MyDNS
E n d p o i n t

DNS Security Wherever You May Roam

ThreatSTOP's MyDNS is the first and only fully recursive DNS Firewall available as a light-weight agent for modern Windows and Mac OS X endpoints. MyDNS provides unparalleled security protection and advanced customization options and privacy features unavailable in other commercial DNS filtering solutions, ensuring DNS requests made by protected endpoints remain private to your devices and your network.

Unlike other DNS security services available in the marketplace, MyDNS retains all the privacy protections of a local, on-premise DNS security solution. Instead of forwarding DNS requests to a 3rd-party, allowing external parties full visibility into the resulting data, MyDNS policy rules and the enforcement to block or re-direct DNS requests is contained within the agent and kept private to your organization.

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.

MyDNS 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.

MyDNS Defense Benefits

- **Lightweight and efficient, adds powerful DNS security capabilities without negatively impacting endpoint or DNS lookup performance.**

- **Protects on and off-network, perfect for remote workers, WFH, branch office, roaming devices, and critical assets.**

- **Gain visibility into every connected device through powerful reporting. View device hostnames trying to communicate with attackers.**

- **Easily managed by an SMB security team-of-one, but powerful and granular enough for sophisticated enterprise teams. Deploys in seconds.**

- **Flexibility to configure access levels and group policy. Three selectable DNS modes, including fully-recursive, with support for DNSSEC.**

- **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 NGFW, Router, UTM, WAF or even a transparent bridge becomes a security weapon powered by ThreatSTOP, capable of blocking more threats daily than all your other security controls combined. Let us prove it with a free trial, sign-up today at *www.admin.threatstop.com/register*
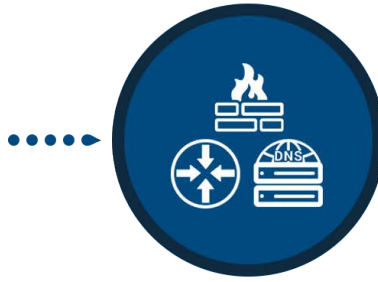
Threat Intelligence Collection

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 or redirect unsafe and unwanted DNS requests. See devices trying to talk to attackers.
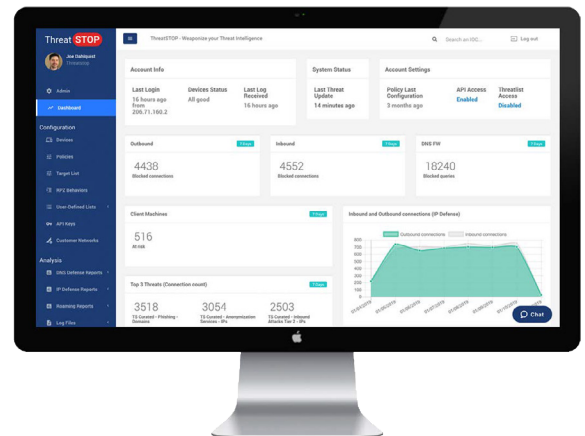
Scalable & Reliable

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.