

# Advanced Threat Prevention

Stop Zero-Day Threats and Exploits in Real Time with Precision AI

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 publicly accessible versions of popular red team tools, bad actors have dramatically improved the speed and success of covert attacks. Additionally, it has become easy and inexpensive for malicious actors to find vulnerabilities, exposures, and other unknown open doors that offer the lowest barrier to entry for a cyberthreat.

# The Intrusion Prevention System (IPS) Reimagined

Palo Alto Networks Advanced Threat Prevention is the industry's first [intrusion prevention system \(IPS\)](#) that stops zero-day command-and-control (C2) attacks and unknown exploits completely inline. It goes beyond traditional IPS capabilities, delivering industry-leading protection against known and unknown threats. Advanced Threat Prevention is part of a suite of advanced Cloud-Delivered Security Services available for hardware and software firewalls, including the VM-Series and CN-Series, and Prisma® Access.

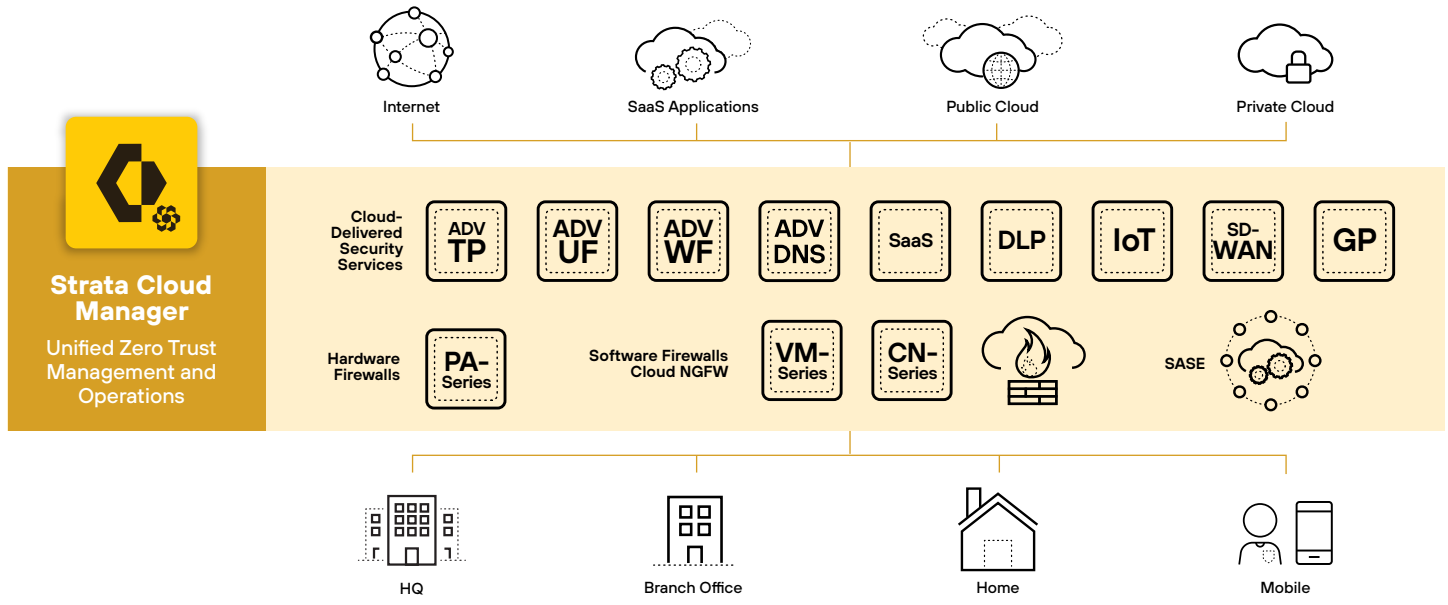


Figure 1: Palo Alto Networks Cloud-Delivered Security Services

## Key Benefits

- Inline prevention of zero-day and known attacks from adversarial tools.
- Inline prevention of exploits for known and never-before-seen vulnerabilities.
- Industry-leading, ML-powered, real-time detection of web-based threats.
- Comprehensive visibility into attacks, inspecting all network traffic for threats.
- Powered by industry-leading threat intelligence from Unit 42® and Advanced WildFire®.

## Product Capabilities

### Powered by Precision AI

Palo Alto Networks harnesses the full potential of AI with Precision AI™. Made up of machine learning, deep learning, and generative AI, Palo Alto Networks Cloud-Delivered Security Services take the best of each technology and integrate it into its security services to better detect and prevent rapidly evolving threats. Key attributes of Precision AI follow.

### AI-Powered Security Models

To be effective in cybersecurity, threat detection must be as close to 100% accurate as possible. This becomes extremely challenging given the evasive and sophisticated nature of today's threat actors who use various tools and techniques to obfuscate their activity. To successfully identify threats and combat attackers' techniques, security-specific combinations of AI technologies are required.

Advanced Threat Prevention uses machine learning to analyze and block malicious threats. Deep learning is used to analyze larger volumes of threats and enable security models to detect more evasive and zero-day threats. With the mass adoption of generative AI by threat actors, security models are now trained on and identify AI-generated threats.

### High-Fidelity Data

AI is only as effective as the data it trains on. Palo Alto Networks Precision AI leverages rich and diverse threat data to continuously train its security models, giving Advanced Threat Prevention comprehensive insights into the new and emerging malware threats. Data is collected from the entire product portfolio, 70,000+ global customers, Advanced WildFire, partners, third-party threat intelligence sources, and internal threat analysis teams.

### Act in Real Time

Given the speed at which today's threat actors operate, security can no longer rely solely on threat signature databases. Instead, analysis must operate inline in real time to detect highly evasive techniques and identify new threats. Leveraging the power and scalability of the cloud ensures the delivery of a verdict instantly to prevent patient zero.

With Precision AI, Advanced Threat Prevention helps customers stay ahead of today's adversaries. Its inline AI-powered models continuously train on rich and diverse threat data to gain insights into new and never-seen-before threats. These insights make Advanced Threat Prevention the industry's first IPS to stop zero-day attacks inline, stopping 60% more zero-day injection attacks, and 48% more highly evasive command-and-control traffic than traditional IPS solutions.

### Industry-Leading Advanced Threat Prevention

Advanced Threat Prevention detects and prevents exploits and evasive tactics at the network and application layers. Various detection methods are employed to provide protection based on the specific nature of the threat observed, including signature matching, machine learning, and inline deep learning models. This is available on all our Next-Generation Firewalls (NGFWs) and in Prisma Access.

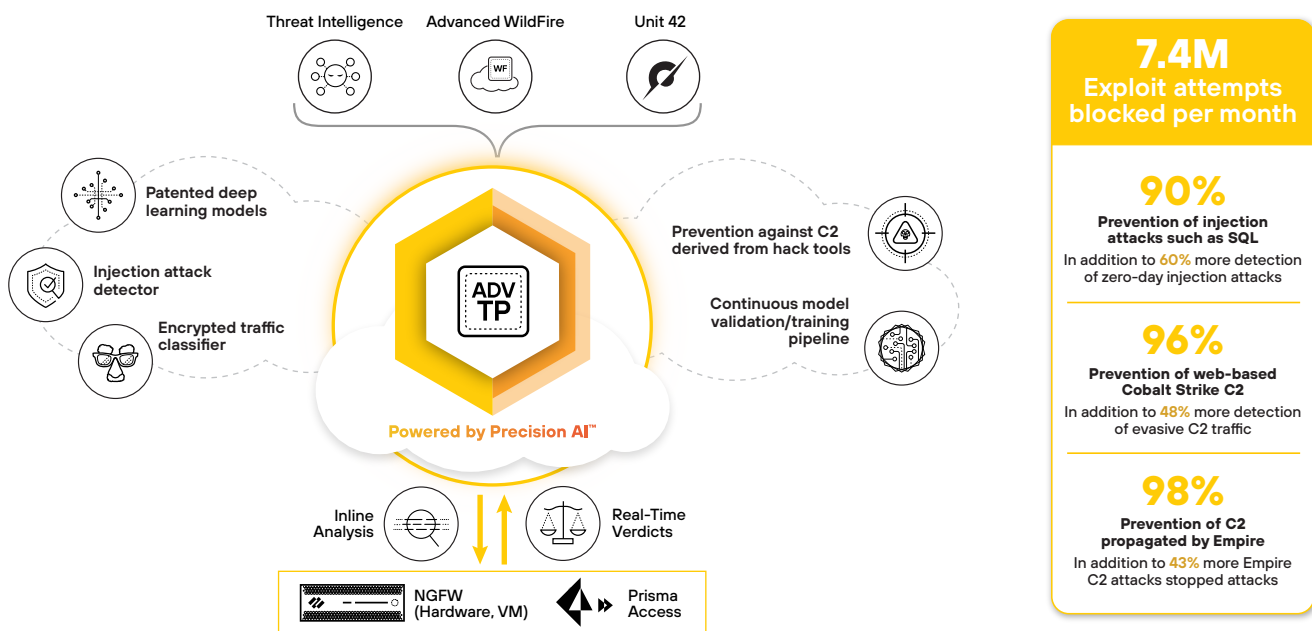


Figure 2: Palo Alto Networks Advanced Threat Prevention

## Command-and-Control (C2) Detection

Advanced Threat Prevention uses patented inline deep learning models to prevent unknown and evasive C2 traffic from popular red team tools such as Cobalt Strike and Empire. These models are continuously updated in the cloud to prevent emerging attacks. Advanced Threat Prevention also prevents unknown web-based attacks. Combined with signature-based detections, this capability provides robust prevention against adversarial attacks.

## Exploit Prevention

Advanced Threat Prevention uses cloud-based machine learning models regularly updated with the latest training datasets to prevent unknown command injection and SQL injection exploits. It includes signature-based prevention for thousands of known vulnerabilities and industry-leading response times for critical and high CVEs for top vendors.

## Malware Prevention

Advanced Threat Prevention blocks malware attacks at the network layer with inline signature-based detections, combined with Advanced WildFire, which adds protection for known and unknown variants before they reach the target host.

Key antimalware features include:

- Protection against malware concealed within common file types.
- Prevention of malware hidden within compressed files and web content.
- High-fidelity datasets and intelligence from our [Unit 42 Threat Research team](#).
- Signatures generated from billions of samples collected by Palo Alto Networks.

## Core Intrusion Prevention Service

In addition to the above, our core intrusion prevention technology offers:

- Custom signature compatibility with Snort and Suricata rules.
- Signatures tailored to software vulnerabilities and command-and-control attacks.
- Heuristic-based analysis, protocol decoder-based analysis, protocol anomaly based protection, and custom easy-to-configure vulnerability signatures.
- Inspection and classification of traffic while detecting and blocking malware and vulnerability exploits in a single pass.
- Curated IP address blocklists.








| Category-Defining Network Threat Prevention |  |  |  |  |   |   |   |
|---|--|--|--|--|---|---|---|
| Threat Category                             |  Vulnerability  |  Brute Force                              |  Antivirus  |  File Identification                  |  Malicious IP                       |  Command and Control   |  Unknown Command and Control   |
| Protection Against                          | <ul style="list-style-type: none"> <li>• Exploit attempts</li> <li>• Vulnerabilities</li> <li>• Evasion techniques</li> <li>• Obfuscation attempts</li> <li>• SQL injection</li> </ul> | <ul style="list-style-type: none"> <li>• Port scans</li> <li>• Buffer overflows</li> <li>• Protocol fragmentation</li> </ul> | <ul style="list-style-type: none"> <li>• Content-based signatures, not hash-based</li> <li>• Known malware and unknown variants</li> </ul> | <ul style="list-style-type: none"> <li>• Known bad or risky file types</li> <li>• Identify password protected</li> </ul> | <ul style="list-style-type: none"> <li>• Known malicious</li> <li>• High-risk</li> <li>• Bulletproof hosting</li> </ul> | <ul style="list-style-type: none"> <li>• Command shells</li> <li>• Malicious domains</li> <li>• Payload inspection</li> <li>• DNS sinkholing</li> </ul> | <ul style="list-style-type: none"> <li>• Unknown and evasive C2</li> <li>• Cobalt Strike and other malleable C2</li> <li>• Over SSL, HTTP, unknown-top, unknown-udp applications</li> </ul> |

Figure 3: Advanced Threat Prevention protection capabilities

# Best-in-Class Cloud-Delivered Security Services Powered by Precision AI

## Benefit from Comprehensive and Best-in-Class Security for Your Entire Network

The typical enterprise's attack surface has grown significantly with the mass adoption of hybrid work, cloud, internet of things (IoT), and software as a service (SaaS). Furthermore, the threat landscape is rapidly intensifying due to easily being able to access and use hacker-friendly tools and resources in their campaigns. Traditional network security solutions and approaches are no longer effective. With Palo Alto Networks Cloud-Delivered Security Services, customers can benefit from best-in-class, real-time security to help them protect all users, devices, and data in their network, regardless of location.

Palo Alto Networks security services use the power of Precision AI inline to stay ahead of threat actors and stop new and never-before-seen threats in real time. Through shared threat intelligence across over 70,000 customers worldwide, they have insights into emerging threats and can act proactively. Finally, seamless integration with NGFWs and SASE eliminates security gaps and offers customers a single pane of glass to view and manage their security.

Table 1: Palo Alto Networks Cloud-Delivered Security Services

| Product                                      | Description   |
|--|---|
| Advanced Threat Prevention                   | Stop known and unknown exploits, malware, spyware, and C2 threats with the industry's first prevention of zero-day attacks, stopping 60% more zero-day injection attacks and 48% more highly evasive command-and-control traffic than traditional IPS solutions.    |
| Advanced WildFire                            | Ensure safe access to files with the industry's largest malware prevention engine, blocking 26% more evasive malware and turning detection into prevention 60X faster.  |
| Advanced URL Filtering                       | Ensure safe access to the web and prevent 40% more threats in real time than traditional filtering databases with the industry's first prevention of known and unknown phishing attacks, stopping up to 88% of malicious URLs at least 48 hours before competitors. |
| Advanced DNS Security                        | Protect your DNS traffic and stop advanced DNS-layer threats, including DNS hijacking, all in real time with 2X more DNS-layer threat coverage than competitors.  |
| Next-Generation Cloud Access Security Broker | Discover and control all SaaS consumption in your network with visibility into 60K+ SaaS apps and protect your data with 28+ API integrations.  |
| IoT Security                                 | Secure your blind spot and protect every connected device unique to your vertical with the industry's most comprehensive Zero Trust solution for IoT devices, discovering 90% of devices within 48 hours.   |

**Table 2: Advanced Threat Prevention Security Features and Licensing Summary**

| Feature                             | Capabilities Activated with the Advanced Threat Prevention Subscription Attached to NGFW  |
|-------------------------------------|---|
| Precision AI                        | Use of machine learning, deep learning, and generative AI to train security models for more accurate detection of advanced and never-before-seen malware variants, including those generated by AI.   |
| Signature-Based Detection           | There are three types of Palo Alto Networks threat signatures, each designed to detect different types of threats as the network traffic is scanned: <ul style="list-style-type: none"> <li>• <b>Antivirus signatures:</b> Detect viruses and malware found in executables and file types.</li> <li>• <b>Antispyware signatures:</b> Detect C2 activity, where spyware on an infected client is collecting data without the user's consent and/or communicating with a remote attacker.</li> <li>• <b>Vulnerability signatures:</b> Detect system flaws that an attacker might otherwise attempt to exploit.</li> </ul>   |
| Machine Learning                    | Able to rapidly discover patterns in data to identify threats far faster than humans.   |
| Inline Deep Learning                | <ul style="list-style-type: none"> <li>• In addition to the signature-based detection mechanism, Advanced Threat Prevention provides an inline detection system to prevent unknown and evasive C2 threats, including those produced through the Empire framework, as well as command injection and SQL injection vulnerabilities.</li> <li>• A subset of machine learning.</li> <li>• Requires tremendous volumes of real-world threat data to be effective.</li> <li>• Detects today's most challenging unknown attacks 6X faster.</li> </ul>  |
| Injection Attack Detector           | The deep learning, ML-based detection engines in the Advanced Threat Prevention cloud analyze traffic for unknown C2 and vulnerabilities, which utilize SQL injection and command injection to protect against zero-day threats.  |
| Local Deep Learning                 | <ul style="list-style-type: none"> <li>• Enables faster verdict determination through deep learning technology delivered locally on the firewall.</li> <li>• Local deep learning enables our fastest verdict determination, delivering our quickest response times yet—a significant advantage for our <b>high-throughput customers</b>. This feature doesn't replace our cloud-based ML threat analysis. Rather, it complements it seamlessly. It provides a mechanism for rapid, local deep learning-based analysis of zero-day and other evasive unknown C2 threats over HTTP or HTTPS, directly on the firewall.</li> </ul> <p>Requirements:</p> <ul style="list-style-type: none"> <li>• The local deep learning feature will only be available on PAN-OS® 11.2 or above.</li> <li>• Requires an ATP subscription.</li> <li>• On supported hardware and software firewalls.</li> </ul> |
| Automated False Positive Correction | Automated system to continuously monitor the performance of each detection service against a set of metrics such as number of malicious detections, false positive rate, and false negative rate.   |
| Ground Truth System                 | Ground truth system for each of the detection services that automatically labels the detection results. Samples of labeled detection results will be further reviewed by expert security researchers at Palo Alto Networks.   |
| Management and Reporting            | Reports are generated that can include the tools/techniques used by the attacker, the scope and impact of the detection, as well as the corresponding cyberattack classification as defined by the MITRE ATT&CK® framework. Advanced Threat Prevention can be managed by Palo Alto Networks Panorama® and web interface, API, and Strata™ Cloud Manager.  |



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

© 2024 Palo Alto Networks, Inc. A list of our trademarks in the United States and other jurisdictions can be found at <https://www.paloaltonetworks.com/company/trademarks.html>. All other marks mentioned herein may be trademarks of their respective companies.  
 strata\_ds\_advanced-threat-prevention\_070424