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...

Security Operating Platform

Security requires simplicity. The Security Operating Platform® was designed so your teams can operate simply and efficiently to protect your organization. The platform prevents successful attacks and stops attacks in progress to secure the enterprise, the cloud, and the future.

Secure the Enterprise

Prevent attacks with the industry-defining network security platform. Built for simplicity, our tightly integrated innovations are easy to operate, delivering consistent protection across network, cloud, and mobile users.

Next-Generation Firewall

App-ID

Content-ID

User-ID

Panorama

DNS Security

Threat Prevention

URL Filtering

WildFire

GlobalProtect

Traps

Next-Generation Firewalls

(Physical and Virtualized)

Palo Alto Networks Next-Generation Firewalls stop cyberattacks while simplifying security. Innovations are tightly integrated into the platform, replacing disconnected point products. Physical, virtualized, and cloud-delivered deployment options provide consistent protection wherever your data and apps reside. We have always set the standard, keeping you on the cutting edge while simplifying security.

Our Next-Generation Firewalls deliver consistent visibility and granular control for strengthened security, with automation and analytics for immediate prevention as well as tightly integrated services that simplify security and replace disconnected tools.

PAN-OS®, the software that powers our Next-Generation Firewalls, keeps you on the cutting edge with tightly integrated innovations. It simplifies your operations through analytics and automation while giving you consistent protection through exceptional visibility and control across data center, perimeter, branch, mobile, and cloud networks.

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.

Content-ID

Content Classification Technology

Content-ID™ technology delivers a new approach based on the complete analysis of all allowed traffic, employing multiple advanced threat prevention technologies in a single, unified engine. 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.

Panorama

Network Security Management

Panorama™ provides centralized network security management, simplifying administration while delivering comprehensive controls as well as deep visibility into network-wide traffic and security threats. Panorama manages rules and dynamic security updates so you can keep up with ever-evolving network threats. With a single rule base for firewall, threat prevention, URL filtering, application awareness, user identification, file blocking, and data filtering, you can reduce administrative workloads and improve your overall security posture.

Panorama can manage all your firewalls wherever they are: at the perimeter, in a data center, or in the cloud. Its APIs and Dynamic Address Groups help you automate policy workflows that adapt to changes, such as addition, moving, or deletion of servers. The fully customizable Application Command Center provides comprehensive, correlated insight into current and historical network and threat data.

DNS Security Service

Prevention of Attacks Using DNS

Our DNS Security service applies predictive analytics to disrupt attacks that use DNS for command and control (C2) or data theft. Tight integration with Palo Alto Networks Next-Generation Firewalls gives you automated protection and eliminates the need for independent tools. Shared threat intelligence and machine learning rapidly identify threats hidden in DNS traffic. DNS Security service predicts and stops malicious domains from domain generation algorithm-based malware while quickly detecting C2 or data theft that employs DNS tunneling with machine learning-powered analysis. Through integration with Next-Generation Firewalls, dynamic response can automatically find infected machines and quickly respond in policy. 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 provides signatures that block known client- and server-side vulnerability exploits, malware, and command and control. It inspects all traffic for threats regardless of port, protocol, or encryption—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.

We use a uniform signature format for all threats to ensure speedy processing by performing all analysis 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 both the packet header and payload. 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 by machine learning. Automated protections block access to malicious sites that deliver malware and steal credentials, resulting in 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.

In order 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® is a malware prevention service that automatically detects and stops unknown attacks. 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 attacks 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 zero operational impact.

WildFire detects unknown threats with data from a growing global community in the tens of thousands of customers. By using shared data, it can quickly identify and prevent advanced attacks. WildFire sources data from the industry's largest enterprise malware analysis community, including threat intelligence submitted from networks, endpoints, clouds, and third-party partners.

WildFire automates prevention and gains threat intelligence for advanced attacks. Within minutes, you can get immediate automated protections across your entire platform, stopping malware, malicious URLs, DNS-based attacks, and command and control. WildFire seamlessly integrates with Palo Alto Networks 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.

GlobalProtect

Mobile User Security

GlobalProtect™ is a network security service for endpoints that enables you to protect your mobile workforce by extending the Security Operating Platform 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 clouds and data centers. It enables support for per-app VPN using integrations with enterprise mobility management offerings, including AirWatch®, Microsoft Intune®, and MobileIron®.

Traps

Endpoint Protection and Response

Traps™ for endpoint protection and response stops threats and coordinates enforcement with both network and cloud security to prevent successful cyberattacks. Traps blocks known and unknown malware, exploits, and ransomware by observing attack techniques and behaviors. Additionally, it enables you to automatically detect and respond to sophisticated attacks by using machine learning and artificial intelligence (AI) techniques with data collected from endpoints, networks, and clouds.

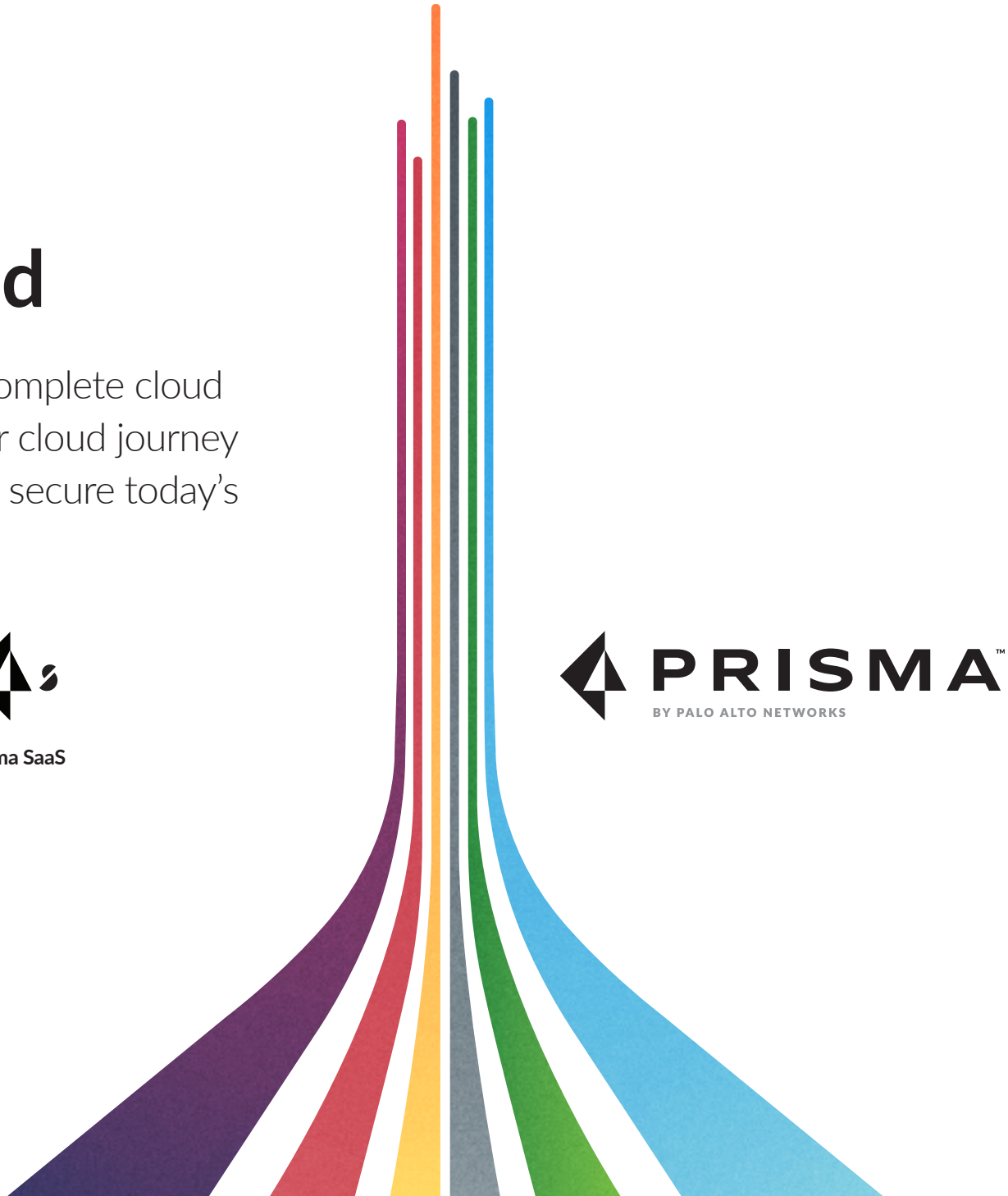
Secure the Cloud

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 Public Cloud

Prisma SaaS



PRISMA™
BY PALO ALTO NETWORKS

Prisma Access

Cloud-Delivered Mobile User Security

Prisma™ Access helps your organization deliver consistent security to your remote networks and mobile users. It's a generational step forward in cloud security, using a cloud-delivered architecture 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. 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 things like sizing and deploying hardware firewalls at your branches, or building out and managing appliances in collocation facilities. Prisma Access uses Cortex™ Data Lake for centralized analysis, reporting, and forensics.

Prisma Public Cloud

Public Cloud Threat Protection, Governance, and Compliance

Prisma™ Public Cloud is the industry's most comprehensive threat protection, governance, and compliance offering. It dynamically discovers cloud resources and sensitive data across GCP™, AWS®, and Azure® to detect risky configurations and identify network threats, suspicious user behavior, malware, data leakage, and host vulnerabilities. It eliminates blind spots across your cloud environments and provides continuous protection with a combination of rule-based security policies and class-leading machine learning.

Prisma Public Cloud also vastly simplifies the task of managing compliance across the multi-cloud landscape and supports audit-ready reports across the industry's most complete library of supported frameworks—including CIS, NIST, PCI, HIPAA, GDPR, ISO, SOC 2, and more—with a single click. Powered by APIs with seamless integrations across your cloud environments, threat intelligence, and remediation tools, only Prisma Public Cloud delivers a truly integrated, frictionless experience—no agents or proxies required.

Prisma SaaS

Secure SaaS Access

By offering advanced data protection and consistency across software-as-a-service applications, Prisma™ SaaS reins in the risks. It addresses your cloud access security broker (CASB) needs and provides advanced capabilities in the areas of risk discovery, data loss prevention, compliance assurance, data governance, user behavior monitoring, and advanced threat prevention. Now, you can stay compliant while preventing data leaks and business disruption.

Prisma SaaS functions as a multi-mode CASB, offering in-line and API-based protection working together to minimize the range of cloud risks that can lead to breaches. With a fully cloud-delivered approach to CASB, you can secure your SaaS applications through the use of in-line protections to safeguard in-line traffic with deep application visibility, segmentation, secure access, and threat prevention as well as API-based protections to connect directly to SaaS applications for data classification, data loss prevention, and threat detection.

Secure the Future

Cortex™ is the industry's only open and integrated AI-based continuous security platform that constantly evolves to stop the most sophisticated threats.

Cortex

Cortex Data Lake

Cortex XDR

AutoFocus

Demisto

CORTEX™
BY PALO ALTO NETWORKS

Cortex

AI-Based Continuous Security Platform

Cortex™ delivers radical simplicity and significantly improves security outcomes through automation and unprecedented accuracy. The platform uses rich data from tightly integrated sensors across your enterprise to enable new apps from Palo Alto Networks and third-party Cortex partners. Cortex constantly evolves to deliver disruptive new innovations for security, analytics, and automation. You can recoup time to solve unique and complex problems by automating significant parts of your IT and security operations.

Cortex Data Lake

Cloud-Based Data Collection, Storage, and Analysis Service

Cortex™ Data Lake enables AI-based innovations for cybersecurity with the industry's only approach to normalizing your enterprise's data. It automatically collects, integrates, and normalizes data across your security infrastructure. The cloud-based service is ready to scale from the start, eliminating the need for local compute or storage, providing assurance in the security and privacy of your data. Cortex Data Lake enables you to effortlessly apply advanced AI and machine learning with cloud-scale data and compute. With trillions of multi-source artifacts for analytics, and by constantly learning from new data sources, Cortex Data Lake significantly improves the accuracy of security outcomes.

Cortex XDR

Cloud-Based Detection and Response

Cortex XDR™ breaks the silos of traditional detection and response by natively integrating network, endpoint, and cloud data to stop sophisticated attacks. Taking advantage of machine learning and AI models across all data sources, it identifies unknown and highly evasive threats from managed and unmanaged devices. Cortex XDR speeds alert triage and incident response by providing a complete picture of any threat, revealing the root cause automatically. By stitching together different types of data and simplifying investigations, Cortex XDR reduces the time and experience required at every stage of security operations, from alert triage to threat hunting. Tight integration with enforcement points lets you quickly respond to threats and apply the knowledge gained from investigations to greatly reduce the surface area of risk through continual use.

AutoFocus

Contextual Threat Intelligence

AutoFocus™ is a contextual threat intelligence service that speeds your ability to analyze threats and respond to cyberattacks. Instant access to community-based threat data from WildFire, enhanced with deep context and attribution from our Unit 42 threat research team, saves time. Your security teams get detailed insight into attacks with pre-built Unit 42 tags that identify malware families, adversaries, campaigns, malicious behaviors, and exploits without the need for a dedicated research team.

AutoFocus improves the speed and precision of attack response by automatically surfacing high-impact threats and indicators to help you prioritize investigations. Automated protection delivered to your Next-Generation Firewalls makes it simple to turn raw intelligence into realtime enforcement across your environment. AutoFocus can organize third-party threat intelligence feeds and share relevant indicators using MineMeld™, a threat intelligence syndication engine hosted in AutoFocus. Security teams can instantly enrich third-party tools and SIEMs with an easy-to-use API for access to collected intelligence. With all in-house and third-party data consolidated in one system, you can quickly investigate, correlate, and pinpoint malware's root cause without adding dedicated malware researchers or more tools.

Demisto

Security Orchestration, Automation, and Response (SOAR)

Demisto Enterprise is the only security orchestration, automation, and response (SOAR) platform that combines security orchestration, incident management, and interactive investigation to serve security teams across the incident lifecycle. Demisto's orchestration enables security teams to ingest alerts across sources and execute standardized, automated playbooks for accelerated incident response. Demisto's playbooks are powered by hundreds of integrations and thousands of security actions, striking the right balance between rapid machine execution and nuanced human oversight. These playbooks are further complemented by realtime investigation capabilities so security teams can rapidly iterate to solve emergent threats. Each incident in Demisto has a war room view, which is a shared collaborative workspace where analysts can chat with each other, run commands in realtime, and have their actions documented for future learning. Fully customizable summaries, dashboards, and reports ensure complete visibility across the attack lifecycle. With Demisto, security teams can future-proof security operations to reduce mean time to respond, maintain consistent incident management processes, and increase analyst productivity.

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