



## Benefits

- Scans all traffic in full context of applications and users
- Prevents threats at every stage of the cyberattack lifecycle
- Uses unique Single-Pass Architecture for high throughput without sacrificing security
- Receives daily, automatic updates on new threats, with zero-day threat protection delivered in as few as five minutes by the WildFire service
- Automatically generates command-and-control signatures at machine scale and speed

# Threat Prevention

Organizations face a barrage of attacks by threat actors around the world looking to make a profit. Today's attackers are well-funded and well-equipped. They use evasive tactics to succeed in gaining a foothold in the network, launching high-volume and sophisticated attacks while remaining invisible to an organization's traditional defenses through techniques such as packet obfuscation, polymorphic malware, encryption, multiphase payloads, and fast-flux DNS.

To make matters worse, network security products are still using the same defensive strategies employed before the threat landscape evolved. Traffic is only inspected on certain ports and, while adding single-function devices to the defensive stack may help alleviate a particular problem, it results in poor visibility and performance. This has left gaping holes in network defenses because security solutions are fractured and difficult to manage, while attackers are increasingly adept at penetrating them.

## Enable the Application, Prevent the Threat

Applications are an integral part of how companies do business and, because of that, they've made themselves increasingly available to users by entering networks using encrypted channels through nonstandard ports and port-hopping to guarantee users always have access.

Unfortunately, advanced threats take advantage of such application behavior to get free rides into networks, undetected. They tunnel within applications, hide in SSL-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 intrusion-prevention 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. By leveraging User-ID™ and App-ID™ technology on our Next-Generation Firewalls to add context to all traffic on all ports, the Threat Prevention engine never loses sight of the threat, regardless of the evasion technique.

The Threat Prevention subscription includes intrusion prevention, network anti-malware, and command-and-control (C2) protections.

## Eliminate Threats at Every Phase

Countless breaches over the years can be attributed to attackers bypassing a single-purpose defensive tool. To ensure holistic protection, the Threat Prevention subscription brings together multiple defensive mechanisms:

- **Heuristic-based analysis** detects anomalous packet and traffic patterns, such as port scans, host sweeps, and DDoS flooding attacks.
- **Easy-to-configure, custom vulnerability signatures** allow you to tailor intrusion prevention capabilities to your network's unique needs.
- **Other attack protection capabilities**, such as blocking invalid or malformed packets, IP defragmentation, and TCP reassembly, protect against attackers' 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.

### 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.

## Malware Protection

In-line 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 the network without introducing significant latency, which is a serious drawback of network antivirus offerings that rely on proxybased 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:

- **In-line, 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® Office documents and PDFs.
- **Updates from WildFire® malware prevention service**, ensuring 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 other 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 otherwise would 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.

### Command-and-Control Protection

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 at machine speed and scale.

## Scan for All Threats in a Single Pass

The Palo Alto Networks 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, adding significant latency and dramatically slowing throughput performance. We use a uniform signature format for all threats to ensure rapid processing by performing all analysis 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 evasive techniques. All of this happens within one scan, so your network traffic remains as fast as you need it to be.

### WildFire Integration

Extend your protection against zero-day malware and exploits with the WildFire service. WildFire is the industry's most advanced analysis and prevention engine for highly evasive zero-day malware and exploits. The cloud-based service employs a unique multi-technique approach that combines dynamic and static analysis, innovative machine learning techniques, and bare metal analysis to detect and prevent even the most evasive threats.

### Attack Surface Reduction

#### SSL Decryption

The vast majority of enterprise network traffic is encrypted with SSL, which leaves a gaping hole in network defenses if it's not decrypted and scanned for threats. Our platform's built-in SSL Decryption can selectively to decrypt inbound and outbound SSL traffic. After traffic is decrypted and confirmed as safe, it's re-encrypted and 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,<sup>1</sup> 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 WildFire for analysis to determine if they contain zero-day malware.

#### Drive-By-Download Protection

Unsuspecting users can inadvertently download malware merely by visiting their favorite web pages. Users or even owners of websites may be unaware that the site has 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. Prevent attacks from new and rapidly changing domains by tying this feature to URL filtering and file blocking policies.

### Easy and Accurate Mitigation

#### DNS Sinkhole

Our C2 protection goes a step further by providing sinkhole capabilities for outbound requests to malicious DNS entries, preventing exfiltration and accurately identifying the victim. Configure the sinkhole so that any outbound request to a malicious domain or IP address is instead redirected to one of your network's internal IP addresses. This effectively blocks

C2 communication, preventing those requests from ever leaving the network. A report of the hosts on your network making those requests is compiled, even though those hosts sit behind the DNS server. Incident response teams have a daily list of compromised machines on which to act, without the added stress of remediation crunch-time because communications with the attacker have already been cut off.

#### Automated Correlation Objects

Our Threat Prevention technology identifies the presence of advanced threats through the monitoring and correlation of network traffic and threat logs, enabling you to quickly identify infected users and analyze strange behavior patterns. The correlation objects leverage threat research from Unit 42 as well as unknown threat analysis from WildFire and User-ID to correlate traffic anomalies and indicators of compromise, ensuring you can quickly and accurately identify infected devices on your network.

## Leverage Global Threat Intelligence to Prevent Attacks

Detailed threat logs aren't merely housed within the same management interface but shared among all prevention mechanisms to provide context. We leverage global threat intelligence through WildFire to automatically discover unknown malware and deliver protections to our entire customer base, keeping them continuously secured against the latest advanced threats.

## DNS Monitoring

Protect your organization against rapidly evolving malware networks and malicious websites by leveraging Palo Alto Networks DNS-based analysis. Benefit from a vast network of intelligence by enabling passive DNS monitoring, which feeds into our database of malicious domains and is then used in generating protections across our global customer base.

## Unit 42 Threat Research

The Palo Alto Networks threat research team, Unit 42, applies human intelligence to identify critical zero-day vulnerabilities in Adobe, Apple, Google, Microsoft, and other ecosystems. By proactively identifying these vulnerabilities, developing protections for our customers, and sharing the information with the security community, we are removing attackers' means to threaten users and compromise enterprise, government, and service provider networks.

