's most comprehensive product suite for security operations, empowering enterprises with best-in-class detection, investigation, automation, and response capabilities.

AutoFocus


Cortex Data Lake


Cortex XDR


Cortex XSOAR

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 intel embedded in any tool through a custom threat feed and agile APIs.

Cortex Data Lake

Good Data Built for Security Analytics

Cortex™ Data Lake enables you to collect, transform, and integrate your enterprise's security data to enable Palo Alto Networks solutions, including Cortex XDR, Prisma Access, and Next-Generation Firewalls.

Cortex XDR

Extended Detection and Response

Cortex XDR™ empowers security operations to cut through the noise and focus on real threats. The product reimagines how you find advanced, hidden attacks with integrated endpoint, network, and cloud data. Teams can slash complexity and replace disjointed point products with a unified platform for prevention, detection, investigation, and response.

Cortex XDR accurately detects threats by analyzing rich data with behavioral analytics and machine learning. It provides a complete picture of each incident and reveals the root cause, allowing you to investigate threats eight times faster than before. The unique offering simplifies every stage of security operations, from alert triage to threat hunting, lowering analyst experience and time requirements. Tight integration with enforcement points accelerates containment, enabling you to stop attacks before the damage is done.

Cortex XSOAR

Extended Security Orchestration, Automation, and Response (XSOAR)

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

 | 3000 Tannery Way | Santa Clara, CA 95054 | Support: +1.866.898.9087 | www.paloaltonetworks.com