Threat STOP

Protective DNS (PDNS)

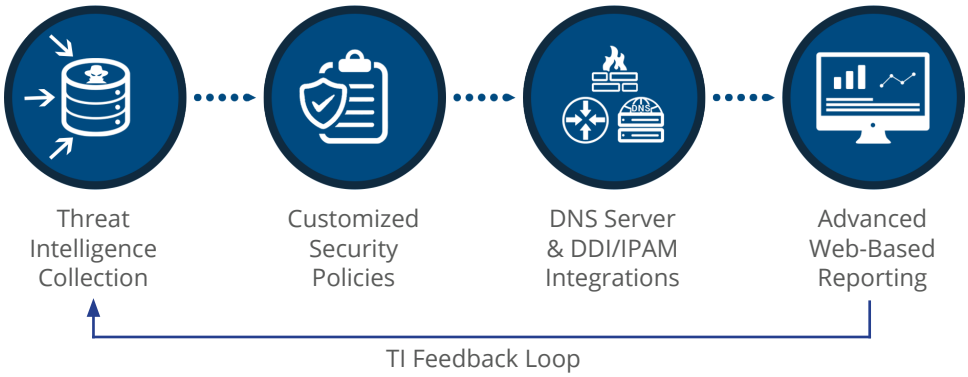
Enterprise-grade Protective DNS that is easy to use, at a price the midmarket can afford.

Mitigate Threats with Protective DNS

Meet and exceed DNS Security guidance from the National Security Agency (NSA) and the Cybersecurity & Infrastructure Security Agency (CISA) with a simple to implement, affordable cloud service.

Protective DNS (PDNS) secures every Internet connected device by comparing DNS traffic and threat intelligence to block harmful requests. Not all PDNS solutions are equal, ThreatSTOP stands-out in critical areas:

- **Privacy and Operational Security** - Our service runs on your designated DNS servers or ours, on-prem, managed, or hosted
- **Complete Protection** - Block IP-to-IP connections, integrates with popular Firewalls, Routers, Switches, IDPS and more.
- **Ease-of-Use and Efficiency** - Built to save time for security teams, the platform centralizes and automates PDNS, freeing up your team.



Get the benefits of a mature threat intelligence program:

- Drop unwanted & unsafe DNS requests early, before they do damage
- Redirect on threat type, like phishing, to a walled garden or sandbox
- See devices trying to talk to attackers so you can quickly take action

Key Benefits:

Block Threats Proactively:

Stop more than 92% of threats before they cause damage. Deploys from scratch in under an hour.

See Every Connected Device:

Gain visibility into all connected devices with powerful reporting. See devices attempting to communicate with attackers.

Keep Your DNS Private:

Preserve privacy and operational security by implementing PDNS on local and/or designated DNS servers you control.

Powerful, but Easy-to-Use:

Easy enough for an SMB team-of-one, but powerful enough for a mature enterprise security team.

sales@threatstop.com
760-542-1550
threatstop.com

Threat STOP

Privacy & OPSEC are Mission Critical

The Department of Defense (DoD) guides organizations to use designated DNS servers for privacy and security as a component of the Cybersecurity Maturity Model Certification (CMMC).

PDNS products that require users and devices to send all DNS traffic outside of your network will introduce privacy issues, and may breach Operational Security. ThreatSTOP integrates with your designated DNS servers, preserving your privacy and control.

Scales to Protect Networks of Any Size

DNS is necessary for everything from servers to laptops, and IoT. ThreatSTOP's PDNS solution deploys fast, typically in under an hour, and integrates with all your existing devices to protect everything using DNS.

ThreatSTOP PDNS is compatible with:

- **On-premise Physical** - DNS servers and DDI/IPAM appliances
- **Virtualized Appliances** - All popular DDI/IPAM and DNS servers
- **In the Cloud** - AWS, Azure, and Google public and private cloud
- **On Endpoints** - Windows and macOS endpoints via an agent

No designated DNS server? We will help you set one up for free!

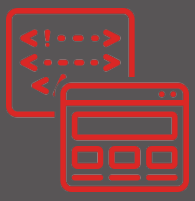
World-Class Reliability and Performance

ThreatSTOP Protective DNS is a SaaS cloud service operated across multiple world-class data centers offering N+1 or better redundancy on all systems.

Through anycast network technology, customers are ensured higher availability and resilience against brute force attacks. With audited security protocols, the service meets the ISO standard SSAE 16 for SOC 1, 2 and 3, Type II reports.

No New Hardware or Network Changes Required:

Delivered as a cloud service that's broadly compatible with DNS and DDI systems you already use today, and plan to use tomorrow.



Capable, High-Performance PDNS:

Outperforms OEM offerings from DDI/IPAM vendors on their own appliances due to ThreatSTOP's patented technology, and many:1-RPZ capabilities.

Feature-Rich, and More Affordable:

Advanced features such as reporting, email alerts, CheckIOC research, analyst access and 900+ feeds are included!

sales@threatstop.com +1 760 542 1550 www.threatstop.com