AKAMAI DATASHEET

API Security ShadowHunt

API Security ShadowHunt is a managed threat hunting service that expands your security team with expert analysts skilled in API threat hunting. Ideal for understaffed teams or those lacking API security expertise, API Security ShadowHunt is an outsourced solution that helps you reduce risk. Threat hunters work as an extension of your team to detect and report on the most clandestine and obfuscated attacks hiding in your API traffic.

How API Security ShadowHunt works

ShadowHunt operations begin with the API activity data in the API Security platform. These automated analytics detect behavioral deviations and vulnerability exploits, and machine learning signals are delivered to ShadowHunt analysts for investigation. This is where human expertise begins.

Since analysts are familiar with customer API estates, they will rapidly identify active threats and create and transmit a ShadowHunt Alert. If there is ambiguity in the findings, an analyst will contact a ShadowHunt subscriber for clarification. Analysts and the API Security research team consume threat intelligence information to deliver periodic emerging threat reports to all service customers.

API Security plus human expertise

The API Security platform offers comprehensive API Security features, including:

- **API discovery:** Broad and continuous API discovery
- **Risk posture:** Understand your API risks
- **Threat detection using behavioral analytics:** Our big data, cloud-based analytics engine examines all API activity over time continually detecting API abuse
- **Prevention and response:** Customized, conditional response playbooks enhance security and API DevSecOps processes
- **Investigation and threat hunting:** Powerful investigative capabilities provide the ability to hunt for threats hiding in your API traffic

Threat hunting is one of the most advanced capabilities of the API Security platform. The API Security ShadowHunt service is intended for customers that lack either the tools, expertise, or time to hunt for threats.

BENEFITS TO YOUR BUSINESS

The peace of mind that experts are examining your API activity

The detection of more security threats lurking in your API data

More time for your team while Akamai focuses on API security

Actionable insights for software development and IT operations

Improved visibility into API behavior with additional scrutiny

Akamai

API Security ShadowHunt services you can rely on

Alerts: *Notification of a threat in your API estate*. The most important element of the API Security ShadowHunt service is the alert, transmitted immediately upon confirmation of an active incident. Alerts include:

- Incident findings and analysis
- Threat intelligence summary pertaining to the incident
- Remediation recommendations

Threat reports: *Gain early API security intelligence*. The API Security ShadowHunt Emerging Threat Report is based on the team's access to global threat intelligence, input from the API Security research team, and ongoing threat hunting activities. The Emerging Threat Report includes:

- Details of new API vulnerabilities, threats, or attacks identified by the team
- Effects on your API estate
- Recommendations for remediation, as needed

Monthly reviews: *Full visibility into your API estate*. The ShadowHunt Monthly Threat Report is delivered to all API Security customers in the first week of each month. It includes:

- A summary of ShadowHunt Alerts and Emerging Threat Reports sent in the previous month
- An overview of your API estate
- A comparison of API activity from the past two months
- Security headlines from the API industry

Ask the experts: Service subscribers have access to the API Security ShadowHunt team for questions and discussions about both Alerts and Emerging Threat Reports.

Why API Security?

API Security applies the principles of extended detection and response (XDR) to the challenge of securing APIs from vulnerabilities and API abuse. Only API Security aggregates API activity into its cloud-based big data environment, followed by complex data enrichment and organization. This unique architecture enables continuous API discovery, risk scoring, context-aware behavioral analytics to detect API abuse and threats, and threat hunting. The API Security architecture includes privacy by design, wherein any API activity destined for the data lake can be tokenized.

Threat hunting expertise to protect your APIs

The growth in API deployments can place strains on organizations' IT security departments. The API Security ShadowHunt service expands your security staff today.

Speak with an expert to learn more.

Support

Published 08/23