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 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 control across data center, perimeter, giving you consistent protection through exceptional operations through analytics and automation while 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.

**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.

**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.

**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.
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.