

ThreatSTOP vs. Akamai Battle Card

Solution Overview

ThreatSTOP protects every device on your network against attacks and the exfiltration and corruption of data. ThreatSTOP's cloud-based solution transforms global, real-time threat intelligence into continuously updated and actionable policy rules. These dynamic policies are enforced by your existing network edge devices (such as firewalls, routers and DNS servers) to protect against a constantly changing landscape of new and emerging threats.

ThreatSTOP's flexibility empowers you to tailor block and allow policies on a device-by-device basis to perfectly fit your evolving network and security needs. Powerful reporting delivers visibility to the threats targeting, or already inside of your network.

- Curate intelligence data from top security community & trust group sources; integrate with proprietary data.
- Create tailored policies leveraging real time threat intelligence to protect your network.
- Block attacks and prevent data theft and corruption. Materially reduces network load.
- Report on blocked attacks and affected internal machines to speed remediation.

Features	ThreatSTOP IP Defense	ThreatSTOP DNS Defense	Akamai ETP
Create & modify policies	Yes	Yes	Yes
IP protection	Yes	Yes	No
Domain protection	No	Yes	Yes
Inbound attack protection	Yes	No	No
Block/Allow decision made locally	Yes	Yes	No
DNS resolution outside network	No	No	Yes
Integrate custom / proprietary threat feeds	Yes	Yes	Yes
Compatible with all devices on the network	Yes	Yes	No
Custom allow list creation	Yes	Yes	Limited
Bypassed with IP Proxy sites	No	No	Yes
WAF-based threat intelligence	No	No	Yes

ThreatSTOP Key Features

- Users create and maintain their own protection policies to block and allow what fits their security needs.
- Policies are dynamically and continuously updated using comprehensive threat intelligence to deliver present-moment protection against new and emerging threats.
- Solution runs on the network device or via on premise management VM, no delay or added bandwidth is introduced by offloading the block/allow decision.
- Compatible with all market-leading network edge devices including firewalls, routers, etc; no expensive new hardware upgrades needed.
- Cross-platform compatibility makes it easy to manage security across all heterogeneous devices from a centralized point.
- Highly efficient implementation does not add undue processing or memory load on your network devices.
- Actionable reporting delivers visibility to blocked inbound and outbound traffic to make remediation efficient and effective.

Competitive Disadvantages

- Lack of granular protection, solution is domain constricted – no meaningful IP protection.
- No inbound protection, outbound DNS only.
- Client endpoints circumventing protection using IP proxy sites to "surf the web freely."
- Limited policy customization options to fit customer business/security needs.
- Priced for enterprises with large minimum buy-ins.
- No protection on networks that enforce use of their DNS gateway. (hotels, starbucks, hotspots)

Selling Points

- ETP is a Cloud-based DNS solution. ThreatSTOP is a security web service that integrates with your on-prem DNS Server, where enforcement happens locally. With ThreatSTOP, there are not the privacy concerns associated with a Cloud-based DNS solution.
- ETP uses a single source of threat intelligence data that derives from their internal security team. TS utilizes 800+ authoritative threat intelligence partners.
- ETP has basic reporting, while ThreatSTOP provides preconfigured summary and email reports, detailed drill downs, IOC level metadata and Passive DNS. (ETP advertises simple categorical domain and URL lookups)
- Logging: ETP logs are retained for 30 days and export only as a CSV file. TS retains full reporting for a minimum of 30 days, also with SIEM integration capability.
- ETP Roaming Solution is basically a VPN, while ThreatSTOP is a locally enforced agent on your device.
- All DNS requests sent to ETP have DNSSEC enabled. DNSSEC can make DNS feel slower and increase payload size. ThreatSTOP has the option to enable or disable.
- ETP works at the domain level meaning malicious URLs/IPs on "good" domains are an unprotected threat, and like most WAF's/URL filtering solutions you will encounter over-blocking and need reclassification. Clients can use IP proxy sites to entirely circumvent protection and expose risk to the network either naively or maliciously.