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

The World's First ML-Powered Next-Generation Firewall Will Help You Stop Zero-Day Threats in Zero Time with Nebula, the 10.2 Release of Our Industry-Leading PAN-OS

Security capabilities on the Palo Alto Networks ML-Powered NGFW are delivered in an integrated platform that offers application, user and device-based policies, decryption of encrypted traffic, networking capabilities, high availability, and a host of cloud-delivered security subscriptions. Core security capabilities are built into the PAN-OS operating system, which powers all Palo Alto Networks ML-Powered NGFWs. Additional security capabilities are available through the deployment of Cloud-Delivered Security Services on the ML-Powered NGFW.

With the integrated platform, all Cloud-Delivered Security Services work seamlessly with each other. Also, the ML-Powered NGFWs' single-pass architecture ensures no additional performance overhead when enabling additional features.

Seamlessly integrated with our industry-leading NGFWs, our Cloud-Delivered Security Services use the network effect of 85,000 customers to instantly coordinate intelligence and protect against all threats across all vectors. Eliminate coverage gaps across your locations and take advantage of best-in-class security delivered consistently in a platform to stay safe from even the most advanced and evasive threats.

The ML-Powered NGFW is available in hardware (PA-Series), software (VM-Series and CN-Series), and cloud-delivered (Prisma Access) form factors.

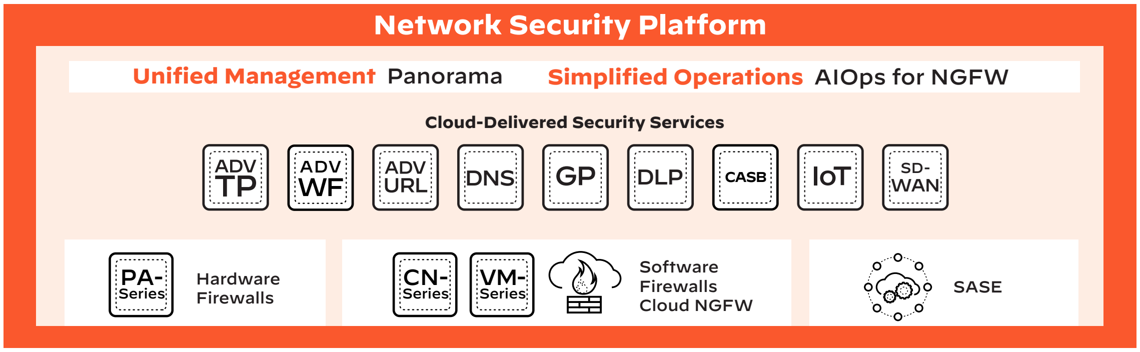

Figure 1: Firewall as a platform

This document provides a comprehensive list of the security features of the ML-Powered NGFW, as well as security features available through the deployment of all available cloud-delivered security subscriptions.

PAN-OS Technologies

The native firewall features available on all NGFW form factors are 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, TLS/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. Moving from port-based legacy firewall rules to App-ID-based ones dramatically reduces the opportunity for attack.
User-ID	Define policies that safely enable applications based on users or groups of users in outbound or inbound directions. User-ID integrates with a wide range of user identity repositories so that your policies follow your users and groups regardless of location. User repositories include wireless LAN controllers, VPNs, directory servers, browser-based captive portals, proxies, GlobalProtect, and more.
Cloud Identity Engine	Aggregate and centralize least-privileged access information by enabling redistribution of user information (User-ID, IP-Tag, User-Tag, quarantine list, and IP-port user mappings) across all locations. Consistently authenticate and authorize users regardless of location and where user identity stores live, and effortlessly enable access based on user identity to quickly move towards a Zero Trust security posture—all using a point-and-click configuration automatically synchronizing identity across identity providers. Identity and authentication providers that are supported include all SCIM-compliant providers (e.g., Azure AD, Okta, Ping, Google Identity Cloud), Microsoft AD, and LDAP.

Table 1: PAN-OS Technologies (continued)

Technology	Description
TLS/SSL Decryption	Inspects and applies policy to TLS/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. Built-in Network Packet Broker allows Palo Alto Networks Next-Generation Firewalls to intelligently forward all traffic to third-party tools, optimizing network performance and helping to maximize existing security tool efficacy.
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 multipath routing (ECMP) can provide additional redundancy and cost-efficiency by balancing sessions over available internet connections. A large-scale VPN simplifies 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.
Web Proxy Support	Consolidate and simplify both your firewall and proxy features in a single platform equipped with best-in-class security services, including Advanced URL Filtering, DNS Security, Advanced WildFire, Advanced Threat Prevention, Enterprise DLP, SaaS Security, and IoT Security. This support provides simplified management while providing flexible deployment options. Note: Web Proxy support is available on PA-1400 Series, PA-3400 Series, and VM-Series 300, 500, and 700 or VM flex licensing with at least 4 vCPU.
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 and 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 data organization. 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 and 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 allow list 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.
5G Security	Delivers 5G-native security built to safeguard service provider and enterprise 5G transformation and multi-access edge computing (MEC).

Software Subscription: Advanced Threat Prevention

Leverage industry-first prevention of zero-day attacks with full-featured IPS, antimalware, and command-and-control (C2) protection capability (per-device subscription for unlimited users). Find more information here.

Table 2: Benefits of Advanced Threat Prevention

Benefit	Description
Intrusion Prevention System (IPS)	Blocks vulnerability exploits, brute-force attempts, 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 several methods, including signature matching, anomaly detection, and inline deep learning for real-time prevention of unknown threats. Advanced Threat Prevention also offers the ability to import and automatically apply signatures and rules in popular formats, such as Snort and Suricata. In addition, Advanced Threat Prevention provides multiple curated IP block lists based on Unit 42 observed and shared threat intelligence. Vulnerability-based signatures are updated a minimum of three times a week, with critical updates provided as needed. They protect against a range of exploits with threat intelligence from the Advanced 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.
Antimalware	Uses a stream-based engine that blocks files inline at very high speeds, detecting known malware and unknown variations of known malware families. IPS and antimalware 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 (Antispyware)	Using an industry-first combination of signatures and cloud-based preventions, Advanced Threat Prevention stops known and unknown malicious covert 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.
Vulnerability Protection	Stops known and unknown exploits using a combination of signatures and multiple deep learning and machine learning models to detect common OWASP Top 10 security risk techniques, such as SQL and command injection. This prevents initial infection due to unknown or unpatched vulnerabilities.

Software Subscription: Advanced URL Filtering

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

Table 3: Benefits of Advanced URL Filtering

Benefit	Description
Safe Web Access	Protects users from web-based attacks like phishing in real time with inline deep learning modules on the Next-Generation Firewall. Advanced URL Filtering can detect and prevent never-before-seen and highly evasive web-based threats in milliseconds without requiring analyst intervention. Advanced URL Filtering analyzes real customer content as opposed to web crawler data. 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	Easily adopt security best practices as part of your Next-Generation Firewall policies to minimize the risk of an 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 multifactor authentication to block the use of stolen credentials, and block high-risk file types from website categories to prevent accidental malware downloads.
Maximized Operational Efficiency	Eliminate the need to deploy and manage additional hardware for web security. You can radically simplify your rules administration through application- and user-based policy, allowing your staff to 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: Advanced WildFire

Stop evasive malware with Advanced WildFire, the largest cloud-based prevention engine that uses machine learning and crowdsourced intelligence to protect organizations from the hardest-to-detect threats (per-device subscription for unlimited users). Find more information here.

Table 4: Benefits of Advanced 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, cloud, and third-party partners. Advanced WildFire uses machine learning, static, dynamic, and intelligent run-time memory analysis capabilities working in our custom-built hypervisor to detect and prevent even the most evasive threats.
Inline, Machine Learning-Based Prevention	Includes an inline, machine learning-based engine powered by threat models continually homed 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 delivering those protections to all Advanced WildFire subscribers in seconds.
File Behavior Analysis	Uses detailed behavior analysis to help you 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.
Multivector Analysis and Visibility	Combines the cloud scale of Advanced WildFire with advanced file analysis and URL crawling to deliver Multivector Recursive Analysis, a unique and comprehensive solution that prevents multistage, multihop attacks. Unlike other solutions, Advanced WildFire can follow multiple stages of attack from a file analysis standpoint, even if execution fails in a given stage. When Advanced 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 displays 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. Multiversion analysis ensures Advanced 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.
Intelligent Runtime Memory Analysis	Efficiently tracks malicious activity during runtime and creates memory captures when something interesting happens. Memory snapshots are analyzed during runtime, and protections are automatically generated and delivered across all enforcement points even before the analysis is concluded. This advanced malware memory analysis technique provides unmatched efficacy and speed while allowing organizations to identify and stop highly evasive and targeted attacks.

Software Subscription: DNS Security

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

Table 5: Benefits of DNS Security

Benefit	Description
Prediction and Blocking of New Malicious Domains	Through predictive analytics and machine learning-powered detections, DNS Security prevents the latest and most sophisticated DNS-layer threats in real time. Customers benefit from comprehensive visibility and coverage across all of their users, devices, and locations within their network.
Industry-First Detections	Uses industry-first detections to prevent C2, data exfiltration, phishing, and malware delivery.

Table 5: Benefits of DNS Security (continued)	
Benefit	**Description**
Actionable Insights	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 their 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 prevent DNS-layer threats 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 responses 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.

Software Subscription: IoT/OT Security

Protect every device on your network with the most comprehensive Zero Trust security for smart devices, allowing you to stop threats and control the risk of IoT, IoMT, OT, and Bluetooth devices on your network. IoT Security has three customized products for enterprises, healthcare providers, and industrial corporations, making it easy to see and secure the devices unique to each vertical. Find more information on Enterprise IoT Security and Medical IoT Security here.

Table 6: Benefits of IoT Security	
Benefit	**Description**
Quickly Discover and Assess Every Device	Identifies and classifies all IoT, IoMT, and OT devices in your network, including those never seen before, with machine learning and App-ID. Classification includes more than 50 attributes, including name, type, vendor, model, firmware, OS, location, VLAN, subnet, ports, applications, activity, and profile. 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.
Easily Segment and Enforce Least-Privileged Access	Implement security best practices with context-aware segmentation to restrict lateral movement between IoT and IT devices. Risk-based policy recommendations from IoT Security allow control of IoT device communication. 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.
Protect Against Known and Unknown Threats	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.
Simplify Your Operations	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). Find more information here.

Table 7: Benefits of SD-WAN	
Benefit	**Description**
Integrated Best-in-Class Security	Deliver consistent, integrated security across branch, data center, and cloud by leveraging the industry's leading ML-Powered NGFW to protect applications, users, and devices against all threats.
Optimized Performance	Optimize your performance by gaining the flexibility to leverage Prisma Access hubs, data center hubs, or branches for application access. Intelligently route traffic based on application performance with zero restrictions on bandwidth availability.
Simplicity	Simplify branch onboarding using Prisma Access hubs and data centers as the global backbone. Centrally manage security and networking policies for data centers, hubs, and branches to reduce operational complexity and cost while improving collaboration between NOC and SOC teams.

Software Subscription: GlobalProtect

Deliver security to any user and any device, anywhere (per-device subscription). Find more information here.

Table 8: 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 all applications, including modern cloud-native apps, legacy private apps, and SaaS apps.
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 Prisma Access and any Next-Generation Firewall. The HIP enforces 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, SAML 2.0, client certificates, biometric sign-in, and a local user database. Once GlobalProtect authenticates the user, it immediately provides Prisma Access and any 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, and prevent it from infecting other users and devices.

Software Subscription: SaaS Security Inline

SaaS Security Inline protects an organization's unsanctioned but tolerated apps. SaaS Security Inline is a service that resides inline on NGFW or Prisma Access to provide visibility into sanctioned, tolerated, and unsanctioned SaaS services being accessed by users. SaaS Security Inline complements SaaS Security API capabilities to provide an integrated next-generation cloud access security broker (Next-Gen CASB) solution.

Table 9: Benefits of SaaS Security Inline	
Benefit	**Description**
Shadow IT Discovery	Using ACE (App-ID Cloud Engine) technology, SaaS Security Inline automatically discovers new SaaS apps to keep pace with new and emerging SaaS apps, identifying 50,000+ SaaS apps (and growing!) using machine learning algorithms to achieve a high level of accuracy and speed.
Shadow IT Control	Enables you to author SaaS policy rule recommendations based on a combination of applications, users and groups, categories, activities, device posture (personal vs. corporate) and Enterprise DLP data profiles. Collaborate with your firewall administrator on SaaS security policy rules to control intentional and unintentional risky SaaS apps and user activity, allowing access to corporate SaaS apps only for legitimate users.
Visibility and Reporting	Delivers an up-to-date combined view of both unsanctioned and sanctioned SaaS application usage across categories and subcategories, including content marketing, collaboration and productivity, and ERP.
Risk Assessment	Exposes risky SaaS applications being used in your application ecosystem. The risk score is between 1 (low risk) and 10 (high risk). This is based on over 32 compliance attributes, including COPPA, CJIS, and GDPR; vendor attributes, including Founded, App Domains, and Employee Count, and SaaS Security Inline Report with visibility data aggregated across all SaaS apps; and risk score customizing tools. It enables you to manually change the risk score for individual SaaS applications without changing the underlying calculation method or adjusting the weights for the underlying attributes and allowing SaaS Security Inline to recalculate and apply the risk score automatically.
Risk Categorization	Identifies safer alternatives to risky SaaS applications with advanced filters, including drill-down views for granularity to locate the SaaS app that meets your organization's risk tolerance. NPS score metric assesses customer satisfaction with SaaS applications; and tagging, both custom and default, to differentiate sanctioned SaaS apps from unsanctioned SaaS apps being used by employees in your organization for efficient monitoring and policy enforcement.

Software Subscription: DLP

Get integrated data protection coverage—across every network, cloud, and user. By delivering consistent policies across all distributed control points from a single cloud-delivered DLP engine, Enterprise DLP enables a unified approach at egress points, the edge, and the cloud, all in a single, easy-to-manage pane of glass.

Table 10: Benefits of DLP	
Benefit	**Description**
Protect Physical Networks	Delivered via PA-Series Next-Generation Firewalls, Enterprise DLP inspects web traffic to automatically detect, monitor, and protect sensitive data in motion.
Protect Virtual Networks	Embedded in VM-Series firewalls, Enterprise DLP protects sensitive data in motion across on-premises, hybrid, and multicloud environments.
Protect SaaS Apps	Delivered through our Next-Generation CASB, Enterprise DLP discovers sensitive data across sanctioned and unsanctioned cloud apps, including modern collaboration apps and minimizes leaks and exposures.
Protect Public Cloud Infrastructures	Delivered through Prisma Cloud, Enterprise DLP protects sensitive data stored across public cloud infrastructures.
Protect SASE and Hybrid Workforce	Delivered through Prisma Access, Enterprise DLP protects sensitive data in motion across networks, branch offices, and mobile users.

Subscription: AIOps for NGFW

Take advantage of the industry's first domain-centric AIOps for NGFW that redefines firewall operational experience by interpreting, predicting, and resolving problems before they become business-impacting. AIOps, launched earlier in 2022, processes 49 billion metrics every month across 60,000 firewalls, and proactively shares 24,000 misconfigurations and 17,000 firewall health issues with customers for resolution every month. AIOps for NGFW can be used on all PA-Series firewalls, VM-Series firewalls, and Panorama deployments that run on PAN-OS 10.0 and above. AIOps is available in two versions: a free version and a premium (paid) version (subscription based on the number of firewalls managed). Check out the feature set in both versions here. Find more information here.

Table 11: Benefits of AIOps for NGFW	
Benefit	**Description**
Proactively Strengthen Security Posture	Provides built-in best practices, combined with policy recommendations customized to your unique deployment, and helps reduce the attack surface and strengthen security posture. Best practice recommendations are powered by machine learning (ML) based on industry standards, security policy context, and advanced telemetry data collected from all Palo Alto Networks firewalls. AIOps guards against violations of best practices and enables remediation of inefficiencies in security policies before committing a change to security policy on Panorama, instead of remediating after the change has been pushed to the firewalls, helping organizations strengthen defenses against cyberattacks and optimizing time and resources.
Proactively Resolve Firewall Disruptions	Gain insights across your deployment and reduce NGFW downtime with proactive insights to maintain optimal firewall health and performance, and keep your NGFWs running smoothly. AIOps can intelligently predict firewall health, performance and capacity problems up to seven days in advance and provides actionable insights to resolve the predicted disruptions.
Achieve a Unified View into Security Effectiveness	Get a unified view into the activity seen in your organization across applications, threats, networks, users, and security subscriptions like DNS Security, Advanced WildFire, and DNS Security. AIOps leverages shared network and threat intelligence to help you understand the most dangerous and zero-day threats in your network that your best-in-security has prevented across your infrastructure and ones that need your attention.

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). Find more information here.

Table 12: Capabilities of Panorama

Capability	Benefit
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 preproduction 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.
AIOps Plugin	Proactively enforces best practices when making changes by validating your commits to inform you if a policy needs work before committing it to Panorama.
Software Upgrade	Panorama skip version upgrade provides a shorter, more straightforward, single reboot upgrade process that fits into a typical maintenance window. This eliminates multiple reboots and simplifies the upgrade for HA pairs and managed firewalls to provide a solution to benefit from the latest PAN-OS security innovations.

Technical Support

Get expert technical assistance when minutes matter.

Table 13: Palo Alto Networks Support Programs

Program	Description
Standard	Provides baseline services for maintaining your Palo Alto Networks deployment, including online support tickets via the Customer Support Portal, access to LIVEcommunity, product documentation, and FAQs. Customers will also get subscription service updates, software updates, hardware return and replacement services, and assisted support access.
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 (See SLAs for response times.), next-business-day return materials authorization (RMA) replacement, and Security Assurance. • **Security Assurance**: This 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 the collection of logs and IoCs, and expedite hand-off to your preferred incident response vendor.

Table 13: Palo Alto Networks Support Programs (continued)

Program	Description
Platinum	Enhances your in-house resources with technical experts available to support your Palo Alto Networks deployment. This level includes all Premium Support features and: • **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 the 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. • **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. • **Investment minimum**: Platinum Support has investment minimum thresholds that need to be met to purchase.
Focused Services	Provides personalized support through a designated customer advocate. Under this program, you are assigned a customer success manager to provide tailored support, including weekly reviews, root cause analysis for critical issues, release review, upgrade planning, and a quarterly business review. Your customer success 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 about our Customer Support plans.

Professional Services

Maintain confidence in your deployment, configuration, and operations.

Table 14: 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 platform's features 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. See the Service Descriptions for full details.
QuickStart Services	Expedites your successful deployment of firewall-as-a-service components with day-one protection. Expert planning and execution adhere to best practices, providing risk mitigation at every step. QuickStart Services are available for: • **Platform deployment**: Panorama and Next-Generation Firewall • **Subscriptions**: Threat Prevention, URL Filtering, DNS Security, SaaS Security, IoT Security, Enterprise DLP, SD-WAN hub deployment, and branch expansion • **Capability adoption**: User-ID, App-ID, SSL Decryption, and GlobalProtect See the Service Descriptions for full details.

Table 14: Palo Alto Networks Professional Services (continued)	
Offering	**Description**
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. Click here for details.
Extended	Provides access to product expertise, ongoing configuration assistance, and security threat specialists to continuously improve your security and 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 about our Professional Services offerings.

Education and Training

Keep your users skilled and educated with an array of educational services.

Table 15: Palo Alto Networks Education Services	
Offering	**Description**
Instructor-Led Training	Get the most out of your Palo Alto Networks investment with instructor-led cybersecurity training and curriculum. Authorized Training Partners (ATPs) deliver authorized Palo Alto Networks training courses in classroom and virtual delivery formats through public open enrollment and private onsite training.
Digital Learning	Learn at your own pace with a complete set of free digital learning courses that cover all the elements of our Next-Generation Firewall technology, from fundamentals to specialized role-based learning.
Credentialing	Palo Alto Networks Education Services provides a large portfolio of role-based certifications and microcredentials aligning with Palo Alto Networks cutting-edge cybersecurity technologies. Receiving a certification demonstrates that you're committed to cybersecurity and that your work aligns to set standards. Being a certified professional increases credibility and improves job efficiency and professional marketability.

Read more about our Educational Service 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