ThreatSTOP

threatstop.com

DNS Defense

Weaponize Your Threat Intelligence

Your organization is under constant surveillance by threat actors looking for gaps in your security posture. Automated scanners actively seek out open ports to gain access to your network, while employees pick up malware from infected websites and phishing emails. You have invested in a battery of overlapping security tools, yet the breaches continue.

Make it stop. ThreatSTOP DNS Defense is a powerful service that prevents unwanted and dangerous outbound connections from your network, and prevents data theft. Unlike other tools that only integrate into a SIEM or notify you of threats, ThreatSTOP neutralizes malware that has bypassed your firewall, IDS/IPS, web filter and endpoint security. Then, ThreatSTOP's real-time reporting provides the visibility you need to remediate threats.

Service Overview

ThreatSTOP DNS Defense is a highly effective, proactive security solution that blocks advanced threats from completing their mission, be it DDos attacks, data theft or corruption, or phishing. It delivers up-to-the-minute protection against advanced attacks, and enhances your existing security posture by adding a powerful layer of security that functions at the DNS level, and delivers granular control over the actions taken against outbound network queries. Actions include the ability to block, log and allow, or redirect queries to walled gardens.

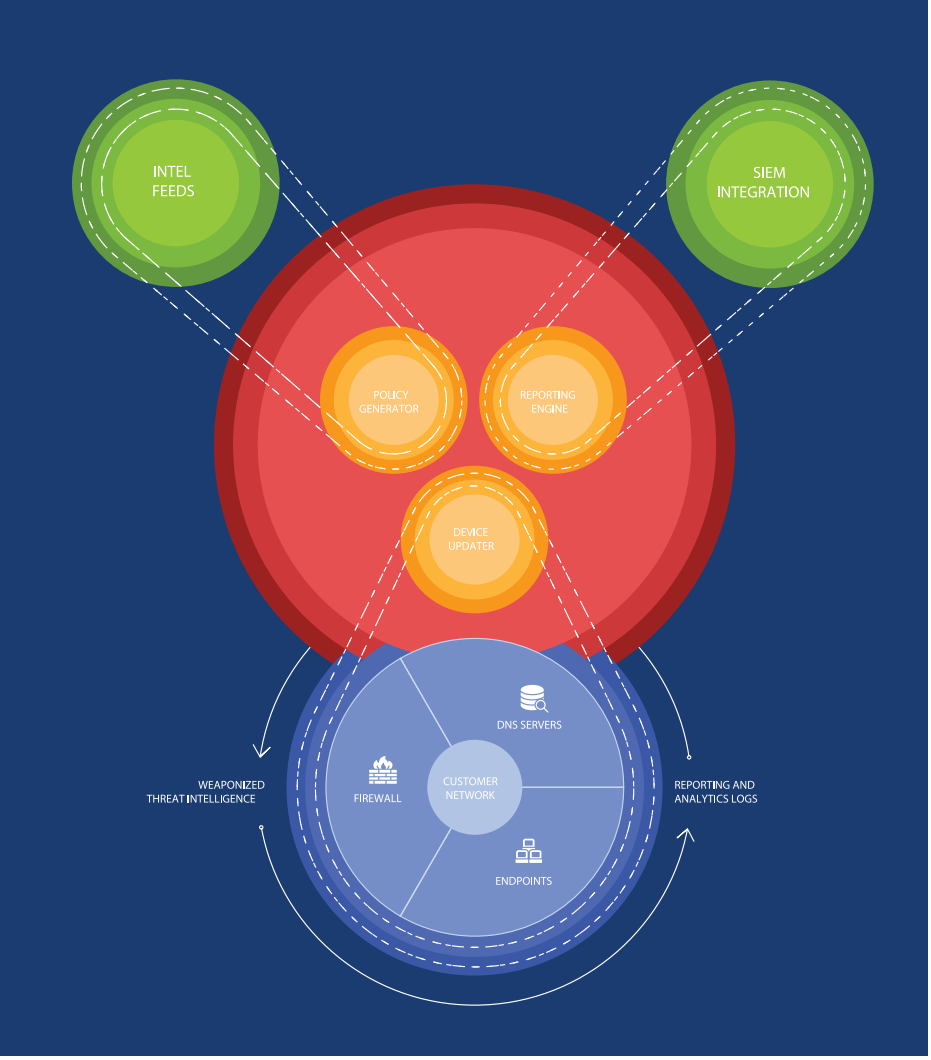
The service protects your network and devices by automatically delivering best-in-class threat intelligence driven security policies to your DNS server for enforcement on outbound traffic. A cloud-based service, it is easy to deploy and manage, and does not require upgrades to your infrastructure or new hardware. Once deployed, ThreatSTOP DNS Defense provides immediate relief by preventing the exfiltration or corruption of data, defending against crypto and ransomware attacks, and blocking unwanted outbound connections that consume bandwidth and pose risks to network security.

Best-in-Class Threat Intelligence

ThreatSTOP DNS Defense leverages the company's comprehensive and authoritative database of IP addresses, domains and the infrastructure used for cyberattacks. When selecting a threat intelligence service, it is not the size of the database, but accuracy that is important. ThreatSTOP's world-class security team curates the latest threat information and cross-correlates threat data against multiple public and private sources to ensure a high degree of accuracy and prevent false positives. Policies you customize are continuously and automatically updated to protect your network against new and emerging threats.

Key Benefits

- **Automatically deliver the latest actionable threat intelligence to DNS servers based upon user-defined policies, creating a DNS Firewall.**
- **Granular controls empower you to block, allow and log, or redirect DNS queries by IP and domain, including wildcards.**
- **Prevents data theft and corruption by stopping malware from "phoning home" to threat actors. Prevents activation of ransomware such as Cryptowall and Cryptolocker.**
- **Cloud-based service that's easy to manage and provides protection for your critical DNS infrastructure.**



How it Works

1. Select from expertly-crafted threat protection policies, tailor a perfect fit by creating your own whitelists and blocklists.
2. Policy updates are sent automatically to your DNS Server containing up-to-the-minute threat intelligence to protect against current threats.
3. The DNS Firewall can now enforce those policies to protect your network from inbound attacks and outbound malicious connections.
4. Event logs are generated providing visibility into the traffic that was blocked prior to reaching your network.
5. View powerful reports about the threats targeting your environment, and details of potentially infected devices to expedite remediation.

Additional Benefits

Scales to Protect Network 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

The service is operated across multiple world-class agship data centers oering 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.