Advanced Threat Prevention

Reimagine IPS: Prevent Zero-Day Threats in Real Time

One of the leading problems for network defenders today involves the rise of highly evasive and automated attacks. With access to sophisticated tool sets, adversarial as-a-service offerings, and versions of popular red team tools, bad actors have dramatically improved the speed and success of covert attacks. It has also become easy and inexpensive for malicious actors to find any vulnerabilities, exposures, and other unknown open doors that offer the least barrier to entry for a cyberthreat. We see that attackers are increasingly taking advantage of the windows of exposure—before vendors can patch vulnerable software—with zero-day exploits doubling year over year.[1] In addition, the 73% year-over-year rise in attacks using the highly customizable Cobalt Strike tool is just the start of this new wave of highly evasive attacks plaguing organizations today.[2] Encryption is another method attackers are leveraging to bypass traditional security controls, with reports showing that the vast majority of malware is now delivered through encrypted connections.[3] Network security must evolve to stop highly evasive and unknown threats.

1. Patrick Howell O'Neill, "2021 has broken the record for zero-day attacks," MIT Technology Review, September 23, 2021.
2. Selena Larson and Daniel Blackford, "Cobalt Strike: Favorite Tool from APT to Crimeware," Proofpoint, June 29, 2021.
3. *Internet Security Report – Q2 2021*, WatchGuard Technologies, September 30, 2021.

Intrusion prevention or detection systems (IPS/IDS) are considered the foundation for network security to detect and deter the latest known threats. However, attackers are employing new techniques that make it easier to evade even today's "next-generation" IPS solutions. Traffic is typically 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 and patch vulnerabilities to confidently avoid data breaches. Most importantly, modern IPS solutions have not provided an answer for real-time prevention of unknown threats in critical phases of the attack lifecycle.

The Intrusion Prevention System Reimagined

Go beyond traditional IPS capabilities with Palo Alto Networks Advanced Threat Prevention, extending industry-leading protection against known threats to the prevention of the unknown. Advanced Threat Prevention is the industry's first IPS to stop zero-day attacks completely inline. Reduce your organization's window of exposure by stopping 90% of injection attacks and preventing 60% more zero-day exploits targeting software and web application vulnerabilities. If a threat actor is somehow able to infiltrate your network, receive protection at the last opportunity to stop an in-flight attack before a communication channel with the malicious actor is established. Advanced Threat Prevention prevents 96% of web-based hack tools such as Cobalt Strike and detects 48% more evasive command and control compared to our industry-leading Threat Prevention solution.

Providing the widest visibility, Advanced Threat Prevention detects and blocks threats on any and all ports instead of invoking signatures based on a limited set of predefined ports. Our worldwide community of customers shares collective global threat intelligence, significantly reducing the success rate of advanced attacks by stopping them as they are encountered.

Business Benefits

The Advanced Threat Prevention security service enables you to:

- **Reduce business risk by preventing zero-day threats inline.** Prevent 96% of web-based Cobalt Strike, and detect 48% more evasive and unknown command and control compared to our industry-leading Threat Prevention solution. Prevent 90% of unknown injection attacks, and detect 60% more zero-day exploits compared to our industry-leading Threat Prevention solution.
- **Eliminate cost and management for stand-alone IPS.** Benefit from 45% breach reduction[4] and leverage Snort and other powerful IPS capabilities integrated with our NGFW for a single security policy rule base.
- **Gain visibility into attacks, assuring your organization is protected.** Inspect all traffic for threats, regardless of port, protocol, or encryption.
- **Reduce the resources needed to manage vulnerabilities and patches.** Automatically block known malware, vulnerability exploits, and C2 with 100% effectiveness.[5]
- **Take advantage of full threat detection and enforcement of prevention controls** without sacrificing performance.

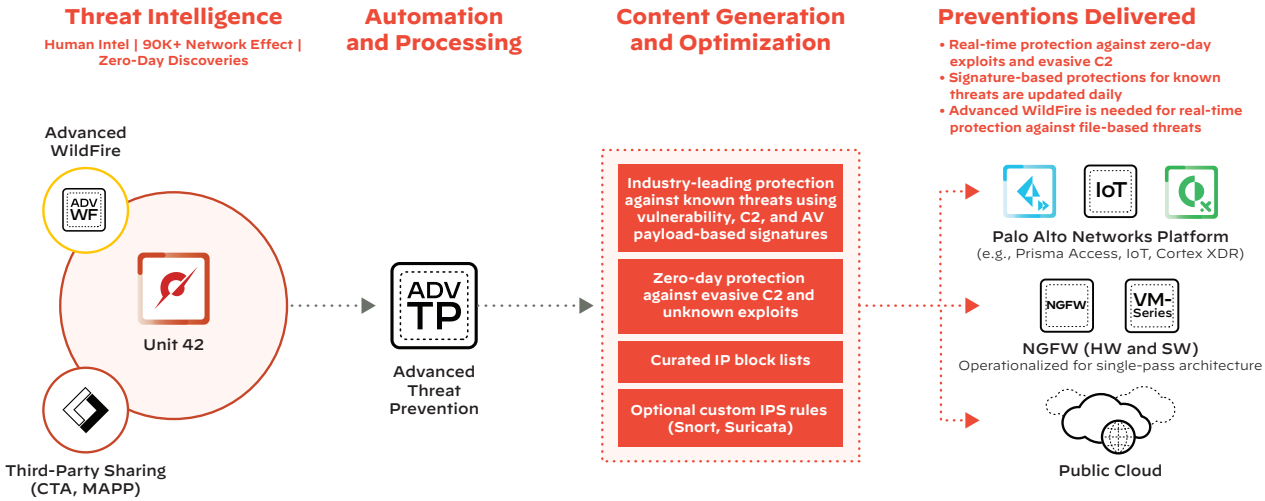

Figure 1: Palo Alto Networks Advanced Threat Prevention

4. *Palo Alto Networks Cloud-Delivered Security Services Enhance Security And Compound Benefits Of Other Network Security Investments*, a Forrester Consulting Total Economic Impact™ Spotlight commissioned study conducted by Forrester Consulting on behalf of Palo Alto Networks, January 2021.
5. *Next Generation Firewall Comparative Report*, NSS Labs, July 17, 2019.

Advanced Threat Prevention benefits from our other cloud-delivered security subscriptions with daily updates that stop exploits, malware, C2, spyware, etc. A necessity for every Palo Alto Networks Next-Generation Firewall, Advanced Threat Prevention can speed the prevention of new unknown threats to real time when paired with other Palo Alto Networks subscriptions, including the Advanced WildFire malware prevention service for 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, to provide comprehensive protection across the entire attack lifecycle.

Key Capabilities

Leverage Industry-Leading 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 decode and analyze protocols and use 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, ensuring all allowed traffic is well-intentioned and devoid of evasion techniques. Within our intrusion prevention technology, we offer:

- **Heuristic-based analysis** that detects anomalous packet and traffic patterns, such as port scans, host sweeps, and denial-of-service (DoS) attacks.
- **Protocol decoder-based analysis** that statefully decodes the protocol and then intelligently applies signatures to detect network and application exploits.
- **Protocol anomaly based protection** that detects non-RFC-compliant protocol usage, such as an overlong URI or FTP login.
- **Easy-to-configure, custom vulnerability signatures** that 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.

Protect Against Malware

Inline malware protection—through signatures based on payload, not hash—blocks malware before it ever reaches the target host. This includes known malware, highly evasive 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 zero-day malware**. Signatures for all types of malware are generated directly from billions of samples collected by Palo Alto Networks, including previously unknown highly evasive malware sent to Advanced WildFire, our Unit 42 Threat Research team, and third-party research and technology partners worldwide.

Integrate with Advanced WildFire

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

Scan All Threats in a Single Pass

The Advanced Threat Prevention engine inspects and classifies traffic and detects and blocks 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 Advanced 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, important details about a packet are identified, such as 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, the context provided by the arrival order and sequence of multiple packets is also analyzed 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.

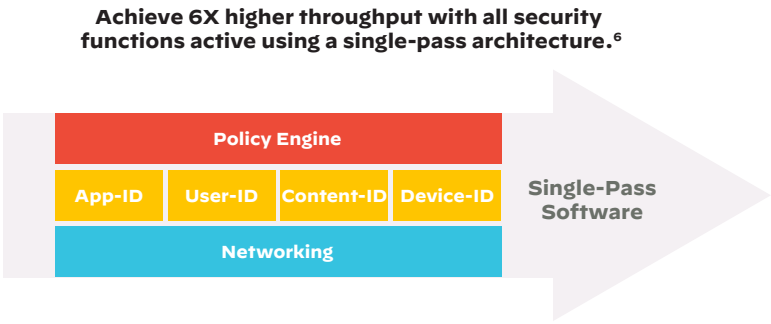

Figure 2: Palo Alto Networks NGFW Single-Pass Architecture

Zero-Day Prevention Inline

Advanced Threat Prevention introduces industry-first real-time prevention of zero-day threats, such as unknown exploit attempts and evasive command and control. Hackers are constantly monitoring software vendor bulletin boards for new vulnerability announcements they can leverage for initial access to a corporate network or to perform remote code execution. In fact, threat actors can begin to exploit a new CVE within 15 minutes of disclosure.[7] Traditional approaches struggle to detect these unknown exploits, leaving the door open for bad actors to enter an organization's network and establish a command-and-control channel. Since malware communications must be observed in the wild first before protections can be released, organizations may suffer from being patient zero of an attack.

Advanced Threat Prevention addresses this challenge by providing multiple deep learning and machine learning models to detect common OWASP Top 10 security risk techniques, such as SQL and command injection. These models also detect evasive C2 inline and in real time. This is done by leveraging a combination of the high-fidelity dataset from Advanced WildFire, signals from soak sites, and intelligence from our Unit 42 Threat Research team. As traffic traverses the firewall, a 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 previously unknown exploit attempts and command and control. Specific models also identify C2 traffic from tools such as Cobalt Strike over key protocols such as HTTP, SSL, Unknown UDP, and Unknown TCP.

90%

prevention of injection attacks such as SQLi.

In addition, **60%** more detection of zero-day injection attacks.

96%

prevention of web-based Cobalt Strike C2.

In addition, **48%** more detection of evasive C2 traffic.

Utilize Custom Signature Compatibility

Advanced Threat Prevention also provides flexible support for Snort and Suricata rule conversion, providing easy-to-configure custom signatures. This support completely eliminates the need for standalone IPS or IDS solutions. 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.

6. https://start.paloaltonetworks.com/security-without-compromise.html
7. *Unit 42 Incident Response Report*, Palo Alto Networks, July 26, 2022.

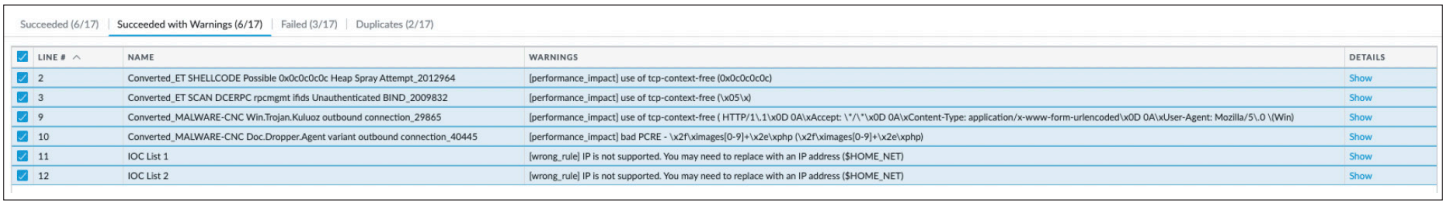

Figure 3: Snort support on PAN-OS

Gain Additional Context on Threats in Your Environment

Leverage threat analytics data and threat intelligence from the Threat Vault API to improve your incident response processes. Through a programmatic RESTful API, access threat signature metadata and pertinent information to determine existing threat coverage, assist in threat alert investigation, and enrich incident response tickets.

Reduce the Attack Surface

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

SSL Decryption

The vast majority of enterprise network traffic is encrypted. This leaves a potential gap in network defenses if that traffic is 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

Reduce the likelihood of a malware infection by preventing dangerous file types known to hide malware from entering your network. Executable files constitute a massive share of the malicious files used in spear phishing attacks. These files, combined with employee negligence, constitute a major security risk. File blocking functionality can be combined with User-ID, a standard feature on the Palo Alto Networks NGFW, 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 when their site has been compromised. Our Advanced Threat Prevention technology identifies potentially dangerous downloads and sends a warning to the user to ensure that the download is intended and approved. Within Advanced Threat Prevention, the detection of such "phishing kit" landing pages, as well as the 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 Services 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 Advanced Threat Prevention or any of the following security subscriptions:

- **Advanced Threat Prevention**: Stop known exploits, malware, spyware, and command-and-control (C2) threats while utilizing industry-first prevention of zero-day attacks. Prevent 60% more unknown injection attacks and 48% more highly evasive command-and-control traffic than traditional IPS solutions.
- **Advanced WildFire malware prevention**: Ensure files are safe by automatically preventing known, unknown, and highly evasive malware 60X faster with the industry's largest threat intelligence and malware prevention engine.
- **Advanced URL Filtering**: Ensure safe access to the internet and prevent 40% more web-based attacks with the industry's first real-time prevention of known and unknown threats, stopping 88% of malicious URLs at least 48 hours before other vendors.
- **DNS Security**: Gain 40% more threat coverage and stop 85% of malware that abuses DNS for command and control and data theft without requiring changes to your infrastructure.
- **Enterprise DLP**: Minimize the risk of a data breach, stop out-of-policy data transfers, and enable compliance consistently across your enterprise, with 2X greater coverage than any cloud-delivered enterprise DLP.
- **SaaS Security**: The industry's only Next-Generation CASB natively integrated into the Palo Alto Networks SASE offers proactive SaaS visibility, comprehensive protection against misconfigurations, real-time data protection, and best-in-class security.
- **IoT Security**: Safeguard every "thing" and implement Zero Trust device security 20X faster with the industry's smartest security for smart devices.
- **AIOps**: AIOps for NGFW redefines firewall operational experience by empowering security teams to proactively strengthen security posture and resolve firewall disruptions.

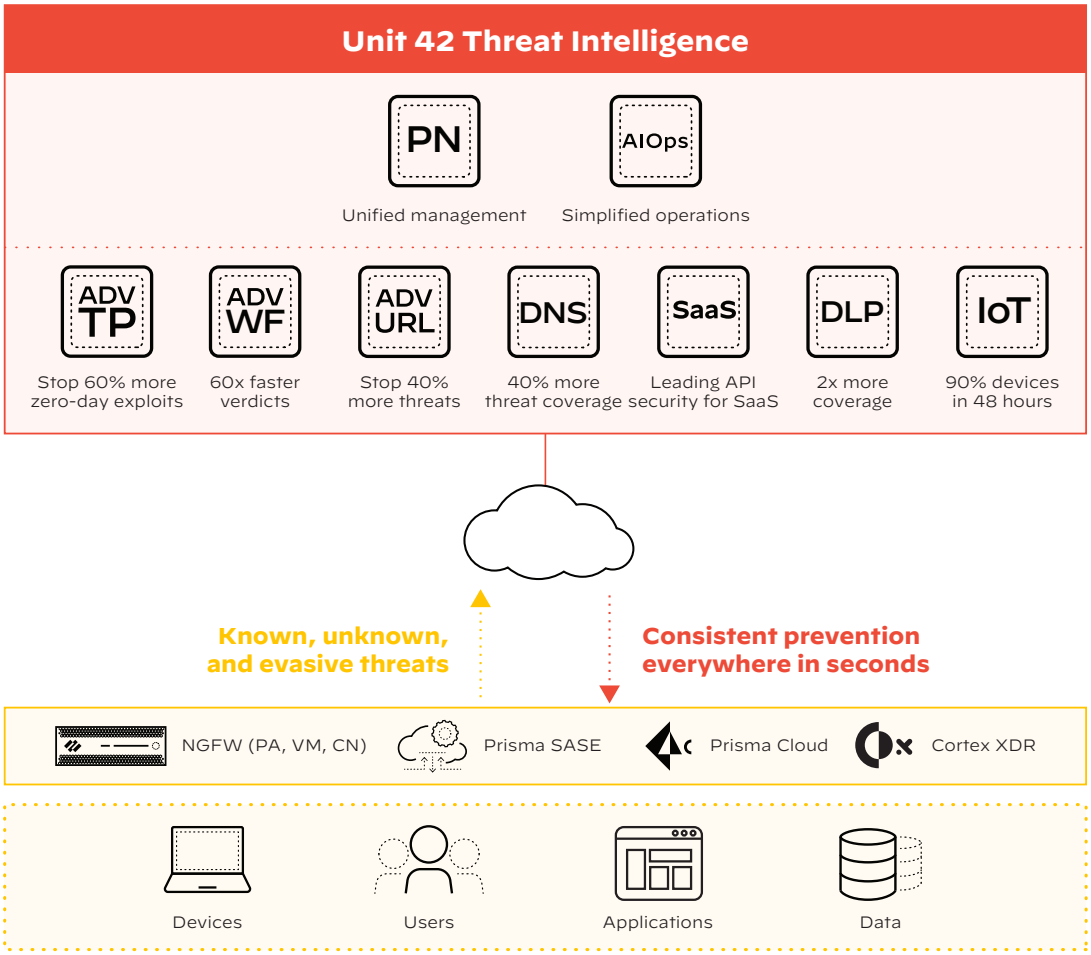

Figure 4: Palo Alto Networks Cloud-Delivered Security Services

Operational Benefits

The Advanced Threat Prevention subscription enables you to:

- **Lock down zero-day risk.** Automatically prevent unknown exploits and evasive C2 attacks inline.
- **Reduce actionable events and workload for the SOC.** Inline blocking of threats in real time saves time and resources spent on investigation post-execution.
- **Gain comprehensive security for all data, applications, and users.** Scan all traffic with full context around applications and users.
- **Deploy Snort signatures.** Automatically convert, sanitize, upload, and manage custom Snort and Suricata rules.
- **Gain additional context on threats in your environment.** Obtain threat metadata, indicators, signature release history, changelists, reports, and PCAPs via the Threat Vault API, and automate your incident response processes.
- **Leverage cloud scale to automate security.** Receive automatic updates and new capabilities over time to stay ahead of the changing threat landscape.
- **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.

Table 1: Privacy and Licensing Summary

Privacy with the Advanced 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	To use the Advanced Threat Prevention subscription, you will need Palo Alto Networks Next-Generation Firewalls running PAN-OS 10.2 or later for the prevention of unknown C2 and PAN-OS 11.0 or later for the prevention of unknown exploits.
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.
Advanced Threat Prevention License	Advanced 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, Bundles, 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