

Akamai Managed Service for API Security

The rapid adoption of APIs has expanded the attack surface, leaving enterprises vulnerable to new and emerging threats. Protecting APIs is no longer optional — it's essential to safeguard your business-critical operations. However, with limited cybersecurity resources and expertise, security teams find it challenging to identify and respond to API-specific threats. Akamai Managed Service for API Security empowers organizations to tackle these challenges head-on. With around-the-clock, expert-led incident investigation and rapid response, Akamai Managed Service for API Security ensures the protection of your APIs, enabling you to focus on driving innovation.

As APIs increase in complexity and prevalence, the threats against them increase as well. Simultaneously, a shortage of cybersecurity talent leaves security teams unable to keep up with the expanding attack surface. Additionally, the skills gap in API security exacerbates the problem, as practitioners frequently lack the training or expertise to effectively identify and address API vulnerabilities. Without adequate resources, organizations struggle to investigate critical API findings, mitigate risks, and implement permanent solutions.

These challenges lead to increased vulnerability to high-impact API security incidents, jeopardizing the confidentiality, integrity, and availability of business systems and data.





Akamai Managed Service for API Security is designed to augment your security operations center (SOC) and provide an expert-driven approach to protecting your APIs. Our proactive monitoring and response solution acts as an extension of your security organization, enhancing your SOC team with API security analysts who investigate and respond to runtime incidents.

Key components of the solution include:

- **Proactive monitoring:** Advanced anomaly detection for identifying and assessing malicious or high-risk API activities
- **Incident investigation:** Thorough analysis of security events to provide actionable recommendations and suggest root-cause solutions
- **Scalable protection:** Around-the-clock access to Akamai's Security Operations Command Center (SOCC) for faster and more effective mitigation of attacks

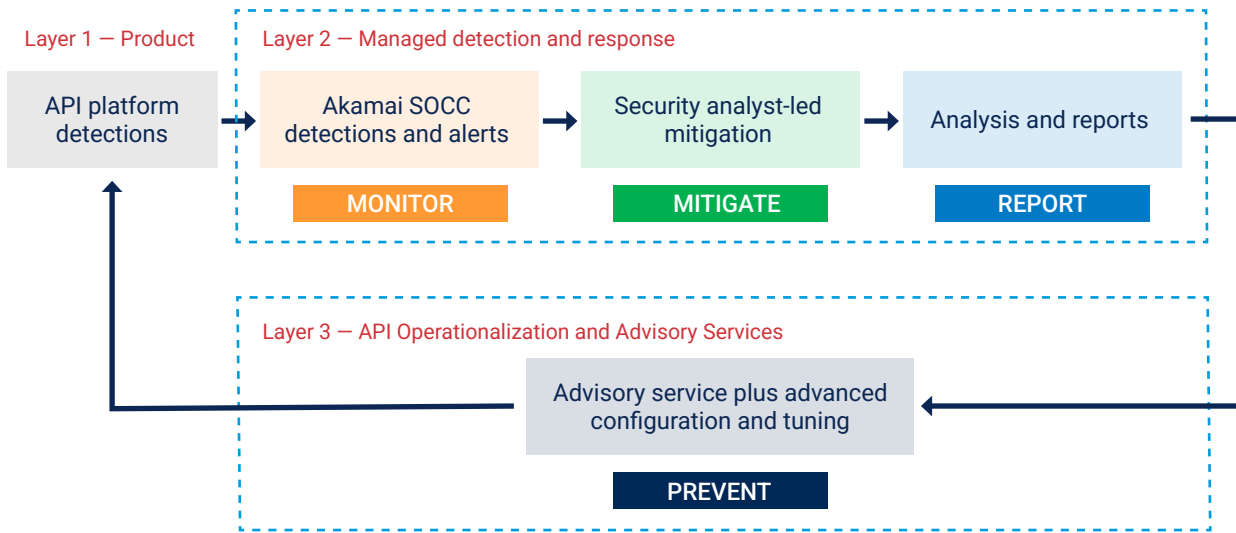
With our managed services, you can enhance your organization's readiness to respond to API attacks, identify high-impact attacks sooner, and act upon recommendations from API security-trained analysts for blocking attacks, resolving false positives, and fixing root causes. Akamai Managed Service for API Security enables organizations to operationalize API security, helping you reduce the impact of attacks and implement a robust, scalable defense strategy.

Benefits for your business

-  **Comprehensive API protection**
A single managed service integrates with your broader security strategy and minimizes risks to your systems and data
-  **Expert-led security management**
Akamai's global SOCC provides advanced threat intelligence and proactive incident management
-  **Faster incident resolution**
24/7 monitoring streamlines the detection, investigation, and mitigation of security incidents
-  **Scalable security operations**
API security experts augment your team to strengthen your defense capabilities



How it works



Key features

- **24/7 monitoring and support**
Attacker detection, mitigation assistance, and access to domain experts
- **Threat hunting**
Analysis of runtime behaviors and identification of posture weakness
- **API Operationalization and Advisory Services**
Ongoing expert security guidance and customization
- **Professional services**
Ongoing professional services configuration assistance
- **Support advocacy**
Assistance to manage security escalations and improve supportability over time
- **Enhanced SLA**
Faster response SLAs for product break/fix

Interested in learning more about Akamai Managed Service for API Security?

Contact your sales representative today.