Business Benefits

- **Keep your organization safe from the latest DNS-based threats.** Using inline machine learning, identify and disrupt the latest attacks that abuse DNS.
- **Reduce costs and consolidate vendors with DNS security tools.** Extend your NGFW investment and save time in operations with a single coordinated network security stack for all alerts, policies, rule violations, IDPS, web security, malware analysis, and DNS.
- **Enjoy the latest security innovations with no user impact.** Built on a modular, cloud-based architecture, DNS Security seamlessly adds new detection, prevention, and analytics capabilities without requiring reconfiguration, unlike other solutions.
- **Optimize your security posture.** Use your DNS Security Analytics dashboard to ensure NGFWs with significant DNS traffic are protected.

DNS Security

Predict and Disrupt Today's Most Sophisticated DNS-Based Attacks

The Domain Name System (DNS) is wide open for attackers. Its ubiquity and high traffic volume make it easy for adversaries to hide malicious activity. The Palo Alto Networks Unit 42 threat research team identified that 80% of malware uses DNS to initiate command-and-control (C2) procedures. Attackers can also abuse DNS using a multitude of techniques to deliver malware and exfiltrate data. Unfortunately, security teams often lack basic visibility into how threats use DNS that would enable them to respond effectively. Current approaches lack automation; drown you in uncoordinated data from independent tools; or require changes to DNS infrastructure that can not only be bypassed, but also require continual maintenance. It's time to take back control of your DNS traffic.

DNS Security gives you real-time protection, applying industry-first protections to disrupt attacks that use DNS. Tight integration with Palo Alto Networks Next-Generation Firewall (NGFW) gives you automated protections, prevents attackers from bypassing security measures, and eliminates the need for independent tools or changes to DNS routing. DNS Security gives your organization a critical new control point to stop attacks.

The DNS Security Difference

Built in the cloud, DNS Security is a subscription service that works natively with your NGFW to secure your DNS traffic.

Shared threat intelligence and machine learning (ML) rapidly identify any threats hidden in DNS traffic. Cloud-based protections are delivered instantly, scale infinitely to all users, and are always up to date. A purpose-built analytics dashboard provides full visibility into your DNS traffic along with one-click context for any attack the DNS Security service detects. DNS Security delivers:

- **Unparalleled protection from DNS-based threats** through groundbreaking inline ML algorithms that predict and identify new and advanced threats, disrupting attacks.
- **Security that can't be bypassed** by changing DNS settings.
- **Incredible ease of deployment**—simply turn on and manage your subscription through your NGFW. Don't worry about rerouting your DNS traffic or working through lengthy change management processes.
- **Maximized operational efficiency** by securing your DNS traffic through the Palo Alto Networks platform.

Key Capabilities

Protect Against the Latest and Most Advanced DNS-Based Attacks

Beyond malware, phishing, and other traditional threats, adversaries also exploit DNS to establish reliable C2, attack hosts inside the corporate network from the internet, perform distributed denial-of-service (DDoS) attacks, and even cause reputational harm by taking over your domains. Modern DNS-layer security must be able to identify and disrupt these attacks.

Detecting and preventing sophisticated DNS-layer network attacks and data exfiltration techniques requires ML algorithms that can rapidly analyze DNS traffic and get ahead of threats. It also requires robust threat intelligence to inform those algorithms and measures designed to protect against specific attack techniques. Finally, it requires enforcement points to block or sinkhole malicious DNS activity once identified.

The DNS Security service predicts and stops malicious domains with instant enforcement through the NGFW, protecting you against automated attacks. Our ML-enabled detection engines (see table 2) solve key emerging DNS-based attacks, such as ultra-slow DNS tunneling, dangling DNS, and DNS rebinding. DNS Security can even predict new malicious domains right after their registration, before they can be used against you. DNS Security's comprehensive, market-leading protections provide you with the most effective security regardless of DNS settings, configurations, and deployment model.

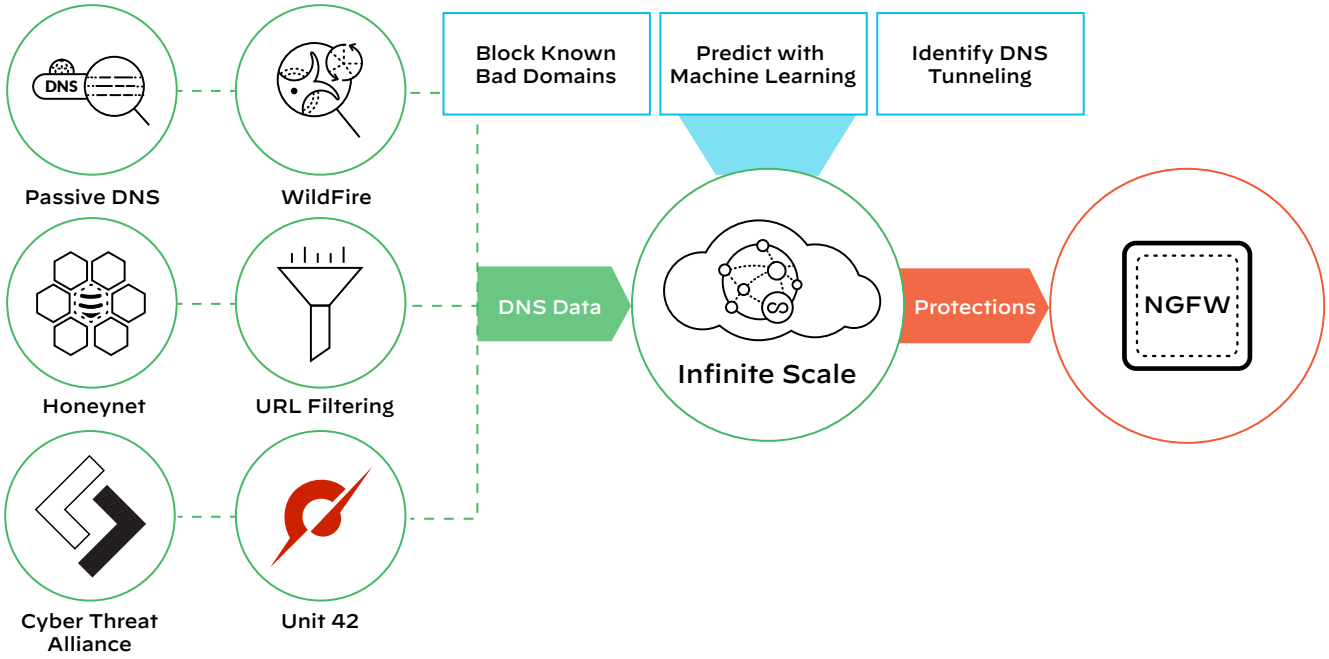

Figure 1: Rich DNS data powering ML for protection

Stop Known Threats

The DNS Security subscription offers limitless protection against tens of millions of malicious domains, identifying them with real-time analysis and continuously growing global threat intelligence. Our cloud database scales with data from a large and ever-expanding threat intelligence sharing community, adding to Palo Alto Networks sources that include:

- **WildFire® malware prevention service** to find new C2 domains, file download source domains, and domains in malicious email links.
- **URL Filtering** to continuously crawl newfound or uncategorized sites for threat indicators.
- **Passive DNS and device telemetry** to understand domain resolution history seen from thousands of deployed NGFWs, generating petabytes of data per day.
- **Unit 42 threat research** to provide human-driven adversary tracking and malware reverse engineering, including insight from globally deployed honeypots.
- **More than 30 third-party sources** of threat intelligence to enrich data and ensure you have coverage.

Leverage Category-Based Action

Create policies specific to DNS traffic types. All DNS queries are checked against our scalable cloud database in real time to determine appropriate enforcement actions. DNS Security uses ML to rapidly detect and categorize threats over DNS. Based on those categories, the most effective responses are automatically implemented through granular policy-based actions. Set policy to block, alert, or sinkhole based on categories that include malware, DGA, DNS tunneling, C2, dynamic DNS, or newly registered domains. With granular categories of DNS traffic (see table 1), administrators can craft custom policies to handle good, malicious, and suspicious domains independently.

Identify and Quarantine Infected Systems

Use automation to prevent the spread of infection. Automate dynamic response to find infected machines and quickly respond in policy. When attacks using DNS are identified, security administrators can automate the process of sinkholing malicious domains on the NGFW to cut off C2, rapidly identify infected users on the network, and even isolate them. Combining malicious domain sinkholing, Dynamic Address Groups (DAGs), and logging actions enables automation of detection and response workflows, saving analysts time by removing the slow and manual processes other solutions require.

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:

- **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, time stamps, 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.

Table 1: DNS Security Categories

Command-and-Control (C2)	This category includes URLs and domains used by malware and/or compromised systems to surreptitiously communicate with an attacker's remote server to receive malicious commands or exfiltrate data (this includes DNS tunneling detection and DGA detection).
Dynamic DNS (DDNS)	DNS Security detects exploitative DDNS services by filtering and cross-referencing DNS data from various sources to generate candidate lists which are then further validated to maximize accuracy.
Malware	Malicious domains host and distribute malware and can include websites that attempt to install various threats (e.g., executable files, scripts, viruses, drive-by downloads).
Newly Registered Domains (NRD)	Newly registered domains are new, never-registered domains that have been recently added by a TLD operator or entity. While new domains can be created for legitimate purposes, the vast majority are often used to facilitate malicious activities, such as operating as C2 servers or distributing malware, spam, PUP/adware.
Phishing	Phishing domains attempt to lure users into submitting sensitive data, such as personal information or user credentials, by masquerading as legitimate websites through phishing or pharming.
Grayware	Grayware domains generally do not pose a direct security threat; however, they can facilitate vectors of attack, produce various undesirable behaviors, or might simply contain questionable/offensive content.
Parked	Parked domains are typically inactive websites that host limited content, often in the form of click-through ads, which may generate revenue for the host entity but generally do not contain content that is useful to the end user.
Proxy Avoidance & Anonymizers	Proxy avoidance and anonymizers are services that are used to bypass content filtering policies.

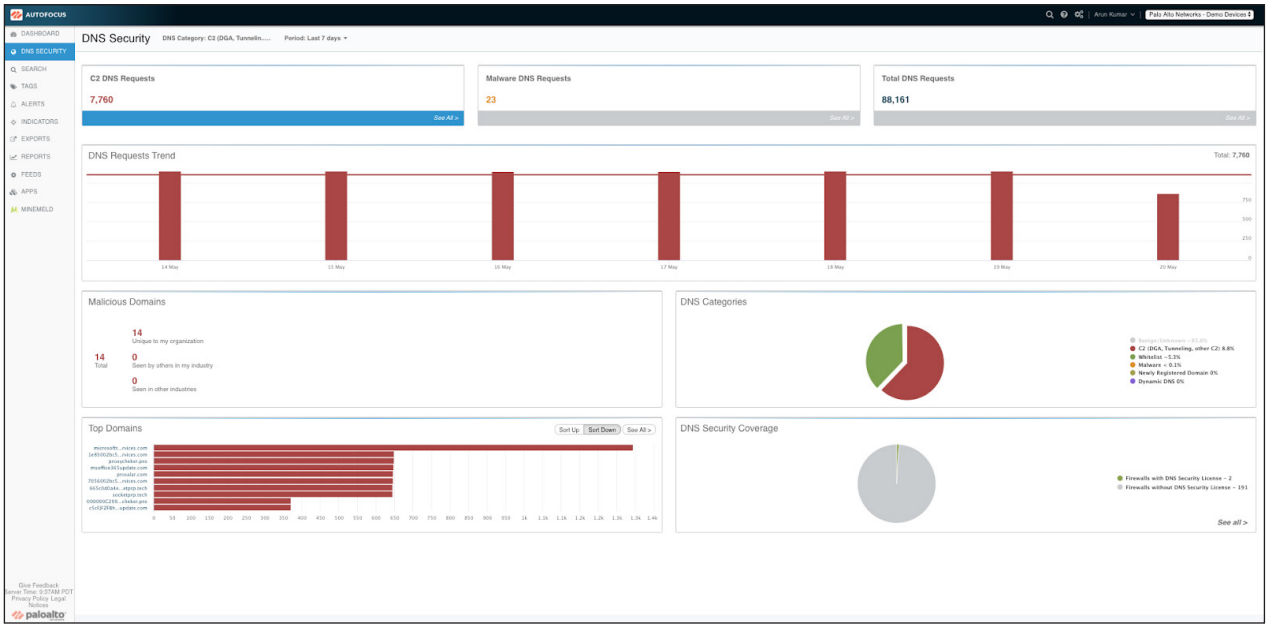

Figure 2: DNS Security Analytics dashboard

The Power of Palo Alto Networks Security Subscriptions

Detect and Prevent Advanced Threats with Cloud-Delivered Security Services

Today, cyberattacks have increased in volume and sophistication, scaling to 45,000 variants within 30 minutes, using multiple threat vectors or advanced techniques to deliver malicious payloads within your enterprise. Traditional and disparate security challenges organizations to protect their users, devices and applications, creating security gaps, increasing management overhead for security teams, and hindering business productivity with inconsistent access and visibility. Seamlessly integrated with the industry-leading Next-Generation Firewall platform, our Cloud-Delivered Security Services use the network effect of 80,000 customers to instantly coordinate intelligence and provide protections for all threats across all threat vectors. Eliminate coverage gaps across all enterprise locations and take advantage of best-in-class security delivered consistently in a platform, so you can be safe from even the most advanced and evasive threats.

Threat Prevention: Goes beyond traditional intrusion prevention system (IPS) to prevent all known threats across all traffic in a single pass without sacrificing performance

- **Advanced URL Filtering:** Provides best in class web protection while maximizing operational efficiency with the industry's first real-time web protection engine and industry-leading phishing protections
- **Wildfire:** Ensures files are safe with automatic detection and prevention of unknown malware powered by industry-leading cloud-based analysis and crowd-sourced intelligence from over 42,000 customers
- **DNS Security:** Harnesses the power of machine learning to detect and prevent threats over DNS in real-time and empowers security personnel with the intelligence and context to craft policies and respond to threats quickly and effectively.
- **IoT Security:** Provides the industry's most comprehensive IoT Security solution delivering ML-powered visibility, prevention, and enforcement in a single platform
- **Enterprise DLP:** The industry's first cloud-delivered enterprise DLP that consistently protects sensitive data across networks, clouds, and users
- **SaaS Security:** Delivers integrated SaaS Security, that lets you see and secure new SaaS applications, protect data and prevent zero day threats at the lowest TCO.

Operational Benefits

The DNS Security subscription enables you to:

- **Deploy with ease.** Tight integration with the NGFW platform means you're simply turning on a service without having to reroute your DNS traffic to outside resolvers **that attackers can easily bypass.**
- **Get protection without performance impact.** Advanced security is seamlessly applied to DNS queries in real time, with no business impact.
- **Maintain full visibility into DNS traffic.** The visual dashboard gives network security engineers and SOC analysts alike a fast visual assessment of your organization's DNS usage.
- **Customize response through DNS categories.** Easily set up policies in line with your risk profile by automating responses based on DNS traffic types.

Table 2: DNS Security Features	
Feature	**Description**
ML-Based Inline Protection	Uses ML-based analysis to identify advanced DNS-based threats (listed under DNS security detectors).
Cloud Database	Contains tens of millions of known malicious domains, enabling you to block phishing, malware, and other high-risk categories.
DNS Security 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 known 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.
DNS 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.
DNS Security Detectors	—
Domain Generation Algorithm (DGA)	Identifies the use of DGAs, which generate random domains on the fly for malware to use as a way to call back to a C2 server.
Dictionary DGA	Identifies DGA domains based on dictionary words.
DNS Tunneling	Prevents the use of this technique, which exploits the DNS protocol to tunnel malware and other data through a client-server model.
Ultra-Slow DNS Tunneling	Disrupts ultra-low/slow DNS tunnels that spread tunneled data and exploits across multiple domains and use very slow rates to evade detection, stealing data or sending additional malicious payloads into your network.
Fast Flux Domains	Prevents fast flux, a technique cybercriminals use to cycle through bots and DNS records. Fast flux networks are used for phishing, malware distribution, scams, and botnet operations.
DNS Rebinding Attacks	Prevents DNS rebinding attacks, which can be used to move laterally and attack services inside the corporate network from the internet.
Dangling DNS Attacks	Prevents dangling DNS attacks, which take advantage of stale DNS zone data to take over domains and cause reputational harm or launch phishing attacks.
NXNS Denial-of-Service Domains	Protects users from connecting to domains that can be used to launch DDoS attacks.
Malicious Newly Registered Domains (NRD)	Uses predictive analysis to identify domains registered by malicious actors at the time of registration.

Table 3: Privacy and Licensing Summary	
Privacy with DNS Security Subscription	
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 datasheets.
Licensing and Requirements	
Requirements	To use the Palo Alto Networks DNS Security subscription, you will need: • Palo Alto Networks Next-Generation Firewalls running PAN-OS 9.0 or later • Palo Alto Networks Threat Prevention license
Recommended Environment	Use 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.
DNS Security License	DNS Security requires a standalone license, delivered as an integrated, cloud-based subscription for Palo Alto Networks Next-Generation Firewalls. It is also available as part of the Palo Alto Networks Subscription ELA, VM-Series ELA, or Prisma Access.

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