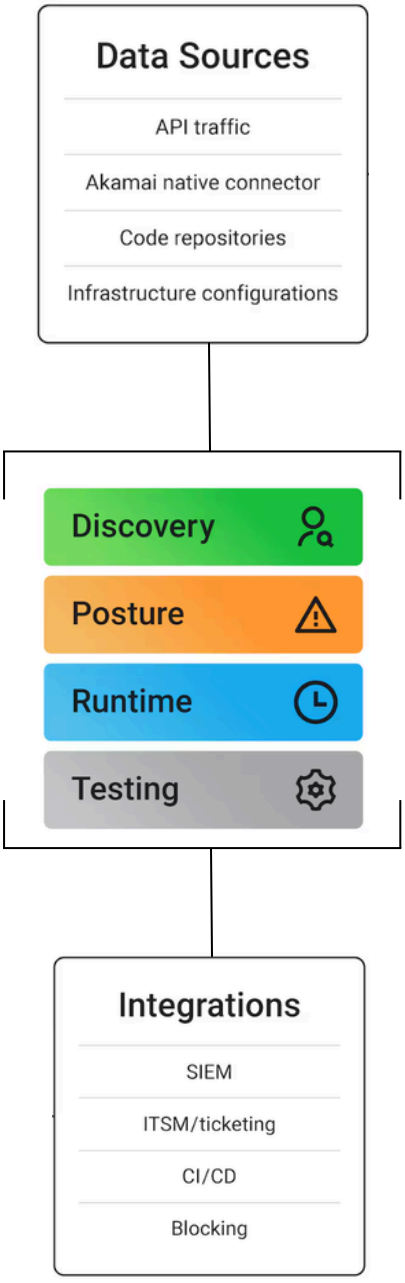
AKAMAI PRODUCT BRIEF

API-Security

APIs drive your business every day — connecting it with partners, suppliers, and customers. But every API also expands your attack surface, and threat actors know it. API attacks are growing and evolving fast, often in ways your web application and API protection may not detect. And without a comprehensive inventory of your APIs, your team will have a blind spot and your organization's APIs will be unprotected.

Our platform protects APIs throughout their entire lifecycle, from development to production. Built for organizations that expose APIs to partners, suppliers, and users, API Security discovers your APIs, understands their risk posture, analyzes their behavior, and stops threats from lurking inside.



API protection for GenAI workflows

Instant visibility and protection for all your APIs, from legacy to GenAI, LLM, and MCP servers. Learn how to identify vulnerabilities and analyze API behavior so you can detect attacks and remediate risk in this fast-growing attack surface.

Find and eliminate hidden API security risks

Discover your complete API estate

Automatically discover, inventory, and tag shadow, zombie, and AI-related APIs to enable instant governance and compliance.

Identify vulnerable APIs

Audit for the API vulnerabilities and misconfigurations that attackers target, including all of the OWASP API Top 10.

Prevent API abuse and attacks

Use contextual insights to identify risks such as data leakage, suspicious behavior, malicious bots, and API attacks.

API Security's critical capabilities

Discovery

It's not uncommon to have APIs that no one knows about. Without an accurate inventory, however, your business is exposed to a range of security risks. Stop the guesswork and let us help you:

- Locate and inventory all your APIs regardless of configuration or type, including RESTful, GraphQL, SOAP, XML-RPC, JSON-RPC, and gRPC
- Detect dormant, legacy, and zombie APIs
- Identify forgotten, neglected, or otherwise unknown shadow domains
- Eliminate blind spots and uncover potential attack paths

Testing

Applications are being developed at the fastest pace we've ever seen. Which means it's easier for a security vulnerability or design flaw to go undetected. Take advantage of our API security testing suite to:

- Automatically run 200+ tests that simulate malicious traffic, including the OWASP API Security Top 10 threats
- Discover vulnerabilities before APIs enter production to reduce the risk of a successful attack
- Inspect your API specifications against established governance policies and rules
- Run API-focused security tests on demand or as part of a CI/CD pipeline

Detection

Simple API misconfigurations can leave you defenseless against cybercriminals. Once inside, hackers can quickly access and exfiltrate your sensitive data. Use our platform to:

- Automatically scan infrastructure to uncover misconfigurations and hidden risks
- Create custom workflows to notify key stakeholders of vulnerabilities
- Identify which APIs and internal users are able to access sensitive data
- Assign severity rankings to detected issues to prioritize remediation

Response

It's no longer a question of if but when your organization will be attacked, which means you need to be able to detect and block attacks in real time. Use our artificial intelligence/machine learning–based anomaly detection to:

- Monitor for data tampering and leakage, policy violations, suspicious behavior, and API attacks
- Analyze API traffic without additional network changes or difficult-to-install agents
- Integrate with existing workflows (ticketing, security information and event management [SIEM], etc) to alert security/operations teams
- Prevent attacks and misuse in real time with partial or fully automated remediation

BENEFITS FOR YOUR BUSINESS

Discover

Understand your API attack surface. Reduce the costs of API inventories and documentation updates. Improve compliance with regulatory requirements and internal policies.

Test

Reduce remediation costs by finding issues earlier. Improve code quality without sacrificing speed. Increase revenue by accelerating time to market.

Detect

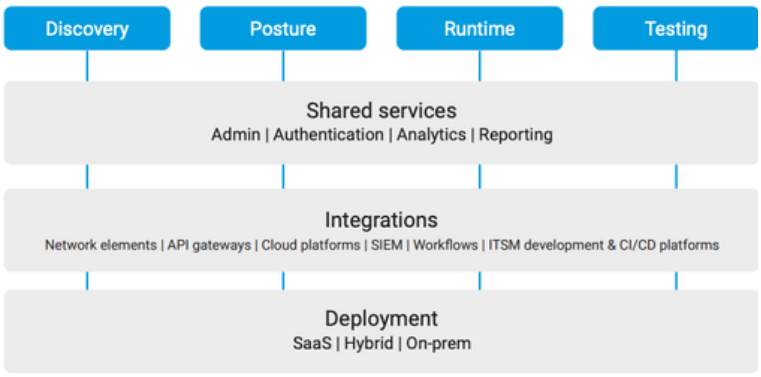
Gain critical business context by learning exactly what happened. Deduce why it is a problem and uncover its potential impact. Determine how you should remediate.

Respond

Reduce risk by stopping attacks immediately. Reduce costs by remediating vulnerabilities before exploitation. Reduce lost revenue from downtime.

The Akamai difference: Block at the edge

Akamai App & API Protector discovers and mitigates API threats for apps and APIs running through Akamai Connected Cloud and can block any traffic that contains potential threats uncovered by API Security. When deployed together, Akamai's API protections offer comprehensive and continuous visibility into APIs, and allow you to discover, audit, detect, and respond to API security concerns across the full application estate.



Features

- *Assess API traffic* with a native connection to Akamai CDN and find APIs in source code to identify the types of sensitive data that your APIs can access
- *Automatically discover, inventory, and tag* all APIs connecting to GenAI models, LLMs, and AI services, including shadow and unmanaged endpoints
- *Detect* APIs connected to Model Context Protocol (MCP) servers to identify shadow integrations and ensure safe AI agent adoption
- *Analyze* APIs for OWASP Top 10 API Security Risks and prioritize vulnerabilities by impact for rapid remediation
- *Understand API context* with visualizations of business logic, physical network infrastructure, and API traffic flows
- *Continuously monitor* for compliance with regulatory requirements, industry standards, and internal policies
- *Identify* anomalous usage, API attacks, data leakage, tampering, and policy violations
- *Block API attacks and set up workflows to accelerate remediation, or leverage* Managed Security Service *to increase your SOC effectiveness*
- *Fully integrate* with your existing CI/CD pipelines and automatically run 200+ tests that simulate malicious traffic

Evolane Guardian

Standard support is offered 24/7/365 for all Akamai customers. In addition to on-demand professional services for consulting or single-project work, Evolane provides levels of guardian services

Akamai Select Partnership

Akamai's portfolio of advanced security and video delivery solutions is backed by Evolane's unparalleled customer service, analytics and 24/7 monitoring. Founder Kristof Haeck worked together with Akamai throughout his career and got to know the platform in all its facets. As someone who only chooses who and what he believes in, it didn't take long for Kristof to become an Akamai Select Partner to continue the successes.

This title is reserved for partners who continue to invest to provide the right product knowledge and product configuration! With more than 15 years of experience with Akamai's solutions, our engineers are now as certified as can be and we got to do some great projects for amazing companies. This is how Evolane combines the benefits of a trusted local partner with the ingenious technology of an international company.

To learn more, click here and visit our Akamai partnerpage on the Evolane website.