THREAT PREVENTION

Comprehensive exploit, malware, and command and control protection for your network

Organizations face a frequent barrage of attacks by threat actors around the world looking to make a profit. Today's attackers are much different from the attackers of 15 years ago. They use evasive tactics to succeed in gaining a foothold in your network while remaining invisible to traditional network defenses, from packet obfuscation and encryption to multi-phased payloads and fast-flux DNS.

Purpose-built within the next-generation security platform, Threat Prevention Services protect networks from a wide range of threats.

- Scan all traffic in full context of applications and users
- Prevent threats at every step of the Cyber Attack Lifecycle
- Single-pass scanning architecture allows for high throughput, even when all threat prevention features are enabled
- Single policy table reduces management overhead
- Daily, automatic updates for protections against new malware and malicious DNS entries

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, that results in poor visibility and performance. This has left a dangerous situation, where gaping holes are present in network defenses because security solutions are fractured and difficult to manage, while attackers are increasingly adept at penetrating them.

Palo Alto Networks® has redefined network security with our Zero Trust platform approach to threat prevention. We safely enable applications by providing protection against advanced threats at every phase in the cyberattack lifecycle, and we do this using a multi-function platform that analyzes all traffic across all ports and protocols in a single scan.

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 non-standard ports, and by hopping from open port to open port to guarantee users always have access.

Unfortunately, advanced threats take advantage of the new way in which applications make themselves available to users, leveraging them for a free ride into the network undetected. They tunnel within applications, hide within SSL-encrypted traffic, and take advantage of unsuspecting targets to get a foothold within the network and execute malicious activity.

Palo Alto Networks protects your network against these threats by providing multiple layers of prevention, confronting threats at each phase of the attack. Our Threat Prevention subscription includes Intrusion Prevention, Network Anti-Malware, and Command-and-Control (CnC) protections and shields the network from advanced threats by identifying

and scanning all traffic — applications, users, and data, encrypted or not, across all ports and protocols.

Eliminate Threats at Every Opportunity

In nearly every recent breach, the targeted organization had a single-function defensive tool in place that was bypassed. 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.

Security Recommended

Palo Alto Networks is the only vendor to achieve a 100% block rate for all live "drive-by" exploits in NSS Labs' 2015 Next Generation Intrusion Prevention System (NGIPS) test.

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 alert on and block malicious traffic patterns. Stateful pattern matching detects attacks across multiple packets, taking into account arrival order and sequence, making sure all allowed traffic is well-intentioned and not using evasion techniques.

- Protocol decoder-based analysis statefully decodes the protocol and then intelligently applies signatures to detect network and application exploits.
- 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 network or application vulnerability.
- Protocol anomaly-based protection detects non-RFC compliant protocol usage, such as overlong URI or FTP login.
- Heuristic-based analysis detects anomalous packet and traffic patterns, such as port scans, host sweeps, and DoS flooding attacks.
- Other attack protection capabilities, such as blocking invalid or malformed packets, IP defragmentation, and TCP reassembly, are utilized for protection against evasion and obfuscation methods employed by attackers.
- Easy-to-configure, custom vulnerability signatures allow you to tailor intrusion prevention capabilities to your network's unique needs.

In addition to these traditional intrusion prevention capabilities, Palo Alto Networks provides the unique ability to detect and block threats on any and all ports, instead of invoking signatures based on a limited set of predefined ports. By leveraging App-ID™ within our next-generation firewall, which identifies all traffic on all ports, the threat prevention engine never loses sight of the threat, regardless of port evasion.

Malware Protection

In-line malware protection blocks malware before it ever reaches the target host, through signatures that are based on payload, not hash. Palo Alto Networks malware protections block known malware and any variants, including those that haven't been seen in the wild yet. The stream-based scanning engine protects the network without introducing significant latency, which is a serious drawback of network antivirus offerings that rely on proxy-based scanning engines. Palo Alto Networks stream-based malware 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, stand-alone 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, ensuring protection against brand-new malware used in the most recent attacks.

Signatures for all types of malware are generated directly from millions of live samples collected by Palo Alto Networks, including previously unknown samples sent to WildFire, a global network of honeypots, and other leading third-party research organizations around the world.

Command-and-Control (Spyware) Protection

We know 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 command-and-control (CnC) channel, using it to pull down additional malware, issue further instructions, and steal data. Our CnC protections hone in on those

CONTENT-BASED vs. HASH-BASED SIGNATURES

Signatures based on content, i.e., payload, can detect patterns in the body of the file that indicate what the file is supposed to do.

Signatures based on hash look and match on the fixed encoding of a 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.

Using hash-based signatures is like determining whether the contents of a box have spoiled based only on the box design, instead of looking at what's inside.

unauthorized communication channels and cut them off by blocking outbound requests to malicious domains and from known CnC toolkits installed on infected devices.

DNS Sinkhole

Our CnC 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 CnC communication, preventing those requests from ever leaving the network, regardless of the frequency or time of day they're made, and compiles a report of the hosts on your network making those requests. Incident response teams have a daily list of compromised machines on which to act, without the added stress of remediation crunch time, because the communications with the attacker are cut off.

WildFire

Protections against newly discovered malware and command-and-control domains are delivered to Threat Prevention protection libraries daily via WildFire™, our virtual malware analysis environment, keeping your protection up to date, so you're protected against the latest advanced threats and multiple stages in the attack lifecycle.

Automated Correlation Objects

Palo Alto Networks includes the ability to identify the presence of advanced threats through the monitoring and correlation of network traffic and threat logs, so you can quickly identify infected users and analyze strange behavior patterns. The correlation objects leverage threat research from Unit 42, unknown threat analysis from WildFire, combined with User-ID™ to correlate traffic anomalies and indicators of compromise, to quickly and accurately identify devices on your network that are infected. Unknown or anomalous TCP and UDP and a variety of potentially suspicious behaviors, such as repeated download patterns, the use of dynamic DNS, exploit attempts, and other key factors are tracked and compiled into alerts providing you with a list of users who are infected and the indicators of compromise that led to the diagnosis.

Complete Visibility and Reduced Risk

SSL Decryption

Nearly 40 percent 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 has built-in SSL decryption, which can be used 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

Around 90 percent of malicious files used in spear phishing attacks are executables. That, combined with the fact that 59 percent of security incidents are the result of employee negligence, means that your users 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, like executables, 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 to risk that makes sense for the diverse requirements of your organization. Further decrease the number of attack opportunities by sending all allowed files to WildFire for analysis to determine if they contain never-before-seen malware.

Drive-By Download Protection

Unsuspecting users can inadvertently download malware merely by visiting their favorite Web page. Often the user or even the owner of the website may be unaware that the site has been compromised. Palo Alto Networks 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.

Leverage Global Threat Intelligence to Prevent Attacks

Detailed logs of all threats 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.

Passive DNS Network

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.

World-Class Research

The Palo Alto Networks threat research team is a world-class research organization dedicated to the discovery and analysis of threats, applications, and their respective network behavior. The team works to provide protections against an expansive list of exploits by reverse engineering new vulnerabilities. Each year, Palo Alto Networks' threat research team discovers and reports more Microsoft product vulnerabilities than any other security vendor.

Palo Alto Networks is also the home of Unit 42, a team of experts that analyzes threat data accumulated by our global intelligence community to identify and investigate cutting-edge attack methods, malware, and active threat campaigns, and report on unfolding trends within the black hat space.

Scan for All Threats in a Single Pass

The Palo Alto Networks Threat Prevention engine represents an industry first by inspecting and classifying traffic, and detecting and blocking both

malware and vulnerability exploits in a single pass. Traditional threat prevention technologies require two or more scanning engines, which adds significant latency and dramatically slows throughput performance. Palo Alto Networks uses a uniform signature format for all threats to ensure speedy processing by performing all analysis in a single, integrated scan, eliminating redundant processes common to solutions that use multiple scanning engines.

Our Threat Prevention technology combs through 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 that packet, including the application used, source and destination, if the protocol is RFC compliant, and whether the payload contains an exploit or malware. 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 analysis and signature matching happens within one scan, so your network traffic remains as fast as you need it to be.

Threat Prevention Throughput

Model	Threat Throughput
PA-200	50 Mbps
PA-500	100 Mbps
PA-2020	200 Mbps
PA-2050	500 Mbps
PA-3020	1 Gbps
PA-3050	2 Gbps
PA-3060	2 Gbps
PA-5020	2 Gbps
PA-5050	5 Gbps
PA-5060	10 Gbps
PA-7050	100 Gbps*
PA-7080	160 Gbps*

*DSRI-enabled

4401 Great America Parkway
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

pan-ds-threat-prevention-112515