Threat STOP

Protective DNS (PDNS)

Everything Needs DNS, Even Threats

ThreatSTOP's Protective DNS (PDNS) solutions meet and exceed guidance provided by the National Security Agency (NSA) and the Cybersecurity & Infrastructure Security Agency (CISA). Protecting DNS works by striking at the weakness of 92% of attacks: their reliance on DNS.

DNS is foundational, and all Internet connected things need it. On the web, everything good and bad begins with a DNS request - visiting a website, opening an email, getting phished. By comparing real-time DNS requests to ThreatSTOP's extensive threat intelligence, malicious and unwanted DNS requests that would lead to breach or damage can be prevented at scale, across all devices, with granular visibility of what's blocked and why.

Unlike hosted DNS filtering services that violate privacy and suffer from high false positive rates, gaps in threat coverage, and latency issues, ThreatSTOP's DNS Defense uses local enforcement to solve that solves privacy issues and adds no latency, even with very large policies.

Threat Intelligence: Quality, Speed & Coverage

The threat landscape moves incredibly fast. Threat intelligence products must also be lightning fast to prevent attacks at scale before they change and move again. To achieve the coverage needed for whatever the next attack brings, intelligence must be gathered from many reputable sources. Once assembled, this threat data must be analyzed and enhanced to before it's applied to users, devices and real-time network traffic.

DNS Defense is powered by the ThreatSTOP SaaS platform - aggregating more than 850 feeds, tracking over 25 million IoCs, providing 600+ policy categories, and maintaining a false positive rate under 0.02% for multiple years. It's like having a virtual enterprise security team.

Protective DNS Benefits

- **Block threats up front. Stop more than 92% of threats before they can cause any damage by acting on unsafe DNS requests.**
- **Gain visibility into every connected device through powerful reporting. View devices trying to communicate with attackers.**
- **Easily managed by an SMB security team-of-one, but powerful and granular enough for sophisticated enterprise teams. Deploys from scratch in under 20 minutes!**
- **Delivered as a cloud service that's broadly compatible with DNS and DDI systems you already use today, and plan to use tomorrow.**
- **Outperforms OEM offerings from DDI/IPAM vendors on their own appliances due to ThreatSTOP's patented Policy Builder, no limit on threat categories or actions.**
- **Advanced features such as reporting, email alerts, CheckIOC research, analyst access and 600+ policy categories are included!**

New Security, Not New Hardware

Your networks are full of appliances capable of blocking threats if they only knew how to spot them. ThreatSTOP provides this capability as a cloud service. ThreatSTOP when integrated with your Active Directory, or Infoblox appliance, BIND server, PowerDNS, efficientIP, F5 or other supported device becomes a DNS Firewall powered by ThreatSTOP, capable of blocking more threats daily than all your other security controls combined. Let us prove it at *www.admin.threatstop.com/register*

How it Works

Threat Intelligence Collection

900+ threat feeds included
Human & machine curated
IP addresses and domains

Customized Security Policies

Fully customizable policies
600+ selectable categories
Custom block and whitelists

Network Device Integrations

Automated policy updates
NGFW, DNS, Router, Switch
IDP, WAF, SIEM and more

Advanced Web-Based Reporting

View & analyze blocked threats
Identify affected client devices
Custom email reports & alerts

Get the security benefits of a mature threat intelligence program

Predict and prevent threats that are otherwise expensive, noisy distractions. Drop unwanted traffic and commodity attacks early, before they can do damage. See devices trying to talk to attackers.

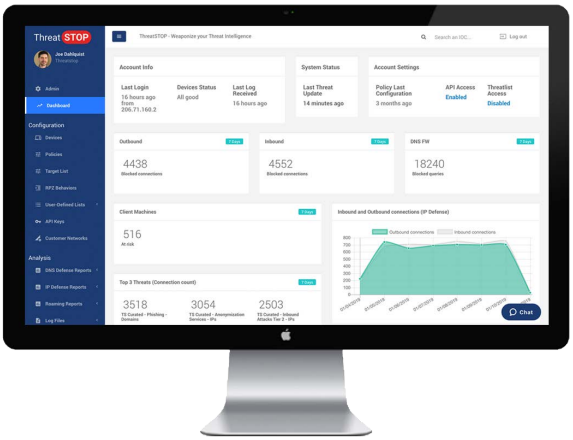
Scalable & Reliable

Scales to Protect Networks of All Sizes

A broad-based solution that leverages DNS to protect every device connected to your network, it can protect any network, from virtual cloud networks to branch LANs to the largest carrier networks. It protects all devices, any port, any protocol and any application.

World-Class Hosting, Reliability and Performance

IP Defense is operated across multiple world-class flagship data centers offering N+1 or better redundancy on all systems. Through implementation of anycast network technology, customers are ensured higher availability and resilience against brute force attacks. With audited security protocols, the service meets the international service organization reporting standard SSAE 16 for SOC 1, 2 and 3, Type II reports.



ThreatSTOP is a SaaS company that develops cloud-based, automated threat intel and policy solutions for corporate network ecosystems. To request a demo or speak with a salesperson, please contact sales@threatstop.com or call 760 542 1550. Visit www.threatstop.com for more information.