Threat STOP

DNS Defense

Our Intelligence, Your Device

Harness the power of ThreatSTOP's cutting-edge intelligence directly on your existing DNS systems with DNS Defense. As a SaaS solution, DNS Defense seamlessly integrates with Active Directory, BIND, Infoblox, and more. It proactively identifies and stops threats early, powered by 900+ threat intelligence sources that track and block the infrastructure used by cybercriminals. With predictive feedback loops and customer-specific block and allow lists, DNS Defense offers adaptive, highly customizable protection without new hardware requirements.

🛡 Features And Benefits

Proactive DNS Threat Protection:
- Identify and block harmful and unwanted DNS requests before they reach your network devices.
- Leverage curated intelligence from over 900 threat feeds.

Predictive Policy Customization:
- Tailor policies with customer-specific block and allow lists for highly granular security.
- Automate and outsource 24/7 policy updates to stay ahead of threats.

Comprehensive Device Integration:
- Deploy on any existing or future DNS systems like Active Directory, BIND, and Infoblox.
- Extend protection to remote and roaming endpoints using the MyDNS agent.

Granular Application Control:
- Control traffic from third-party proxies, free VPN providers, social media, and remote desktop access.
- Prevent misuse and unauthorized access to sensitive applications.
- More applications rolling out continuously to allow you to better secure your network.

Advanced Reporting Tools:
- Monitor network security with rich reports available in the ThreatSTOP portal or your SIEM.
- Utilize research tools like Check IOC to identify infected hosts and investigate threats.

Cost-Effective Solution:
- Save money by adding robust security to existing devices.
- Reduce bandwidth consumption and minimize endpoint infections.

Improved Network Security Efficiency:
- Block communication attempts to criminal infrastructure across all ports and protocols.
- Customize policies to match your organization's unique security posture.
- Automate threat intelligence updates and optimize policy application.

Why Choose ThreatSTOP DNS Defense?

ThreatSTOP DNS Defense makes your existing DNS systems better by incorporating over a decade of expertise and intelligence into your network devices. Our proactive protections ensure continuous defense against malware, ransomware, phishing, and other cyber threats. By combining cloud-based policy updates, seamless integrations, and powerful reporting tools, DNS Defense provides unmatched security for all your DNS needs.

👥 Connect with Customers, Disconnect from Risks

To explore how DNS Defense can deliver proactive protections across your network, visit our product page . Discover how our solutions can transform your digital security landscape, with pricing that fits businesses of all sizes. **Get started with a Demo today!**

Start A Free 30-Day Trial

Join us in fortifying your DNS security landscape with ThreatSTOP DNS Defense.
Sign up today to:

1. Pick a security policy tailored to your network's needs.
2. Integrate DNS Defense with your device and start blocking threats automatically.
3. Review detailed reports on the protection gained.