Threat STOP

Solution Guide

Using ThreatSTOP to Implement **Protective DNS (PDNS) Solutions**

Executive Summary

There's a lot of buzz about Protective DNS (PDNS) and with good reason. Like any hot industry term, much of the PDNS buzz is just vendor noise. We've cut through that and dissected it here using key takeaways and vendor selection criteria from the NSA and CISA on implementing PDNS.

ThreatSTOP wrote the book on PDNS. New and existing vendors are jumping on the DNS Security bandwagon with solutions that are bolt-on afterthoughts and marketing heavy.

By stopping outbound DNS resolution to malicious sites, damage is prevented rather than reduced or remediated after the fact. Our Threat Intelligence Data Feed accuracy is light years ahead of the competition, ensuring that your risks from "zero day" attacks remain miniscule.

The value to your business from preventing a breach is immeasurable. With an easy learning curve for your IT team and a low TCO, ThreatSTOP protects what is important to you – your business and reputation – delivering ROI immediately.

What is PDNS?

The best of the best, NSA and CISA agree – your smartest dollar will always be spent on DNS Security.

The term PDNS sprung-up rapidly during January of 2021 after the NSA (National Security Agency) and CISA (Cybersecurity and Infrastructure Security Agency) published new recommendations in a Guide to Protective DNS Services.

The NSA-CISA PDNS guide followed NSA guidance from earlier in Jan. 2021 recommending organizations use only "enterprise-designated DNS resolvers", and avoid 3rd party resolution, encrypted or not. These statements, and the guidance, make a clear endorsement of two important DNS security areas:

- Designating and controlling your own DNS resolvers.
- Making DNS protective by not resolving potentially harmful requests.

In aggregate, this signals that DNS Security – aka PDNS – is on the path to becoming a standard.

PDNS Prevents Breaches:

ThreatSTOP PDNS is proactive, preventative and affordable, and reduces the chance of attacks causing damage or breaches.

Quick & Easy Deployment:

Be ready to roll-out PDNS swiftly and on your timetable. ThreatSTOP deploys, anywhere, everywhere, and in less than an hour.

Orchestration & Automation:

ThreatSTOP includes vast, curated Threat Intelligence to stay ahead of the fast moving threat landscape.

PDNS Providers

There are over 100 DNS security vendors today. No comprehensive list exists, and the NSA-CISA guidance covers only 8 commercial providers that already sell PDNS to Government entities. You should consider these vendors, and others when selecting PDNS.

Based on more than a decade of experience as a vendor of PDNS, ThreatSTOP finds the list of capabilities in the guidance (pg. 3 figure) to be incomplete, missing considerations such as:

- **Privacy** - who sees your DNS requests and why
- **False Positive Rates** - Threat intelligence methods and quality
- **Reporting** - Accurately identify potentially infected devices
- **Custom Lists** - Have granular control over what gets blocked

...as well as a slew of other critical PDNS capabilities that were omitted. Organizations must weigh their requirements against vendor capabilities to make the right choice.

But to be clear, ThreatSTOP's PDNS products meet and exceed the requirements listed in the NSA-CISA guidance. (See figure on next page.)

PDNS Capabilities

PDNS capabilities, in guidance from NSA-CISA, that ThreatSTOP easily exceeds:

Capability	MyDNS (Roaming)	DNS Defense
Blocks malware domains	Yes	Yes
Blocks phishing domains	Yes	Yes
Malware Domain Generation Algorithm (DGA) protection	Yes	Yes
Leverages machine learning or other heuristics to augment threat feeds	Yes	Yes
Content filtering	Yes	Yes
Supports API access for SIEM integration or custom analytics	Yes	Yes
Web interface dashboard	Yes	Yes
Validates DNSSEC	Yes	Yes
DoH/DoT capable	Yes	Yes
Enables customizable policies by group, device, or network	Yes	Yes
Deploys across hybrid architectures	Yes	Yes

Everything Starts with DNS

Everything good and bad that happens on the Internet begins with a DNS request; clicking a link, watching a video, getting phished. A DNS request precedes almost everything, making it ideal as a security control:

- **Prevents Ransomware from activating by interrupting the C2C request for encryption keys.**
- **Blocks phishing attacks by preventing the DNS requests that lead to malware payload and exploit kit downloads.**
- **Identifies and blocks new, novel and "Zero-Day" threats that reuses attacker IP, nameserver, and hosting infrastructure.**
- **Effortlessly drops commodity-grade threats before they can cause damage, preventing up to 85% of breaches that occur.**

Critical Considerations

Organizations should also consider the following when selecting a PDNS solution:

Privacy

What can be construed from the DNS requests made by users and devices in your network? Everything from your software choices, to upcoming M&A might be spelled-out in your DNS requests in clear-text.

Controlling DNS

Sending traffic to a 3rd party might be an OPSEC breach for some organizations or auditors. ThreatSTOP enforces on designated servers instead.

Hardware and Software

ThreatSTOP is different. Our cloud service integrates with any DNS platform you have today, or tomorrow. If you don't have one, we'll help you set up a free one on-prem or in the cloud.

Effort and Ease-of-Use

Stretched security team? ThreatSTOP customers say our PDNS reduces their load, saving time and money, freeing staff to work on other tasks that can't be automated.

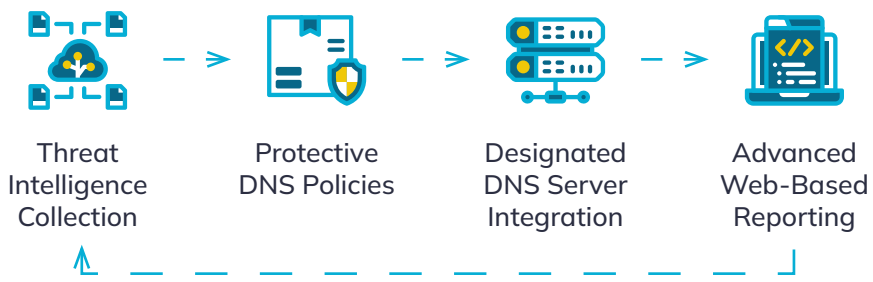
Threat Intelligence

PDNS's efficacy relates directly to the quality and coverage of the threat intelligence used. ThreatSTOP aggregates 900+ TI feeds and publishes our false positive rates (180-day avg. 0.002%).

Reporting & Remediation

PDNS must pinpoint the hosts making harmful DNS requests for quarantine, analysis, or remediation. ThreatSTOP helps your team quickly respond and keep the network clean.

TI Feedback Loop



900+ TI Feeds

Threat coverage and accuracy of PDNS directly relates to Threat Intelligence quality and speed

Multi-tenant Solutions

Sharing DNS servers with other organizations (or the public) is a privacy disaster. Insist on local or private-cloud multi-tenancy

Accelerated ROI

PDNS solutions should be priced to grow with you, not penalize you for being too small or big, or having lots of IoT

Extensible & Robust

PDNS works best integrated. RESTful API services enable rich front and back-end integrations with other products

Why PDNS, Why Now?

ThreatSTOP's Chief Scientist, Dr. Paul Mockapetris, invented the Domain Name System (DNS) in 1983. Over time there's been security enhancements (NOTIFY, IXFR, DNSSEC), but the DNS is not secure. In fact, DNS abuse continues to grow and expand, ranging from Denial of Service (DDoS) to data theft via DNS Tunneling.
Today DNS is used in more than 92% of all cyber-attacks.

PDNS answers the growing, urgent need for DNS security. PDNS is not a change to the DNS protocol; it's a **security service** that augments how DNS works by comparing DNS data to Threat Intelligence. When PDNS identifies a malicious domain, IP, or nameserver in the course of receiving and resolving a DNS request, **protective action is taken automatically, and early enough that damage can be entirely avoided in most cases.**

PDNS and CMMC

It's not just the NSA and CISA pushing DNS security to the forefront. Due to the criticality of securing DNS, the Department of Defense (DoD) included DNS filtering in the Cybersecurity Maturity Model Certification (CMMC) standard (SC.3.192).

The DoD has added new language around DNS filtering to its security standards, making PDNS a prerequisite for Maturity Level 3. PDNS is likely to become a standard requirement across all cybersecurity levels for government entities. Within the next two years, PDNS will be expected of most enterprise organizations.

Our recommendation is:

Any company seeking to do business with any government agency - state, local, or federal - should be prepared to incorporate PDNS to comply with these requirements.

Ready to Act Quickly:

ThreatSTOP PDNS is deployed rapidly, in flexible manners, ensuring it can meet your schedules and budgets for implementation as standards are introduced.

Cyber Maturity Help:

ThreatSTOP helps organizations level-up their Cyber Maturity in order to meet new regulatory requirements. PDNS is a perfect and easy place to start.

A PDNS Ecosystem:

PDNS is not a siloed security control, and it works best when integrated into a defensive strategy that talks with other network and security assets.

Importance of Privacy

There are no free lunches. Companies offering to secure your DNS requests, but requiring you to send your DNS requests to them are in the business of selling your data. This was true of OpenDNS, now Cisco Umbrella, and its true of the dozens of seemingly overnight competitors offering public/shared DNS resolvers that perform only the filtering capability of PDNS.

Privacy considerations should be at the foremost when considering PDNS providers. What can be gleaned from the DNS requests made by devices and users in your organization? Virtually everything:

- **Network map** of Software, hardware and security controls
- **Vulnerabilities** and versioning of connected devices
- **Insider information** such as M&A or IPO activity
- **Employee activity**, social media, and personal information

If the guidance from the NSA-CISA and DoD are taken seriously, as they should be, having any DNS servers performing DNS services other than your own designated DNS servers introduces risk and runs counter to the guidance provided. For some, 3rd party visibility to your DNS traffic has serious implications (e.g. HIPAA and Financial PII), and could be a breach of operational security.

Visibility is Critical

Blocking a DNS request nets immediate security value – things go downhill fast when machines connect to malicious hosts. But performing a malicious DNS query is often a symptom of more serious host or network infections. To solve this challenge, PDNS solutions must provide Granular reporting that clearly indicates:

- **Host** making the query (hostname, Private IP, MAC address)
- **Timestamp** to correlate with other events
- **Security action** and the trigger that caused the action
- **Indicator of Compromise** and Threat Intelligence

This is critical to performing security-enhancing actions like identifying, quarantining and remediating infected machines. Insist to see reports you will use to perform these critical activities.

Your PDNS Policies

No two organizations are the same, and this extends to security policies.

What you choose to prevent or allow may differ from others.

Policies must be highly customizable to prevent gaps in protection or false positives. ThreatSTOP has:

- Over 600 selectable policy blocks to fine-tune your policies.
- Unlimited custom lists for adding IP and domain records you want in your policies.
- RESTful API services for programmatically integrating 3rd party or in-house TI feeds.
- Custom policies that can be defined for users, groups, locations and more.
- Full RBAC and audit trails to prevent or track unauthorized policy changes.

Final PDNS Considerations

Using a PDNS provider as part of your overall security strategy is likely to become the standard for enterprise organizations, government agencies, educational institutions, and other businesses that are at a high risk for network security attacks.

Ease of deployment is crucial. Your organization will likely need to roll out a solution swiftly, and will want a PDNS tool that can be implemented within your timeframe and budget constraints.

Roaming Clients are essential, especially in a work-from-home environment where users are no longer protected by the company network. These users might be working on personal devices that have no security software installed - increasing your company's security risk. MyDNS offers protection for Windows and MacOS by providing a critical first layer of protection no matter where your employees are working from.

Content filtering capabilities are an added benefit of a PDNS service. They allow your organization to block inappropriate content such as pornography, social media, gambling sites, etc.

And you can implement this content filtering through custom policies to give you control over who sees what content based on role, department, or group.

Doing PDNS Right

PDNS shouldn't be overly complex to implement, should require very little if any effort to maintain, and should not break your budget.

Find a PDNS provider that exhibits DNS security expertise, offers multiple ways to implement their solutions, and that works with companies like yours in size and budget.

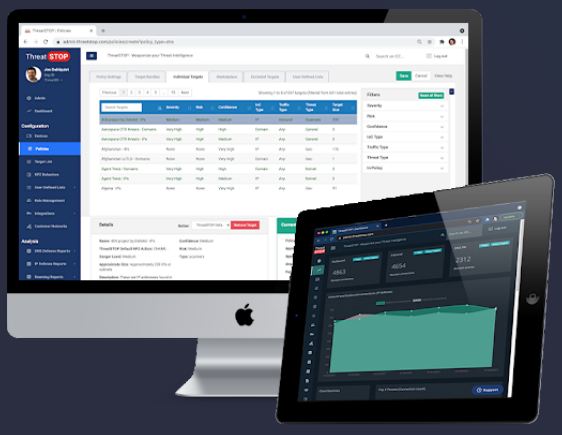
- Originators and innovators of PDNS and DNS Security for 10+ years
- Products and pricing that make sense for any size organization
- Feature-rich, stable PDNS products that have been improved over years of customer use, not overnight me-too solutions

Why ThreatSTOP?

ThreatSTOP has pioneered DNS Security over the last decade. Our customers have become our tireless marketing department, and know from hands-on experience that ThreatSTOP PDNS is the most effective security control available at any price.

ThreatSTOP was started in 2009 by Founder and CEO, Tom Byrnes, a long-standing member of the global cybersecurity community. His mission: Give organizations of any size the same cybersecurity protection that Fortune 1000 companies have.

Few companies have the resources to curate threat intelligence feeds into machine readable enforcement policies. Fewer still have the resources to update their network devices with policies. ThreatSTOP addresses those gaps with a cloud-based platform that stops attacks before they become breaches.



Reach out

sales@threatstop.com

760-542-1550

threatstop.com