ML-Powered Next-Generation Firewall Technologies, Subscriptions, and Services

The world's first and only ML-Powered Next-Generation Firewall will help you stay ahead of unknown threats, see everything—including IoT—and reduce errors with automatic policy recommendations. It's available in hardware (PA-Series), software (VM-Series and CN-Series), and cloud-delivered (Prisma™ Access) form factors.

PAN-OS Technologies

No software subscription is required for the technologies shown in table 1.

Table 1: PAN-OS Technologies

Technology	Description
App-ID™	Classifies all of your applications, across all ports, all the time, regardless of port, SSL/SSH encryption, or technique used to evade detection. Unlike legacy firewalls that depend on Layers 3 and 4 as the first layers of control before application classification is applied, our Next-Generation Firewalls directly apply App-ID along with other Layer 7 controls, like User-ID.
User-ID™	Integrates with a wide range of user identity repositories so that your policies follow your users and groups regardless of their location. User repositories include wireless LAN controllers, VPNs, directory servers, browser-based captive portals, proxies, and more.
SSL Decryption	Inspects and applies policy to SSL/SSH-encrypted traffic, both inbound and outbound, including for traffic that uses TLS 1.3 and HTTP/2. For privacy and regulatory compliance, you can enable or disable decryption flexibly based on URL, source, destination, user, user group, and port.
Site-to-Site IPsec VPN	Supports site-to-site tunnels over IPv4/IPv6 and IKEv1/IKEv2 to ensure compatibility. For multiple connection sites, equal-cost multi-path routing (ECMP) can provide additional redundancy and cost-efficiency by balancing sessions over available internet connections. Large-scale VPN simplifies the process for deploying a hub and spoke VPN topology with branch firewalls.
Remote Access	Provides a secure remote access or virtual private network (VPN) solution and always-on security by extending the Next-Generation Firewall protection to mobile users. Note: Additional advanced features are available with the GlobalProtect subscription. See Software Subscription: GlobalProtect for details.
Custom URLs	Maintains logs of access to any URL, and filters based on user-maintained, custom categories. Note: Additional advanced features are available with the URL Filtering subscription. See Software Subscription: URL Filtering for details.
QoS	Provides basic quality of service (QoS), controlling traffic leaving the firewall according to the network or subnet, and extends the power of QoS to classify as well as shape traffic according to application and user.
Data Filtering	Controls the transfer of sensitive data patterns, including credit card and Social Security numbers, in application content or attachments. The file transfer function controls file transfer functionality within an individual application, allowing application use while preventing undesired inbound or outbound file transfers.
Application Command Center (ACC)	Provides an interactive, graphical summary of the applications, users, URLs, threats, and content traversing your network. The graphical representation lets you interact with the data and see the relationships between events on the network so that you can uncover anomalies or find ways to enhance your network security rules. You can also personalize your view of your network.
Logging	Shows overall traffic, applications, users, threat, URL, and data filter logging to facilitate the organization of data. Logs can be kept for individual firewalls, entire networks of firewalls, or any subset of a network. For large networks, you can either deploy dedicated log collectors (sold separately as M-Series appliances), or subscribe to the cloud-based Cortex™ Data Lake to increase the log storage capacity and simplify network design.
Reporting	Includes, as a standard, a detailed, customizable software-as-a-service (SaaS) application usage report that provides insight into all SaaS traffic—sanctioned and unsanctioned—on your network. You can also create custom reports based on your needs as well as easily schedule, download, and share them with others in your organization.
Fully Documented XML API	Enables you to integrate our Next-Generation Firewalls with third-party solutions from both inbound and outbound perspectives.
Policy Automation	Enables you to use information from third-party sources to drive security policy updates dynamically through a combination of Dynamic Address Groups, VM monitoring, and the XML API.
Policy Optimizer	Identifies port-based rules so you can safely convert them to application-based rules, enabling you to whitelist applications you want to allow and deny access to all others, which improves your security posture. Restricting application traffic to default ports prevents evasive applications from running on nonstandard ports.

Software Subscription: IoT Security

Protect your network with the industry's only internet of things (IoT) security product that discovers and secures unmanaged IoT and OT devices in your network using a unique combination of machine learning and Next-Generation Firewall capabilities.

Table 2: Benefits of IoT Security

Benefit	Description
Complete Visibility into All Unmanaged Devices	Identifies and classifies all IoT and OT devices in your network, including those never seen before, with machine learning and App-ID. Classification includes more than 50 attributes, such as name, type, vendor, model, firmware, OS, location, VLAN, subnet, ports, applications, activity, and profile.
In-Depth Risk Assessment	Uses a machine learning-powered approach to crowdsource behavioral profiling, anomaly detection, vulnerability and vendor information, network and application usage, and risk scoring to enable your security teams to make fast and accurate decisions.
Easy Segmentation	Provides full device context to segment your IT and IoT, allowing only trusted behavior and reducing risk across the entire cyberattack lifecycle.
Built-in Policy Enforcement	Offers policy recommendations based on risk assessment results that can be automatically enforced using a Device-ID™ policy construct that seamlessly integrates with your existing Next-Generation Firewalls.
Native Prevention	Uses cloud-delivered security subscriptions like Threat Prevention, DNS Security, URL Filtering, and WildFire to keep IoT devices secure from all known and unknown threats. See IoT alerts with added device context among all others in your Next-Generation Firewalls.
Easy Deployment	Integrates natively into your Next-Generation-Firewalls in any location and requires no additional sensors or enforcement agents. Simply add the cloud-delivered IoT Security subscription to seamlessly increase visibility and integrate workflows for your security teams into all unmanaged devices.

Software Subscription: SD-WAN

Enable secure branch connectivity (per-device subscription required on the edge device and the hub device).

Table 3: Benefits of SD-WAN

Benefit	Description
Natively Integrated Security and Connectivity	Eliminates the need to deploy and configure multiple appliances at the branch because it natively integrates security and connectivity. You can enable SD-WAN capabilities such as path metrics, path selection, dynamic steering, forward error correction (FEC), and packet duplication right from your Next-Generation Firewall.
Centralized Management	Removes the need for disparate solutions by enabling you to manage security and connectivity from a single, intuitive interface.
Consistent Branch Security	Extends the same, consistent security from your data center and cloud to your branch offices.

Software Subscription: GlobalProtect™

Deliver security to any user and any device, anywhere (per-device subscription).

Table 4: Benefits of GlobalProtect

Benefit	Description
Remote Access	Provides secure access to internal and cloud-based business applications from laptops, tablets, and smartphones. You can control access and enforce policies for websites and applications, including SaaS applications.
Host Information Profile	Checks the endpoint to get an inventory of how it's configured and builds a host information profile (HIP) that's shared with the Next-Generation Firewall. The Next-Generation Firewall uses the HIP to enforce application policies that only permit access when the endpoint is properly configured and secured.
Remote and Internal User Authentication	Supports all existing PAN-OS authentication methods, including Kerberos, RADIUS, LDAP, client certificates, and a local user database. Once GlobalProtect authenticates the user, it immediately provides the Next-Generation Firewall with a user-to-IP address mapping for use by User-ID™ technology.
Device Quarantine	Strengthens your security by providing a reliable, automated approach to identifying and quarantining compromised endpoints. Utilizing the endpoint's immutable characteristics, you can identify a compromised device and restrict its network access as well as prevent it from infecting other users and devices.

Software Subscription: Threat Prevention

Leverage full-featured IPS, anti-malware, and command-and-control (C2) protection (per-device subscription for unlimited users).

Table 5: Benefits of Threat Prevention

Benefit	Description
Intrusion Prevention System (IPS)	Blocks vulnerability exploits, buffer overflows, and port scans. Additional capabilities, like blocking invalid or malformed packets, IP defragmentation, and TCP reassembly, protect you from attackers' evasion and obfuscation methods. 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®. Vulnerability-based signatures are updated weekly and protect against a range of exploits in seconds with threat intelligence from WildFire® malware prevention service. Threat signatures are applied for applications, irrespective of port, for inbound and outbound traffic, in stark contrast to legacy security devices that rely on ports. Further, policy-based SSL decryption ensures that IPS functionality is applied to encrypted traffic.
Anti-Malware	Uses a stream-based engine that blocks inline at very high speeds, detecting known malware as well as unknown variations of known malware families. IPS and anti-malware address multiple threat vectors with one license, eliminating the need to buy and maintain separate IPS and proxy-based products from legacy security vendors.
C2 Protection (Anti-Spyware)	Stops malicious outbound communications stemming from malware infections, passively analyzes DNS queries, and identifies the unique patterns of botnets. This reveals infected users and prevents secondary downloads and data from leaving your organization.

Software Subscription: URL Filtering

Identify and prevent access to malicious websites (per-device subscription for unlimited users).

Table 6: Benefits of URL Filtering

Benefit	Description
Safe Web Access	Protects users by automatically preventing web-based attacks, including those that use phishing, C2, and exploit kits. Phishing and JavaScript-based attacks are detected inline through machine learning on the Next-Generation Firewall and blocked in milliseconds without requiring analyst intervention. URLs are classified into benign or malicious categories you can easily build into firewall policy for total control of web traffic. You can address any compliance or regulatory issues by controlling web access based on organizational policy.
Policies Based on Web Category and User Group	Lets you easily adopt security best practices as part of your Next-Generation Firewall policies to minimize opportunities for attack. You can apply selective SSL decryption based on website categories to find threats hidden in encrypted traffic while maintaining privacy; prevent data loss by stopping in-process credential theft and implementing multi-factor authentication to block use of stolen credentials; and block high-risk file types from website categories to prevent accidental malware downloads.
Maximized Operational Efficiency	Eliminates the need to deploy and manage additional hardware for web security. You can radically simplify your rules administration through application- and user-based policy to let your staff focus on business priorities. Protect your users without sacrificing the speed of your web-based applications through a combination of local URL category database and immediate cloud URL lookups.

Software Subscription: WildFire®

Protect your organization against previously unknown threats (per-device subscription for unlimited users).

Table 7: Benefits of WildFire

Benefit	Description
Unknown Threat Detection with Advanced Analysis	Identifies unknown threats with shared data from the industry's largest enterprise malware analysis community, including threats submitted from networks, endpoints, clouds, and third-party partners. WildFire uses complementary analysis engines, including machine learning as well as static, dynamic, and other advanced analysis capabilities. These engines work in our custom-built hypervisor with bare metal analysis to stop advanced attacks built to evade sandboxes.
Inline, Machine Learning-Based Prevention	Includes an inline, machine learning-based engine powered by threat models continually honed in the cloud, delivered in physical and virtual Next-Generation Firewalls. This innovative, signatureless capability prevents malicious content (e.g., portable executable files and dangerous fileless attacks stemming from PowerShell®) completely inline, with no cloud submission step.
Protection from Unknown Threats	Automatically generates protections across the attack lifecycle when a new threat is first discovered, blocking malicious files, access to malicious URLs, and C2 traffic, and then delivers those protections to all WildFire subscribers in seconds for most new threats.
File Behavior Analysis	Uses detailed behavior analysis to help you to understand how newly discovered malware operates. Integrated logs enable you to quickly identify infected users and investigate potential breaches with detailed analysis of, and visibility into, unknown threat events.
Cloud-Based Prevention	Employs a unique cloud-based architecture, providing automatic prevention based on global threat intelligence, without the headache of having to implement and manage separate devices for web and email at every ingress/egress point in your network. You can stay ahead of attackers with cloud-delivered, modular architecture, continuously delivering innovative new detection engines with zero operational impact.
Multi-Vector Analysis and Visibility	Combines the cloud scale of WildFire with advanced file analysis and URL crawling to deliver Multi-Vector Recursive Analysis, a unique and comprehensive solution that prevents multi-stage, multi-hop attacks. Unlike other solutions, WildFire can follow multiple stages of attack from a file analysis standpoint, even if execution fails in a given stage. When WildFire visits embedded links or links in emails as part of its email link analysis, it updates URL Filtering if any corresponding webpages host exploits or display phishing activity. This workflow unifies analysis across web and file attack vectors while enabling a unique, holistic view of a campaign over multiple stages.
Comprehensive File Execution	Executes unknown files in multiple OS and application versions simultaneously to fully understand the scope of a threat. Multi-version analysis ensures WildFire analysis is thorough, unlike sandboxes that require golden images, which could deem a malicious file benign simply because the target OS or application version wasn't specified in the golden image.

Software Subscription: DNS Security

Apply predictive analytics to disrupt attacks that use DNS for C2 or data theft (per-device subscription for unlimited users).

Table 8: Benefits of DNS Security

Benefit	Description
Prediction and Blocking of New Malicious Domains	Automatically prevents tens of millions of malicious domains identified with real-time analysis and continuously growing global threat intelligence. You can predict and stop malicious domains from domain generation algorithm-based malware with instant enforcement, and enjoy limitless protection for malicious domains with a cloud-based database for infinite scale that is always up to date.
Neutralized DNS Tunneling	Uses machine learning-powered analysis to quickly detect C2 or data theft employing DNS tunneling. Automated policy actions let you rapidly neutralize DNS tunneling threats without analyst intervention.
Intelligence to Act on Threats Over DNS	Provides deep insight into threats through threat reporting capabilities, delivering full visibility into DNS traffic at macro, industry, and organizational levels. DNS analytics capabilities empower security personnel with the context to optimize your security posture, confidently craft policies, and rapidly remediate security events. Palo Alto Networks combines best in-class detection with the analytics and inline enforcement necessary to protect DNS in real time.
Simplified Security Through Automation	Eliminates the need for independent DNS security tools or changes to DNS routing with Next-Generation Firewall integration. You can automate dynamic response to find infected machines and quickly respond in policy while seamlessly taking advantage of the latest DNS security innovations through our extensible, cloud-based architecture.

Network Security Management: Panorama™

Take advantage of streamlined, powerful, and efficient network security management—available as an appliance or virtual machine—for multiple Next-Generation Firewalls, regardless of their form factor or location (subscription based on the number of firewalls managed).

Table 9: Benefits of Panorama

Benefit	Description
Network and Device Configuration	Enables central management of devices and security configurations for all groups of firewalls across form factors. This lets you streamline configuration with features such as device group hierarchies, template stacking, and role-based access control (RBAC).
Device Configuration Import	Lets you easily import pre-production firewalls or firewalls outside an existing configuration into a Panorama deployment in just a few clicks, making the transition from managing individual firewalls to a centrally managed configuration fast and easy.
Single Security Rule Base	Improves your security and streamlines your operations with a single security rule base for all policies, capabilities, and subscriptions.
Central Visibility (ACC)	Provides deep visibility and comprehensive insights into network traffic and threats via the Application Command Center (ACC). Use the ACC for centralized visibility into your network and security to help you make informed decisions.
Automatic Correlation Engine	Correlates indicators of compromise (IOCs) across the network and automatically confirms compromised hosts, saving valuable time sifting through log data manually. This helps reduce data clutter to identify compromised hosts and surface malicious behavior.
Dedicated Log Collectors	Consolidates log collection with dedicated collectors, cutting back on backhaul requirements and offering deployment flexibility for larger deployments—ideal for distributed Next-Generation Firewall deployments.

Support Subscriptions

Maintain trust when minutes matter.

Table 10: Palo Alto Networks Support Programs

Program	Description
Standard	Provides baseline services for maintaining your Palo Alto Networks deployment, including direct access to product experts, case management, an online Customer Support Portal, documentation and FAQs, subscription services updates, feature releases and software updates, hardware return and replacement services, and assisted support access. Hours: Monday through Friday, 7 a.m. to 6 p.m. Pacific time
Premium	Offers faster assistance and increased support engineer availability for the most critical issues. This level includes all Standard Support features in addition to Premium Support hours, next-business-day return materials authorization (RMA) replacement, and Security Assurance. Hours: 24/7 year-round • **Security Assurance**: When you detect suspicious activity in your network, Security Assurance gives you access to our security experts with unique threat intelligence tools and practices for your Palo Alto Networks footprint. Our team will help orient initial investigations, facilitate collection of logs and IOCs, and expedite hand-off to your preferred incident response vendor.
Platinum	Enhances your in-house resources with technical experts available to support your Palo Alto Networks deployment. This level includes all Premium Support features as well as: • **Direct access to a dedicated team of senior engineers**: Interact with a senior engineer trained to quickly understand and resolve your unique challenges. • **Platinum Support availability**: Enjoy 24/7 support for issues of all severities, with Platinum senior engineers available around the clock to assist. • **Platinum Support response time**: Get 15-minute response times for critical issues. To ensure your mission-critical deployment operates at peak performance, Platinum Support delivers an enhanced support service-level agreement. • **Security Assurance**: When you detect suspicious activity in your network, Security Assurance gives you access to our security experts with unique threat intelligence tools and practices for your Palo Alto Networks footprint. Our team will help orient initial investigations, facilitate collection of logs and IOCs, and expedite hand-off to your preferred incident response vendor. • **Planned event assistance**: If scheduled at least seven days in advance, our Platinum senior engineers can assist you with proactive maintenance activities, such as software upgrades or feature activation. Platinum engineers can also be on call to assist as needed during business events.

Table 10: Palo Alto Networks Support Programs (continued)

Program	Description
Platinum	• **On-site assistance for critical issues**: For critical issues (Severity 1) outside the capabilities of remote troubleshooting, a field engineer may be dispatched to your location at the discretion of the Palo Alto Networks Platinum Support management team. • **Failure analysis**: In the event of hardware failure, upon request, Palo Alto Networks will analyze the replaced unit and send you the results of the investigation.
Focused Services	Provides personalized support through a designated customer advocate. Under this program, you are assigned a services account manager who will provide tailored support, including weekly reviews, root cause analysis for critical issues, release review and upgrade planning, and a quarterly business review. Your services account manager will become deeply familiar with your implementation and business priorities to proactively drive best practices and help continuously improve your security posture. Learn more.

Read more information on our Customer Support plans.

Professional Services

Maintain confidence in your deployment, configuration, and operations.

Table 11: Palo Alto Networks Professional Services

Offering	Description
Design and Architecture Services	Ensures a solid foundation for your implementation with a high-level architecture design or targeted designs for platform components. • **High-Level Design Service**: We provide a high-level architecture design, based on best practices and your business requirements, that you can execute to adopt the features of the platform in a meaningful way to meet your technical and business requirements. • **Targeted Design Service**: Deep dive on a specific platform capability, such as Panorama, User-ID, SSL Decryption, etc., to create an implementation design and deployment plan. • **Dedicated architect**: Extend your team with a dedicated resource to help design a flexible security architecture and perform strategic planning with your team to continuously reduce risk with your Palo Alto Networks technology.
QuickStart Services	Expedites your successful deployment of firewall-as-a-service components with day-one protection. Expert planning and execution adhere to best practices, provide risk mitigation at every step. QuickStart Services are available for: • **Platform deployment**: Panorama, Next-Generation Firewall • **Subscriptions**: Threat Prevention, URL Filtering, SD-WAN hub deployment, and branch expansion • **Capability adoption**: User-ID, App-ID, SSL Decryption, GlobalProtect
Optimization and Automation Services	Assists you in customizing your Palo Alto Networks technology deployments to optimize operations, simplify investigations, and empower your team with effective use of capabilities. • **Security Operations Integration Service for NGFW**: Customize the configuration of your Next-Generation Firewalls and Panorama deployment to provide consistent incident handling, simplify operations with automation, and improve response times. • **Security Automation Service for Panorama and ServiceNow**: Automate policy management by combining the power of ServiceNow with the management capabilities of our Panorama technology.
Expertise as a Service	Provides access to product expertise, ongoing configuration assistance, and security threat specialists to continuously improve your security as well as stay on top of ever-changing threats and evolving business challenges. • **Resident engineer**: Gain a designated expert focused on your organization. Your resident engineer understands your business needs from the inside out and is uniquely qualified to advise you on getting the most out of your Palo Alto Networks deployment • **Consulting Services**: Access experts to assist with targeted projects or on-site needs.

Read more information on our Professional Services offerings.

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