Threat Prevention

Best-in-Class IPS Solution for Known Threats[1]

Organizations face a barrage of attacks from threat actors driven by various motives, including profit, ideology/hacktivism, or even organizational discontent. Today's attackers are well-funded and well-equipped. They use evasive tactics to gain footholds in target networks and launch advanced attacks at high volume. By leveraging sophisticated playbooks to breach an organization, attackers move laterally and extract valuable data, all while remaining invisible to traditional independent defenses.

Business Benefits

- **Eliminate cost and management of standalone IPS.** Leverage Snort and other powerful IPS capabilities, integrated with our NGFW for a single security policy rule base.
- **Gain visibility into attacks, ensuring your organization is protected.** Inspect all traffic for threats, regardless of port, protocol, or encryption.
- **Reduce resources needed to manage vulnerabilities and patches.** Automatically block known malware, vulnerability exploits, and C2.
- **Take advantage of full threat detection and enforcement** of prevention controls without sacrificing performance.

1. *2019 Next Generation Firewall Comparative Report*, NSS Labs, July 17, 2019, https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/nss-2019/nss-labs-2019-ngfw-security.pdf.

To make matters worse, traditional intrusion prevention or detection systems (IPS/IDS) still use the same defensive strategies they did before the threat landscape evolved. Traffic is only inspected on certain ports, and while adding single-function devices to the defensive stack may alleviate certain problems, it results in poor performance and a lack of overall visibility. Furthermore, the basics are often left uncovered, putting the onus on security teams who are not properly resourced to identify or patch vulnerabilities to confidently avoid data breaches. According to a 2019 Ponemon survey, 67% of respondents feel they have insufficient time and resources to mitigate all vulnerabilities to avoid breaches.[2]

Comprehensive Exploit, Malware, and Command-and-Control Protection for Your Network

Palo Alto Networks Threat Prevention service protects your network by providing multiple layers of security, confronting threats at each phase of an attack. In addition to traditional IPS capabilities, Threat Prevention has the unique ability to detect and block known threats on any and all ports instead of invoking signatures based on a limited set of predefined ports.

Our latest innovation, Advanced Threat Prevention, builds on the existing capabilities of Threat Prevention to stop zero-day attacks inline—an industry first. (See the "Stop Zero-Day Threats Inline" callout for more.)

Our worldwide community of customers shares collective global threat intelligence, significantly reducing the success rate of advanced attacks by stopping them shortly after they are first encountered. Threat Prevention benefits from our other cloud-delivered security subscriptions for daily updates that stop exploits, malware, malicious URLs, and command and control (C2). A necessity for every Palo Alto Networks NGFW, Threat Prevention can speed prevention of new unknown threats to near-real time when paired with additional Palo Alto Networks security services, including Advanced WildFire malware prevention service for unknown file-based threats, Advanced URL Filtering for web-borne attacks, DNS Security for attacks using the Domain Name Service, and IoT Security for unmanaged device visibility and context.

Stop Zero-Day Threats Inline

Palo Alto Networks Advanced Threat Prevention is the industry's only IPS to reliably stop never-before-seen C2 attacks and exploit attempts. With custom-built inline deep learning engines, block 60% more zero-day injection attacks, in addition to 48% more highly evasive command and control compared to traditional IPS solutions. Learn more here.

Key Capabilities

Enable the Application, Prevent the Threat

Applications are integral to how companies do business. Because of that, they've been made more readily available to users by entering networks using encrypted channels through nonstandard ports (often to bypass stateful inspection firewalls) and port-hopping to guarantee users always have access.

Unfortunately, advanced threats take advantage of this behavior to get free rides into networks, undetected. They tunnel within applications, hide in encrypted traffic, and prey on unsuspecting targets to get a foothold within a network and execute malicious activity.

We protect your network against these threats by providing multiple layers of prevention, confronting threats at each phase of the attack. In addition to traditional IPS capabilities, Threat Prevention can detect and block threats on any and all ports. Instead of invoking signatures based on a limited set of predefined ports, Threat Prevention leverages User-ID and App-ID technology on our ML-Powered NGFWs to add context to all traffic, enabling the Threat Prevention engine to never lose sight of a threat, regardless of evasion techniques.

An increasing amount of enterprise traffic is being obscured by TLS/SSL encryption, and adversaries are exploiting the resulting lack of visibility to launch attacks and introduce more risk to your business. Our ML-Powered NGFWs offer native decryption, and Threat Prevention offers the ability, via policy, to selectively decrypt and inspect TLS/SSL traffic to strike an appropriate balance between security and performance.[3]

Eliminate Threats at Every Phase

Countless breaches over the years can be attributed to attackers bypassing single-purpose defensive tools. To ensure holistic protection, the Threat Prevention subscription, with its tight integration with our ML-Powered NGFWs, brings together multiple defensive mechanisms:

- **Heuristic-based analysis** detects anomalous packet and traffic patterns, such as port scans, host sweeps, and denial-of-service (DoS) attacks.

2. *Gaps in Resources, Risk and Visibility Weaken Cybersecurity Posture*, Ponemon Institute, February 2019, https://www.balbix.com/app/uploads/Ponemon-Survey-Vuln-Management-.pdf.
3. To view throughput with Threat Prevention enabled for a specific Palo Alto Networks firewall, see the product summary spec sheet.

- **Easy-to-configure, custom vulnerability signatures** allow you to tailor intrusion prevention capabilities to your network's unique needs, even importing rules from popular open source formats such as Snort and Suricata.
- **Other attack protection capabilities**, such as blocking invalid or malformed packets, IP defragmentation, and TCP reassembly, protect against evasion and obfuscation techniques.

Palo Alto Networks employs natively integrated defensive technologies to ensure that when a threat evades one technology, another catches it. The key to effective protection is to use security features that are purpose-built to share information and provide context around both the traffic they're inspecting and the threats they're identifying and blocking.

Scan for All Threats in a Single Pass

The Threat Prevention engine represents an industry first by inspecting and classifying traffic as well as detecting and blocking both malware and vulnerability exploits in a single pass. Traditional threat prevention technologies require two or more scanning engines and multiple rule bases that need to be managed separately, adding significant latency and management overhead while dramatically slowing throughput performance. We use a uniform signature format for all threats to ensure rapid processing by performing all analyses in a single, integrated scan, eliminating redundant processes common to traditional solutions.

Our Threat Prevention technology combs each packet as it passes through the platform, looking closely at byte sequences within both the packet header and payload. From this analysis, we're able to identify important details about a 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 provided by the arrival order and sequence of multiple packets to catch and prevent evasion techniques. All of this happens within one scan, so your network traffic remains as fast as you need it to be.

Leverage Intrusion Prevention

Threat-based protections detect and block exploit attempts and evasive techniques at both the network and application layers, including port scans, buffer overflows, remote code execution, protocol fragmentation, and obfuscation. Protections are based on signature matching and anomaly detection, which decodes and analyzes protocols and uses the information learned to send alerts and block malicious traffic patterns. Stateful pattern matching detects attacks across multiple packets, taking into account arrival order and sequence, and making sure all allowed traffic is well-intentioned and devoid of evasion techniques. Within our intrusion prevention technology:

- **Protocol decoder-based analysis** statefully decodes the protocol, and then intelligently applies signatures to detect network and application exploits.
- **Protocol anomaly-based protection** detects non-RFC-compliant protocol usage, such as an overlong URI or FTP login.
- **Easy-to-configure, custom vulnerability signatures** allow us to tailor intrusion prevention capabilities to your network's unique needs.

Because there are many ways to exploit a single vulnerability, our intrusion prevention signatures are built based on the vulnerability itself, providing more thorough protection against a wide variety of exploits. A single signature can stop multiple exploit attempts on a known system or application vulnerability.

Use Custom Signatures for Emerging Threats

Threat Prevention also provides flexible support for Snort and Suricata rule conversion, providing rapid protection for newly discovered vulnerabilities. This support, along with ongoing custom signature development, addresses a key use case and underlying goal for IPS in addition to completely eliminating the need for standalone IPS or IDS solutions. Namely, signature coverage for unconfirmed or emerging vulnerabilities acts as a stopgap before a verified update can be deployed to all of your organization's software and applications. With the conversion support, you can automatically convert, sanitize, upload, and manage Snort and Suricata rules, allowing you to take advantage of intelligence feeds while saving time and effort imposed by traditional signature-based IPS technologies. You can leverage exposed APIs to automate the process of applying new Snort rule coverage across your environment.

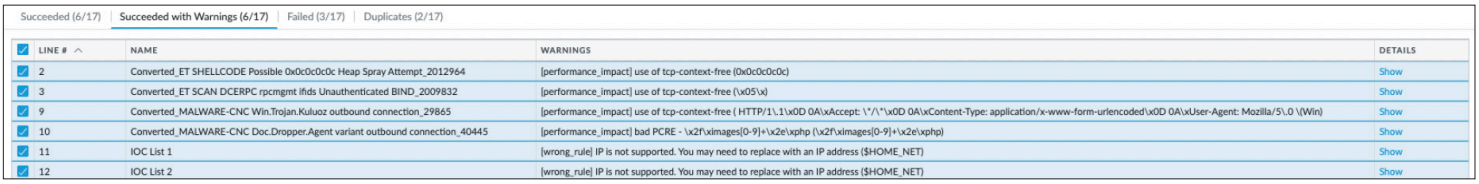

Figure 1: Snort support on PAN-OS

Protect Against Malware

By using signatures based on payload, not hash, inline malware protection blocks malware before it ever reaches the target host. This includes known malware and future variants, even those not yet seen in the wild. Our stream-based scanning engine protects your network without introducing significant latency, which is a serious drawback of network antivirus offerings that rely on proxy-based scanning engines. Stream-based scanning inspects traffic as soon as the first packets of the file are received, eliminating threats as well as the performance issues associated with traditional standalone solutions. Key antimalware capabilities include:

- **Inline, stream-based detection and prevention** of malware hidden within compressed files and web content.
- **Protection against payloads** hidden within common file types, such as Microsoft 365 documents and PDFs.
- **Updates from Advanced WildFire** to ensure protection against highly evasive malware.

Signatures for all types of malware are generated directly from billions of samples collected by Palo Alto Networks, including previously unknown malware sent to Advanced WildFire, our Unit 42 threat research team, and third-party research and technology partners around the world.

Payload-Based vs. Hash-Based Signatures

Signatures based on payload detect patterns in the body of a file that can be used to identify future variations of that file, even if the content has been slightly modified. This allows us to immediately identify and block polymorphic malware that would otherwise be treated as a new unknown file.

Signatures based on hash match on the fixed encoding unique to each individual file. Because a file hash is very easily changed, hash-based signatures are not effective at detecting polymorphic malware or variants of the same file.

Integrate with Advanced WildFire

Extend your protection against zero-day malware and C2 attacks with the Advanced WildFire service, the largest cloud-based prevention engine that uses machine learning, a custom hypervisor, and crowdsourced intelligence to protect organizations from the hardest-to-detect threats. The cloud-based service employs a unique multitechnique approach that combines static, dynamic, and introspective analysis to detect and prevent highly evasive malware. Once identified, Threat Prevention applies verdicts in real time to all ML-Powered NGFW form factors, instantly stopping threat proliferation across your enterprise.

Protect Against Command and Control

There's no silver bullet when it comes to preventing all threats from entering the network. After initial infection, attackers will communicate with the host machine through a C2 channel, using it to pull down additional malware, issue further instructions, and steal data. Our C2 protections home in on those unauthorized communication channels and cut them off by blocking outbound requests to malicious domains and from known C2 toolkits installed on infected devices.

Palo Alto Networks goes beyond standard automation of C2 signatures based on URLs and domains. We automatically generate and deliver researcher-grade C2 signatures based on malicious traffic seen by Advanced WildFire at machine speed and scale. These signatures are payload-based and can detect C2 traffic even when the C2 host is unknown or changes rapidly. You can extend overall C2 protection even further with the DNS Security subscription, which can defeat adversary attempts to hide C2 channels using DNS tunneling tactics.

Extend Protection Against Zero-Day Attacks with Advanced Threat Prevention

Malicious actors are leveraging automation and readily available tooling, such as Cobalt Strike, to increase zero-day attacks while using evasion techniques, such as encryption and encoding, to bypass traditional security solutions.

Extend industry-leading Threat Prevention capabilities to block all known exploits, C2, and malware, including encrypted traffic. Palo Alto Networks Advanced Threat Prevention prevents 96% of web-based Cobalt Strike C2, in addition to 90% of injection attacks such as SQLi.

With purpose-built deep learning engines, Advanced Threat Prevention leverages multiple deep learning and machine learning models running in the cloud. The models are aligned to key protocols, such as SSL, HTTP, unknown UDP, and unknown TCP with specific models also identifying C2 traffic from tools such as Cobalt Strike.

As traffic traverses the firewall, a small prefiltered portion of traffic goes to the cloud for analysis, with a response sent back to the firewall to determine if the traffic should proceed. Based on these tuned models and integration with the NGFW, Advanced Threat Prevention provides real-time inline prevention of zero-day attacks.

Learn more about Advanced Threat Prevention here.

Reduce the Attack Surface

Working seamlessly with the built-in, prevention-focused features of the ML-Powered NGFW, Threat Prevention and the added capabilities from Palo Alto Networks cloud-delivered security subscriptions enable you to significantly reduce your organization's attack surface and associated business risk. This section provides some examples of the complementary technologies.

SSL Decryption

The vast majority of enterprise network traffic is encrypted, which leaves a gaping hole in network defenses if it's not decrypted and scanned for threats. Our platform's built-in SSL Decryption service can selectively decrypt inbound and outbound SSL traffic. After decryption, all traffic is fully inspected and—if confirmed to be safe—re-encrypted before being allowed through to its destination.

File Blocking

Executable files constitute a massive share of the malicious files used in spear phishing attacks, and employee negligence is considered a major security risk, since many may not know what's safe and what isn't. Reduce the likelihood of a malware infection by preventing dangerous file types known to hide malware, such as executable files, from entering your network. File blocking functionality can be combined with User-ID to block unnecessary files based on users' job roles, making sure all users have access to the files they need and providing you with a granular way to reduce your exposure based on your organization's requirements. You can further decrease the number of attack opportunities by sending all allowed files to Advanced WildFire for analysis to determine if they contain zero-day malware.

Drive-by Download Protection

Unsuspecting users can inadvertently download malware merely by visiting a favorite website—even a site's owners may not know it's been compromised. Our Threat Prevention technology identifies potentially dangerous downloads and sends a warning to the user to ensure that the download is intended and approved. Within Threat Prevention, detection of such "phishing kit" landing pages as well as detection of web shell files (which aim to enable remote administration of web servers to target other internal systems) are packaged and delivered as spyware signatures. You can extend these capabilities and prevent attacks from new and rapidly changing domains by tying this feature to Advanced URL Filtering and file blocking policies.

The Power of Palo Alto Networks Security Subscriptions

Today, cyberattacks have increased in volume and sophistication, using advanced techniques to bypass network security devices and tools. This challenges organizations to protect their networks without increasing workloads for security teams or hindering business productivity. Seamlessly integrated with the industry's first ML-Powered NGFW platform, our cloud-delivered security subscriptions coordinate intelligence and provide protections across all attack vectors, providing best-in-class functionality while eliminating the coverage gaps disparate network security tools create. Take advantage of market-leading capabilities with the consistent experience of a platform, and secure your organization against even the most advanced and evasive threats. Benefit from Threat Prevention or any of our security subscriptions:

- **Advanced Threat Prevention**: Reliably stop known exploits, malware, malicious URLs, spyware, C2, and prevent 60% more zero-day injection attacks and 48% more highly evasive command and control than traditional IPS solutions.
- **Advanced WildFire malware prevention**: Ensure files are safe by automatically detecting and preventing unknown malware 60x faster with the industry's largest malware prevention engine to stop 26% more highly evasive threats with speed and scale.
- **Advanced URL Filtering**: Enable safe access to the internet with the industry's first real-time prevention of known and unknown websites, stopping 76% of malicious URLs 24 hours before other vendors.
- **DNS Security**: Gain 40% more DNS-attack coverage and disrupt the 80% of attacks that use DNS for command and control and data theft, without requiring any changes to your infrastructure.

Operational Benefits

The Threat Prevention subscription enables you to:

- **Gain comprehensive security for all data, applications, and users**. Scan all traffic with full context around applications and users.
- **Automate security with less manual work**. Get automatic updates for new threats.
- **Deploy Snort signatures**. Automatically convert, sanitize, upload, and manage Snort and Suricata rules to detect emerging threats and take advantage of intelligence.
- **Keep your network secure with granular, policy-based controls**. Go beyond simply blocking malicious content to controlling specific file types, reducing the risk to your entire organization.
- **Lock down C2 risk**. Automatically generate C2 signatures at machine scale and speed.

- **Enterprise DLP**: Minimize risk of a data breach, stop out-of-policy data transfers, and enable compliance consistently across your enterprise with 2x greater coverage of any cloud-delivered enterprise DLP.
- **SaaS Security**: Stay ahead of the SaaS explosion with the industry's only Next-Generation CASB to automatically see and secure all apps across all protocols.
- **IoT Security**: Safeguard every "thing" and implement Zero Trust device security 20x faster with the industry's smartest security for smart devices.

Table 1: Threat Prevention Throughput on the PA-Series

Model	Threat Prevention Throughput
PA-220	320 Mbps
PA-410	685 Mbps
PA-440	1 Gbps
PA-450	1.6 Gbps
PA-460	2.4 Gbps
PA-820	840 Mbps
PA-850	1 Gbps
PA-3220	2.3 Gbps
PA-3250	2.7 Gbps
PA-3260	4.3 Gbps
PA-5220	8.8 Gbps
PA-5250	21.4 Gbps
PA-5260	31.4 Gbps
PA-5280	31.4 Gbps
PA-7050	226.2 Gbps
PA-7080	387.6 Gbps

Note: Refer to the respective product summary spec sheets for the most up-to-date information.

Table 2: Privacy and Licensing Summary

Privacy with Threat Prevention Subscription	
Trust and Privacy	Palo Alto Networks has strict privacy and security controls in place to prevent unauthorized access to sensitive or personally identifiable information. We apply industry-standard best practices for security and confidentiality. You can find further information in our privacy datasheets.
Licensing and Requirements	
Requirements	To use the Threat Prevention subscription, you will need Palo Alto Networks Next-Generation Firewalls running PAN-OS.
Recommended Environment	Palo Alto Networks Next-Generation Firewalls deployed in any location, as both internal and external sources, may introduce network-based threats involving exploits, malware, spyware, C2, URLs, and more into your network.
Threat Prevention License	Threat Prevention requires a standalone license, delivered as an integrated, cloud-based subscription for Palo Alto Networks Next-Generation Firewalls. It is also available as part of the Palo Alto Networks Subscription ELA, Firewall Flex, or Prisma Access.

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