Advanced DNS Security

The Industry's Most Comprehensive DNS Security Solution, Offering 2X More DNS-Layer Threat Coverage Than Competitors and Industry-First, Real-Time Protection Against Network-Based DNS Hijacking Attacks

The Domain Name System, otherwise known as DNS, has become an extremely popular target for today's threat actors. Due to the amount of bidirectional traffic it carries and its critical role in how we use the internet, it presents many opportunities for attackers. The Palo Alto Networks Unit 42® Threat Research team identified that 85% of malware uses DNS to initiate command-and-control (C2) procedures, in addition to phishing attacks, ransomware, and data exfiltration. Attackers are constantly finding new ways to abuse DNS, including the resurgence of DNS hijacking. Attackers use this technique to modify DNS records of legitimate domains to redirect unsuspecting users to their malicious site. This can be done by changing the IP address of a legitimate domain or by exploiting misconfigured domains. Therefore, with these types of techniques being used by today's threat actors, it's now more important than ever to secure your DNS traffic.

The Most Comprehensive Protection of Your DNS Traffic

Palo Alto Networks Advanced DNS Security

Powered by Precision AI, Advanced DNS Security is the industry's leading DNS security solution that gives you industry-first, real-time protections against new and advanced DNS-layer threats. Advanced DNS Security leverages inline AI-powered detection models that can analyze DNS request and DNS response data in real time, giving it the ability to identify never-before-seen malicious domains and DNS hijacking attempts. These models are continuously trained on rich and diverse threat data, allowing Advanced DNS Security to identify malicious activity with extreme accuracy.

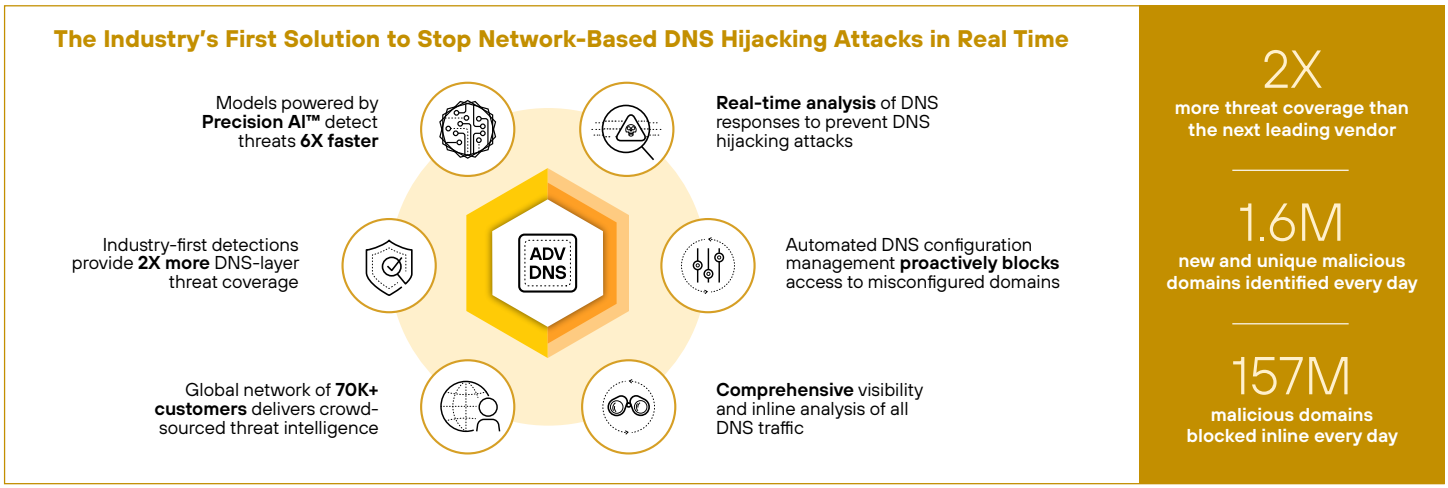

Figure 1: Palo Alto Networks Advanced DNS Security

Key Capabilities

Powered by Precision AI

Palo Alto Networks harnesses the full potential of AI with Precision AI™. From machine learning to deep learning and generative AI, Advanced DNS Security, along with other Palo Alto Networks Cloud-Delivered Security Services, takes the best of each technology and integrates it to better detect and prevent rapidly evolving threats. Key attributes of Precision AI consist of AI-powered security models, high-fidelity data, and action in real time.

AI-Powered Security Models

To be effective in cybersecurity, Precision AI must be as close to 100% accurate as possible to find malicious activity and avoid alerting on false positives. However, this becomes extremely challenging given the evasive and sophisticated nature of today's threat actors who use various tools and techniques to obfuscate their threats from security scanners. To successfully identify threats and combat attackers' techniques, security-specific combinations of AI technologies are required.

From its inception, Advanced DNS Security used machine learning to analyze structured data and identify malicious DNS traffic patterns. Thereafter, deep learning was integrated to analyze larger volumes of unstructured data that enabled security models to better predict evasive and never-before-seen threats. And now, with the mass adoption of generative AI by threat actors, security models are trained on threat samples generated by AI to also identify AI-generated attacks.

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 DNS Security comprehensive insights into the new and emerging DNS-layer threats seen every day. Data sources include threat intelligence collected from over 70,000 global customers, third-party threat databases, and user DNS traffic.

Real-Time Action

Given the speed in which today's threat actors operate, security can no longer solely rely on threat signature databases, which can only prevent known threats. Instead, security must operate in real time. Analysis must occur inline and be done on real network traffic to see through evasion techniques and to identify net new threats. Additionally, security must utilize the power and scalability of the cloud to deliver a verdict instantly and prevent anything malicious before patient zero is infected.

With Precision AI, Advanced DNS Security helps customers stay ahead of today's adversaries. Its inline AI-powered models continuously train on rich and diverse threat data to gain insights on new and advanced DNS-layer threats. These insights make Advanced DNS Security the industry's most comprehensive DNS security solution, with industry-first detections and 2X more threat coverage than competing solutions.

Natively Integrated in a Single Platform

With a rapidly expanding attack surface, enterprises are required to add new security tools to their stack to ensure they're protecting every vector in their network. However, these stacks often consist of point solutions that lack integration, which result in security gaps and cause operational complexity. With its tight integration with the Strata™ Network Security Platform, Advanced DNS Security works natively with any of Palo Alto Networks form factors, including hardware, software, and cloud Next-Generation Firewalls. Furthermore, Advanced DNS Security works in tandem with Palo Alto Networks Cloud-Delivered Security Services and shares threat intelligence and provides security across all attack vectors, delivering best-in-class protection and eliminating security gaps caused by disparate security stacks. Take advantage of industry-leading capabilities with the consistent experience of a platform and secure your organization against even the most advanced and evasive DNS-layer threats.

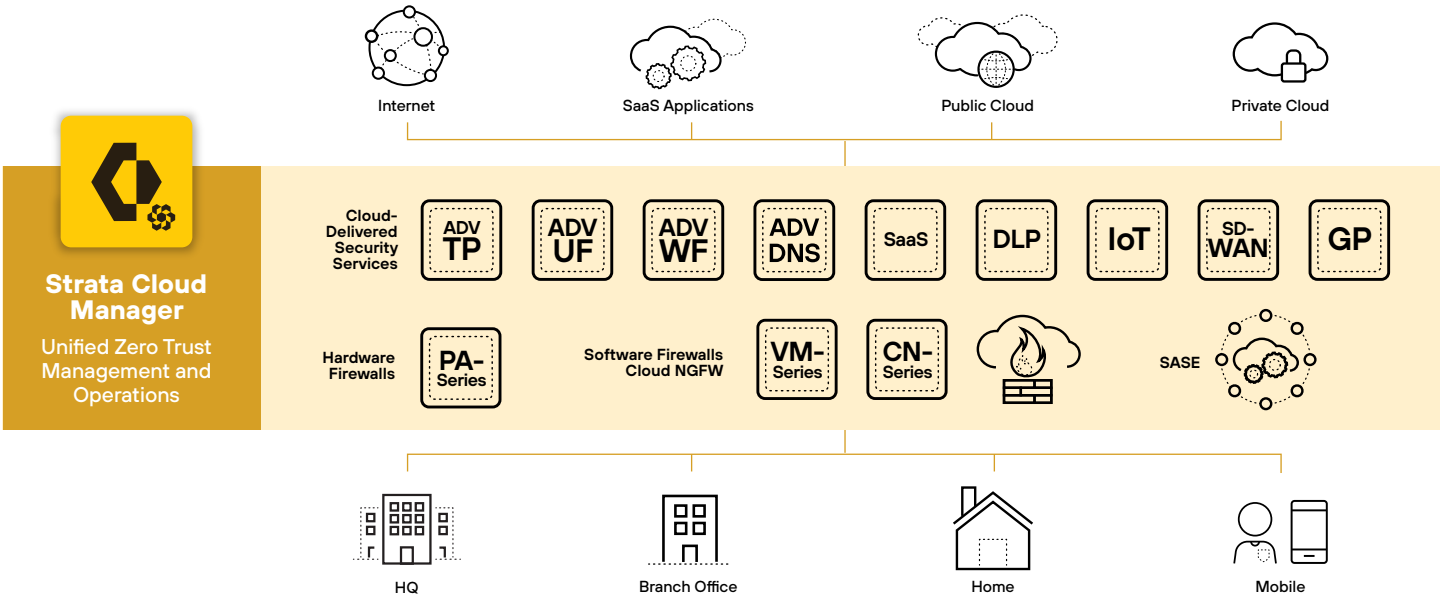

Figure 2: Palo Alto Networks Strata Network Security Platform

Get Insight from DNS Analytics

Give your security personnel the context they need to take action. Threat reporting capabilities allow deeper insights into threats than ever before, delivering full visibility into DNS traffic with:

- Automated discovery and monitoring of a customer's public-facing domains to block access to misconfigured domains.
- Complete history across any domain via an easy-to-use dashboard to help inform where domains are coming from, validate what is malicious, and support incident triage and response.
- Context around DNS events that will show you what kind of domains are being queried and with what frequency, timestamps, passive DNS information for each domain, WHOIS information, and any associated malware tags.
- Security hygiene to keep track of what security capabilities are enabled by your NGFWs across your estate, allowing you to quickly eliminate any blind spots.

Inspect All Types of DNS Traffic

Gain visibility into and protect all types of DNS traffic, such as plain-text DNS, DNS over TLS (DoT), and DNS over HTTPs (DoH), including those going to unknown resolvers:

- Real-time inspection of both DNS requests and DNS responses.
- Leverage decryption on your firewall to inspect encrypted DNS traffic, such as DoH and DoT.
- Sinkhole and quarantine infected users in your network.
- Leverage Strata Cloud Manager for complete visibility of all your DNS traffic, including insights into trends, all in a single dashboard.
- Secure all types of DNS traffic including those that are directed to unknown DNS resolvers.

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 NGFW 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 command-and-control (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, stopping up to 22% more unknown malware and turning detection into prevention 180X faster than competitors.
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 spots 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 DNS Security Features

Feature	Description
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 DNS-layer threats, including those generated by AI.
Real-Time Analysis and Prevention	Inline analysis of DNS request and response data for end-to-end protection of the DNS query journey and real-time enforcement delivered from the cloud to prevent patient zero.
DNS Analytics	Provides threat reporting capabilities that allow full visibility into DNS traffic, along with the full DNS context around security events and traffic trends over time.
DNS Sinkholing	Enables you to forge a response to a DNS query for a malicious domain and cause that malicious domain name to resolve to a definable IP address given to the client. Client attempts to access the sinkhole address can be logged and trigger automated actions (e.g., quarantine). This technique can be used to identify infected hosts on the network.
Security Categories	Allows you to define separate policy actions as well as a log severity level for a specific signature type. You can create specific security policies based on the nature of a threat (e.g., C2, dynamic DNS, malware, newly registered domain, phishing, grayware, parked domain, proxy avoidance, and anonymizers) according to your network security protocols.

Table 3: Advanced DNS Security Detection Categories	
Category	**Description**
Callback Domains	DNS-based indirection for reliable phone-home.
High-Risk Domains	Proactive protection from likely malicious domains.
DNS Record Attacks	Domain takeovers through DNS zone hacks and abuse.
DNS Protocol Attacks	Distributed denial-of-service (DDoS) exploitation and lateral movement.
Covert Channels	Abuse of DNS protocol for stealthy data theft and command and control.
DNS Response Attacks	Real-time detection of network-based DNS hijacking.

Table 4: Privacy and Licensing Summary	
Privacy with Advanced DNS Security	
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 datasheet.
Licensing and Requirements	
Requirements	To use the Palo Alto Networks Advanced DNS Security subscription, you'll need: • Palo Alto Networks Next-Generation Firewalls running PAN-OS® 11.2 or later • Palo Alto Networks Threat Prevention license
Recommended Environment	Use Advanced DNS Security with Palo Alto Networks Next-Generation Firewalls deployed in any internet-facing location, as threats involving malicious domains, tunneling, and other abuse of DNS require external connectivity.
Advanced DNS Security License	Advanced DNS Security can be purchased through a standalone license or as part of the Precision AI Network Security Bundle or Enterprise Agreement Bundle. For software firewall customers, Advanced DNS Security can be purchased using Firewall Flex Credits.

Resources

- Advanced DNS Security webpage
- DNS Security datasheet

About This Datasheet

The information provided with this paper that concerns technical or professional subject matter is for general awareness only, may be subject to change, and does not constitute legal or professional advice, nor warranty of fitness for a particular purpose or compliance with applicable laws.

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

strata_ds_advanced-dns-protection_062824