ThreatSTOP

threatstop.com

# Technology Overview

## Weaponize Your Threat Intelligence

The ThreatSTOP® Shield service delivers up-to-the-minute threat intelligence to routers, firewalls and DNS servers to provide an automated, proactive defense against malicious attacks such as ransomware, DDoS, and botnets. A cloud-based service, it works with a customer's existing security devices to automatically block attacks and prevent data theft and corruption.

The service uses threat intelligence as an input to a security platform that delivers proactive protection from threats. Customers set custom policies based on their security posture, then those policies are automatically delivered to and enforced by devices across the network to ensure continuous and reliable protection from inbound attacks, and prevent outbound network communications with threat actors.

## Curate & Correlate Threat Data

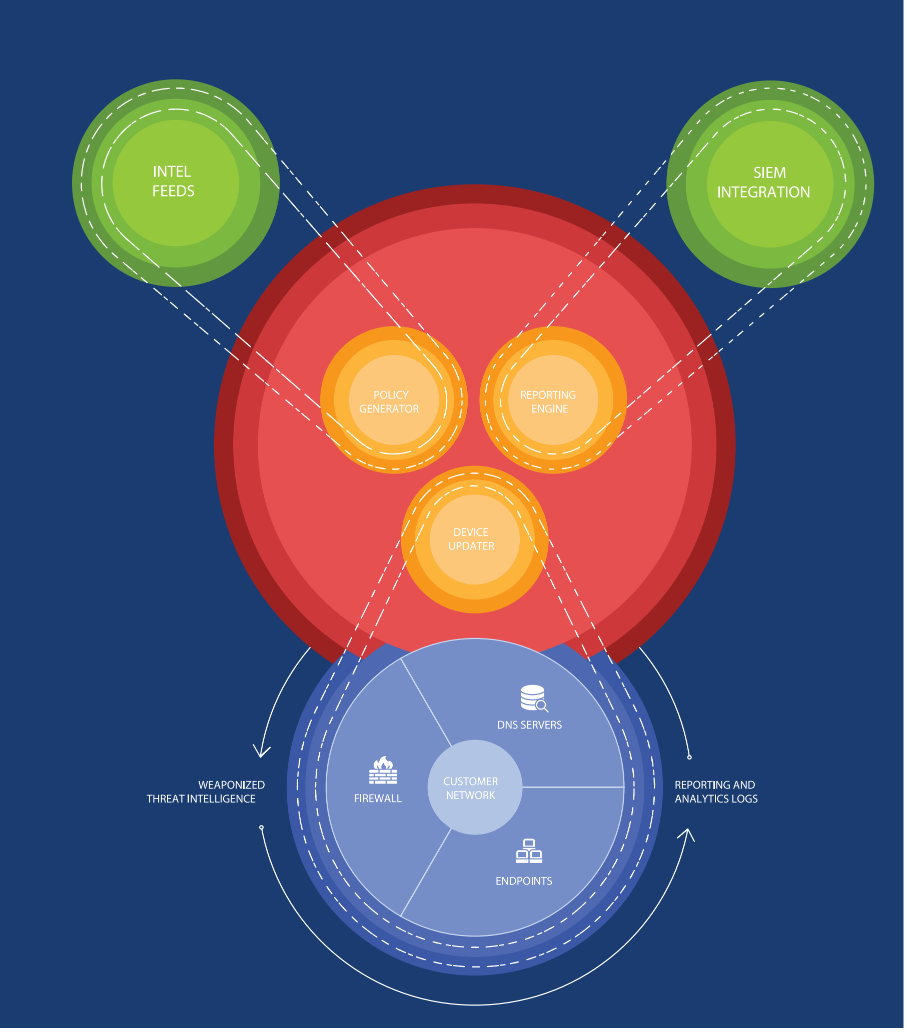
The ThreatSTOP service delivers best-in-class threat intelligence curated from numerous sources including free public sources and paid subscription services, private sources such as invitation-only trust groups and law enforcement, plus its own proprietary research. Public sources include leading malware monitors such as DShield and Spamhaus. ThreatSTOP also has access to private feeds not available to the public due to deep relationships within the security community. Finally, our proprietary sources provide early detection into emerging threats. The Israeli-based ThreatSTOP research lab continuously monitors sensors for indicators of compromise, often finding early instances of new threats. This includes monitoring live traffic and attack data that is then verified, correlated and used to protect customers via the service and shared with the information security community at large.

Our correlation engine filters the raw feeds to produce threat intelligence by evaluating factors such as dates an IP address is first and last seen in the database, frequency of appearance and number of sources reporting on it. The algorithms are weighted for false positives, for example an IP address reported from multiple sources is more likely to be added than one reported multiple times from a single source. The algorithms also continuously remove IP addresses that are no longer actively malicious. ThreatSTOP's curation and correlation systems ensure delivery of only the freshest, most accurate threat intelligence available.

## Create Customized Policies

Once the threat feeds are curated and correlated, they are categorized and made accessible for setting policies via the ThreatSTOP customer portal. Within the portal, customers select from the threat categories that support their specific security posture to develop customized boock and allow policies for their devices. Policies can be set for routers, firewalls and DNS servers across the network, and applied to individual devices or groups of devices. Threat categories include ThreatSTOP Critical, Ransomware, ZeuS, PONMOCUP, Botnet, as well as specific geographical areas.

For larger scale deployments, the ThreatSTOP Centralized Manager (TSCM) allows for the rapid deployment of the service across multiple devices and varying brands of devices in a production environment. This enables management of all devices and policies across a broad network with disparate geographic offices from a single console. The service uses DNS to distribute policies across networked devices. Since every device uses DNS to connect, the service can interface with every device and any device type, regardless of vendor.
Once policies are set, the ThreatSTOP Shield service immediately begins automatically updating policies across the devices with continuously refreshed threat intelligence ensuring they are protected from the latest threats



## 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.

## Block Attacks & Prevent Data Corruption

Once the current threat intelligence data is retrieved, it is placed in the device's memory and every packet passing through is checked against the data. The default mode is to block all traffic to and from IP addresses in the ThreatSTOP database. Requests for malicious IP addresses are blocked based on the customer's policy. The ThreatSTOP service blocks all types of attacks, regardless of attack type including ransomware, Angler kits, phishing attacks, DDoS, Trojans and botnets. Inbound attacks are blocked before they reach the network--dropped at the first SYN packet. This provides three key benefits: (1) significantly reduces the amount of unwanted traffic your devices must manage and bandwidth costs--on average, customers report a 20 percent reduction in bandwidth usage, (2) with less traffic to examine, enables security teams to quickly focus on the more insidious threats, and (3) extends the lifetime of existing devices. The service also prevents outbound communications with threat actors' command and control when attempting to deliver instructions to malware or exfiltrate sensitive or valuable information via botnets.

## Reporting

Once the service is operational in the user's environment, web-based reporting is accessible via the customer portal with real-time feedback on what attacks have been blocked. It provides details on attack type, as well as affected devices to speed remediation. Reports can be forwarded to a SIEM/SEM exported as an Excel file to speed remediation on affected machines. Reports can also be automatically emailed.

Three levels of reports are available: (1) overall blocking status which provides a total number of blocked inbound attacks and outbound instances of communications with threat actors for a specified period of time; (2) summary of blocked addresses with drill downs into the details on source/destination IP addresses, destination port and number of attacks; and (3) individual address analysis with profiles of specific IP addresses in question.

## Feedback Loop

As part of the ThreatSTOP service, log data from customer devices is collected providing visibility into real-world network traffic and attack events. This information is used to improve coverage and accuracy of our data, and reduces the time to detect new malicious attacks. This information is also verified and used to update the threat intelligence database with the latest attack data, as well as shared with a collaborative network of security threat monitors.

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.