ThreatSTOP

threatstop.com

IP 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 IP Defense is a powerful service that blocks attacks before they reach your network, and prevents data theft. Unlike other tools that only integrate into a SIEM or notify you of threats, IP Defense deflects attacks that have bypassed your firewall, IDS/IPS, web filter and endpoint security. Then, IP Defense's real-time reporting provides the visibility you need to remediate threats.

Service Overview

ThreatSTOP's IP Defense is a highly effective, proactive security solution that blocks advanced threats. It delivers up-to-the-minute protection against malware, DDoS and other advanced attacks, and enhances your existing security posture by improving the effectiveness of firewalls, IDS/IPS, routers, switches, endpoint and other security tools.

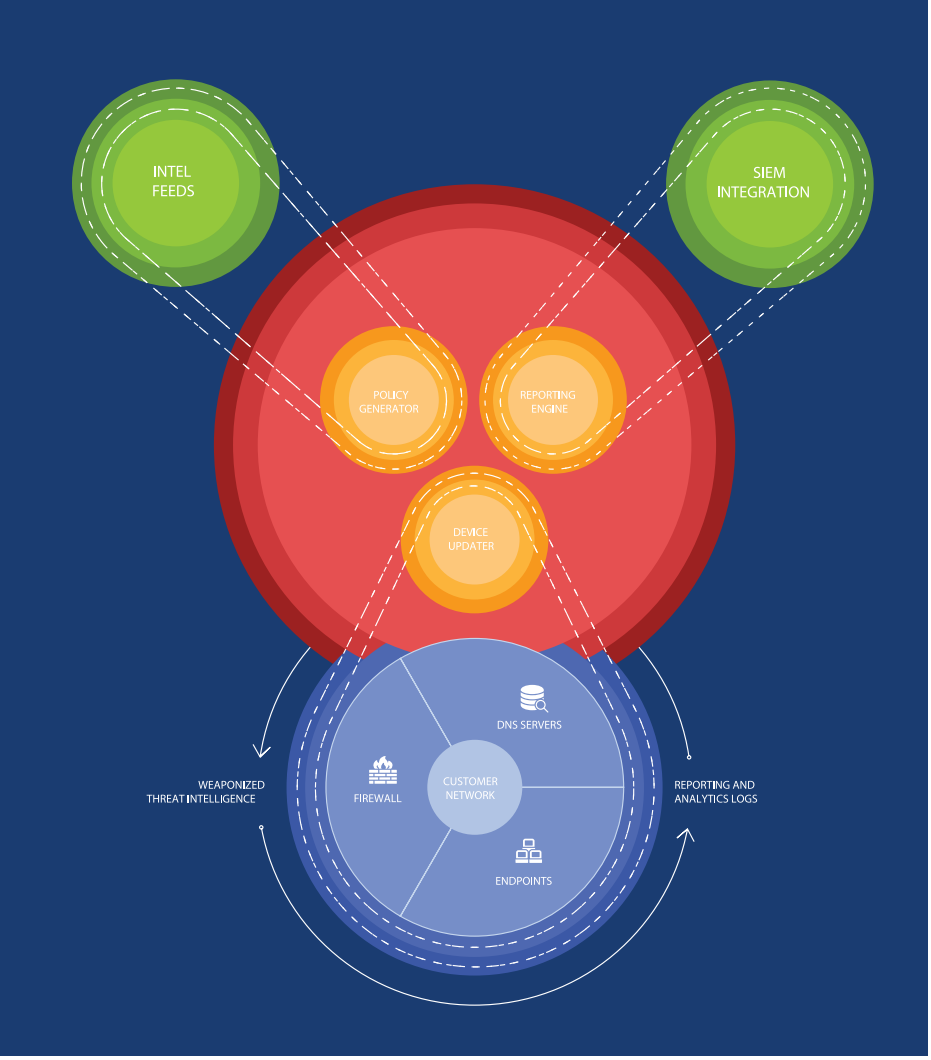
The service protects your network and devices by automatically delivering best-in-class threat intelligence to your perimeter security devices, including firewalls, routers, cloud environments and switches. A cloud-based service, it is easy to deploy and manage, and does not require upgrades to your infrastructure or new hardware. Once deployed, IP Defense provides immediate relief by deflecting attacks and unwanted or malicious traffic.

Best-in-Class Threat Intelligence

The ThreatSTOP IP 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.

Key Benefits

- **Automatically delivers the latest actionable threat intelligence to network devices and DNS servers based upon user-defined policies.**
- **Proactively deflects inbound malware, DDoS and other attacks, regardless of the attack type or vulnerability. Renders your network invisible to scanners, so attackers move on.**
- **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 is easy to manage and provides protection using your existing hardware. Works with leading firewalls, routers and switches.**



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 appliance containing up-to-the-minute threat intelligence to protect against current threats.
3. Devices 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

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.