Intrusion

intrusion.com | 888-637-7770

Shield Stratus

Autonomous Cloud Network Enforcement for AWS Environments

Protect cloud workloads with full-fidelity visibility, reputation-driven enforcement, and autonomous threat prevention designed for modern AWS infrastructure. Shield Stratus is a cloud-native network enforcement platform built to monitor and control inbound and outbound communications across AWS environments **without introducing operational complexity or requiring application redesign.** Designed around AWS Gateway Load Balancer (GWLB) and the GENEVE protocol, Shield Stratus provides transparent inline enforcement that evaluates 100% of network traffic flowing through protected cloud workloads.

Prevention-First Security for the Modern Cloud

Cloud environments continue to expand in scale and complexity, creating visibility gaps across workloads, VPCs, hybrid environments, and east-west communications. Shield Stratus addresses this challenge through Autonomous Network Enforcement powered by Intrusion's proprietary threat intelligence platform containing historical reputation intelligence on more than **8.5 billion IP addresses.**

Every connection is evaluated using decades of behavioral context, reputation analysis, and continuously updated threat intelligence. Known malicious infrastructure is blocked immediately, while unknown or high-risk destinations can be treated as untrusted by default.

This prevention-first model helps organizations reduce exposure to:

- Command-and-control communications
- Data exfiltration attempts
- Malware delivery infrastructure
- DNS tunneling activity
- Ransomware callbacks
- Low-reputation and unknown infrastructure

Why Organizations Deploy Shield Stratus

- **Full-Fidelity Traffic Visibility:** Evaluates 100% of network traffic flowing through protected cloud workloads with no sampling, blind spots, or incomplete telemetry.
- **Autonomous Threat Prevention:** Known malicious communications are blocked automatically, while unknown and suspicious infrastructure can be denied by policy to strengthen Zero Trust enforcement.
- **AWS-Native Deployment Architecture:** Built on AWS Gateway Load Balancer and GENEVE, integrating directly into AWS environments with lightweight IaC templates and minimal operational disruption.
- **Complements Existing Security Investments:** Works alongside existing NGFWs, SIEMs, EDRs, XDRs, and cloud-native security tooling to strengthen prevention and reduce downstream detection workloads.
- **Unified Visibility Through Command Hub:** Centralized reporting, policy management, AI-powered insights, and operational visibility across Shield deployments from a single interface.
- **Designed for Hybrid and Multi-Cloud Growth:** Extends consistent threat intelligence and enforcement across hybrid environments while supporting future expansion into additional cloud platforms.

How Shield Stratus Works

Shield Stratus operates transparently inside AWS environments as an inline packet-filtering and enforcement layer. Traffic flowing between workloads, VPCs, and external destinations is continuously evaluated against Intrusion's global reputation intelligence

platform. Legitimate communications proceed normally, while malicious, suspicious, or low-reputation communications can be blocked before connections fully establish.

Deployment is streamlined through AWS CloudFormation templates and integrates directly with existing AWS networking architectures without requiring major infrastructure redesign.

Organizations can operate Shield Stratus in:

- **Protect Mode** for active autonomous enforcement
- **Observe Mode** for visibility and operational assessment without blocking

Threat intelligence updates occur continuously through Intrusion's Global Threat Engine, allowing protection to evolve automatically as new threats emerge.

Who Benefits from Shield Stratus

- **Cloud and Platform Engineering Teams:** Deploy scalable, threat-intelligent enforcement inside AWS environments without redesigning application architectures or disrupting development workflows.
- **Security Operations Centers (SOCs):** Reduce alert fatigue and improve operational efficiency through autonomous prevention and centralized visibility into cloud communications.
- **MSPs and MSSPs:** Deliver scalable, multi-tenant cloud protection through centralized management and unified visibility across customer environments.
- **Hybrid Enterprises:** Extend consistent enforcement, visibility, and threat intelligence across both on-premises and cloud deployments through the broader Shield ecosystem.

PREVENTION OVER REACTION

Shield Stratus autonomously blocks malicious and untrusted communications before threats escalate, delivering a lighter operational burden and a stronger cloud security posture.

Shield Stratus vs. Traditional Cloud Security Approaches

Capability	Shield Stratus	Native AWS Security	Cloud NGFW
Full-Fidelity Traffic Visibility (100%)	●	—	○
Autonomous Threat Prevention	●	○	○
Reputation-Based Enforcement	●	○	○
Blocks Unknown Infrastructure by Default	●	—	—
AWS-Native GWLB / GENEVE Architecture	●	—	—
Protect & Observe Mode Options	●	○	○
Zero Trust Cloud Enforcement	●	—	○
Unified Multi-Deployment Visibility	●	○	○

● Native Capability ○ Limited Capability — Not Typically Supported

About INTRUSION Inc.

INTRUSION Inc. has delivered advanced cyber threat intelligence and prevention technologies for decades. Leveraging proprietary reputation intelligence built through years of research and government experience, the Shield platform helps organizations proactively reduce risk through prevention-first security and autonomous network enforcement.

Contact Us

888-637-7770
info@intrusion.com
www.intrusion.com