paloalto® NETWORKS

Business Benefits

- **Reduce costs and consolidate vendors with DNS security tools.** Extend your next-generation security 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 Analytics dashboard to ensure all DNS traffic is protected by consistent security policy.

DNS Security

Take Back Control of Your DNS Traffic

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. Palo Alto Networks Unit 42 threat research team identified that almost 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 require continual maintenance. It's time to take back control of your DNS traffic.

Palo Alto Networks DNS Security

To protect against all threats over DNS, customers need superior detection combined with analytics that empower security personnel with the context to quickly and effectively craft policies and respond to threats. Palo Alto Networks DNS Security, a cloud-delivered subscription, applies predictive analytics to disrupt attacks that use DNS for C2 or data theft as they occur. Any threats hidden in DNS traffic are rapidly identified with shared threat intelligence and machine learning. 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.

Tight integration with Palo Alto Networks ML-Powered Next-Generation Firewalls (NGFW) gives you automated protection and eliminates the need for independent tools. Because all traffic goes through the ML-Powered NGFW, DNS Security sees everything and can't be evaded by users or attackers rerouting your DNS settings. You simply turn it on—without any need to deploy additional appliances or change your DNS infrastructure—and your organization now has a critical new control point to stop the large number of attacks that use DNS, while your security teams gain greater context into your traffic and how it is being used.

Key Capabilities

Stop Known Threats

The DNS Security subscription offers limitless protection against tens of millions of malicious domains, identifying them with real-time analysis and a continuously growing global threat intelligence. Our cloud-based 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.

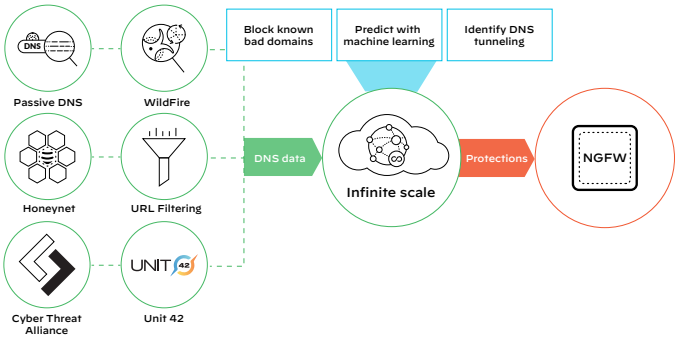

Figure 1: Rich DNS data power machine learning for protection

Predict and Block New Malicious Domains

With the DNS Security service, your ML-Powered NGFW can predict and stop malicious domains from domain generation algorithm-based malware with instant enforcement, protecting you against these automated attacks. Attackers' use of domain generation algorithms (DGA) to randomly create a domain for C2 continues to grow, limiting the effectiveness of blocking known malicious domains and overwhelming the signature capability of traditional security approaches. DNS Security deals with DGA through:

- **Machine learning** to detect new and never-before-seen DGA domains by analyzing DNS queries as they are performed.
- **Easy-to-set policy** for dynamic action to block DGA domains or sinkhole DNS queries.
- **Threat attribution** and context to identify the malware family with machine learning for faster investigation efforts.

Neutralize DNS Tunneling

Detect and prevent advanced attacks in real time. Advanced attackers use DNS tunneling to hide data theft or C2 in standard DNS traffic. The sheer volume of DNS traffic often means defenders simply lack the visibility or resources to universally inspect it for threats. DNS Security:

- **Uses machine learning** to quickly detect C2 or data theft hidden in DNS tunneling. With historical and real-time shared threat intelligence, our algorithms observe the features of DNS queries, including query rate and patterns, entropy, and n-gram frequency analysis of domains to accurately detect tunneling behavior.
- **Extends PAN-OS® signature-based protection** to identify advanced tunneling attempts. DNS Security expands the native ability of our ML-Powered NGFWs to detect and prevent DNS tunneling. Protections are scalable and evasion-resistant, covering known and unknown variants of DNS tunneling.
- **Rapidly neutralizes DNS tunneling** with automated policy action. DNS tunneling is automatically stopped with the combination of easy-to-set policy actions on the firewall and blocking of the parent domain for all customers, ensuring you benefit from our global community.

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 machine learning 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, 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 ML-Powered NGFW to cut off C2, rapidly identify infected users on the network, and even isolate them. Combining malicious domain sinkholing, Dynamic Address Groups, and logging actions enables automation of detection and response workflows, saving analysts time by removing the slow and manual processes other solutions require.

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 ML-Powered NGFWs across your estate, allowing you to quickly eliminate any blind spots.

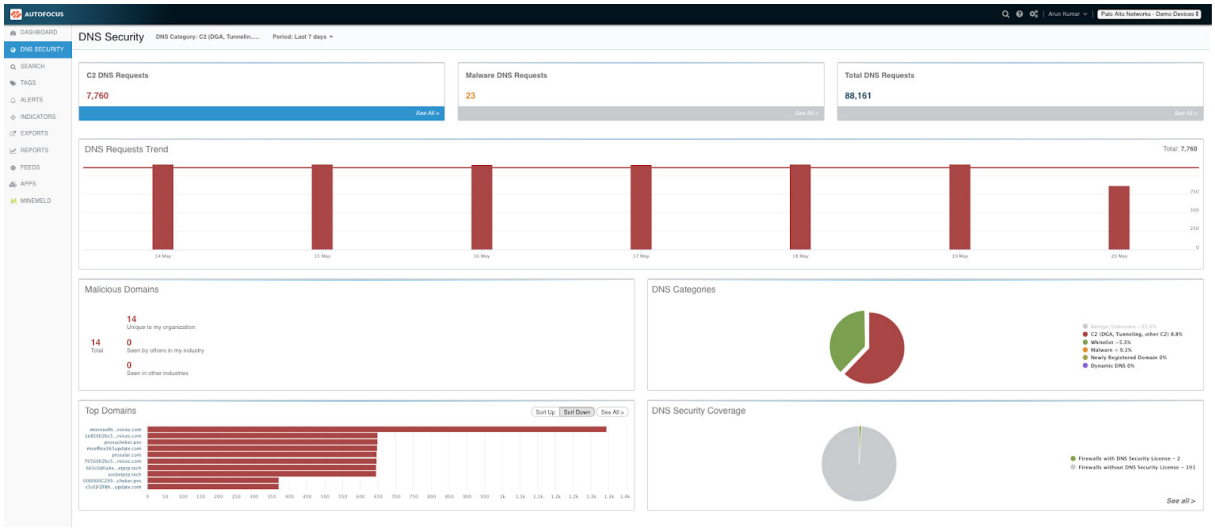

Figure 2: Give your security personnel all the intelligence they need to protect against DNS-based attacks with the DNS Analytics dashboard

Operational Benefits

The DNS Security subscription enables you to:

- **Deploy with ease.** Tight integration with the Next-Generation Firewall 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 report 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.

The Power of Palo Alto Networks Security Subscriptions

Today, cyberattacks have increased in volume and sophistication, using advanced techniques to bypass network security devices and tools. This challenges organizations to protect their networks without increasing workloads for security teams or hindering business productivity. Seamlessly integrated with the industry's first ML-Powered NGFW platform, our cloud-delivered security subscriptions coordinate intelligence and provide protections across all attack vectors, providing best-in-class functionality while eliminating the coverage gaps disparate network security tools create. Take advantage of market-leading capabilities with the consistent experience of a platform, and secure your organization against even the most advanced and evasive threats. Benefit from DNS Security or any of our security subscriptions:

- **Threat Prevention**: Go beyond traditional intrusion prevention system (IPS) solutions to automatically prevent all known threats across all traffic in a single pass.
- **WildFire**: Ensure files are safe by automatically detecting and preventing unknown malware with the industry-leading cloud-based analysis.
- **URL Filtering**: Enable the safe use of the internet by preventing access to known and new malicious websites before users can visit them.
- **IoT Security**: Protect internet-of-things (IoT) and OT devices across your organization with the industry's first turnkey IoT security solution.
- **GlobalProtect™** network security for endpoints: Extend ML-Powered NGFW capabilities to your remote users to provide consistent security everywhere in your environment.

Table 1: 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	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