SECURITY OPERATING PLATFORM

PROTECTING YOUR DIGITAL WAY OF LIFE

paloalto NETWORKS®

PROTECTING OUR DIGITAL WAY OF LIFE

Today's highly digitized world enhances efficiency, business productivity and our general way of life. Yet this digitalization present new and dangerous cyber risks, resulting in an increase in the number of cyberattack victims every year. Businesses continue to adopt cloud, big data analytics and automation. These technological shifts, in combination with increasingly sophisticated threats, new legislation requirements – such as GDPR – and more demanding customers, makes security challenging. A new security approach is needed to keep up with these developments and mitigate risks so businesses can grow without disruption.

Security needs to be agile, consistent and effortless

Organizations need a security architecture that keeps up with digital developments, updated legislation and customer needs. In this complex world, it's impossible to be successful in security with non-integrated, legacy point products. An automated and integrated security platform is needed. Security needs to be agile, effortless and – most of all – it must enable, not obstruct, productivity.

Organizations improve their services through applications, enhancing the user experience and delivering significant competitive advantages. As team adopt cloud, big data analytics and automation to accelerate application delivery, user information, apps and data become increasingly distributed. This modernization leaves such information vulnerable and requires consistent automated security.

Security Operating Platform, rooted in automation and integration

The Palo Alto Networks® Security Operating Platform is built for automation. Accurate analytics allow you to focus on what matters – business priorities – and streamline routine tasks, while leveraging security staff efficiently. Tight integration across the platform and partner applications delivers continuous security across the network, cloud and endpoints, including mobile devices.

SECURITY OPERATING PLATFORM

The Security Operating Platform is Palo Alto Networks third and most recent evolution. It follows our first and second evolutions: the next-generation firewall and endpoint/cloud security, respectively.

This third evolution extends our automated approach, allowing organizations to add new capabilities that build on existing investments in our sensors and enforcement points. Palo Alto Networks innovative apps, along with third parties and customers, can access an organization's specific security data set to share threat intelligence, automate workflows, meet compliance and detect, react and monitor threats.

The platform's foundation contains advanced network, endpoint and cloud security. It is seamlessly extended by cloud-delivered services, such as:

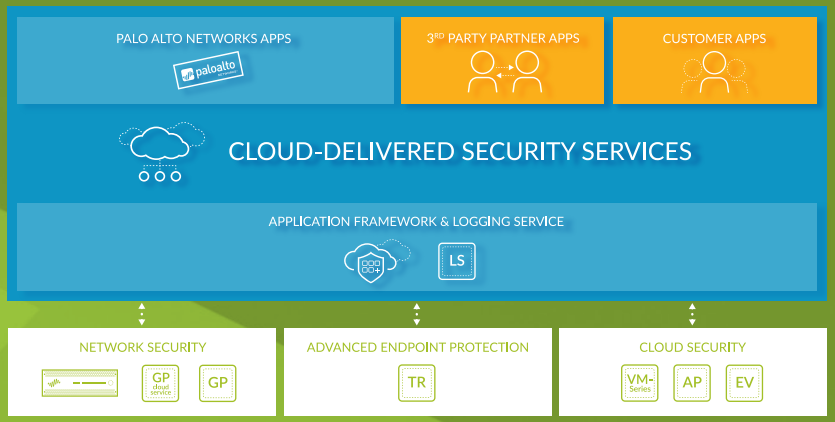
- **Threat Prevention** – blocks known malware, exploits and command-and-control activity on the network.
- **URL Filtering** – provides safe web access, including preventing users from malicious and phishing sites.
- **WildFire** – detects and prevents unknown threats, quickly sharing protections across the platform automatically.
- **AutoFocus** – provides threat intelligence with context to drive proactive response for unknown attacks.
- **MineMeld** – allows the aggregation of third-party threat intelligence and automates prevention from indicators of compromise, or IOCs.

The platform is open and extensible through our Application Framework and Logging Service, which host apps from Palo Alto Networks, third parties and customers. The following elements are also described in this document:

- **Application Framework** – enables to integrate apps into the security operating platform.
- **Logging Service** – provides the ability to centrally store logs in the cloud.
- **Magnifier** – detects active attackers in the organization with behavior-based analytics.

Security Operating Platform, based on Zero Trust

Our Security Operating Platform is based on a Zero Trust approach, which means security is focused on the business outcomes and designed from the inside out, starting with the "crown jewels": the assets and data that need protection. Zero Trust requires determining who gets access to what on a "need to know" or least-privileged basis, and all traffic is inspected and logged.



paloalto NETWORKS®

NETWORK SECURITY

NEXT-GENERATION FIREWALL

Palo Alto Networks Next-Generation Firewall (NGFW) – the first of its kind – serves as the foundation of our Security Operating Platform. It provides granular visibility and control over all applications – even those that try to evade detection by masquerading as legitimate traffic, hopping ports or using encryption (e.g., TLS/SSL or SSH).

The next-generation firewall:

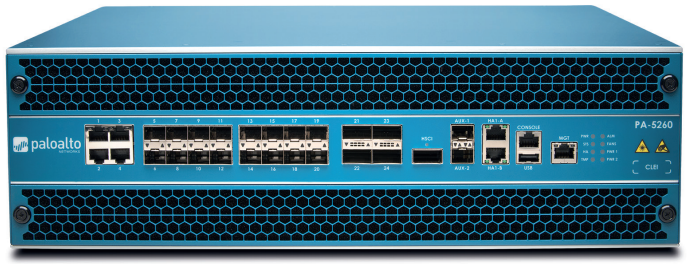
- Inspects and controls content traversing the network to detect and block known and unknown threats in a single pass.
- Proactively identifies and defends against unknown, new or custom malware and exploits.
- Maximizes performance using a single-pass software architecture that scans traffic only once, regardless of which features are enabled.

The NGFW uses a single-pass, parallel-processing architecture that utilizes App-ID™, User-ID™ and Content-ID™ technologies to identify applications and users, and scan the content, respectively. This combination provides the NGFW an unmatched set of network security capabilities.

PA-220

PA-800 Series

PA-5200 Series



App-ID

The App-ID™ application identification engine implemented in the NGFW accurately identifies applications in all traffic passing through the network. App-ID can:

- Automatically identify applications using multiple identification mechanisms, unlike legacy firewalls that identify applications only by their IP addresses, ports and protocols.
- Identify applications disguised as authorized traffic, using dynamic ports, or trying to go through the firewall via an SSL encryption tunnel.

Policy-based decryption is used to secure encrypted traffic:

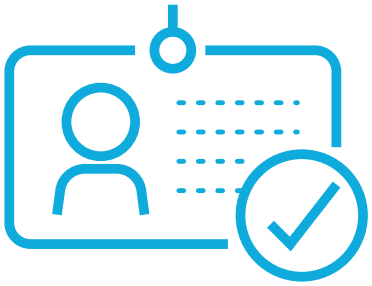
- Applies policy-based identification, decryption and inspection to inbound and outbound SSL traffic.
- Performs policy-based identification and control of SSH-tunneled traffic.

User-ID

Visibility into the application activity at the user level, not just by IP address, allows you to more effectively enable the applications traversing the network. You can align application usage with business requirements and, if appropriate, inform users they are in violation of policy, or even block their application usage outright.

By using User-ID™ user identification technology:

- Policies can be defined to safely enable applications based on users or groups of users, in either outbound or inbound directions; for example, allow only the IT department to use tools such as SSH, telnet and FTP on standard ports.
- With User-ID, policy follows the users no matter where they go – headquarters, branch office or at home – and whatever device they may use.
- Informative reports on user activities can be generated using any one of the predefined reports or by creating a custom report.



Content-ID

Content-ID™ content identification 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.

By using Content-ID, the NGFW can:

- Block vulnerability exploits, buffer overflows and port scans; protect against the evasion and obfuscation methods used by attackers; stop malware outbound communications; block access to known malware and phishing download sites; and reduce the risks associated with the transfer of unauthorized files and data.
- Use a single stream-based approach that simplifies management, streamlines processing and maximizes performance.

NETWORK SECURITY
GLOBALPROTECT

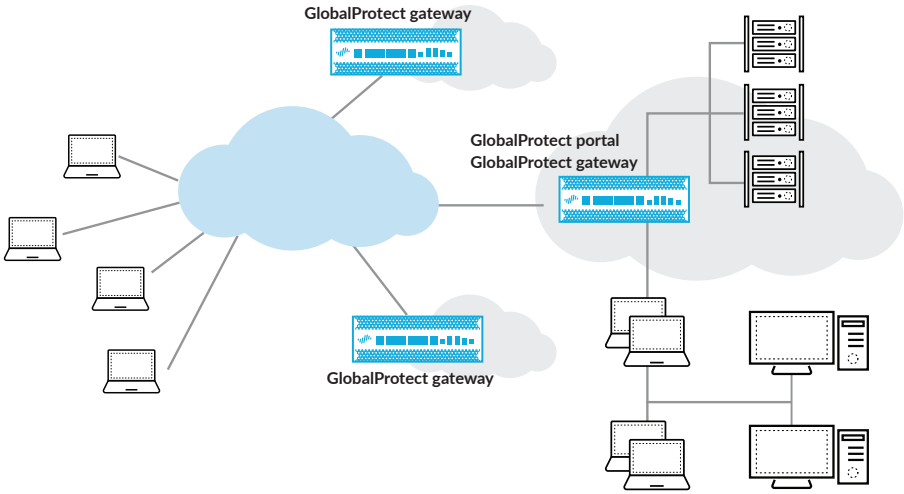
Delivers security to any user, any device, anywhere

GlobalProtect™ network security for endpoints stops targeted cyberattacks, evasive application traffic, phishing, malicious websites, command-and-control traffic, and known and unknown threats by extending the protection of the Security Operating Platform to the mobile workforce.

You can't secure what you can't see. The GlobalProtect subscription brings application traffic by all users to a NGFW for full visibility into application traffic, across all ports, all the time.

Securely enable BYOD and contractor access to applications

GlobalProtect provides secure options for BYOD (Bring Your Own Device). Access applications in the cloud and data center with clientless VPN. Enable support for per-app VPN using integration with enterprise mobility management, including AirWatch®, Intune and MobileIron®.



GLOBALPROTECT CLOUD SERVICE

Organizations must protect all applications and users, but many of them are in locations where this can be difficult. Cloud, branch expansion and mobility move applications and users beyond the perimeter, making traditional network security inefficient and ineffective. Organizations need security that is easy to deploy, simple to operate and scalable across all locations.

GlobalProtect cloud service prevents successful cyberattacks that target your remote networks and mobile users. It provides the full capabilities of the next-generation firewall, delivered as a service. Tight integration across the Security Operating Platform and ecosystem partners simplifies operations and helps your organization scale.

Prevent cyberattacks on the branch and mobile endpoints

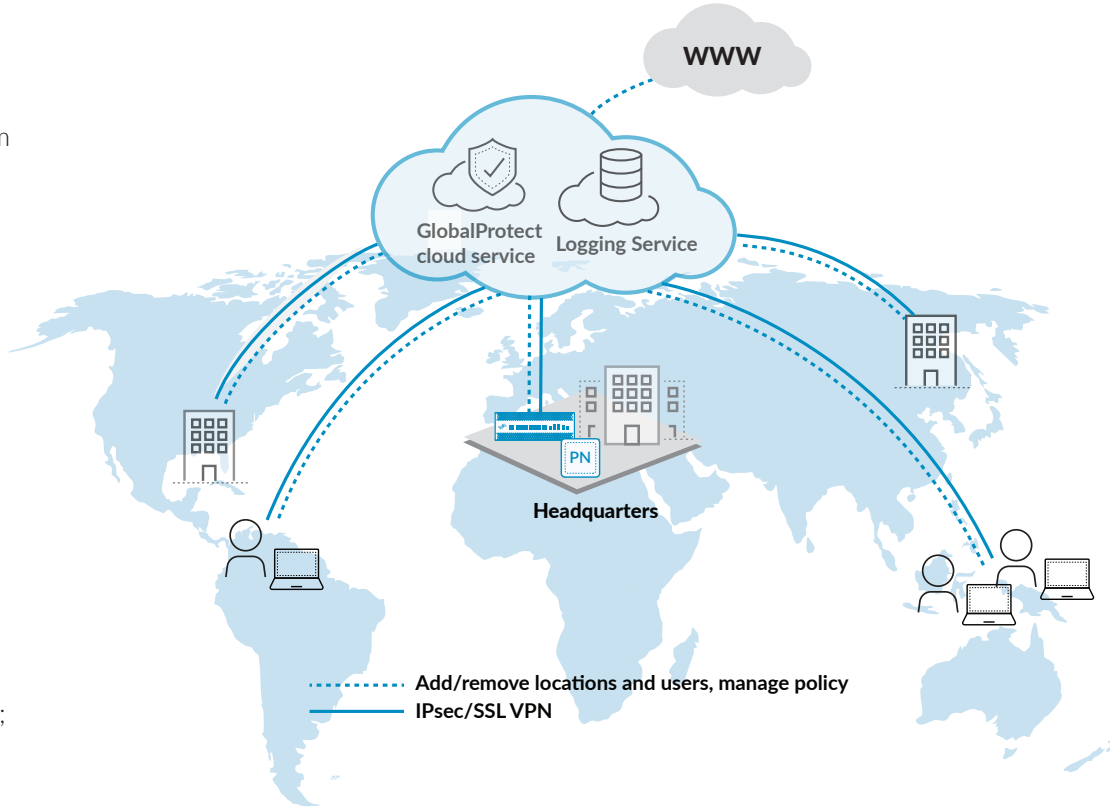
With GlobalProtect cloud service, you can protect branch offices, SD-WAN deployments and mobile users with the full capabilities of your next-generation firewall, delivered as a service. The extension of the NGFW into branches and remote users provides more visibility and higher protection against malware, exploits, ransomware and phishing attacks. It extends security policies across all network, endpoint and cloud devices regardless of location to ensure consistent protection.

Simplify and scale security

GlobalProtect cloud service automates the orchestration and roll out of security services. This time-saving deployment allows you to control operational costs for predictable security spending, with no hardware to install, manage or update; and deploy new platform features as they evolve to increase coverage and scale globally with cloud infrastructure flexibility and reach.

Consume innovations quickly

GlobalProtect cloud service integrates across the enterprise to protect the entire Security Operating Platform. It uses the Application Framework to apply new security innovations from Palo Alto Networks and third parties, all while extending centralized network security policy management across the campus, branch, data center and internal network.



NETWORK SECURITY
PANORAMA

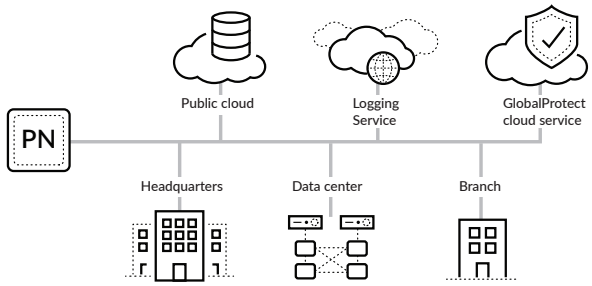
Panorama™ network security management provides static rules and dynamic security updates in an ever-changing threat landscape. Panorama provides a significant reduction of administrator workload and improves overall security posture with a single rule base for firewall, threat prevention, URL filtering, application awareness, user identification, file blocking and data filtering. Panorama provides centralized control of next-generation firewalls for the internet edge, data center, and private and public cloud deployments, managing the security architecture from a single management dashboard platform.

Integrated management platform

View and manage firewall traffic, device configuration, global policies and reports on traffic patterns or security incidents, all from a single console. Panorama is available either as a dedicated management appliance or as a virtual machine.

Panorama provides:

- Streamlined policy management
- Simplified operations
- Unparalleled network and threat visibility
- Comprehensive log collection, including logs from all your NGFWs and Traps flexible deployment options



Logs of next-generation firewalls under Panorama are stored and managed in an integrated manner:

Unified Visibility: Applications of all managed next-generation firewalls, URLs, threats and data (e.g., files and patterns) can be graphically displayed.

Flexible Policy Control: Globally consistent policy control as well as local level policy control are supported, allowing well-balanced security management based on requirements.

Flexible Deployment Options: Deployment with a dedicated management appliance (e.g., M-100, M-200, M500 or M-600), as a virtual machine on VMware® ESXi™, or in public cloud environments, such as Amazon® Web Services and Microsoft® Azure®.

Panorama can be deployed in three different modes:

1. Panorama
2. Management Only
3. Log Collector

- In the Panorama deployment mode, Panorama controls both policy and log management functions for all the managed devices.
- In the Management Only deployment mode, Panorama manages configurations for the managed devices but does not collect or manage logs.
- In the Log Collector deployment mode, Panorama collects and manages logs from the managed devices. This assumes that another deployment of Panorama is operating in Management Only deployment mode.

The separation of management and log collection enables the Panorama deployment to meet scalability, organizational and geographical requirements. The choice of form factor and deployment mode gives maximum flexibility for managing Palo Alto Networks next-generation firewalls in a distributed network.

M-100

M-200

M-500

M-600

Panorama Specifications
Number of Devices Supported
• Up to 1,000
High Availability
• Active/Passive
Administrator Authentication
• Local database • RADIUS • SAML • LDAP • TACACS+
Management Tools and APIs
• Graphical User Interface (GUI) • Command Line Interface (CLI) • XML-based REST API

Public Clouds Supported
Amazon AWS
Microsoft Azure

Private Hypervisor Specifications			
	Management Only Mode	Panorama Mode	Log Collector Mode
Cores Supported	4 CPUs	8 CPUs	16 CPUs
Memory (minimum)	8 GB	32 GB	32 GB
Disk Drive	81 GB system disk	2 TB to 24 TB log storage	2 TB to 24 TB log storage

Public Cloud Instance Types (BYOL License)			
	Management Only Mode	Panorama Mode	Log Collector Mode
Amazon AWS	t2.xlarge m4.2xlarge	m4.2xlarge m4.4xlarge	m4.4xlarge c4.8xlarge
Microsoft Azure	D4_V3 Standard D4S_V3 Standard	D16_V3 Standard	D16_V3 Standard D32_V3 Exceeds

ADVANCED ENDPOINT PROTECTION

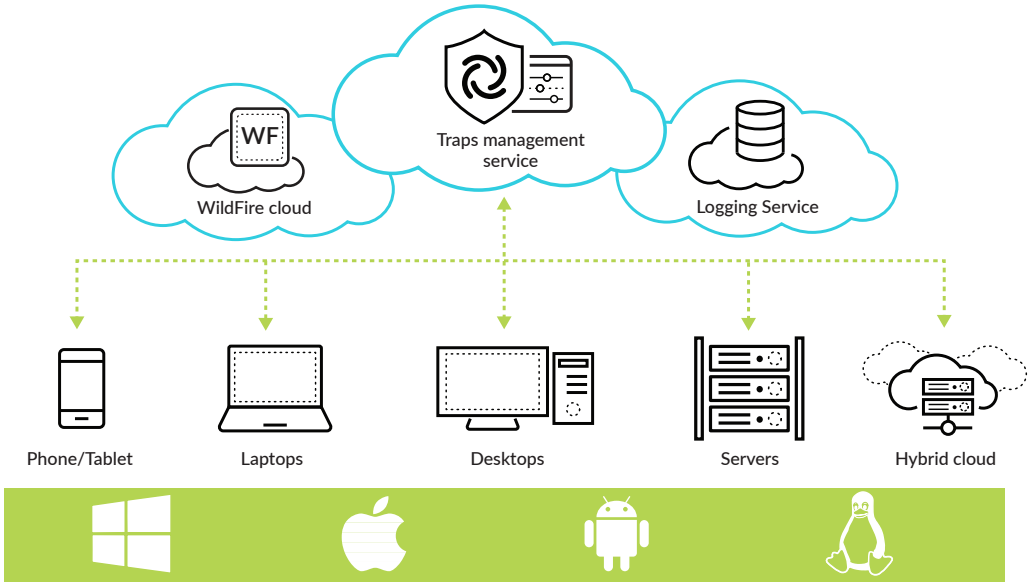
TRAPS

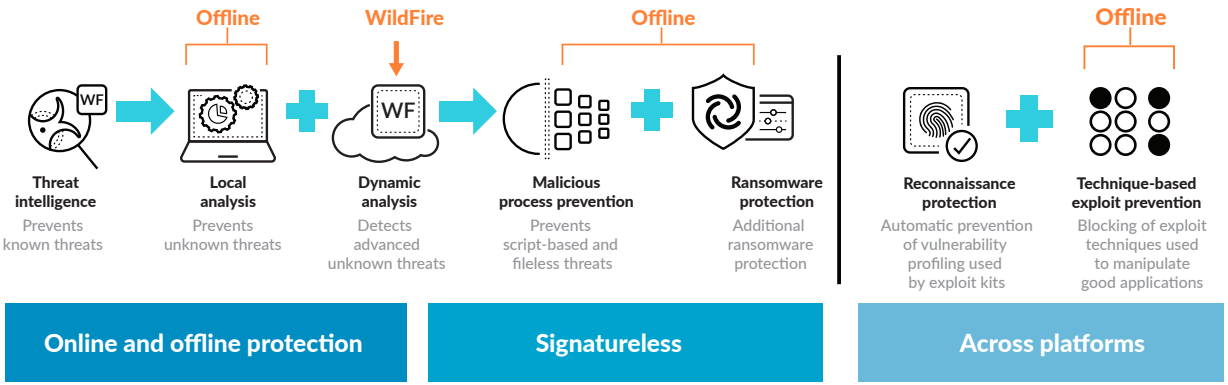
Palo Alto Networks Traps™ advanced endpoint protection stops threats on the endpoint and coordinates enforcement with cloud and network security to prevent successful cyberattacks. As a lightweight agent, Traps minimizes endpoint infections by blocking malware, exploits and ransomware. It can be used for Windows®, macOS®, Android® and Linux operating systems, and can be managed on-premises or from the cloud.

paloalto NETWORKS®

Multiple methods of malware prevention

Traps prevents the execution of malicious files with an approach tailored to combat both traditional and modern attacks. Additionally, administrators can utilize periodic scanning to identify dormant threats, comply with regulatory requirements and accelerate incident response with endpoint context.





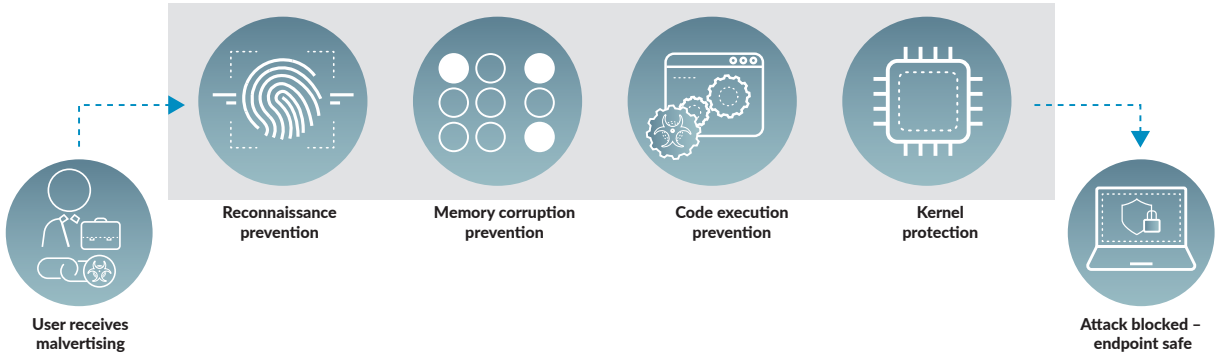
- **Threat intelligence:** Traps leverages the intelligence obtained from tens of thousands of subscribers to the WildFire malware prevention service to continuously aggregate threat data and maintain the collective immunity of all users across endpoints, networks and cloud applications. Traps queries WildFire, and WildFire returns a near-instantaneous verdict on whether the file is malicious or benign. If the file is unknown, Traps proceeds with additional prevention techniques to determine whether it is a threat that should be terminated.
- **Local analysis via machine learning:** If a file remains unknown after the initial hash lookup and has not been identified by administrators, Traps uses local analysis via machine learning on the endpoint – trained by the rich threat intelligence of WildFire – to determine whether the file can run, even before receiving a verdict from the deeper WildFire inspection.
- **Dynamic analysis:** In addition to local analysis, Traps sends unknown files to WildFire for discovery and deeper analysis to rapidly detect potentially unknown malware. WildFire uses independent techniques for high-fidelity and evasion-resistant discovery. These are:
  - **Static analysis** via machine learning – a more powerful version of local analysis, based in the cloud, that detects known threats by analyzing the characteristics of samples prior to execution.
  - **Dynamic analysis** – a custom-built, evasion-resistant virtual environment in which previously unknown submissions are detonated to determine real-world effects and behavior.
  - **Bare metal analysis** – a hardware-based analysis environment specifically designed for advanced threats that exhibit highly evasive characteristics and can detect virtual analysis.

If WildFire determines a file to be a threat, it automatically creates and shares a new prevention control with Traps and other components of Palo Alto Networks Security Operating Platform in as few as five minutes, ensuring the threat is immediately classified as malicious and prevented, should it be encountered again.

- **Malicious process prevention:** Traps prevents script-based and fileless attacks by default with out-of-the-box, fine-grained controls over the launching of legitimate applications, such as script engines and command shells.
- **Ransomware protection:** In addition to existing multi-method prevention measures, including exploit prevention, local analysis and WildFire, Traps monitors the system for ransomware behavior. Upon detection, it immediately blocks attacks and prevents encryption of customer data.

Multiple methods of exploit prevention

Traps is unique for its ability to prevent exploits through technique identification and a protection focused model. Traps targets the techniques that any exploit-based attack must use to manipulate a software vulnerability.



Multiple methods of prevention stop zero-day attacks

By preventing these techniques, Traps is able to protect unpatched systems, unsupported legacy systems, applications IT is unaware of – commonly known as shadow IT – and never-before-seen exploits, also called zero-day exploits.

Traps delivers exploit prevention using multiple methods, including:

- **Pre-exploit protection:** Traps prevents the vulnerability-profiling techniques exploit kits use prior to launching attacks. By blocking these techniques, Traps prevents attackers from targeting vulnerable endpoints and applications, effectively preventing the attacks before they begin.
- **Technique-based exploit prevention:** Traps prevents known, zero-day and unpatched vulnerabilities by blocking the exploitation techniques attackers use to manipulate applications.
- **Kernel exploit prevention:** Traps prevents exploits that leverage vulnerabilities in the operating system kernel to create processes with escalated privileges. Traps also protects against new exploit techniques used to execute malicious payloads, such as those seen in 2017's WannaCry and NotPetya attacks.

By blocking the techniques, Traps provides customers three important benefits:

1) **Protects unpatchable applications and shadow IT.**
2) **Minimizes the risks associated with delayed patching.**
3) **Prevents zero-day exploits from succeeding.**

Besides malware and exploit prevention, Traps is also capable of:

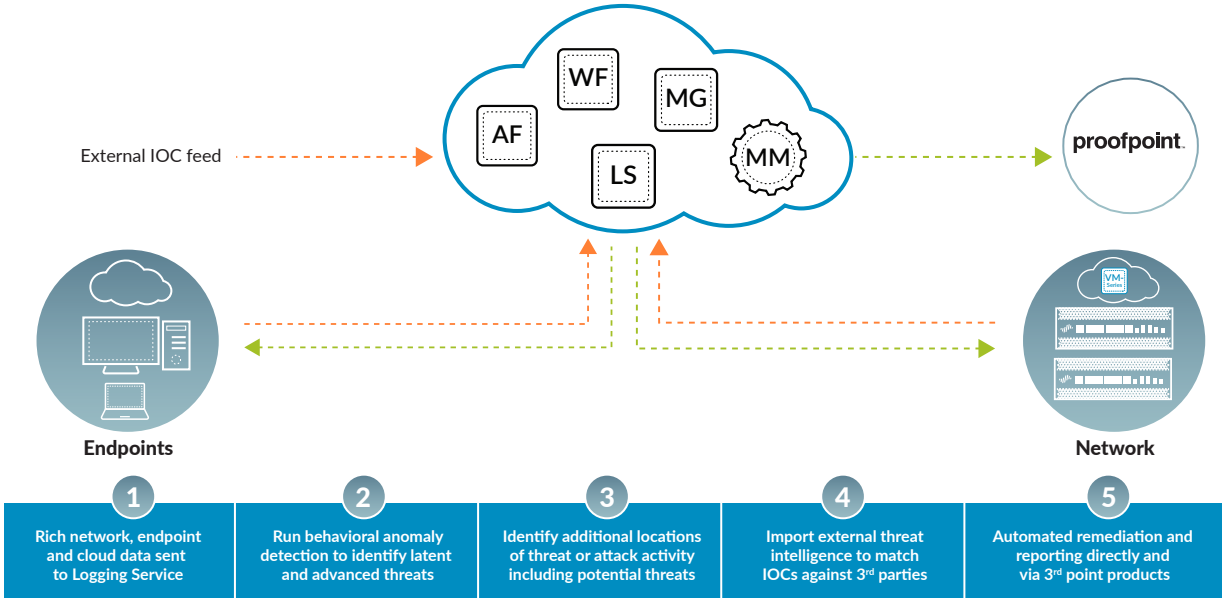
- **Scanning:** Administrators can scan endpoints and attached removable drives for dormant malware, with an option to automatically quarantine it for remediation when found.
- **Admin override policies:** Traps enables organizations to define policies based on the hash of an executable file, controlling what is or isn't allowed to run in their environments.
- **Malware quarantine:** Traps is capable of immediately quarantining malicious executable files, DLLs and Office files to prevent propagation or execution attempts of infected files.
- **Grayware classification:** Traps enables organizations to identify non-malicious but otherwise undesirable software, such as adware, and prevent it from running in their environments.
- **Execution restrictions:** Traps enables organizations to easily define policies to restrict specific execution scenarios to reduce the attack surface of any environment.

Coordinated enforcement with network and cloud

Traps plays a key role within the Security Operating Platform.
Traps shares the malware discovered on endpoints with WildFire, which automatically creates and shares new prevention controls with Traps and our NGFWs in as few as five minutes, without human intervention. This enhances the entire security architecture by preventing unknown malware that may have otherwise passed through perimeter defenses to infect unprotected endpoints.

Traps sends its logs to the Logging Service.
This enables security operations teams to view endpoint security logs in the same context as their firewall logs and correlate activities observed on the network and endpoints. This unified picture of security events across the environment enables security teams to detect threats that may have otherwise evaded detection. Plus, in conjunction with automated policies, they can eliminate attack surfaces across their entire environment, from endpoints to firewalls to cloud and SaaS applications.

Traps puts it all together.
Once Traps has identified that there is malware on the endpoint, the endpoint can be automatically added to a Dynamic Address Group with a policy that isolates that endpoint from the rest of the network, and perhaps submits a service ticket to the security team either to remediate the situation or so that when a user calls to report no network connectivity, the security team is aware of the history. What was once a manual process, can now be done automatically, without human intervention.

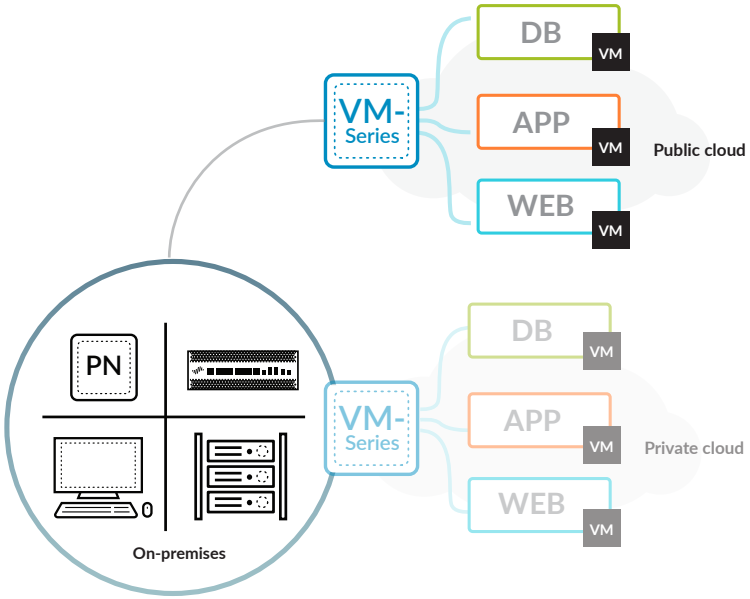


CLOUD SECURITY
VM-SERIES

For many organizations, the cloud is the sole route to market for new application deployment. It affords greater agility and scalability, higher performance, and faster access to innovative technologies, all of which help businesses maintain a competitive edge. As a result, data and applications now reside in a multitude of cloud environments (e.g., private clouds, public clouds and SaaS applications). This movement to the cloud requires consistent, automated protections across multi-cloud deployments that prevent data loss and business disruption. Palo Alto Networks understand these needs and developed our cloud security portfolio with these requirements in mind. That's why our cloud security products cover several cloud variants in an agile and consistent way, all highly automated and integrated within the Security Operating Platform:

- **Private Cloud:** VM-Series
- **Public Cloud:** VM-Series, Evident and Traps
- **SaaS:** Aperture

A virtualized form of our next-generation firewall, the VM-Series, can be deployed in a range of private and public cloud computing environments. The VM-Series protects private and public cloud deployments by enabling applications and preventing threats. Traffic is classified based on the application, not the port, giving full visibility into your threat exposure. This allows you to reduce your threat footprint with application-based policies as well as prevent threats and data exfiltration.



Secure virtualized data centers and private cloud

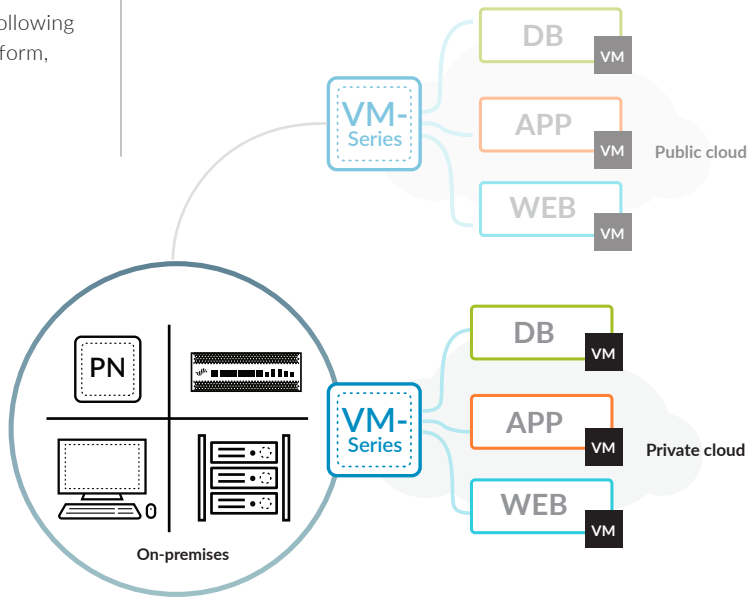
Virtualized data center are essentially a private cloud, and you are responsible for managing all aspects of the virtualization, hardware, compute, networking and security. The VM-Series protects your private cloud infrastructure using application enablement policies while simultaneously preventing known and unknown threats. The VM-Series supports the following private cloud environments: VMware® ESXi™ and NSX®, Cisco® ACI™, Citrix® NetScaler® SDX™, Microsoft® Hyper-V®, and KVM/OpenStack®.

Protect public cloud deployments

Public cloud environments, such as AWS, Microsoft Azure or Google Cloud Platform, provide greater agility, scalability and infrastructure consistency than traditional data centers, yet the risk of data loss and business disruption remain. Embedding the VM-Series in the application development lifecycle to complement native security services can prevent data loss and business disruption, allowing your public cloud migration to accelerate. The VM-Series supports the following public cloud environments: AWS®, Google® Cloud Platform, Microsoft® Azure® and VMware® vCloud® Air™.

Automation is needed for keeping up with your business

VM-Series automation features enable you to expedite the deployment of consistent security in private and public clouds. For example, bootstrapping can automatically provision a VM-Series with a working configuration, complete with licenses and subscriptions, and then auto-register the firewall with Panorama management. VM-Series configuration changes can be automated to dynamically drive security policy updates using native cloud tools and templates based on third-party tools, such as Terraform® and Ansible®, from our LIVE Community.



The VM-Series

The VM-Series consists of five models that deliver App-ID-enabled throughput that ranges from 200 Mbps for the VM-50 to 16 Gbps for the VM-700. To learn more about the performance and capacities of the VM-Series, please see the firewall comparison tool:

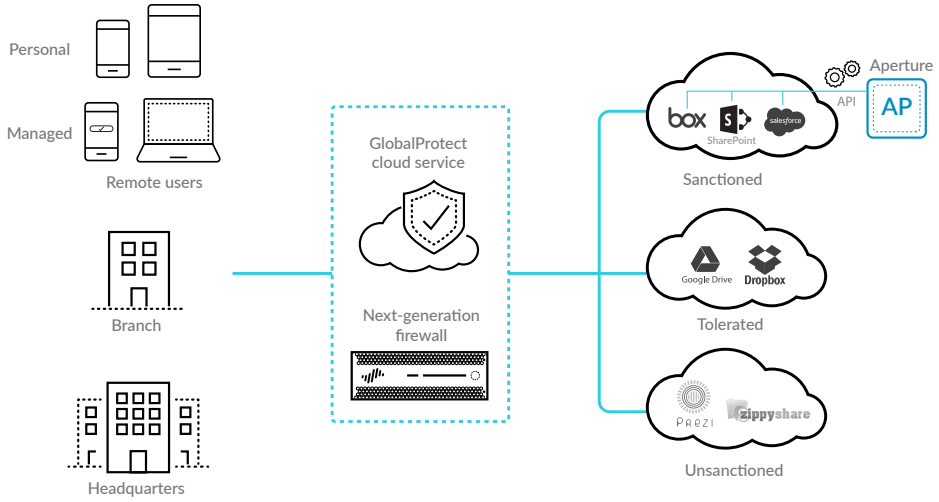
go.paloaltonetworks.com/productselection

CLOUD SECURITY
APERTURE

The use of software as a service, such as Office 365®, Box and Salesforce® provides tremendous value to end users through easy setup and collaboration capabilities. While these innovative SaaS applications greatly increase business productivity, they also contain hidden threats like accidental data exposure, malicious outsiders, promiscuous sharing and so forth.

To start gaining and maintaining control of SaaS usage, you must clearly define the allowed SaaS applications and the behaviors within those applications that are allowed. This requires a clear definition of which applications are allowed, or "sanctioned," and which applications are not allowed, or "unsanctioned," and then putting processes in place to control their access and usage.

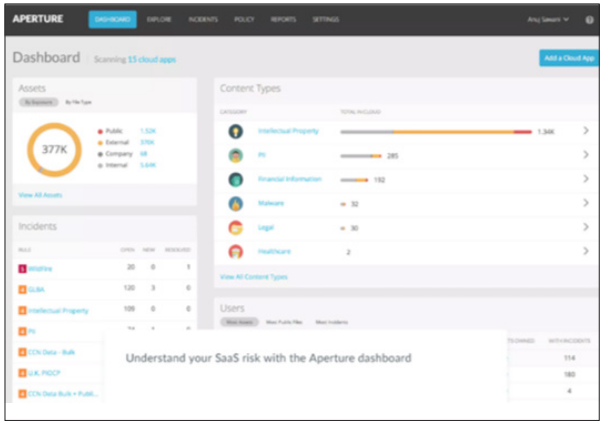
Aperture™ SaaS security service helps mitigate risks. It establishes a direct connection to SaaS applications to provide data classification, data leakage prevention and threat detection so organizations can secure their sanctioned SaaS applications.



Cloud-delivered CASB capabilities

With Aperture you'll meet cloud access security broker, or CASB, needs, including inline capabilities that inspect all traffic – including applications, threats and content – and tie it to the user, regardless of location or device type. Aperture extends these capabilities by connecting directly to cloud applications via an API to gain deep visibility into your data or applications, and it can apply granular policy and consistent control. Aperture delivers complete visibility and reporting, instant classification, and fine-grained enforcement across users, folders and file activities – so you can protect your data in the cloud.

Aperture provides complete visibility across all user, folder and file activity, generating detailed analysis that transitions from a position of speculation to one of full awareness at any given point in time (see the Aperture dashboard that follows). Deep analytics into day-to-day usage allow you to quickly determine data risk or compliance-related policy violations. This provides detailed analysis of user and data activity to enable detailed data governance and forensics.



Aperture enables you to define granular, context-aware policy control to drive enforcement as well as quarantine users and data as soon as violations occur. This enables you to quickly and easily satisfy data risk compliance requirements, such as those related to PCI and PII data, while still maintaining the benefits of cloud-based applications.

Advanced threat prevention

The WildFire malware analysis service integrates with Aperture to provide advanced threat prevention to block known malware, and we are the only CASB to identify and block unknown malware. You can keep threats from spreading through the sanctioned SaaS applications, preventing a new insertion point for malware. New malware discovered by Aperture is shared with the rest of the Security Operating Platform, strengthening your overall security posture.

Aperture Highlights

Aperture is a completely cloud-delivered service, without the need for any proxies or agents. It communicates directly with SaaS applications and looks at data from any source, regardless of the device or location from which the data originates. As Aperture isn't inline, it doesn't impact the latency or bandwidth of applications, and it doesn't affect the end-user experience. It just works.

CLOUD SECURITY
EVIDENT

Public cloud adoption is increasing, and DevOps teams are eager to harness its abilities to accelerate the delivery of apps and services. However legacy security tools can't keep pace with these developments. What's needed is a more complete, automated, frictionless approach to securing public cloud deployments and validating compliance.

Evident, from Palo Alto Networks, brings speed, scale and efficiency to public cloud security monitoring and compliance validation. It delivers a uniquely effective combination of continuous security monitoring, compliance validation and reporting, along with comprehensive storage security. Now, teams can confidently develop and deploy new applications in the cloud faster, simplify security operations, and continuously validate the compliance of their cloud infrastructure.

Continuous monitoring of cloud infrastructure services

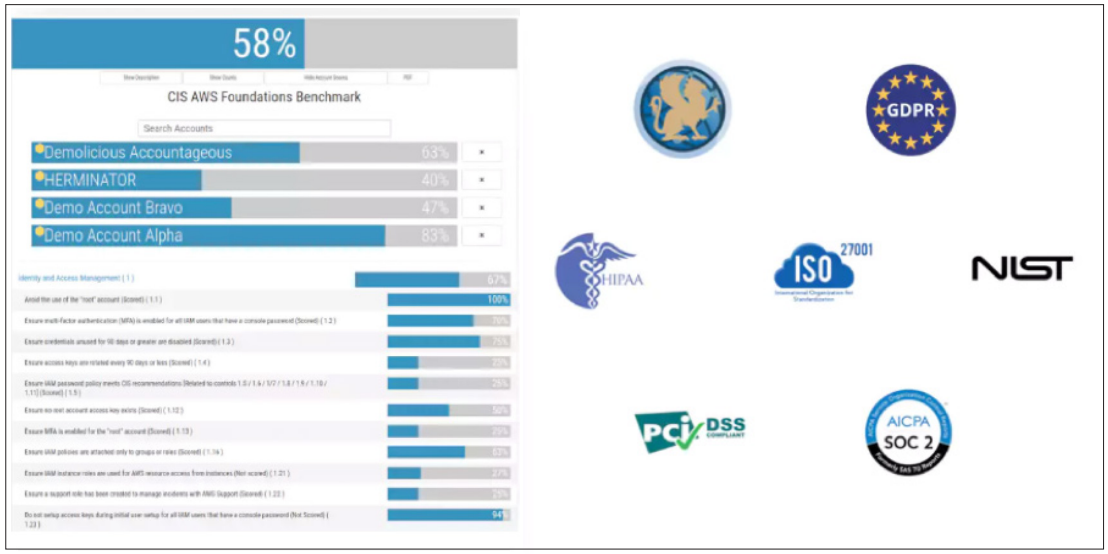
Speed is essential for DevOps teams today more than ever. The public cloud offers the speed and scale to support DevOps requirements, but security cannot be compromised. Evident was built for continuous monitoring of public clouds using the API control plane. By analyzing and prioritizing risks and policy violations, security and DevOps teams have a clear view of the risks in their cloud environment, on an ongoing basis, throughout the application lifecycle.

Using read-only access of the public cloud API, Evident securely collects data about your cloud services and continuously performs checks against security best practices, as well as any custom security checks you've defined, to determine if there are any potentially exploitable vulnerabilities.

Continuous compliance reporting

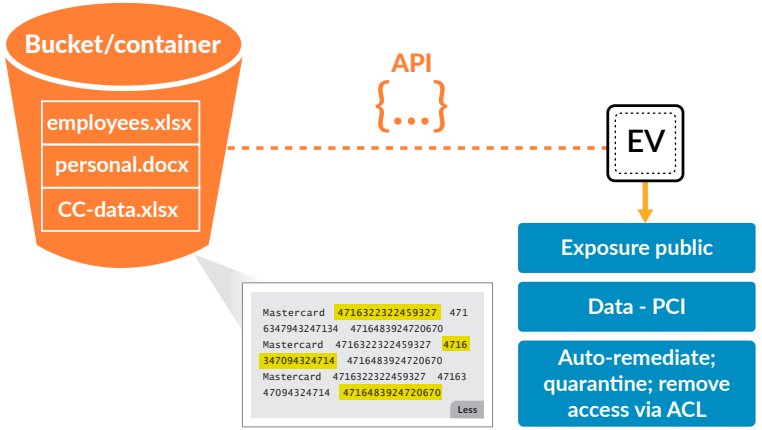
As compliance requirements increase and expand in scope, security leaders, stakeholders and industry regulators are demanding continuous measurement and validation of compliance status.

Evident delivers continuous, automated compliance audits and provides customizable one-click compliance reports. You can continuously monitor compliance by cloud account and use click-through controls to resolve issues. Evident also enables continuous validation of your overall public cloud security posture in the face of fast-changing configurations and development requirements.



Comprehensive storage security

Storage volumes within public cloud services are an often-overlooked source of security threats and attacks. With Evident, you can discover and classify data within containers and buckets; evaluate your exposure based on policy; auto-remediate publicly exposed data; and quarantine malware – so you can be assured that your use of public cloud storage does not expose your company to new security vulnerabilities.



SECURITY SERVICES

APPLICATION FRAMEWORK

Consuming cybersecurity innovations has become nearly impossible. Teams spend more time testing, integrating and operating disconnected tools than stopping threats. Organizations must continue innovating defenses as attackers quickly evolve their tactics. Data needed to fuel analytics is dispersed across multiple tools and formats, limiting its effectiveness. Organizations waste time deploying new sensors every time they want to collect a new piece of data as well as managing point products rather than improving security controls to stay ahead of attackers.

Consume apps from an open ecosystem of innovative developers

The Palo Alto Networks Application Framework enables you to consume security innovations quickly and efficiently. The framework extends the capabilities of the Palo Alto Networks Security Operating Platform with APIs and an SDK that connect apps with rich data, threat intelligence and enforcement points. You can consume apps from an open ecosystem of trusted developers, using apps for detection, analytics, automated prevention and rapid response. The cloud-delivered approach lets you focus on using new capabilities, instead of spending time deploying and operating them. The framework lets you continually improve security by adopting apps from multiple providers, without additional infrastructure.

Rapidly adopt new detection and prevention capabilities

The Palo Alto Networks Application Framework uses innovate apps to solve emerging security needs. In so doing, it minimizes manual efforts, speeds detection response time and automates prevention capabilities.

Harness your data for analytics and action

The Application Framework provides more insight, investment and value from your data, sensors and enforcement points. Specifically, it enriches investigation and accelerates response efforts through attack classification, user and group content, and third-party threat intelligence.

Accelerate response

To prevent successful cyberattacks, security teams must be able to investigate and rapidly – or even automatically – respond to attacks. Working across the platform, the Application Framework automates security enforcement. Teams use their existing Security Operating Platform components as consistent enforcement points, effectively stopping attacks before damage is done. Security analysts streamline prevention for the entire organization, driven from accurate decisions and recommendations.

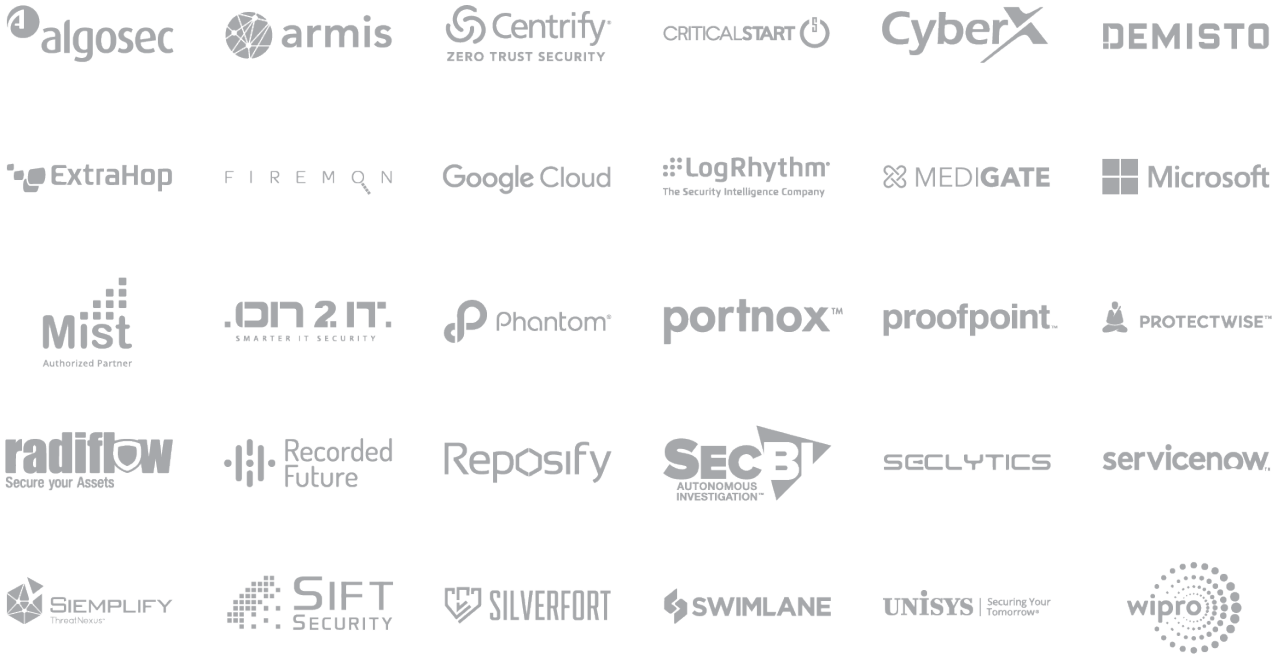
Consume apps from an ecosystem of developers

The Cloud Services Portal on the Application Framework allows users to consumer new applications quickly through cloud delivery and streamlined deployment and usage. This feature allows users to save development time by rapidly building apps with Application Framework APIs and SDK.

Palo Alto Networks Application Framework

Realize the power of the Application Framework with apps

The developer ecosystem is open, allowing the community to continuously solve new security use cases as an extension of the Security Operating Platform. Security teams can quickly consume innovative capabilities without the need to provision additional sensors or enforcement points.



SECURITY SERVICES

WILDFIRE

WildFire® malware prevention service automatically detects and stops unknown attacks. Going beyond traditional sandboxing, threats are identified with advanced analysis to maximize security effectiveness. WildFire automatically delivers protections within minutes across network, mobile and cloud, stopping attackers in their tracks. Stay ahead of the latest attack techniques by using innovative cloud-delivered detection engines that continuously improve using threat data shared across a growing global community.

The largest cloud-delivered malware analysis service in the world, WildFire:

- Uses data sciences to leverage machine learning, combined with advanced malware analysis, which includes static, dynamic and bare metal analysis to execute and analyze suspicious files.
- Generates and distributes protections for detected malware in as few as five minutes.
- Shares malware detection information worldwide in the cloud, and updates both detection logic and the custom-built virtual environment continuously to respond to the latest threats.

More than 24,000 customers worldwide are connected to WildFire and its ability to conduct static analysis (characteristics of a file), dynamic analysis (behavior of a file) and bare metal analysis.

Identify unknowns with a unique multi-technique approach

WildFire utilizes not only static analysis – a look at the characteristics of a file – but also dynamic analysis – a detailed look at the behavior of a file – in its process of detecting unknown threats. In addition, WildFire uses machine learning to apply new knowledge to future analysis requests and bare metal analysis specifically designed to analyze malware that can "hide itself," when it detects a virtual sandbox environment.

As a cloud-delivered service, new capabilities like dynamic unpacking and network traffic profiling are constantly being added to detect the most obfuscated malware:

- Static analysis
- Dynamic analysis
- Machine learning
- Bare metal analysis

The contents are executed and detected on various operating systems, such as Windows and those of mobile devices:

- Various files: Windows PE (EXE and DLL), PDF, Microsoft Office, Java, Android APK, Linux ELF, ZIP, 7ZIP, RAR and Adobe Flash (6.1 and later) are supported.
- Links in emails are accessed and analyzed to know whether the websites contain any threats.

Generate protections in as few as five minutes

After a threat is detected, you need automatic protection from the threat without manual intervention. When WildFire detects new malware, it automatically generates signature protection mechanisms and distributes the indicators of compromise attributes to all WildFire customers worldwide in less than five minutes.

- In addition to anti-malware signatures, C2 signatures, DNS-based callback signatures and malicious URLs are distributed globally in as few as five minutes.
- An average of 230,000 daily protections are delivered through the WildFire service.

Benefit from flexible deployment

WildFire, running in a cloud environment, provides scalability and high expandability of the sandbox environment. However, for customers who don't want to share their data in the WildFire cloud, there's an on-site version appliance available, the WF-500, which also supports various malware analyses:

- An advance malware analysis environment in the cloud that does not require consideration of processing capacity.
- New applications, versions and filetypes are supported as needed.
- Distributed operations are possible, such as files downloaded from the web are analyzed by the cloud service and files attached to email are analyzed by the on-site appliance.

Easily understand WildFire reports

Security managers can access WildFire analysis reports on the management screen or via the WildFire portal and through the AutoFocus dashboard to see how malware will behave and affect the system when the file is opened.

WildFire reports enable incident response teams to quickly and easily respond to new threats and build preventive control measures for them.

SECURITY SERVICES

MAGNIFIER

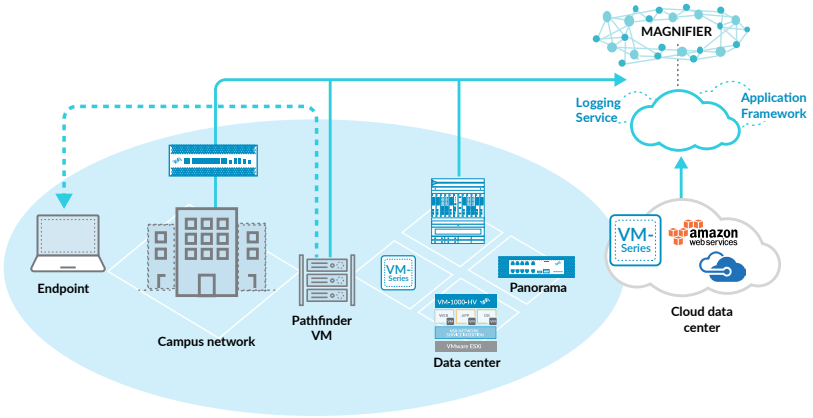
Palo Alto Networks Magnifier™ behavioral analytics rapidly hunts and stops threats with cloud-delivered behavior-based analytics and machine learning.

Magnifier:

- Automatically detects active attacks using supervised and unsupervised machine learning.
- Focuses security analysts on the most critical threats by delivering a small number of actionable alerts.
- Accelerates investigations by interrogating endpoints to find the executable files responsible for attacks.
- Collects comprehensive data at cloud scale with the Logging Service and avoids the need for new network appliances, agents or log servers.

Detect, investigate and eliminate threats fast

Magnifier empowers organizations to quickly find and stop the stealthiest network threats. By analyzing rich network, endpoint and cloud data with machine learning, Magnifier accurately identifies targeted attacks, malicious insiders and compromised endpoints. Security analysts can rapidly confirm threats by reviewing actionable alerts with investigative detail and then leverage Palo Alto Networks Next-Generation Firewall to block threats before the damage is done.



Disrupt every stage of an attack

By thwarting each step of an attack, organizations limit opportunities for attack success. Magnifier detects and stops command and control, lateral movement, and data exfiltration by detecting behavioral anomalies indicative of attack. Magnifier delivers powerful behavior-based protection, augmenting the existing ability of Palo Alto Networks Security Operating Platform to stop attacks across the attack lifecycle.

Automate attack detection with behavioral analytics

Magnifier automatically pinpoints active attacks, allowing security analysts to focus on the threats that matter. It starts by analyzing rich data stored in the Logging Service from our next-generation firewalls, including information on users, devices and applications. Magnifier examines multiple logs, including Enhanced Application Logs, which provide data specifically designed for analytics, allowing Magnifier to track attributes that are nearly impossible to ascertain from traditional threat logs or high-level network flow data.

Swiftly stop attacks with Palo Alto Networks Next-Generation Firewall

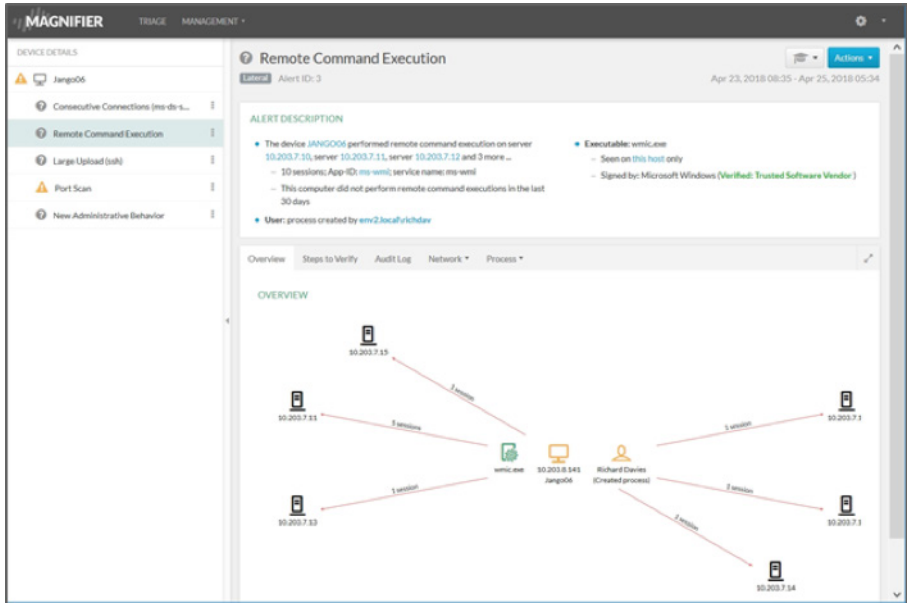
To prevent successful cyberattacks, security analysts must respond quickly when they identify threats. Using their Palo Alto Networks Next-Generation Firewall, analysts can block compromised devices and restrict access to malicious sites to shut down attacks. Magnifier empowers security analysts to efficiently detect, investigate and block advanced threats.

Accelerate investigations with user, device and process context

To reduce investigation time, Magnifier produces a small number of accurate, actionable alerts, as well as information about the user, application and device obtained through App-ID and User-ID technology. Magnifier also eliminates lengthy forensic investigations by interrogating endpoints to determine which process or executable initiated an attack. Then, Magnifier ascertains whether the endpoint process is malicious by integrating with WildFire malware prevention service to analyze the process.

Ease deployment and streamline operations with cloud scale and agility

Palo Alto Networks Security Operating Platform provides a superior approach to detection and response by leveraging existing infrastructure to monitor network activity and a cloud-delivered service for data storage and on-demand scaling. As part of this better approach, our next-generation firewalls monitor network traffic and extract metadata expressly designed for analytics. Magnifier uses this data, along with Pathfinder endpoint analysis, to profile user and device behavior without requiring organizations to provision new network sensors or agents. Our Logging Service delivers efficient log storage that scales to handle the large volumes of data needed for behavioral analytics.



SECURITY SERVICES
AUTOFOCUS

Prioritized threats at your fingertips

AutoFocus™ contextual threat intelligence service saves time and resources through accelerating analysis, correlation and prevention workflows. Unique, targeted attacks are automatically prioritized with full context, allowing security teams to respond to critical attacks faster, without additional IT security resources.

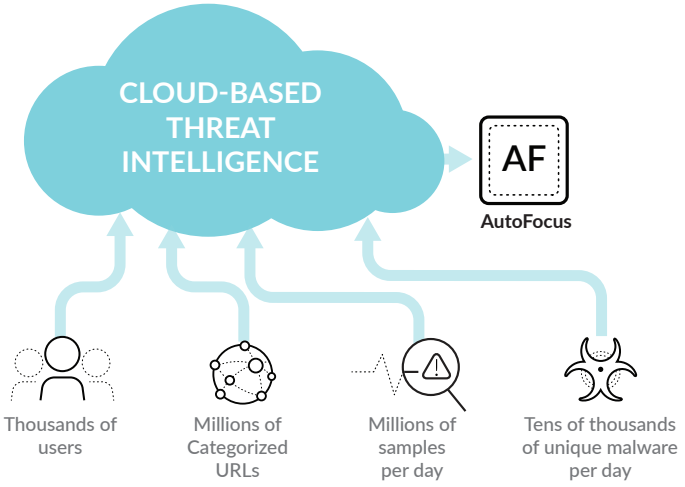
Assistance with determining security priorities

AutoFocus enables you to distinguish the most important threats from everyday commodity attacks. Now, instead of seeing that a malicious event has occurred, you immediately know the context around an attack, such as the malware family, campaign or malicious actor targeting your organization. When identified, AutoFocus will alert your security team about high-priority events, enabling you to take swift action to mitigate their impact.

Visibility into the unknown

AutoFocus provides unprecedented visibility into unknown threats, with the collective insight of tens of thousands of global enterprises, service providers and governments feeding the service. AutoFocus correlates and gains intelligence from:

- WildFire – the industry's largest malware analysis environment
- PAN-DB URL filtering service
- MineMeld – aggregates/correlates third-party intelligence in AutoFocus
- Traps advanced endpoint protection
- Aperture SaaS-protection service
- Unit 42 threat intelligence and research team
- Intelligence from technology partners
- Palo Alto Networks global passive DNS network



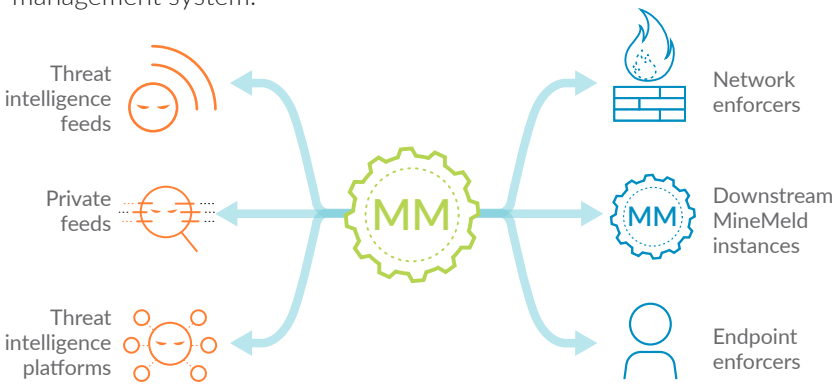
Accelerated analysis and simplified workflows

Legacy approaches to securing the organization rely on aggregating an increasing number of detection-focused alerts with complex analysis workflows after the event.

AutoFocus puts the entire wealth of Palo Alto Networks threat intelligence at your fingertips, dramatically cutting the time it takes to conduct analysis, forensics or hunting efforts. Threat intelligence and context are available directly in PAN-OS®, Panorama management and the AutoFocus portal for in-depth searching across IOCs.

Aggregate third-party intelligence

Organizations rely on multiple sources of threat intelligence to ensure the widest possible visibility into emerging threats, but they struggle to aggregate, correlate, validate and share indicators across different feeds. As part of AutoFocus, the MineMeld™ threat intelligence syndication engine provides a single unified threat feed and indicator management system.



Prevention driven by threat intelligence

Security teams require more than just raw threat intelligence – they need automatic transformation into actionable controls to prevent future attacks. AutoFocus simplifies workflows to create and enforce new controls, from fully automated to user-directed, within the same unified security platform.

Find the important events

Tags & statistical analysis highlight critical events

Who is behind the attack

Identify the actor and attack techniques

Respond to the incident

Block relevant indicators

SECURITY SERVICES
LOGGING SERVICE

Simplify log management to bolster security

Log management shouldn't be complicated or expensive. Unfortunately, many security teams today struggle to store and manage all the log data they need for security. They invest inordinate resources installing, managing and updating complex log infrastructure—rather than investigating threats. To unlock the full potential of machine learning and analytics, security teams need easy, cost-effective log management.

Palo Alto Networks Logging Service simplifies log management and allows you to effectively use your data to prevent attacks. Built for massive scale, the Logging Service provides a secure way to collect log data from your network, endpoints and cloud that is economical and easy to operate. You can get ahead of attackers by employing your data to power security services and innovative Application Framework apps, while avoiding on-premises log collection infrastructure.

Automate log storage with a hands-free cloud-delivered service

The Logging Service collects data across the Palo Alto Networks Security Operating Platform at high scale. Built for big data and analytics, it allows you to take advantage of the latest search, batch processing and streaming technologies without needing specialized IT staff. By eliminating on-premises log storage, you can also avoid burdensome installation and maintenance tasks.

The Logging Service can monitor security events and track system status on the network, endpoints and cloud security infrastructure. Store log data for Panorama network security management, GlobalProtect cloud service and Traps management service in a single location that's accessible by the entire security team. Panorama leverages the Logging Service data to deliver exceptional visibility from a single pane of glass. Panorama uses its analytics and correlation engine to make sense of log data while the Application Command Center provides consolidated visibility and enables you to drill down into specific data sets.

Key benefits

- Collect log data at massive scale using a cloud-delivered service designed for big data and analytics.
- Streamline security operations by storing rich data designed for analytics.
- Automatically detect stealthy threats using innovative security apps that analyze Logging Service data.

Improve agility and ease of use

The Logging Service is ready to scale from the time you start using it. There's no waiting for hardware to ship or investing resources to plan for space, power and high availability requirements of your log infrastructure. We take care of all storage and compute needs to provide analytics and insights you can use. The reliable Logging Service includes built-in hardware redundancy and buffering of log traffic to prevent data loss.

Log storage capacity can be purchased based on current logging needs. If your requirements change in future, you can update your Logging Service subscription. You can log all the data you need for security without worrying about rearchitecting your log infrastructure as your storage demands grow.

Streamline operations by collecting rich, consistent security data

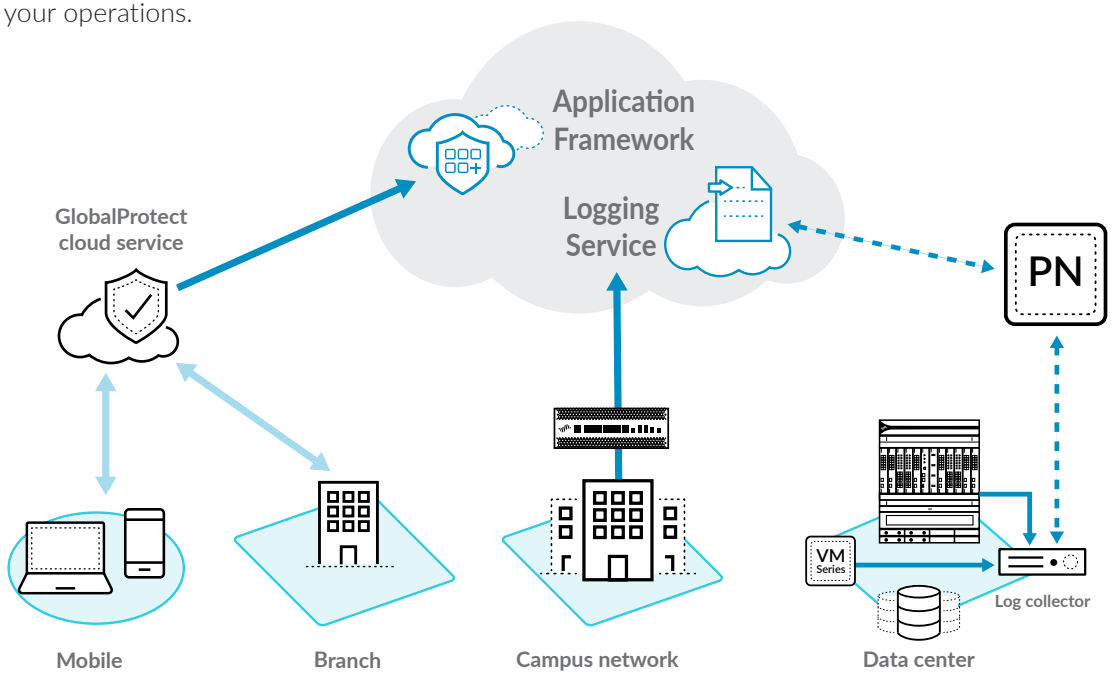
The Logging Service allows for quick implementation of machine learning and analytics by gathering comprehensive, consistent security data that is organized for analytics. There is no need to normalize log data from different sources; you can immediately start analyzing traffic logs, threat logs, application logs, threat intelligence and more without cumbersome data processing.

Because the Logging Service is designed for high performance, security analysts can query indexed data at lightning speed, speeding up their investigations. Plus, you can gain peace of mind knowing the Logging Service has achieved SOC 2 Type II plus certification for security and privacy.

Take advantage of innovative Application Framework apps

The Logging Service allows you to harness the value of your log data for security. You can quickly provision Application Framework apps for analytics, orchestration and more. These apps can access your Logging Service data to uncover threats and satisfy reporting requirements.

The Palo Alto Networks Security Operating Platform provides an efficient way to gather, store and analyze your security data. You can use your security infrastructure as adaptable sensors to collect data, avoiding the need to deploy new network appliances and agents. Most importantly, you can store your data in the Logging Service and allow Application Framework apps, as well as management systems – like Panorama, Traps management service and GlobalProtect cloud service – to use this data to optimize your security and your operations.



Security professionals within organizations seek relevant intelligence about threats to their organizations. Threat intelligence is essential to understanding what's going on in the cyber domain and how it impacts organizations and businesses.

To help protect our way of life in the digital age, Palo Alto Networks established Unit 42 – a world-class threat research team – from the ground up in 2014. Situated within our chief security officer's organization, Unit 42 does not focus on any particular product or service, instead working to help all organizations better understand their adversaries.

Unit 42 comprises experts in malware analysis, reverse engineering, intelligence analysis and threat hunting. Team members placed strategically around the globe work to build relationships with key government and law enforcement agencies. While the team's research is not a service or product itself, Unit 42's work informs the Palo Alto Networks Security Operating Platform. Customers benefit from the interlock between human threat intelligence and automated enforcement with Unit 42-issued AutoFocus tags and WildFire.

Sharing threat intelligence quickly and efficiently across the security community is critical to preventing successful cyberattacks. Palo Alto Networks co-founded the Cyber Threat Alliance, or CTA, in 2014 to enable real-time threat information sharing among cybersecurity organizations. Unit 42 drives this information sharing alliance and works to build relationships with other organizations that can benefit from accurate and timely intelligence. Besides the contribution to the CTA, Unit 42 reports are shared publicly at researchcenter.paloaltonetworks.com/unit42/.

CYBER THREAT ALLIANCE

CUSTOMER SUCCESS
SECURITY LIFECYCLE REVIEW

The Security Lifecycle Review (SLR) summarizes the business and security risks facing an organization, providing an opportunity to review the findings and take joint action on them during an initial evaluation or as part of a regular visibility and security checkup. The review integrates existing Application Visibility data with WildFire malware prevention service, SaaS-based application visibility and more. Findings are based on data collected by an on-site device or submitted to the WildFire cloud during a specified time period, including applications, SaaS-based applications, URL traffic, content types, and known and unknown threats traversing the network.

Benefits of an SLR

- Visibility into the applications and threats exposing vulnerabilities.
- Analysis of all application traffic on the network, the capacity impact of these applications and the relative security risks observed.
- Comparison data for the customer's organization versus their industry peers.
- High-risk URL categories on the network.
- Known and unknown malware information.
- Key areas to focus on for reducing risk exposure.

The Security Lifecycle Review is a complimentary service providing an overview of your network and application risk vulnerabilities.

To utilize the Security Lifecycle Review service, visit go.paloaltonetworks.com/assessmentslr.

CUSTOMER SUCCESS

PREVENTION POSTURE ASSESSMENT

The Prevention Posture Assessment is a comprehensive, vendor-agnostic analysis of your organization's security posture. It covers perimeter, data center, cloud, SaaS, endpoint, analytics, stakeholder alignment and more. It's an opportunity for customers to gain an overall understanding of their posture, gaps, and how different prevention capabilities bridge those gaps. The deliverable is a detailed gap analysis with specific recommendations.

Our PPA is provided to teams willing to gain these insights through time and effort. In the assessment, we hold a guided discussion including all relevant stakeholders from security, IT and DevOps teams. As a group, we discuss the prevention capabilities your organization has deployed in each area of architecture. The assessment helps you and your team understand the deployed prevention capabilities and those that need to be enabled.

Assess your current security strategy

Participating in a Prevention Posture Assessment is an eye-opening experience that provides visibility into your entire organization's security capabilities, pinpoints areas that require improvement, and prioritizes actions to address security gaps.

Adopt a prevention-based architecture

Most organizations adopt new security innovations to keep pace with the increasing sophistication and scale of threats. Unfortunately, if these aren't fully implemented, the result is gaps in your protection. The desire to improve prevention capabilities is faced with challenges in deploying and operationalizing the full feature set of technologies. By adopting a prevention-based architecture, you can resolve these issues. The PPA can help you get started.

Attain a prioritized roadmap for improvements

After your team participates in the PPA guided discussions, we evaluate the current state of the organization and provide a customized report highlighting findings and recommendations that improve protection. These recommendations support the qualitative data collected throughout assessment, and the report can be used as a roadmap to help your organization reach its desired future state.

To participate in a Prevention Posture Assessment, visit go.paloaltonetworks.com/ppa.

CUSTOMER SUCCESS

BEST PRACTICE ASSESSMENT

The Best Practice Assessment is a comprehensive evaluation of your organization's security deployment configurations. It is available to all Palo Alto Networks customers. The assessment analyzes system's policies and compares them against leading best practices in a pass-fail breakdown. For every policy that does not meet best practices, we provide a set of recommendations on how to align with them best practices. The BPA is a complimentary service to you, and it represents our investment in your success.

Increase configuration confidence

Running the BPA in your environment establishes a baseline of controls, measures progress toward enabling additional controls over time, and compares your organization's trends against peers in your industry. The information is intuitively displayed and can be filtered in numerous ways, including by device group and network zone. It also allows you to drill down on configurations not aligned to best practices.

Simple to run

Running a BPA is simple and only requires a tech support file from your NGFW or Panorama deployment. The output is complete in seconds and available for exploration (see the heatmap below). It can be repeatedly run over time to track progress.

Create a roadmap to better prevention

A BPA analyzes your deployment and measures the adoption of capabilities across your security infrastructure:

- Receive a comprehensive security health check and evaluate the status with your existing policy configurations.
- Create a roadmap of critical policy configuration changes and measure the progress of your implementation.
- Leverage tools to improve your prevention capabilities by following our recommended best practices.

For more information visit: go.paloaltonetworks.com/transformationservices.

CUSTOMER SUCCESS
TRANSFORMATION SERVICES

We want you to have all the tools, best practices and assistance necessary to effectively protect your organization from successful cyberattacks. Our goal is to help build and implement a security strategy focused on prevention, automation and operational transformation that fully utilizes your investment. This is a transformation of people, processes and procedures directly aligned with business needs, delivered by Palo Alto Networks Professional Services and our extensive network of partners, enabling a level of confidence that is unprecedented.

Stay ahead of threats with automation

Automation is the key to staying ahead of threats. With transformation services, we will help you automate processes and enhance security controls that dynamically update to match application usage, user activity and content.

Simplify operations to secure the business

Standardizing operations will reduce business risk and increase protection with full feature adoption. Our consultants will help increase efficiency in your operations and provide consistency between your IT and security teams through process integration.

Increase confidence in your controls

Confidence in your controls comes from measurable outcomes aligned with the needs of your business. Configuration confidence and operational confidence are gained through available tools (see the Best Practice Assessment), along with traffic analysis, to assure that the Security Operating Platform is operating as intended. Professional Services consultants and engineers will enable your teams, so they can effectively assess your controls throughout the transformation process.

For more information, visit www.paloaltonetworks.com/services/consulting.html.

Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
Support: +1.866.898.9087

www.paloaltonetworks.com