Supernatural API Security for aws

Ghost Security provides modern, cloud native API security via the Ghost Platform by integrating directly with AWS to empower discovery of all apps and APIs, seamless real-time detection of misconfigurations and threats, and delivers clear, prioritized remediation recommendations to protect against attacks.

92% of organizations have experienced an API-related security incident in the past year.[1] Unfortunately, the significant deployment limitations of conventional API security tools are exposing organizations to coverage gaps, vulnerable attack surfaces, and adding to the already high volume of false positives. Consequently, this results in prolonged mean times to detect and respond to threats and exacerbates team member burnout.

With our ability to understand how attackers could access your most valuable assets, Ghost distills mountains of alerts and data points down to only the most relevant information, increasing efficiency and reducing frustration - we do the hard work so you don't have to.

The Ghost Platform is deployed in 3 phases - Discover, Detect, Defend - each phase offering unique differentiators designed to increase efficiency and reduce complexity for customers. This modern API security solution is designed to stop application breaches while ensuring the following each step of the way: quick time to value, seamless scalability, complete visibility, and minimal disruption.

Achieve the following key outcomes with Ghost Security:

- Immediate ROI with cloud native deployment automation and best in class total cost of ownership.
- Improve security posture with context-aware visibility into your app's underlying AWS infrastructure.
- Continuous operational efficiency with actional alerts leading to reduced MTTD/R.
- Simplify compliance with capabilities that meet data protection and privacy requirements.
- Accelerate business productivity by removing security speedbumps.

Complete Modern API Security

Discover

- Discovery autopilot provides a full view into your external app infrastructure mapped to your AWS footprint.
- Zero Knowledge Deployment leverages Ghost's integration with your AWS environment to guide deployment with ease and eliminate the guesswork.

Detect

- Real-time analysis and full visibility of app traffic via AWS VPC Traffic Mirroring.
- Fingerprints are created using unique markers for higher fidelity detection.
- Continuous endpoint baselining provides immediate outlier anomaly detection.

Defend

- Scale attack prevention in real-time across all app surfaces with native integrations with AWS WAF.
- Dynamic risk ratings empower your team to focus on the issues that matter.

[1] Source: Enterprise Strategy Group, a division of TechTarget Inc. Research eBook, Securing the API Attack Surface.

Discover. Detect. Defend.

Comprehensive API Protection

The Ghost Platform is built on five core tenets. When combined, these principles provide organizations of all sizes, industries, and security maturity levels the insights and capabilities they need to secure all of their apps and APIs in the cloud.

Clear Prioritization with Risk Ratings
Remove Distractions & Prioritize Remediation

Continuous Monitoring & Real-time Anomaly Detection
Passive Traffic Analysis & Fingerprinting

Comprehensive App & API Inventory
Two Phase Approach to API Discovery

Data Residency & Separation
Sensitive Data Never Leaves Your AWS Environment

Zero Knowledge Deployment
Make Confident Monitoring Decisions

Automated Zero Knowledge Deployment

Ghost automatically identifies critical attributes about API behavior and makes sensor deployment recommendations. A deep understanding of your app infrastructure allows automated and intelligent recognition of coverage gaps and potential high risk areas - removing manual and tedious human intervention. Confident deployment decisions are made in minutes, not weeks, leading to less frustration and more effective monitoring.

Comprehensive App & API Discovery

Leveraging both public data sources and deployed sensors, Ghost rapidly identifies both public-facing and internal APIs, facilitating comprehensive mapping within minutes. This dual perspective ensures a thorough understanding of your application landscape, crucial for effective security measures.

Rigorous Approach to Data Residency & Separation

Ghost ensures utmost data security by keeping all raw payload data within the customer's AWS environment, never storing it within Ghost infrastructure. Only pertinent information related to significant signals and events is sent back to Ghost for further analysis.

Continuous Monitoring & Real-time Anomaly Detection

Ghost establishes usage patterns for every application and API, creating baselines for normal traffic behavior. Through continuous traffic analysis, it captures granular insights into infrastructure activity, using machine learning algorithms to detect deviations from expected behavior. Analysts are promptly alerted to potential threats, enabling swift intervention.

Prioritize Response Activities with Dynamic Risk Ratings

Prioritize action based on a dynamic analysis of attack path feasibility, resource exploitability, and overall impact to the organization. Contextualized insights drive automatic validation, save your team from manual triage, and dramatically reduce remediation cycles.