Advanced Threat Prevention

The First IPS to Block Unknown Command and Control in Real Time

One of the leading problems for network defenders today involves the rise of highly evasive and automated attacks. With access to these sophisticated tools, adversarial "as-a-service" offerings, and versions of popular red team tools, bad actors have dramatically improved the speed and success of long-term and covert attacks. The 73% year over year rise in attacks using the highly available and customizable Cobalt Strike tool is just the start of this new wave of highly evasive attacks plaguing organizations today.[1] 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.[2] Network security must evolve to stop highly evasive and unknown threats.

Business Benefits

The Advanced Threat Prevention security service enables you to:

- **Reduce business risk by preventing unknown C2 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.
- **Eliminate cost and management for standalone IPS.** 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 resources needed to manage vulnerabilities and patches.** Automatically block known malware, vulnerability exploits, and C2 with 100% effectiveness.[3]
- **Take advantage of full threat detection and enforcement of prevention controls** without sacrificing performance.

1. Selena Larson and Daniel Blackford, "Cobalt Strike: Favorite Tool from APT to Crimeware," Proofpoint, June 29, 2021, https://www.proofpoint.com/us/blog/threat-insight/cobalt-strike-favorite-tool-apt-crimeware.
2. *Internet Security Report – Q2 2021*, WatchGuard Technologies, September 30, 2021, https://www.watchguard.com/wgrd-resource-center/security-report-q2-2021.
3. *2019 Next Generation Firewall Comparative Report*, NSS Labs, July 17, 2019.

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 or 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.

Best-in-Class IPS with Industry-First Prevention of Unknown Command and Control

Palo Alto Networks Advanced Threat Prevention builds on the industry-leading Threat Prevention security service to protect your network by providing multiple layers of prevention, and confronting both known and unknown threats at each phase of an attack. In addition to industry-leading IPS capabilities, Advanced Threat Prevention has the unique ability to leverage deep learning and machine learning models to block evasive and unknown command and control (C2) channels—completely inline—the last chance to stop an in-flight attack before a communication can be established. 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.

Advanced Threat Prevention benefits from our other cloud-delivered security subscriptions for daily updates that stop exploits, malware, malicious URLs, C2, spyware, etc. A necessity for every Palo Alto Networks Next-Generation Firewall, Advanced Threat Prevention can speed prevention of new unknown threats to near-real time when paired with other Palo Alto Networks subscriptions, including 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.

Key Capabilities

Protect Against Known and Unknown 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. With the increasing use of tool sets such as Cobalt Strike as well as encrypted or obfuscated traffic, it is easier than ever for attackers to create completely customizable command-and-control channels that cannot be stopped with traditional approaches.

Unknown C2 Prevention Inline

Advanced Threat Prevention introduces inline deep learning for real-time enforcement for new and unknown command and control. Drawing on the unique dataset of malware from WildFire in addition to signals from soak sites and our Unit 42 research team, 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. Specific models also identify 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 previously unknown C2.

Payload-Based Signatures

Palo Alto Networks goes beyond standard automation of C2 signatures based on URLs and domains. Our C2 protections home in on those unauthorized communication channels and cut them off by blocking outbound requests to malicious domains and from known toolkits installed on infected devices. We automatically generate and deliver researcher-grade signatures based on malicious traffic seen by 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.

Augmenting C2 Prevention with DNS Security

You can extend overall C2 protection with the DNS Security service to prevent the use of the DNS protocol for not only C2, but data exfiltration as well. DNS attack techniques are found in 80% of known breaches.

Leverage Best-in-Class 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 and ensuring 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

Advanced 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.

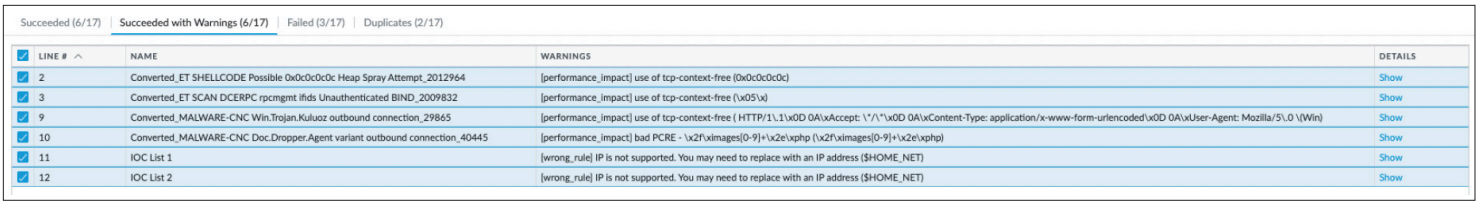

Figure 1: Snort support on PAN-OS®

Protect Against Malware

Inline malware protection—through signatures based on payload, not hash—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 anti-malware 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 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 malware sent to WildFire, our Unit 42 threat research team, and third-party research and technology partners worldwide.

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 WildFire

Extend your protection against zero-day malware and C2 attacks with the WildFire® service, the industry's most advanced analysis and prevention engine for highly evasive zero-day malware and exploits. The cloud-based service employs a unique multitechnique approach that combines dynamic and static analysis, customer hypervisors, and innovative machine learning techniques to detect and prevent even the most evasive threats. Once identified, Advanced Threat Prevention applies verdicts in real time to all ML-Powered NGFW form factors, instantly stopping threat proliferation across your enterprise.

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 subscriptions enable 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, 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™, 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 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 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, 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 Advanced Threat Prevention or any of the following security subscriptions:

- **Advanced Threat Prevention:** Stop known exploits, malware, malicious URLs, spyware, and command and control (C2). Prevent 96% of web-based Cobalt Strike and detect 48% more evasive and unknown command and control than the industry's leading intrusion prevention (IPS) solution.
- **WildFire malware prevention:** Ensure files are safe by automatically detecting and preventing unknown malware 180x faster with industry-largest threat intelligence and malware prevention engine.
- **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.
- **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.

Operational Benefits

The Advanced 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 prevent known and unknown C2 attacks inline.

Table 1: 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 Advanced Threat Prevention subscription, you will need Palo Alto Networks Next-Generation Firewalls running PAN-OS 10.2 or later.
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, Firewall Flex, or Prisma Access (Threat Prevention only).

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