

10 DNS Blind Spots: How Advanced DNS Security Resolver Exposes and Stops Them Inline

A Practical Guide to Closing
Critical DNS Security Gaps

Executive Summary

DNS plays a critical role in every user connection and application workflow, yet most organizations lack visibility into what is happening inside their DNS traffic. Traditional DNS resolvers simply answer queries and do not evaluate intent, behavior, or risk. As a result, security teams are left without the insight needed to determine whether a domain is safe or harmful, creating blind spots across users, devices, locations, and cloud environments.

As modern threats continue to evolve, organizations need confidence that every DNS request is inspected and that malicious domains, including benign domains exhibiting malicious characteristics, are blocked before they can cause harm. They require clear insight into domain behavior, protection that works consistently across all environments, and real-time intelligence that keeps pace with today's threat landscape.

Palo Alto Networks Advanced DNS Security Resolver (ADNSR) builds on the proven capabilities of Advanced DNS Security by extending protection to additional deployment scenarios. A foundation of global intelligence, ADNSR is powered by the scale and depth of our Cloud-Delivered Security Services (CDSS).

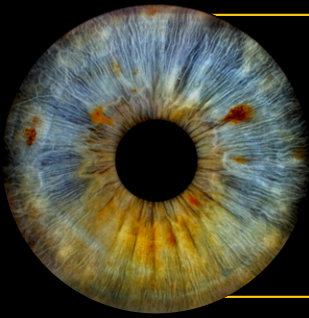
1. Engineering Telemetry Data Summary, Palo Alto Networks CDSS Engineering Team

This ecosystem provides a level of global intelligence that traditional resolvers cannot match:



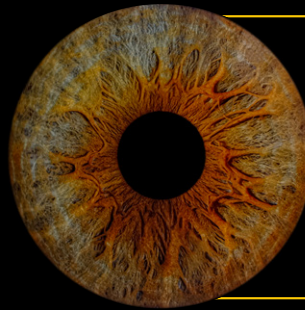
Precision AI[®] is at the core of this approach, as well as deep behavioral inspection that's applied to every DNS request in real time, giving you greater flexibility in how and where you enforce DNS security. This unified approach delivers consistent visibility and automated inline protection across firewalls, SASE, and resolver-based environments.

In this guide, we outline the 10 most common DNS blind spots that pose risks to security teams. We then explain how ADNSR can help your team close those gaps by delivering clarity, consistency, and real-time defense across every user and environment.



Blind Spot 1

Inability to Identify Domain-Generated Algorithms



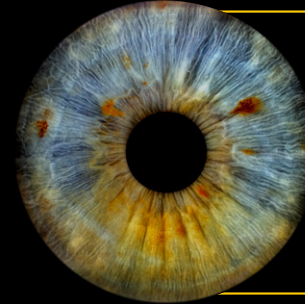
Blind Spot 6

No Behavioral Insight Into DNS Activity



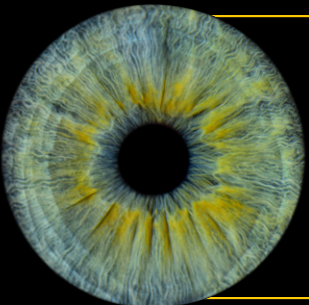
Blind Spot 2

Fast-Flux and Rotating Malicious Infrastructure



Blind Spot 7

DNS Layer Phishing Reaches Users Before Security Intervenes



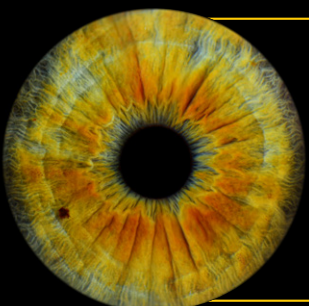
Blind Spot 3

Lack of Visibility Into DNS Tunneling



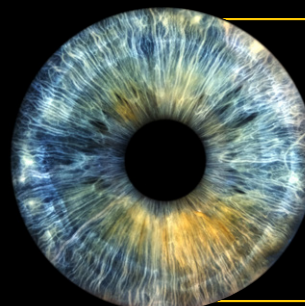
Blind Spot 8

Fragmented Visibility for Remote and Roaming Users



Blind Spot 4

Difficulty Identifying Shadowed or Hijacked Subdomains



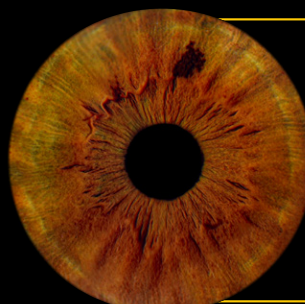
Blind Spot 9

Inconsistent DNS Policies Across Branch, HQ, and Cloud



Blind Spot 5

Limited Context Across the Attack Chain



Blind Spot 10

Limited Logging, Insight, and Forensics



Blind Spot 1

Inability to Identify Domain-Generated Algorithms

Organizations encounter thousands of new domains every day, yet most security teams cannot confidently determine which ones are safe. Modern malware increasingly relies on domain generation algorithms (DGAs) to rapidly create large volumes of domain names that appear legitimate and evade traditional detection methods. As attacker sophistication increases and barriers to entry continue to drop, organizations need reliable ways to evaluate newly observed domains before they are used for malicious activity.

The Challenge

- Organizations cannot confidently determine whether newly observed or unfamiliar domains are safe.
- DGA domains often appear legitimate and evade traditional detection techniques.
- Malware command-and-control (C2) blends well with typical DNS traffic.
- Security teams lack confidence when large volumes of new domains appear rapidly.
- Organizations need early warning signals before malicious domains become active threats.

How Advanced DNS Security Resolver Closes the Gaps

- Identifies domains generated by DGAs based on behavioral characteristics.
- Evaluates newly observed domains to determine whether they resemble legitimate or malicious activity.
- Blocks connections to unsafe domains before users or systems can reach them.
- Enriches domain activity by using intelligence from Advanced WildFire®, Advanced URL Filtering, Advanced Threat Prevention, and Cortex XSIAM®.
- Maintains fast DNS lookups through global points of presence, enabling low-latency resolution while performing deep, real-time inspection.

Outcome

Security teams gain clear visibility into newly observed and DGA-generated domains, enabling earlier detection of malicious activity and reducing uncertainty during the initial stages of an attack.

With 1.1 billion² new domains analyzed every day,

ADNSR uses Precision AI technologies to distinguish between legitimate new infrastructure and malicious DGAs in real time.

2. CDSS Engineering Telemetry Overview: DNS Analytics and Insights, Palo Alto Networks CDSS Engineering Team



Blind Spot 2

Fast-Flux and Rotating Malicious Infrastructure

Domains that frequently change their underlying infrastructure create confusion and uncertainty for security teams. Traditional resolvers cannot tell when a domain begins behaving unpredictably or shifting its IPs and records in ways that signal risk. You need clarity on whether a domain is stable and trustworthy or shows signs of evasive behavior.

The Challenge

- Security teams cannot tell when a domain suddenly begins behaving unpredictably.
- Rapid infrastructure changes make it difficult for security teams to determine if a domain is trustworthy.
- Harmful domains remain reachable long after attackers pivot their infrastructure.
- Distributed environments experience uneven protection, creating risks across sites.
- Security teams need clarity into whether DNS behavior indicates evasive or malicious intent.

Outcome

Organizations achieve predictable protection against a rapidly changing malicious infrastructure, preventing attackers from evading detection through constant domain or IP rotation.

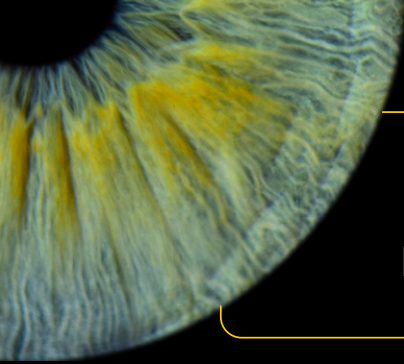
How Advanced DNS Security Resolver Closes the Gaps

- Alerts security teams to domains with unstable or suspicious behavior.
- Blocks access to domains associated with rapidly shifting attacker activity.
- Provides consistent protection across the branch, headquarters, cloud, and remote environments.
- Preserves fast resolution speeds even when performing deep inspection.
- Helps security teams disrupt harmful activity earlier with proactive visibility.

Attackers move fast, but we move faster.

ADNSR leverages a global engine to block up to 7.7 million³ new malicious domains daily, preventing phishing and rotating infrastructure before they reach users.

3. CDSS Engineering Telemetry Overview: DNS Analytics and Insights, Palo Alto Networks CDSS Engineering Team



Blind Spot 3

Lack of Visibility Into DNS Tunneling

Most organizations cannot see when data is transferred through DNS in unintended or unauthorized ways. Covert communication can blend into typical traffic, making it hard for teams to know when sensitive information is leaving the environment. Security teams need visibility into whether DNS is being used properly or misused as a hidden channel.

The Challenge

- Security teams cannot see when sensitive data leaves the organization through DNS.
- Covert communication channels blend into regular traffic and bypass traditional tools.
- Security teams are unaware when malware is using DNS to maintain ongoing communication.
- DNS tunneling creates blind spots that allow threats to persist.
- Remote and roaming users often receive no DNS inspection at all.

How Advanced DNS Security Resolver Closes the Gaps

- Identifies DNS activity that shows signs of hidden data movement or covert communication.
- Surfaces unusual patterns that indicate unauthorized data transfer.
- Blocks tunneling attempts before they reach or leave the organization.
- Provides a full DNS inspection through the Prisma® Access Agent even when the tunnel is disconnected.
- Gives security teams consistent visibility across every device, location, and connection.

Outcome

Hidden data movement and covert communication channels are exposed and stopped, closing DNS blind spots that allow threats to persist undetected.

Nearly 40%⁴ of command-and-control (C2) techniques involve remote access tools, many of which rely on DNS for stealthy communication and persistence.

4. Global Incident Response Report (2026)



Blind Spot 4

Difficulty Identifying Shadowed or Hijacked Subdomains

Security teams often trust well-known parent domains, making it challenging to detect when unauthorized subdomains are created beneath them. Hidden or hijacked subdomains can be used to host harmful content or redirect users to unsafe destinations. Organizations need a way to distinguish legitimate subdomain activity from behavior that signals unauthorized use.

The Challenge

- Security teams trust parent domains and cannot easily see when attackers create malicious subdomains beneath them.
- Threats hide under familiar domains and appear safe.
- Security teams cannot detect unauthorized subdomain creation or unusual behavior.
- Malicious pages or infrastructure load under legitimate domains without warning.
- Security teams lack insight into how subdomains are used across their environment.

How Advanced DNS Security Resolver Closes the Gaps

- Detects subdomain patterns that do not match legitimate usage.
- Identifies newly created subdomains added without authorization.
- Blocks malicious subdomain chains before users can reach them.
- Applies consistent subdomain inspection policies everywhere through Strata™ Cloud Manager.
- Gives Security teams clear visibility into how domains and subdomains are being used.

Outcome

Unauthorized or malicious subdomain activity is identified early, preventing attackers from hiding under trusted parent domains.



Blind Spot 5

Limited Context Across the Attack Chain

DNS events often appear isolated when viewed through traditional tools, making it difficult for security teams to recognize when multiple activities are connected. Without a broader context, they struggle to understand whether DNS activity is part of a larger pattern. Organizations need a unified view that brings DNS activity together with insights from other parts of their security stack.

The Challenge

- Security teams cannot connect DNS activity with behavior seen in other security tools.
- Important signals appear isolated rather than as part of a coordinated attack.
- Early warnings are lost because there is no unified view.
- DNS alerts do not connect to web, endpoint, or identity activity.
- Organizations need a broader picture to understand what is happening.

How Advanced DNS Security Resolver Closes the Gaps

- Correlates DNS activity with URL Filtering, WildFire analysis, firewall logs, and Cortex XSIAM data.
- Reveals when multiple suspicious events are connected.
- Blocks harmful communication early to prevent escalation.
- Maintains fast lookups while providing rich context behind the scenes.
- Delivers consistent inspection for roaming users through the Prisma Access Agent.

Outcome

Security teams view DNS activity in full context alongside related security signals, enabling faster threat recognition and earlier disruption of coordinated attacks.



Blind Spot 6

No Behavioral Insight Into DNS Activity

Repeated, unusual, or automated DNS activity can indicate early signs of compromise, yet most resolvers do not analyze DNS behavior over time. Security teams need insight into whether DNS patterns represent typical usage or emerging threats. Organizations benefit from knowing when behavior shifts away from expected patterns.

The Challenge

- Security teams cannot determine whether repeated or unusual DNS queries indicate malicious activity.
- Automated malware behavior appears identical to regular user traffic.
- Encoded or irregular subdomains go unreviewed.
- Security teams cannot track how DNS behavior evolves over time.
- Early indicators of compromise remain hidden.

How Advanced DNS Security Resolver Closes the Gaps

- Analyzes DNS structure, frequency, and behavior of DNS across time.
- Flags patterns that differ from typical user or system behavior.
- Identifies automated malware activity that traditional tools miss.
- Uses Precision AI to compare local behavior with global patterns.
- Reveals reconnaissance and staging behavior before an attack progresses.

Outcome

Subtle indicators of compromise become visible, enabling teams to intervene before automated or unusual DNS behavior escalates into an active attack.

ADNSR provides deep behavioral insight **to prevent up to 2.06 billion threats inline⁵**, identifying malicious intent and hidden patterns in DNS activity that traditional resolvers simply cannot see.

⁵CDSS Engineering Telemetry Overview: DNS Analytics and Insights, Palo Alto Networks CDSS Engineering Team



Blind Spot 7

DNS Layer Phishing Reaches Users Before Security Intervenes

Phishing remains one of the most common ways users encounter threats, yet many harmful domains bypass DNS resolvers without inspection. Security teams need a way to stop unsafe domains before users load a page or reveal sensitive information. DNS is a critical point for blocking phishing attempts early.

The Challenge

- Security teams cannot stop phishing domains before a user reaches the page.
- Look-alike domains load without review or inspection.
- AI-generated phishing infrastructure appears legitimate to traditional resolvers.
- Security teams have little visibility into early-stage phishing activity.
- Harmful domains are not blocked until after users interact with them.

How Advanced DNS Security Resolver Closes the Gaps

- Blocks suspicious domains during the DNS request, before the browser session starts.
- Identifies newly registered domains associated with phishing behavior.
- Stops credential harvesting and malicious content before users can reach it.
- Uses Precision AI to prevent large volumes of phishing activity at a global scale.
- Protects users on corporate, remote, and personal devices consistently.

Outcome

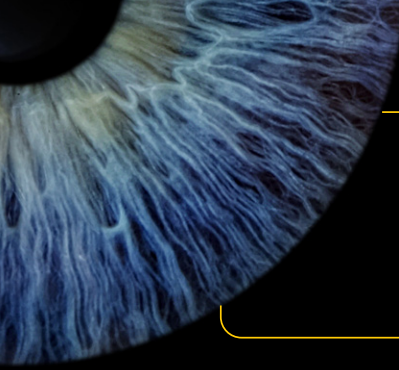
Phishing attempts are blocked at the DNS layer, preventing users from ever reaching malicious destinations or exposing credentials.

Speed is the new battleground.

While traditional detection takes days,

AI-assisted attacks can reach data exfiltration in as little as 25 minutes⁶, making inline DNS blocking your only effective defense.

6. Palo Alto Networks Unit 42, Global Incident Response Report 2025.



Blind Spot 8

Fragmented Visibility for Remote and Roaming Users

Hybrid work has shifted many DNS requests outside the corporate network, reducing visibility and control. Unmanaged networks and remote work locations weaken DNS oversight, creating gaps in protection. Security teams need consistent DNS inspection regardless of where users connect.

The Challenge

- Remote users often bypass DNS security when disconnected from the network.
- Policies cannot be enforced consistently across locations.
- Roaming DNS activity is not logged or monitored.
- Security teams struggle to maintain visibility across distributed environments.

How Advanced DNS Security Resolver Closes the Gaps

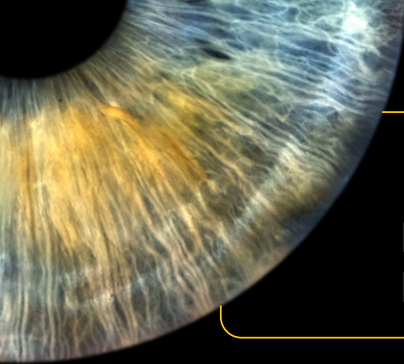
- Maintains DNS inspection and enforcement for Prisma Access Agent users when the tunnel is disconnected.
- Applies DNS logging, inspection, and blocking for supported remote user scenarios.
- Inspects DNS traffic through ADNSR rather than falling back to unmonitored local resolvers.
- Provides centralized visibility into DNS activity for supported remote users through Strata Cloud Manager.

Outcome

When traditional SASE enforcement is unavailable, ADNSR improves DNS visibility and protection for remote users by reducing blind spots caused by tunnel disconnections. This approach delivers more consistent DNS security without impacting user connectivity.

Nearly 80%⁷ of employees with remote-capable jobs now work in hybrid or fully remote setups, shifting DNS activity beyond traditional corporate networks and creating visibility gaps for security teams.

7. Great Place to Work and Gallup, 2025.



Blind Spot 9

Inconsistent DNS Policies Across Branch, HQ, and Cloud

Different sites and environments often use various DNS resolvers, creating inconsistent enforcement and fragmented visibility. Organizations struggle to maintain uniform security policies when DNS infrastructure varies across locations. They need a unified approach to deliver predictable, consistent DNS protection.

The Challenge

- Different locations rely on various resolvers with inconsistent rules.
- DNS visibility becomes fragmented across environments.
- Policy updates require manual changes in multiple places.
- Attackers exploit gaps between locations.
- Maintaining uniform protection becomes difficult.

How Advanced DNS Security Resolver Closes the Gaps

- Enforces a single set of DNS security policies everywhere.
- Eliminates reliance on different resolvers across sites.
- Provides consistent inspection, blocking, and logging.
- Applies updates automatically through a cloud-delivered service.
- Unifies DNS operations in Strata Cloud Manager.

Outcome

ADNSR helps security teams maintain a single, unified DNS security posture across branch, headquarters, and cloud environments, without adding operational complexity.

92–93%⁸ of organizations now operate in multi-cloud environments, often using nearly five different cloud platforms, making it increasingly difficult to enforce consistent security and DNS policies across locations and platforms.

8. Flexera State of the Cloud Report and Spacelift.

Blind Spot 10

Limited Logging, Insight, and Forensics

DNS logs often lack meaningful detail, making it difficult for teams to investigate suspicious activity or determine whether DNS behavior is risky. Security teams need actionable context, correlation with other tools, and reliable visibility to support investigations and rapid response.

The Challenge

- DNS logs provide minimal context and limited value.
- Security teams cannot determine whether DNS behavior is risky.
- DNS alerts cannot be connected to activity from other tools.
- Investigations stall due to a lack of detail.
- Forensic reconstruction is incomplete or slow.

How Advanced DNS Security Resolver Closes the Gaps

- Provides detailed, high-fidelity DNS logs with actionable context.
- Enables an indicator-of-compromise (IoC)-based search across DNS telemetry to quickly investigate known indicators.
- Integrates with Cortex XSIAM for unified investigation and correlation.
- Maps DNS activity to MITRE ATT&CK® techniques for faster threat identification.
- Supports proactive threat hunting and incident response.
- Uses AI Canvas dashboards to surface insights, trends, and anomalies across DNS activity.
- Offers continuous visibility, backed by a 99.999% uptime commitment.

Outcome

High-fidelity DNS telemetry enables faster investigations, more confident threat analysis, and improved response outcomes.

Ransomware is now present in 44%⁹ of breaches, highlighting the need for high-fidelity telemetry to detect threats before they escalate.

9. Verizon, 2025 Data Breach Investigations Report (DBIR).

See DNS Threats Before They Reach Your Environment

Modern organizations need confidence that every DNS request is safe. Traditional resolvers were not designed to inspect behavior or detect malicious intent, which leaves dangerous gaps across users, devices, and environments.

ADNSR delivers inline prevention, deep visibility, and real-time protection across every DNS request. It closes the blind spots that legacy resolvers overlook and provides the clarity and confidence organizations need to protect their environments.

You don't need to wonder what traditional resolvers miss. ADNSR provides the necessary visibility and protection to stop threats before they reach users or systems.

To see how ADNSR delivers broader coverage and deeper insight than traditional resolver-based defenses, [start your 30-day free trial](#).

1. [Engineering Telemetry Data Summary](#), Palo Alto Networks CDSS Engineering Team
2. [CDSS Engineering Telemetry Overview: DNS Analytics and Insights](#), Palo Alto Networks CDSS Engineering Team
3. [CDSS Engineering Telemetry Overview: DNS Analytics and Insights](#), Palo Alto Networks CDSS Engineering Team
4. [Palo Alto Networks Unit 42, Global Incident Response Report \(2026\)](#)
5. [CDSS Engineering Telemetry Overview: DNS Analytics and Insights](#), Palo Alto Networks CDSS Engineering Team
6. [Palo Alto Networks Unit 42, Global Incident Response Report 2025](#)
7. [Great Place to Work and Gallup, 2025](#)
8. [Flexera State of the Cloud Report and Spacelift](#)
9. [Verizon, 2025 Data Breach Investigations Report \(DBIR\)](#)

About Palo Alto Networks

As the global cybersecurity leader, Palo Alto Networks (NASDAQ: PANW) is dedicated to protecting our digital way of life via continuous innovation. Trusted by more than 70,000 organizations worldwide, we provide comprehensive AI-powered security solutions across network, cloud, security operations and AI, enhanced by the expertise and threat intelligence of Unit 42®. Our focus on platformization allows enterprises to streamline security at scale, ensuring protection fuels innovation. Explore more at www.paloaltonetworks.com.



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

© 2026 Palo Alto Networks, Inc. A list of our trademarks in the United States and other jurisdictions can be found at <https://www.paloaltonetworks.com/company/trademarks.html>. All other marks mentioned herein may be trademarks of their respective companies.
Strata_ADNSR_Handbook_02052026