ThreatSTOP

SentryWire
PACKET CAPTURE PLATFORM

Alliance Technology Group

IP Defense & Packet Capture

Forensic Analysis & Network Edge Protection with SentryWire™ Powered by ThreatSTOP™

Weaponize Your Threat Intelligence

Every Network Needs Real-Time Threat Visibility & Enforcement.

The pace of today's threat landscape makes it impossible to keep network firewalls, routers, switches and IDS/IPS solutions updated using manual methods, and security and operations teams need accurate, real-time alerts when threats are identified within their networks. SentryWire and ThreatSTOP's joint solution captures and analyzes network packet traffic at line-speeds of 1Mbps to 100Gbps while rapidly identifying and alerting the sources and targets of an attack. The solution empowers network security, operations, and remediation teams with instant visibility into network threats so they can take action before threats become breaches.

Together, SentryWire and ThreatSTOP deliver a cost-effective forensic and audit solution using 100% full network packet capture and flexible data retention capabilities spanning months or years' to fulfill compliance and regulatory requirements. Furthermore, ThreatSTOP's cloud-based platform is easily extended to existing network enforcement devices such as firewalls, routers, and DNS servers to begin proactively blocking threats identified by the SentryWire device over all ports and protocols.

ThreatSTOP™ / SentryWire™ Joint Solution

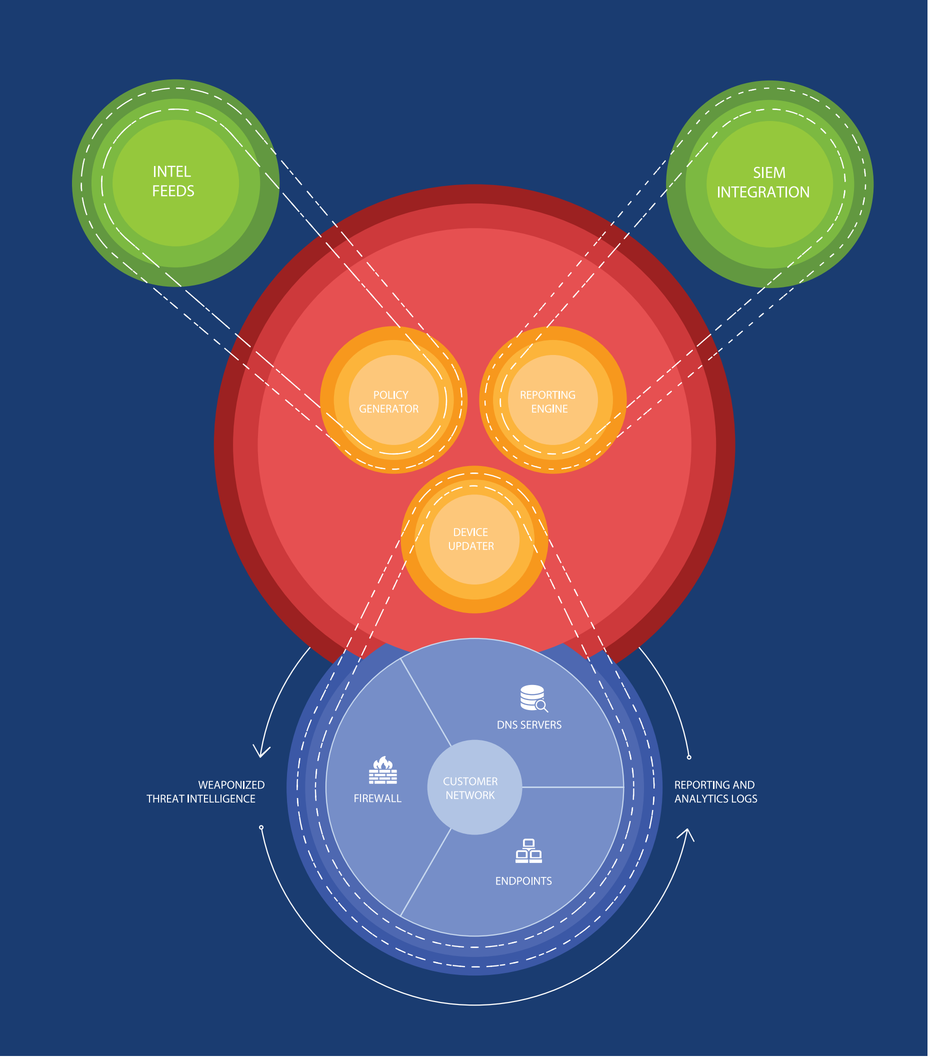
Based on ThreatSTOP's IP Defense cloud security service, the joint solution leverages a comprehensive threat intelligence engine containing real-time threats aggregated from nearly 60 unique threat intelligence feed sources. The engine utilizes both human security analysis and proprietary algorithms to curate, sanitize, and remove false positives. This comprehensive understanding of the fast-moving threat landscape allows for accurate and automated identification of threats present in network traffic entering or leaving the network perimeter.

Unlike other tools that only integrate into a SIEM, are highly prone to false positives, or notify you of threats hours, days, or even months after they occurred, the SentryWire and ThreatSTOP solution alerts on real-time packet traffic where the source or destination IP address is known to be currently malicious. These alerts can be indicative of external attacks in progress, or threats that have bypassed firewall, IDS/IPS, web filter and endpoint security, and are attempting outbound communication with criminal C2 infrastructure. Joining ThreatSTOP with SentryWire produces a detailed, near-real time trace of the actual traffic involved in the attack - giving organizations the ability to respond to threats faster, eliminate business disruption, collect evidentiary-quality audit logs and conduct detailed forensic investigations.

Key Benefits

- **Network packet capture and alerting powered by ThreatSTOP, leveraging the most comprehensive real-time threat intelligence engine available.**
- **Captures, filters, flags and logs network traffic to deliver timely alerts based on Suricata rules of interest to enable deep packet forensic capabilities and proactive threat response.**
- **Automatic delivery of actionable, real-time threat intelligence to rapidly identify harmful or unwanted network traffic entering or leaving the network.**
- **Easily extended to provide proactive blocking of inbound and outbound threats, over all ports and protocols, with ThreatSTOP's cloud service compatible with leading firewall, router, and DNS platforms.**

SentryWire
PACKET CAPTURE PLATFORM



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.

ThreatSTOP IP Defense

ThreatSTOP's IP Defense weaponizes threat intelligence data by delivering it directly to existing TCP/IP enforcement devices such as firewalls, routers, switches, and load balancers. This intelligence data is updated in near real time via a patented distribution mechanism. When a Bot or other malware attempts to enter the network or "call home," ThreatSTOP IP Defense prevents this from happening by blocking the connection.

- ThreatSTOP's detection engine maintains an active database of untrustworthy IP addresses. The database is continuously updated, and policy updates to enforcement devices is automated.
- Enforcement devices securely upload logs to ThreatSTOP resulting in robust, interactive reporting that shows deflected external attacks and infected internal hosts.
- The platform is vendor-agnostic and out-of-the-box compatible with all leading network appliance vendors.

SentryWire™

SentryWire provides a cost-effective solution for 100% full network packet capture with retention capabilities spanning months or years' worth of packets. The ThreatSTOP comprehensive database is integrated with the SentryWire Suricata rules engine to provide real-time filtering on known IPS signatures and state actor threat lists, enabling alerting and network traffic analysis for deeper attack forensics and rollback of transactions against impacted data stores. SentryWire supports lossless capture rates from 1MB to 100Gbps and delivers raw storage compression and compaction of 5 to 30X at roughly 20% of the cost of other solutions.
Together, this joint solution enables security analysts and incident response personnel to be more effective and efficient in preventing and responding to network and data breach attempts. The combined solution enables analysts to accurately zero-in on devices where infiltration attempts are detected and then examine attack related network traffic and data within seconds or minutes of detection and alerting.

ThreatSTOP is a SaaS company that develops cloud-based, automated threat intel and policy solutions for corporate network ecosystems. SentryWire provides enterprise class full packet capture for incident response. To request a demo or speak with a salesperson, please contact sales@sentrywire.com or call 443-254-4381. Visit www.sentrywire.com for more information.