Advanced DNS Security

Inspect Every DNS Request and Response in Real Time, Covering 2X More DNS Threats Than Our Closest Competitor

The Domain Name System (DNS) is essential to internet functionality, but it's also one of the most exploited layers in the modern attack surface. Its high volume of bidirectional traffic and foundational role in network communication make it a prime vector for threat actors.

Palo Alto Networks Unit 42® found that 85% of malware leverages DNS to establish command-and-control (C2) communication, alongside other tactics such as phishing, ransomware delivery, and data exfiltration. DNS is also increasingly targeted through DNS hijacking—a technique in which attackers manipulate DNS records to redirect users to a malicious infrastructure, often by exploiting misconfigurations or vulnerabilities.

As attackers evolve their techniques, traditional security tools often fall short in inspecting and blocking malicious DNS activity in real time, leaving organizations vulnerable to malicious actors. To defend against today's DNS-layer threats, organizations need advanced, real-time protection that can detect and stop malicious queries before they do damage.

Key Benefits

- Stops advanced and evasive DNS threats.
- Protects against never-before-seen threats.
- Reduces alert fatigue and false positives.
- Enhances security posture.
- Protects productivity and user experience.
- Supports compliance mandates.

Palo Alto Networks Advanced DNS Security

Powered by Precision AI®, Advanced DNS Security is the industry's leading DNS-layer defense, delivering real-time protection against new and advanced threats. It uses inline, AI-powered detection models to analyze every DNS request and response in real time, enabling precise identification of never-before-seen malicious domains, DNS tunneling, C2 activity, and network-level DNS hijacking. Continuously trained on rich and diverse threat intelligence, these models detect malicious activity with exceptional accuracy.

As enterprises adopt hybrid work, implement multicloud strategies, and connect more internet of things (IoT) devices, their exposure at the DNS layer increases significantly. Attackers are taking advantage, using automation and evasion techniques to bypass traditional defenses. Advanced DNS Security helps organizations stay ahead by inspecting traffic in real time and stopping threats before they can impact users or data.

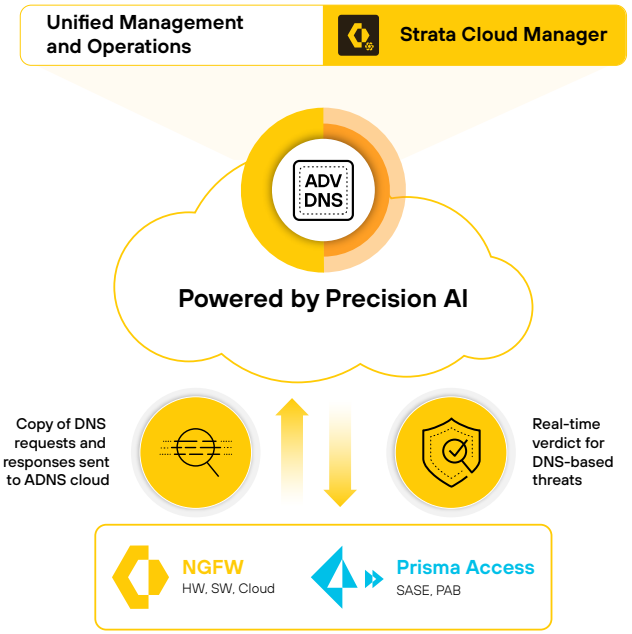

Figure 1. Advanced DNS Security

New Advanced DNS Security Resolver

As organizations become more distributed and adopt multicloud strategies, securing DNS traffic across diverse environments is more critical than ever. To meet this need, we offer a resolver-based deployment option for Advanced DNS Security—Advanced DNS Security Resolver (ADNSR)—delivering powerful, AI-driven threat prevention to any environment with unmatched speed and simplicity. This option provides the same high-fidelity protection as our firewall and SASE-integrated offerings.

The Advanced DNS Security Resolver is purpose-built for this modern reality, delivering intelligent threat prevention with effortless deployment. As a cloud-delivered DNS resolution service, complete with 99.999% availability, Advanced DNS Security Resolver makes it easy to protect your entire organization, regardless of where your users or infrastructure are located. It's built for fast, flexible deployment across multivendor environments, delivering real-time DNS-layer protection that covers 2x more DNS threats than our closest competitor.

With a simple DNS redirect to our cloud-hosted resolver, you can activate enterprise-grade protection in minutes, enabling consistent, always-on security across hybrid environments and multivendor infrastructures. Seamlessly integrated with Strata™ Cloud Manager, Advanced DNS Security Resolver provides centralized visibility and unified policy control on the Strata platform. This enables organizations to maintain high performance, streamline operations at scale, and meet requirements related to DNS visibility and threat prevention.

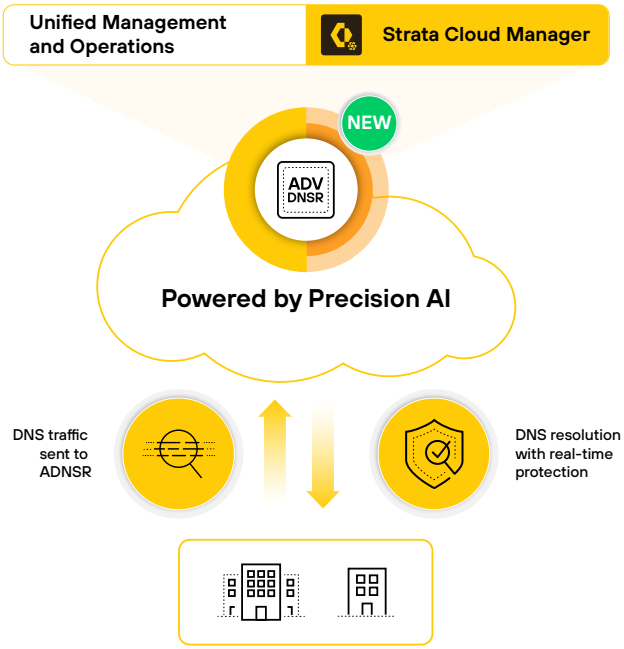

Figure 2. Advanced DNS Security Resolver

Advanced DNS Security Resolver offers:

- **Precision AI:** Our proprietary AI system, trained on the industry's most comprehensive, high-fidelity threat data, delivers deep insight into attacker behavior across the network, cloud, endpoint, and DNS layers.
- **Dual-layer inspection:** Inspects both DNS requests and responses to deliver visibility and detection that traditional solutions might miss, covering 2x more DNS threats than our closest competitors.
- **Stronger security outcomes:** Blocks advanced threats, like C2, DNS tunneling, and data exfiltration. Reduces risk in hybrid and distributed environments.
- **Enterprise-grade SLAs, centralized control:** Provides 99.999% availability and central policy management through Strata Cloud Manager. Ensures reliability and operational simplicity.
- **Simplified onboarding:** Activates protections instantly by redirecting your DNS traffic.
- **Consistent protection:** Delivers intelligent DNS-layer security regardless of location or infrastructure—branch sites and cloud workloads.

Industry-First Detections

Our Advanced DNS Security delivers unmatched breadth in DNS-layer threat detection, covering both request-side and response-side attacks. With over 30 advanced detection techniques across six major threat categories, it's the industry's first solution to offer comprehensive, real-time protection against DNS-based threats.

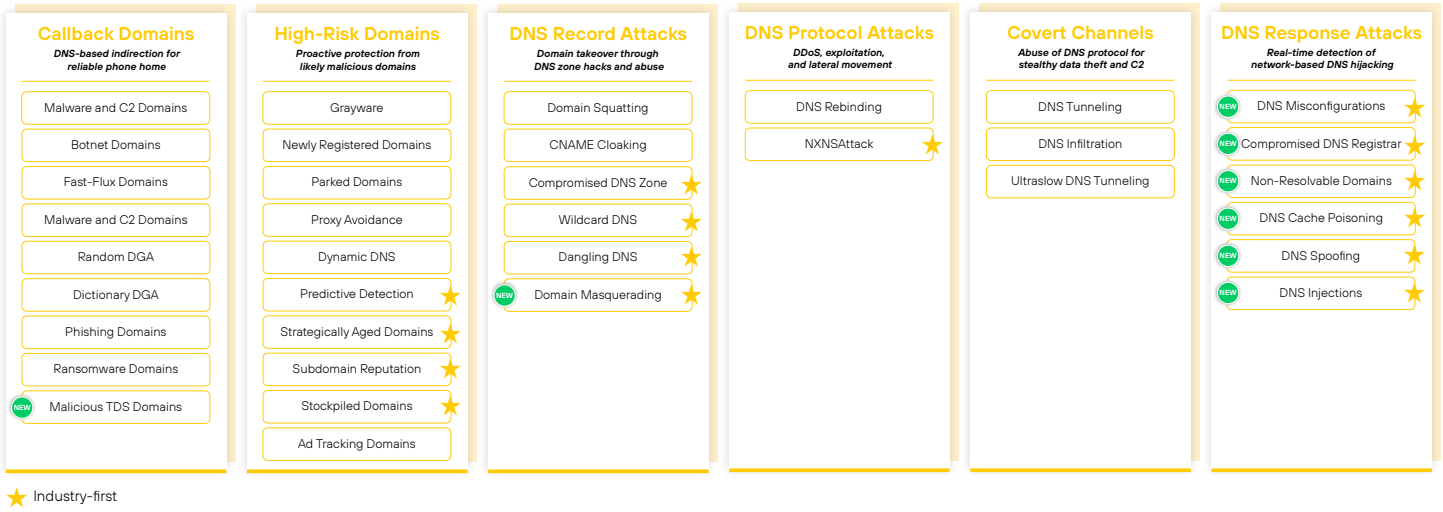

Figure 3. Advanced DNS Security Resolver

Key Capabilities

Powered by Precision AI

Advanced DNS Security is powered by Precision AI, which combines machine learning (ML), deep learning, and generative AI to detect and prevent advanced DNS threats in real time, including DNS tunneling, C2 activity, and domain hijacking.

Precision AI is built on three pillars: advanced AI models, real-time enforcement, and high-fidelity threat data collected from over 70,000 global customers, third-party intelligence, and DNS traffic patterns. This rich data continuously trains the models to identify emerging threats with exceptional accuracy.

We first applied ML to Advanced DNS Security to detect malicious DNS patterns and later incorporated deep learning to uncover evasive threats in large-scale, unstructured data. Now, as attackers adopt generative AI, we train our models on AI-generated threats, enabling DNS protection to evolve as fast as the threat landscape.

Flexible Deployment with Advanced DNS Security Resolver

As part of the Advanced DNS Security portfolio, Advanced DNS Security Resolver provides a fast and simple way to onboard DNS protection by redirecting traffic to our cloud-hosted, resolver-based service. This approach enables full DNS-layer inspection and is ideal for securing hybrid, multicloud, and distributed environments. ADNSR inspects both DNS requests and responses—a capability unique to us that delivers deep visibility and precise threat detection. This dual-layer inspection provides comprehensive coverage against DNS-layer attacks, making ADNSR the most complete resolver-based DNS security solution available.

Real-Time Action

Today's attackers operate at high speed, and security must keep pace with them. Static threat signature databases alone can't stop evasive or unknown threats. Effective defense requires real-time detection that operates inline with live network traffic. Advanced DNS Security analyzes DNS requests and responses as they occur, using the power and scalability of the cloud to deliver instant verdicts and block threats before they reach patient zero.

Natively Integrated in a Single Platform

Advanced DNS Security is tightly integrated with the Strata Network Security Platform, working seamlessly across all our form factors—hardware, software, and cloud firewalls. It also integrates with other Cloud-Delivered Security Services, sharing threat intelligence to close security gaps and deliver consistent, best-in-class protection across all attack vectors. Bringing these capabilities together into a single platform reduces complexity and strengthens defense against advanced DNS-layer threats.

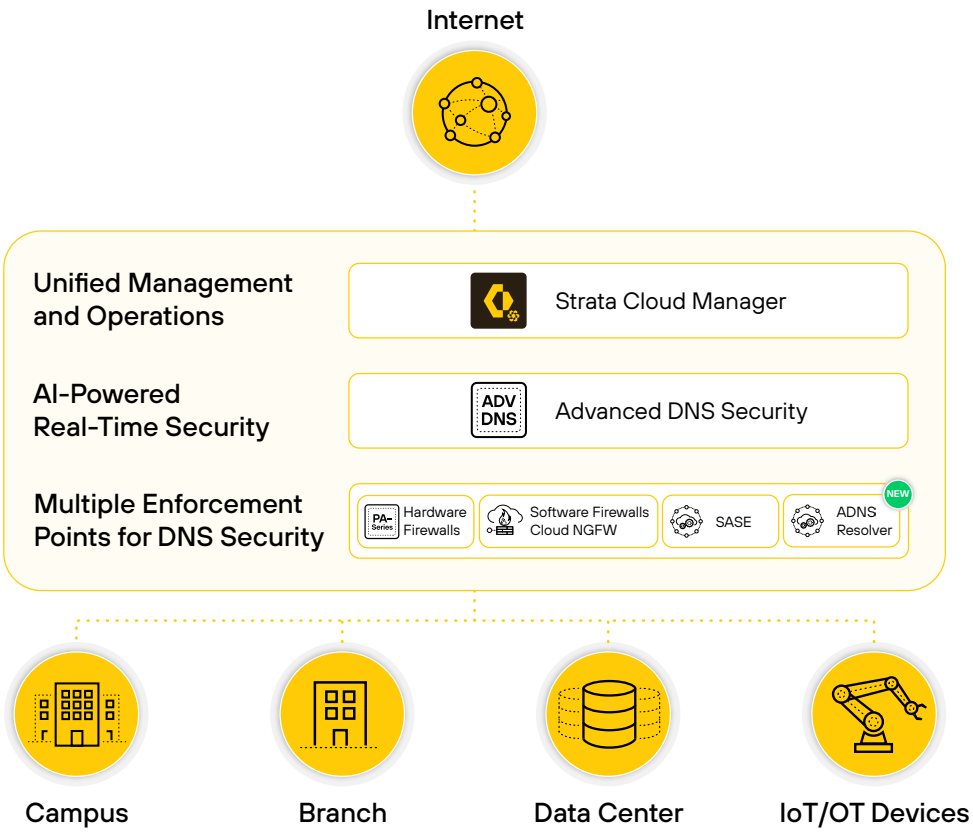

Figure 4. Strata Network Security Platform

Gain Insights into DNS Analytics

Advanced DNS Security equips security teams with rich DNS telemetry and contextual insights to accelerate threat detection and response. It continuously monitors public-facing domains to help prevent access to misconfigured or high-risk assets. A centralized dashboard offers historical views of domain activity, supporting incident investigations and risk assessments. With such data as query frequency, timestamps, passive DNS, WHOIS records, and malware associations, teams can gain a deeper understanding of DNS behavior, validate the protections in place, and identify potential blind spots across the environment.

Inspect All Types of DNS Traffic

Advanced DNS Security offers comprehensive protection for all DNS traffic, including plaintext DNS, DNS over TLS (DoT), and DNS over HTTPS (DoH), even when directed to unknown resolvers. It uses firewall-based decryption to analyze encrypted sessions and automatically sinkholes and quarantines infected users upon detecting malicious activity. With centralized monitoring through Strata Cloud Manager, security teams gain complete visibility and actionable insights from a single, unified dashboard.

Use Cases

- Block DNS-layer threats in real time, using inline inspection of both DNS requests and responses.
- Stop DNS-based C2 communications from malware using fast flux, domain generation algorithm (DGA), and other evasive techniques.
- Prevent data exfiltration via DNS tunneling from tools like iodine, dnscat2, or custom malware.
- Detect and block newly registered and suspicious domains often used in phishing, fraud, and zero-day attacks.
- Identify and stop DNS hijacking and manipulation attacks at the network level.
- Augment traditional and SASE deployments with scalable, AI-driven DNS-layer security.
- Enforce DNS-layer security policy controls through PAN-OS® and integrate with broader threat response workflows.
- Gain complete visibility into DNS traffic and suspicious behavior for threat hunting and investigations.
- Use AI and behavioral analysis to detect threats missed by static signature- or domain list-based approaches.

Table 1. Palo Alto Networks Cloud-Delivered Security Services

Product	Description
Advanced Threat Prevention	Stop known and unknown exploits, malware, spyware, and C2 threats with the industry's first prevention of zero-day attacks. It stops 60% more zero-day injection attacks and 48% more highly evasive C2 traffic than traditional IPS solutions.
Advanced WildFire®	Ensure safe access to files with the industry's largest malware prevention engine. It stops up to 22% more unknown malware and turns detection into prevention 180x faster than our 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. This stops up to 88% of malicious URLs at least 48 hours before our 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 our closest competitor.
Next-Generation Cloud Access Security Broker	Discover and control all SaaS consumption in your network with visibility into over 60,000 SaaS apps and protect your data with over 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	Uses ML, 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	Performs 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 complete 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 or content category that is configured as a sinkhole, causing that domain name to resolve to a definable IP address assigned to the client. Attempts by clients to access the sinkhole address can be logged and can trigger automated actions (e.g., quarantine). You can use this technique to identify infected hosts on the network. Additionally, Advanced DNS Security Resolver offers a custom block page feature. It enables organizations to display tailored messages to users when access to malicious or restricted domains is blocked, enhancing both security awareness and user experience.
Security Categories	Enables you to define separate policy actions and 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 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	
Category	**Description**
Privacy with Advanced DNS Security	
Trust and Privacy	We've implemented strict privacy and security controls to prevent unauthorized access to sensitive or personally identifiable information. We apply industry-standard best practices for security and confidentiality. Find more information in our Advanced DNS Security Privacy Datasheet.
Advanced DNS Security Licensing and Requirements	
Requirements	To use our Advanced DNS Security subscription, you need: • Palo Alto Networks NGFWs running PAN-OS 11.2 or later • Palo Alto Networks Threat Prevention license
Recommended Environment	Use Advanced DNS Security with Palo Alto Networks NGFWs deployed in any internet-facing location, because threats involving malicious domains, tunneling, and other abuse of DNS require external connectivity.
Advanced DNS Security License	Purchase Advanced DNS Security through a standalone license or as part of the Precision AI Network Security Bundle or Enterprise Agreement Bundle. For software firewall customers, purchase Advanced DNS Security using Firewall Flex Credits.

Table 5. Advanced DNS Security Resolver Licensing and Requirements	
Category	**Description**
Requirements	Advanced DNS Security Resolver is a separate offering and requires its own license, distinct from the Advanced DNS Security license.
Licensing	An active Advanced DNS Resolver license must be maintained to enable and manage Resolver functionality. The license is activated through the Palo Alto Networks Customer Support Portal.
Platform Compatibility	Advanced DNS Security Resolver doesn't have specific PAN-OS or content release requirements. Functionality is available once the license is activated and configured in your management platform (for example, Strata Cloud Manager).

Take Control of Your DNS-Layer Security

Attackers are evolving, and your defenses should too. Advanced DNS Security enables your organization to stop evasive DNS-layer threats in real time across every environment, device, and user. Whether protecting branch offices or cloud workloads, our flexible deployment options, including a new resolver-based solution, deliver consistent protection and complete visibility.

Contact your Palo Alto Networks representative or visit www.paloaltonetworks.com to learn how Advanced DNS Security can help you reduce risk, simplify operations, and stay ahead of modern threats.

Resources

- See our Advanced DNS Security webpage to learn more.
- Start your 90-day free trial.

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-security_091025