ThreatSTOP

Block the Threat Factory, Not Just the Threats

Wouldn't it be nice if your firewalls, routers and DNS servers could know who the bad guys are automatically, and just block them?

Quick Overview

- Web-based SaaS security solution
- Integrates with firewalls, routers, DNS servers, endpoints
- Automates network security policy management
- Proactively blocks all network communications with attackers
- Not another passive solution that just generates alerts
- Scale-up security, cover the whole network, and get dedicated security team results on an SMB budget

ThreatSTOP

Powerful Platform

ThreatSTOP = TIP + SOAR + SIEM

TIP

Threat Intelligence Platform

Acquire hundreds of feeds.
Clean & normalizethe data.
Make the data actionable.

SOAR

Orchestration Automation & Response

Collect security data from TIP
Standardize network policies.
Automate manual processes.

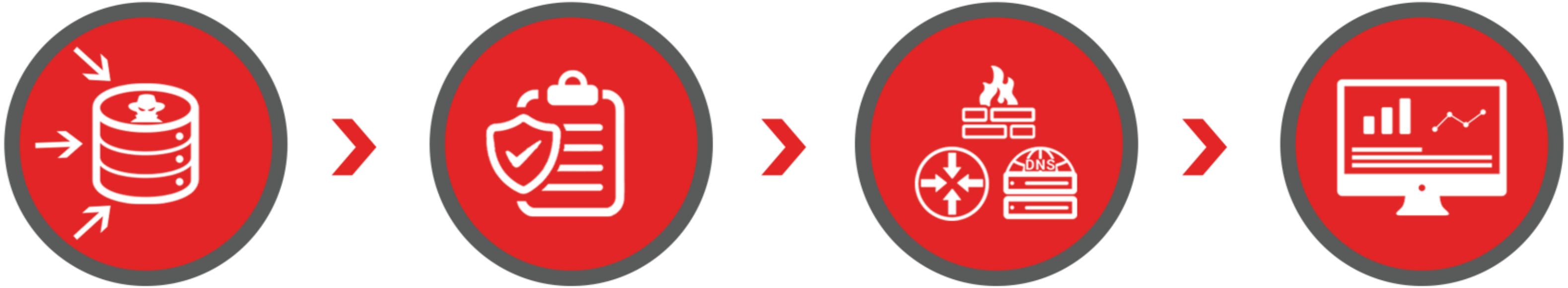
SIEM

Incident & Event Management

Collect security data from TIP.
Import network & device logs.
View & manage security events.

How it Works

Threat STOP



Intelligence Collection

850+threat feeds included
Human & machine curated
Categorized by threat type

Policy Customization

Menu-based policy editing
600+ selectable categories
Add custom white/block lists

Device Integration

NGFW, router, switch, DNS
Automated policy updates
Proactive, real-time blocking

Advanced Reporting

Vizualize all blocked threats
Identify affected host devices
Includes IOC research tools

ThreatSTOP Products

DNS Defense

- Turns DDI/IPAM & DNS servers into a DNS Firewall
- Provides granular, proactive DNS threat protection
- Highly customizable DNS (RPZ) responses

IP Defense

- Block based on IP addresses using existing firewalls, switches, routers, load balancers, etc.
- Inbound & outbound TCP/IP protection
- Filters traffic & improves network performance

Roaming Defense

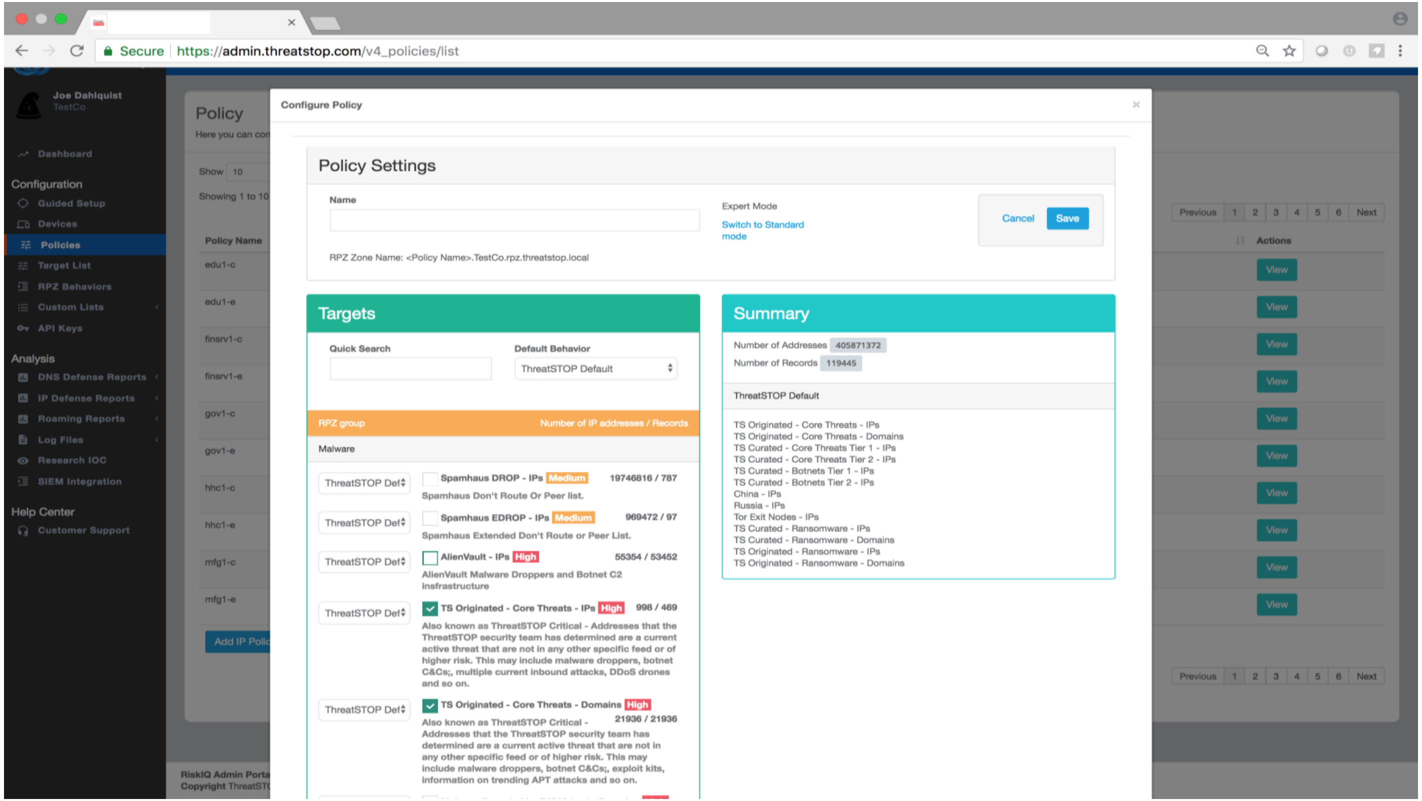
- Compatible with Windows and Mac OS X devices
- Blocks or redirects malicious DNS locally on any network, anywhere
- Integrated reporting with Hostname granularity

Security Integration

- Enrich SIEM/SEM data with dynamic policy exports available in CSV, STIX, Suricata, Snort, REST API

ThreatSTOP

Security Policy Editor



Configure Policy

Policy Settings

Name

RPZ Zone Name: <Policy Name>.TestCo.rpz.threatstop.local

Expert Mode

Switch to Standard mode

Cancel Save

Targets

Quick Search

Default Behavior: ThreatSTOP Default

RPZ group		Number of IP addresses / Records
Malware		
ThreatSTOP Def	□ Spamhaus DROP - IPs Medium Spamhaus Don't Route Or Peer list.	19746816 / 787
ThreatSTOP Def	□ Spamhaus EDROP - IPs Medium Spamhaus Extended Don't Route or Peer List.	969472 / 97
ThreatSTOP Def	□ AlienVault - IPs High AlienVault Malware Droppers and Botnet C2 insfrastructure	55354 / 53452
ThreatSTOP Def	☑ TS Originated - Core Threats - IPs High Also known as ThreatSTOP Critical - Addresses that the ThreatSTOP security team has determined are a current active threat that are not in any other specific feed or of higher risk. This may include malware droppers, botnet C&Cs;, multiple current inbound attacks, DDoS drones and so on.	998 / 469
ThreatSTOP Def	☑ TS Originated - Core Threats - Domains High Also known as ThreatSTOP Critical - Addresses that the ThreatSTOP security team has determined are a current active threat that are not in any other specific feed or of higher risk. This may include malware droppers, botnet C&Cs;, exploit kits, information on trending APT attacks and so on.	21936 / 21936

Summary

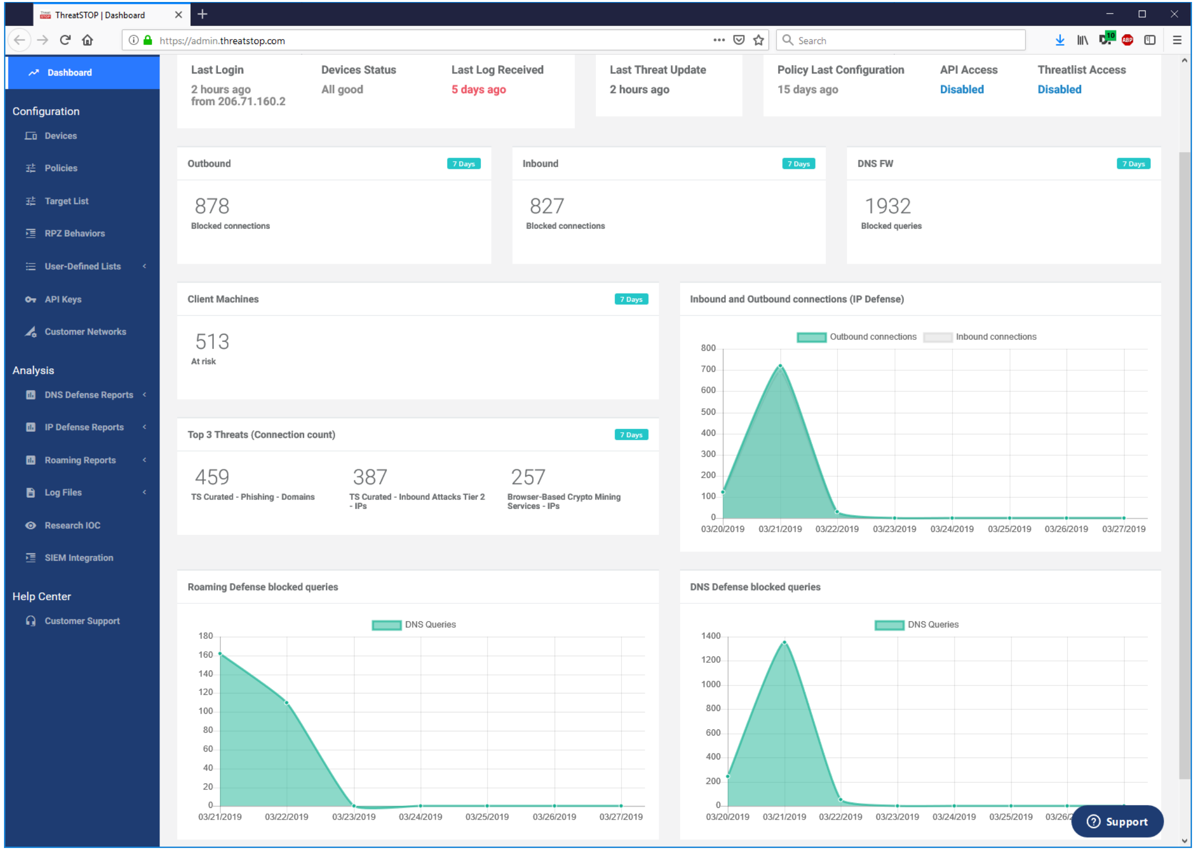
Number of Addresses 405871372

Number of Records 119445

ThreatSTOP Default

TS Originated - Core Threats - IPs
TS Originated - Core Threats - Domains
TS Curated - Core Threats Tier 1 - IPs
TS Curated - Core Threats Tier 2 - IPs
TS Curated - Botnets Tier 1 - IPs
TS Curated - Botnets Tier 2 - IPs
China - IPs
Russia - IPs
Tor Exit Nodes - IPs
TS Curated - Ransomware - IPs
TS Curated - Ransomware - Domains
TS Originated - Ransomware - IPs
TS Originated - Ransomware - Domains

Live Reporting



ThreatSTOP | Dashboard

https://admin.threatstop.com

Last Login: 2 hours ago from 206.71.160.2

Devices Status: All good

Last Log Received: 5 days ago

Last Threat Update: 2 hours ago

Policy Last Configuration: 15 days ago

API Access: Disabled

Threatlist Access: Disabled

Outbound (7 Days): 878 Blocked connections

Inbound (7 Days): 827 Blocked connections

DNS FW (7 Days): 1932 Blocked queries

Client Machines (7 Days): 513 At risk

Top 3 Threats (Connection count) (7 Days)

- 459 TS Curated - Phishing - Domains
- 387 TS Curated - Inbound Attacks Tier 2 - IPs
- 257 Browser-Based Crypto Mining Services - IPs

Inbound and Outbound connections (IP Defense)

Roaming Defense blocked queries

DNS Defense blocked queries

ThreatSTOP

Device Integrations

30-minute setup for firewalls, routers, switches, DNS servers and more

paloalto NETWORKS® A10 CISCO JUNIPer NETWORKS Check Point SOFTWARE TECHNOLOGIES LTD.

Iptables ARISTA FORTINET efficient iP™

Infoblox f5 pfSense UBIQUITI NETWORKS ISC Internet Systems Consortium

VYATTA VitalQIP SentryWire PACKET CAPTURE PLATFORM POWERDNS

VyOS Windows Server 2016 OpenBSD BLUECAT

Cloud Integrations

ThreatSTOP protects cloud workloads, wherever you have them

Microsoft Azure

aws

Google Cloud Platform

ARMOR

rackspace

dinCloud

Summary

- Lightweight, cloud-based solution with minimal footprint
- Automate application of the latest threat intelligence at the points of enforcement
- Affordable, easy to implement & manage
- Prevents inbound & outbound malicious traffic from infecting your network
- Robust reporting, research tools, alerts and more

ThreatSTOP

WHAT WE DO

SaaS Security solutions for SMB and security service providers that deliver proactive network defense capabilities

OUR TEAM

Founder Tom Byrnes, John Bambenek, & Paul Mockapetris lead an all-star tech and security team

HEADQUARTERS

Founded in 2009, we're headquartered in Carlsbad, CA and on the web at: www.threatstop.com

ACHIEVEMENTS

2018 TTT Startup Award
2017 IoT Breakthrough
2016 SD Cybersecurity
2010 DHS - SBIR Award
2003 IEEE Internet Award