ThreatMSS for MSSP and MDR

*Enterprise-Grade Threat Intelligence Solutions
that are Easy-to-Use, at a Price the Midmarket can Afford.*

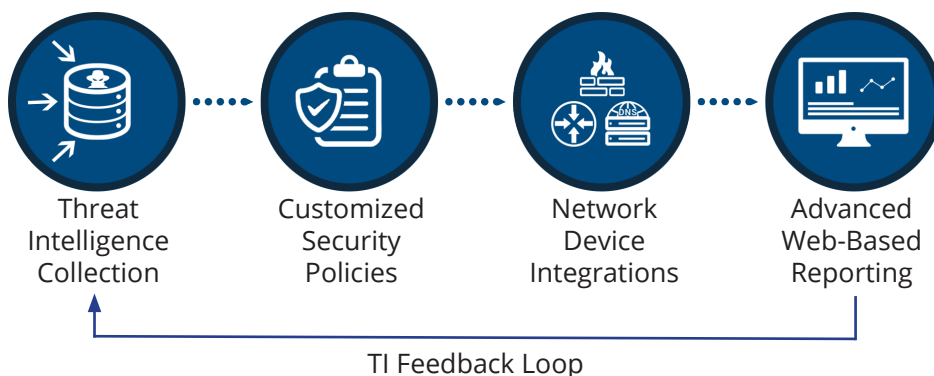## Threat Intelligence Solutions for MSSPs

MSSPs must battle increasing cyber threat volumes and sophistication, a skilled labor shortage that makes scaling difficult, and heavy competition to win and retain clients.

We help MSSPs grow and differentiate by leveraging threat intelligence (TI) and automation to deliver unique, low-touch and high-margin security services. This approach:

- Is proactive, not more reactive alerting.
- Integrates with existing appliances as a SaaS service.
- Detects and stops threats on network edge devices.
- Protects all client devices - office, cloud, and remote.

ThreatMSS provides comprehensive 24/7 threat mitigation and visibility in an easy-to-use, affordable platform. Use TI, the cloud, and automation to see and block more threats, and share that value with your clients in your own branded portal.

How it Works:

Threat Intelligence Collection → Customized Security Policies → Network Device Integrations → Advanced Web-Based Reporting

TI Feedback Loop

Protect Clients Faster & More Profitably:

ThreatMSS uses large-scale TI aggregation and automation to drive down your operational costs of providing continuous threat protection services.

Quick & Easy Deployment:

Deliver premium services that scale. Less than 1 hour to setup and no ongoing maintenance.

Orchestration and Automation:

Gain broad DNS and IP monitoring for all clients, then click to start blocking as a premium service.

sales@threatstop.com
760-542-1550
threatstop.com

1

Threat STOP

Advanced, Affordable TI Platform for MSSPs

Instead of re-purposing TIP, SIEM and SOAR that compare TI to network logs hours or days after events occur, ThreatMSS predicts and prevents threats. This approach:

• Saves time and money. We collect and curate all the TI
• Prevents and reports malicious or unwanted connections.
  Threat dwell time drops to zero days
• Reduces the noise and load on security controls and
  network resources, freeing up bandwidth
• Provides a safe window for response by stopping inbound
  attacks and outbound call-home / exfiltration
• Speeds up remediation through detailed reporting of all
 impacted devices

Differentiated Customer Experiences

Block more threats for clients, do it earlier, and deliver at lower costs than your competitors. This recipe helps our MSSP partners enjoy high customer satisfaction and retention, and free-up limited resources to focus on their clients and business.

Our multi-tenant platform helps MSSPs centrally perform tasks that must be done, but are risky and time consuming:

• Timely IP & domain allow and blocklisting changes
• Making policy and enforcement changes
• Researching IOCs and hunting threats

MSSPs can even offer a branded client-facing portal with reporting and granular role-based access control as a premium service.
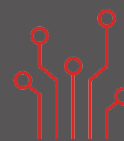
900+ TI Feeds:

The most accurate & complete database of active IP and domain IOCs, built over 10+ years.
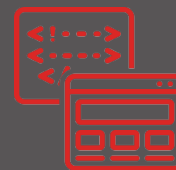
Multi-tenant platform:

Cloud multi-tenancy with RBAC in SOC 2 and 3 compliant hosting. Support for geo-localized GDPR and privacy.

Accelerated ROI:

Flexible pricing and pay as you grow models that drive revenue and cost savings. No hefty up-front or hidden costs, just profitable services clients love

Extensible & Robust:

RESTful API services for rich and reliable MSSP back-end and front-end integrations.

Threat STOP

Create Profitable & Effective Services

Use ThreatMSS to add premium services and generate new lines of recurring revenue. No new staff or skills are required, and partners spend less than 30 min. a week managing the solution.

Deployed as a SaaS integration for MSSP or customer-owned (physical or virtual) appliances, ThreatMSS simplifies TI and security services. For example: a containment service that remotely blocks malicious connections on a firewall or router. Redirect DNS phishing requests to a custom branded page. Incident response leveraging 900+ real-time curated TI feeds.

ThreatMSS utilizes a "pay as you grow" licensing model that enables MSSPs to deliver profitable, competitively priced services.

Privacy & Compliance

Drive better business outcomes that include regulatory and compliance solutions requiring:

• Content filtering
• ITAR and OFAC blocking
• Proxy (anonymization and TOR) denial

ThreatMSS processes no PII data and provides a true Protective

DNS (PDNS) solution without privacy concerns.

Learn more about ThreatMSS and our partner program by visiting our website at **https://threatstop.com/partners**

3

ThreatSTOP MSSP Value

• Increase economies of scale, reduce the cost per incident

• Vastly increase SOC visibility to active threats with real-time TI

• Improve customer satisfaction and retention rates

• Offer remote threat containment, network wide and for all connected devices, with a click

• Maintain existing workbenches and minimize tool sprawl with robust API integrations

ThreatMSS Capabilities

Broad threat data acquisition, curation & network-layer enforcement removes manual steps. Instantly add more than 900 TI feeds and 20 million+ IoCs to the SOC purview.

• Deliver branded, continuous web-based security reporting

• Broad automation integrations with all leading NGFW, UTM, Router, Switch, DDI/IPAM, DNS Servers, IDPS, SIEM, and more

• Local agent support for remote Windows and macOS devices

• Support for rich and robust integrations with existing SOC controls over RESTful APIs

• Granular policy management (WL& BL). Remote monitoring & network-layer containment

• Custom scheduled and on-demand reporting, email alerts, premium feed integrations.

MSSPs Consolidate & Centralize

↓

- Threat Intelligence Automation
- Network Policy Management
- Incident & Event Reporting
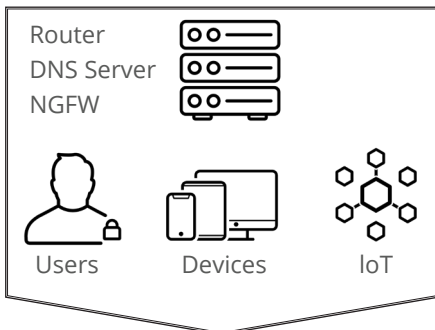- Whitelisting & Block-Listing
- Response & Remediation

Threat **STOP**

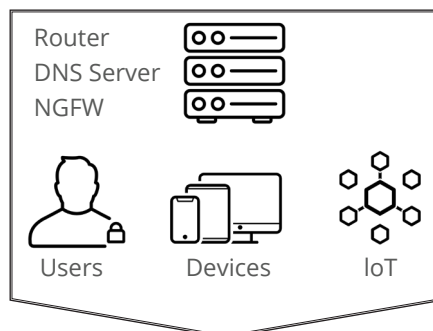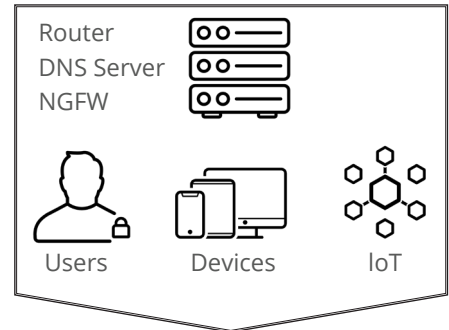Appliance
Event Logs

Standard
Curated Intel

Premium
Intelligence

Router
DNS Server
NGFW

Users   Devices   IoT

Client Tenant

Router
DNS Server
NGFW

Users   Devices   IoT

**Client Tenant
(Premium TI)**

Router
DNS Server
NGFW

Users   Devices   IoT

Client Tenant