paloalto NETWORKS | CYBERSECURITY PARTNER OF CHOICE

Advanced Threat Prevention

Stop Zero-Day Threats and Exploits 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 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 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®

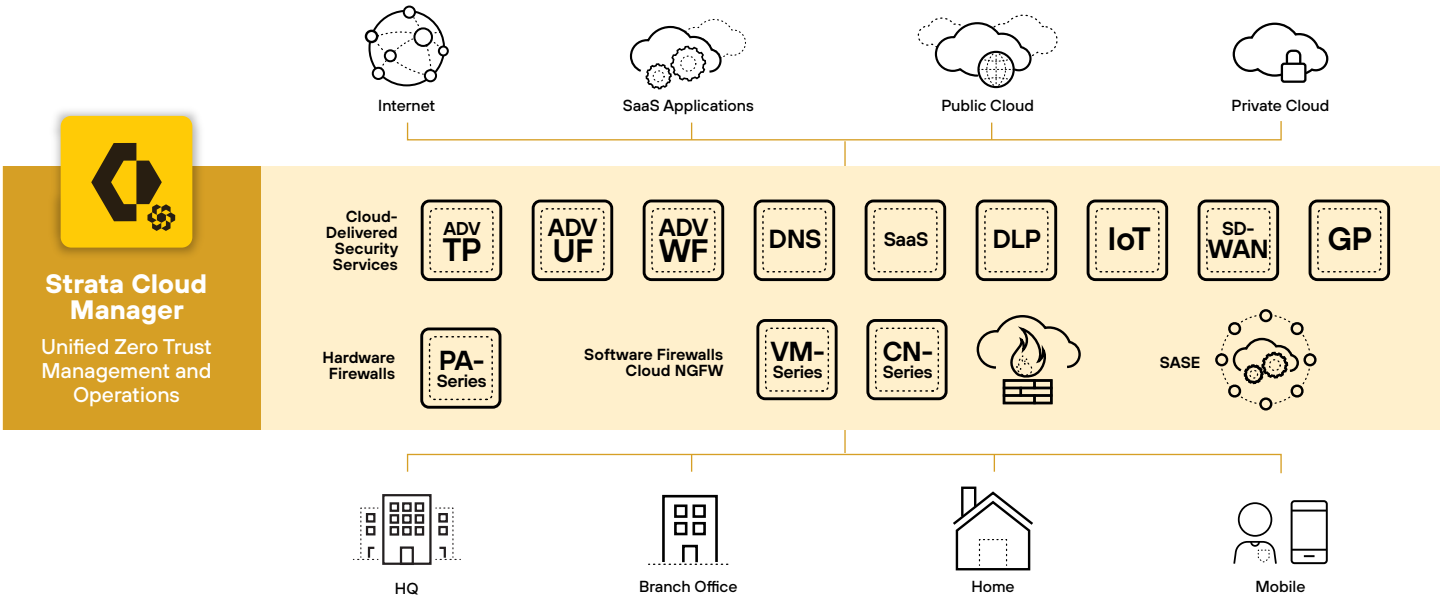

Figure 1: Palo Alto Networks Cloud-Delivered Security Services

Access.

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

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

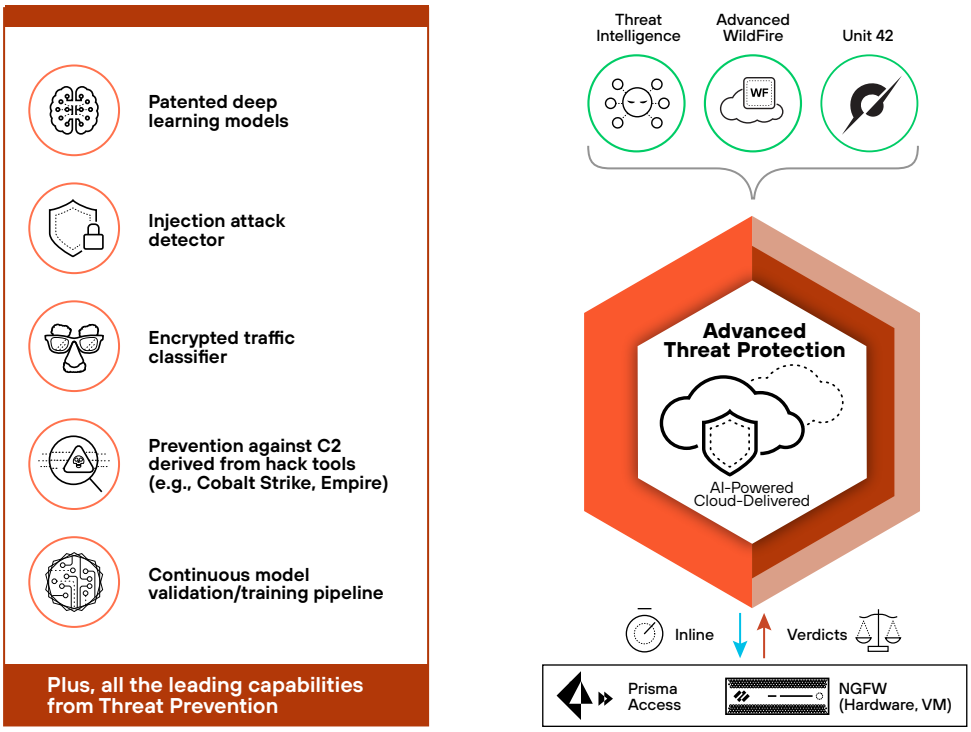

Figure 2: Palo Alto Networks Advanced Threat Prevention

models. This is available on all our Next-Generation Firewalls (NGFWs) and in Prisma Access.

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.

96%
prevention of web-based Cobalt Strike C2.
In addition, **48%** more detection of evasive C2 traffic.*
*Results based on Palo Alto Networks testing.

99%
prevention of C2 propagated by Empire.
In addition, **43%** more Empire C2 attacks were stopped than traditional solutions.*
*Results based on Palo Alto Networks testing.

90%
prevention of injection attacks such as SQLi.
In addition, **60%** more detection of zero-day injection attacks.*
*Results based on Palo Alto Networks testing.

- 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 block lists.

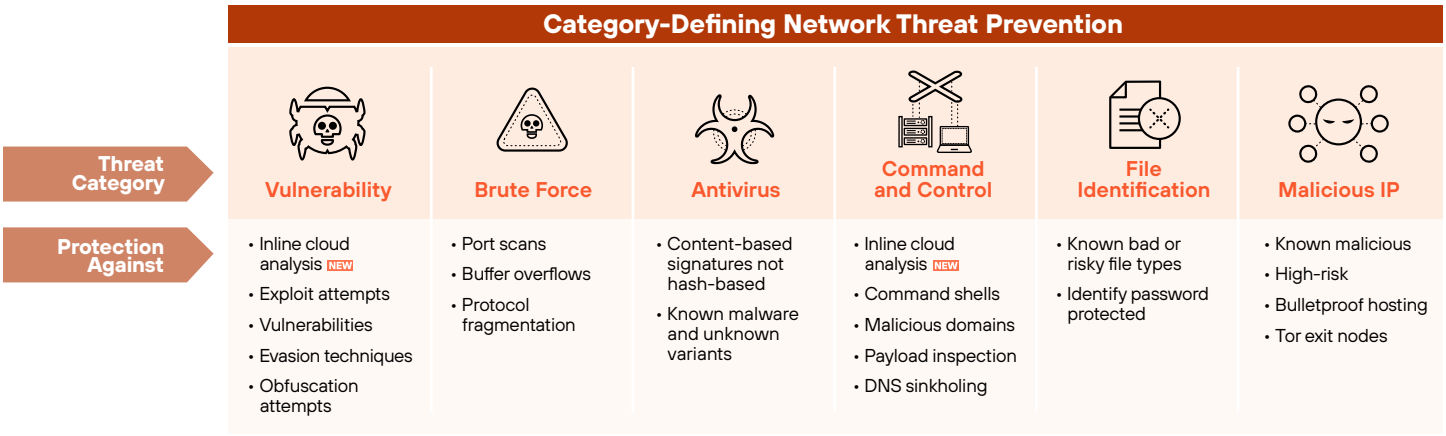

Figure 3: Advanced Threat Prevention features

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

parent_ds_advanced-threat-prevention_022324