AWS WAF Defense

Make your network invisible to attackers!

ThreatSTOP's AWS WAF Defense does the one thing no one else can do, it stops your network from responding to inbound communication from attackers, making your business-critical web applications effectively disappear from the scanners and probes used to carry out active, malicious activities against your company.

Need world class OFAC and ITAR compliance that delivers measurable business value?

ThreatSTOP gives you customizable control over your compliance requirements. AWS WAF Defense works with your existing WebACLs to protect your Amazon infrastructure in any AWS region.

Do you need the same security policy running on your traditional IP networks?

ThreatSTOP's broad multi-vendor compatibility allows you to use the same pre-curated Threat Intelligence enforcement policy wherever you have your assets, whether it's in the data center, on-premises, or in the public cloud – regardless of the vendor specific technologies in play.

No more "vendor after thought" threat intelligence data feeds or monolithic managed rules sets offered by other firewall and threat intelligence providers.

ThreatSTOP delivers policy building blocks curated from hundreds of threat categories, allowing you to create a security protection profile customized to meet your compliance requirements and security objectives.

Threat Intelligence: Quality, Speed & Coverage

The threat landscape moves at Internet speed, not human speed. Your threat intelligence protection must also be lightning fast to prevent attacks when they arrive. It is imperative that new threats are identified and mitigated against as quickly as possible, protecting your business-critical systems.

Identification of threats begins with more than 850 sources of data (feeds). These sources are internal, public, private, commercial, and some are derived from ThreatSTOP's own feedback loops. The feeds are synthesized into policy categories and rigorously sanitized to remove false positives.

Once feed updates have been turned into active protections, they are sent to the ThreatSTOP SaaS platform for automatic propagation to your AWS WAF ruleset.
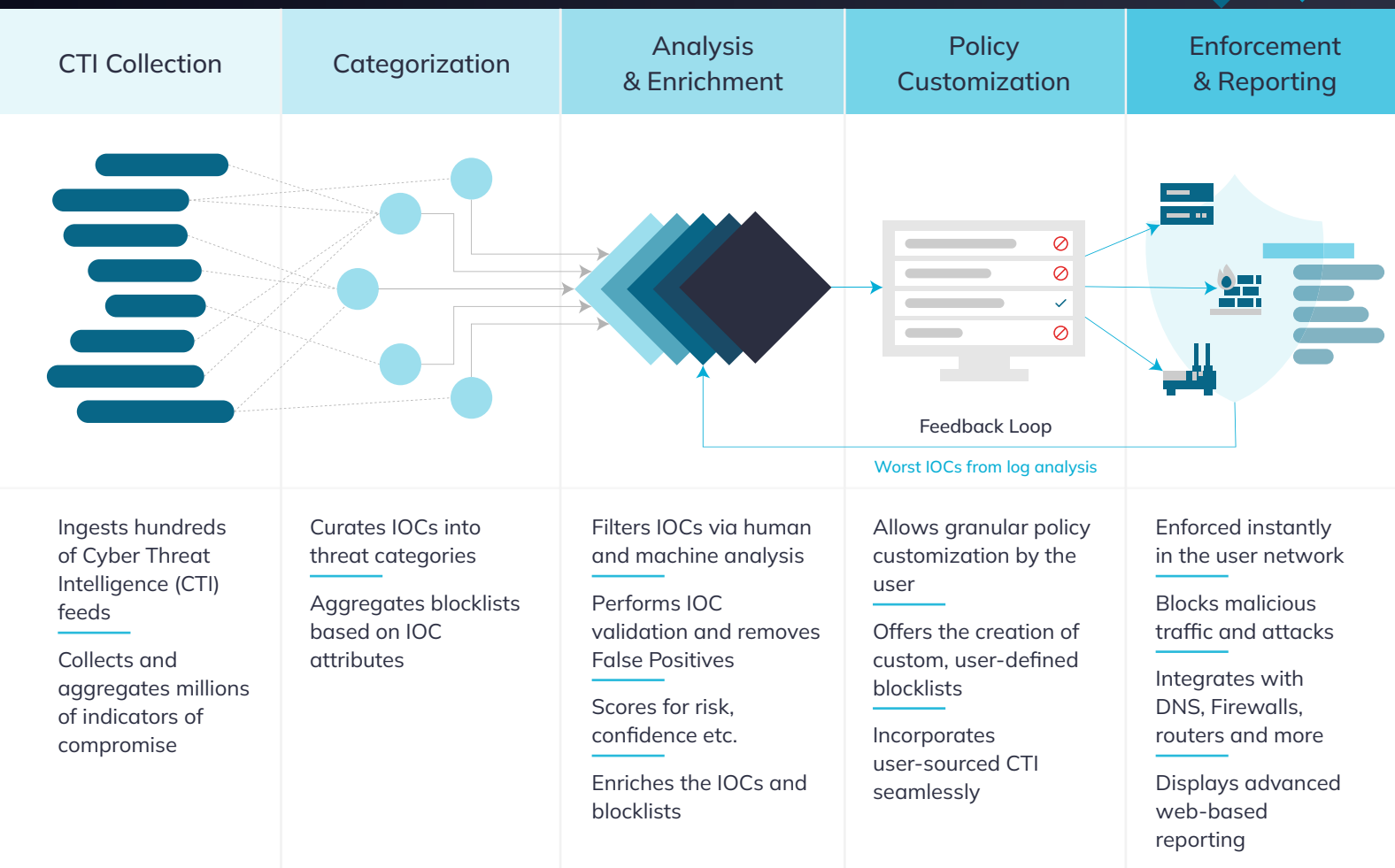
It's like having a virtual enterprise security team, protecting your critical business applications 7x24x365!

AWS WAF Defense Benefits

- ✓ **Automatically drop unwanted inbound and outbound connections** that use bandwidth and lead to network security breaches.

- ✓ **Dramatically reduce the load** on other, expensive security controls to save money and put an end to alerting overload.

- ✓ **Reduce compliance costs** automated ACL updates keep your WAF current with the latest protections and compliance restrictions.

- ✓ **Seamless AWS integration** that is secure and deploys from scratch in under 20 minutes!

- ✓ **Seamless AWS integration** that is secure and deploys from scratch in under 20 minutes!

- ✓ **Works with all your enforcement devices.** Maintain a single security management platform that can be implemented across all your infrastructure.

- ✓ **Advanced features** such as reporting, email alerts, research tools, and analyst access are included!

How ThreatSTOP Works

CTI Collection	Categorization	Analysis & Enrichment	Policy Customization	Enforcement & Reporting

Feedback Loop

Worst IOCs from log analysis

CTI Collection	Categorization	Analysis & Enrichment	Policy Customization	Enforcement & Reporting
Ingests hundreds of Cyber Threat Intelligence (CTI) feeds Collects and aggregates millions of indicators of compromise	Curates IOCs into threat categories Aggregates blocklists based on IOC attributes	Filters IOCs via human and machine analysis Performs IOC validation and removes False Positives Scores for risk, confidence etc. Enriches the IOCs and blocklists	Allows granular policy customization by the user Offers the creation of custom, user-defined blocklists Incorporates user-sourced CTI seamlessly	Enforced instantly in the user network Blocks malicious traffic and attacks Integrates with DNS, Firewalls, routers and more Displays advanced web-based reporting

Effective Reporting

Identify and prioritize potential endpoint infections or policy violations with actionable information. Set focused alerts for sensitive parts of your network or for specific threats like ransomware. ThreatSTOP reporting provides flexibility and visibility into network traffic to minimize the human resources required for verification and remediation of compromise.

Turn-key Privacy & Compliance

- Pre-packaged compliance policies, such as OFAC and ITAR
- Stops potential breaches by blocking exfiltration targets like TOR
- Automatic reporting and alerting on policy violations and malicious activity

Investment Protection
No New Hardware Required

The tools you need to protect your Business-Critical Applications and Customer Data are already in your network! ThreatSTOP takes accurate, actionable intelligence and loads it into the devices (regardless of vendor) that you already own and operate, making your existing firewalls, routers, WAFs, and DNS servers into cornerstone components of your Enterprise security strategy. ThreatSTOP can protect any network infrastructure: from small office networks to large carrier and cloud networks.

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.