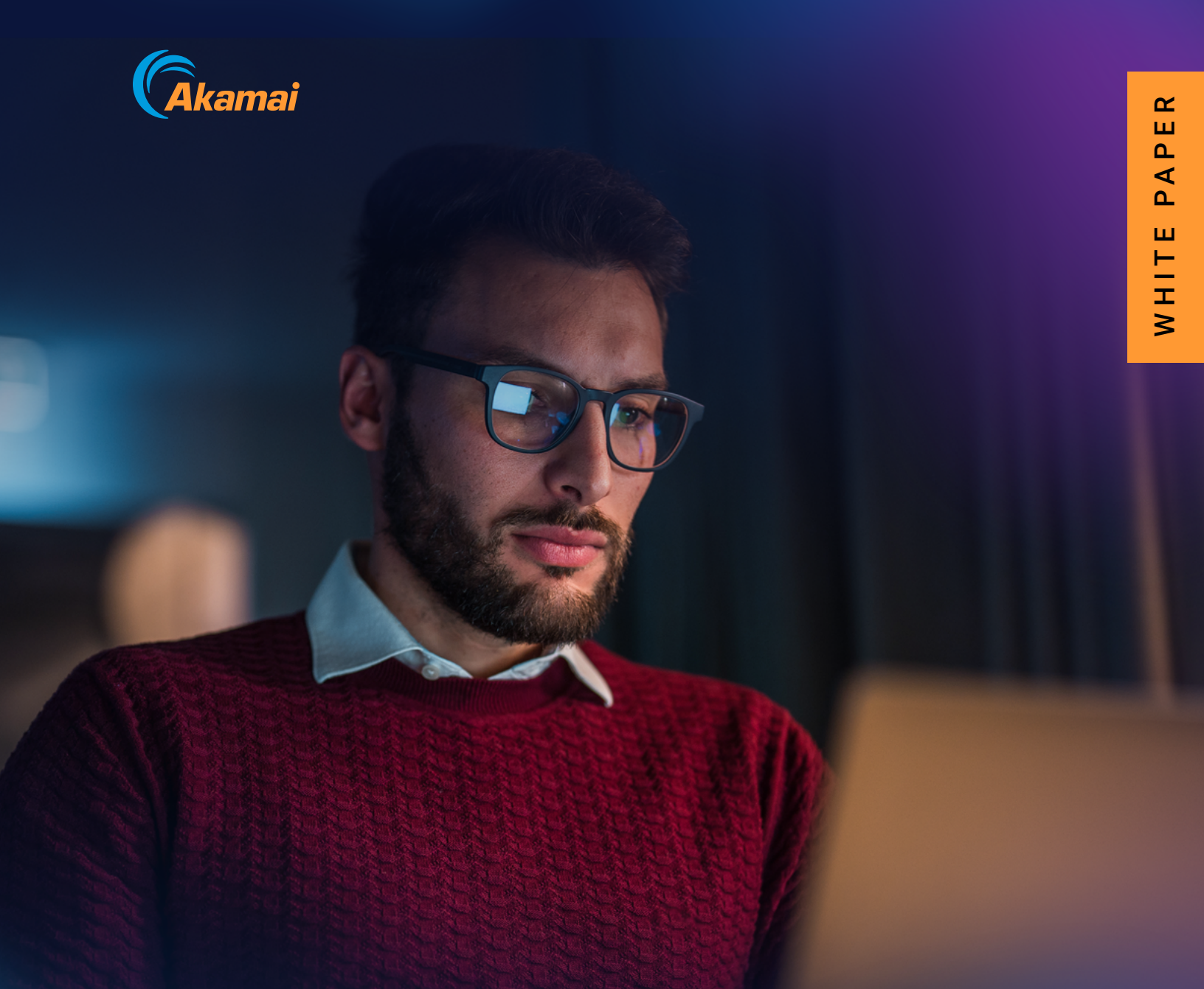
Akamai

WHITE PAPER



A Game Plan for OWASP Top 10 API Security Risks

How Akamai can help you address common API vulnerabilities and threats

OWASP Top 10 API Security Risks		Can Akamai help?
API1:2023	Broken Object Level Authorization	☑
API2:2023	Broken Authentication	☑
API3:2023	Broken Object Property Level Authorization	☑
API4:2023	Unrestricted Resource Consumption	☑
API5:2023	Broken Function Level Authorization	☑
API6:2023	Unrestricted Access to Sensitive Business Flows	☑
API7:2023	Server-Side Request Forgery	☑
API8:2023	Security Misconfiguration	☑
API9:2023	Improper Inventory Management	☑
API10:2023	Unsafe Consumption of APIs	☑

APIs live at the core of an enterprise's digital products, services, and cloud environments. They're also the standard for building and connecting applications as organizations increasingly move to microservices-based architecture for developing apps. However, APIs' constant access to data and critical systems makes them both a revenue driver and an operational risk.

Exposed or misconfigured APIs are prevalent, easy to compromise, and often unprotected. And just one breached API can result in millions of records being stolen.

With 78% of organizations reporting they've experienced API security incidents in a year's span, it's clear that protecting APIs should be a priority. But the API attack surface has quickly risen to a target of choice — much faster than most enterprises have been able to build an understanding of:

API risks

API attack methods

API security controls and capabilities

What does the API attack surface comprise? The short answer is that it's much broader than many organizations realize. The traditional understanding of APIs (e.g., machine-to-machine or third-party APIs) can and should be expanded to include mobile and web application services as a part of the microservices-based architecture. In other words, a web request within that architecture is an API serving as one in a series of calls to various microservices.

78%

of organizations report they've experienced API security incidents in a year's span. Clearly, protecting APIs should be a priority.

On June 5, 2023, the highly regarded Open Worldwide Application Security Project (OWASP) issued the first major update to its initial Top 10 API Security Risks list, which was released in 2019. The updated list addresses how each of these API calls can potentially open security holes and create privacy risks, including:

Poor data validation

Configuration errors

Implementation flaws

Integration gaps between security components

Read on to learn about key OWASP-identified risks and how Akamai's API security solutions can help you mitigate them.

The trouble is that even organizations that claim to have a full inventory of their APIs have a serious gap:

Only **4 in 10** know which of their APIs return sensitive data when called.

API1:2023 — Broken Object Level Authorization

Broken Object Level Authorization (BOLA) vulnerabilities can occur when a client's authorization is not properly validated to access specific object IDs. This vulnerability can provide an opening for attackers to access resources directly, bypassing the anticipated application workflow and gaining unauthorized access to sensitive data. Organizations can reduce this risk by avoiding sole reliance on object IDs that clients pass in their requests. Instead, organizations can use non-guessable, random IDs for objects to ensure robust validation for every object. When appropriate, masking the true ID of objects can provide an additional layer of security.

How Akamai can help

Akamai's vigilant surveillance systems track threats and generate alerts for attempted BOLA exploitation, ensuring immediate attention and action.

Akamai mitigates risk by:

- Identifying BOLA exploitation attempts
- Classifying API endpoints susceptible to BOLA exploitation based on received inputs (e.g., enumerable parameters) as well as the relationships between API objects and properties
- Generating alerts on attempted or successful BOLA exploitation

API2:2023 — Broken Authentication

Broken authentication refers to broad vulnerabilities in the authentication process, exposing the system to attackers who can exploit these weaknesses to compromise API object protection. Typically, attackers capitalizing on broken authentication vulnerabilities manipulate loopholes in the system, such as weak passwords or session replay. To protect against broken authentication vulnerabilities, organizations can establish robust authentication and secrets management mechanisms, such as strong password policies, key rotation, strong token signatures, and encryption keys. Enforcing these stringent policies organization-wide can significantly reduce risk.

How Akamai can help

Akamai fortifies API security by identifying and rectifying weak authentication points, thwarting automated attacks, and proactively alerting on attempted exploitation attempts.

Akamai mitigates this risk by:

- Identifying API endpoints that do not require authentication or do not follow authentication best practices, such as weak token signatures or encryption keys and the acceptance of expired authentication tokens
- Protecting against automated dictionary or credential stuffing attacks through our bot management capabilities
- Handling authorization of JSON Web Tokens using strong token signatures through our API Gateway capabilities
- Generating alerts on attempted BUA exploitation

API3:2023 — Broken Object Property Level Authorization

Broken Object Property Level Authorization (BOPLA) is a security flaw where an API endpoint unnecessarily exposes more data properties than required for its function, neglecting the principle of least privilege.

This flaw can inadvertently provide attackers with excessive data that can then be used to unearth more vulnerabilities or mine for sensitive data. This includes scenarios where properties exclusive to admin-level access can be manipulated by unauthorized users, further compromising system integrity. To ensure security and to prevent attackers from getting or manipulating surplus information, it is critical to provide appropriate access levels and data exposure, impeding potential attackers from exploiting these oversights.

How Akamai can help

Leveraging Akamai's comprehensive tactics, companies are able to mitigate the risks of BOPLA by identifying and cataloging API endpoints and their associated properties.

Akamai mitigates this risk by:

- Identifying and labeling all endpoints and the API properties they expose, such as personally identifiable information (PII)
- Identifying undocumented or shadow API endpoints, objects, and properties, as well as abnormal properties
- Applying security policies on acceptable and defined parameters and properties to ensure data sanitization
- Applying security policies based on the full OpenAPI/Swagger specification and only allowing well-defined API endpoints and methods to access API objects and properties
- Generating alerts on attempted BOPLA exploitations

API4:2023 — Unrestricted Resource Consumption

Unrestricted resource consumption (sometimes called “API resource exhaustion”) is a type of vulnerability where APIs do not limit the number of requests or the volume of data they serve within a given time. This oversight can open the door for attackers who seek to perform denial-of-service (DoS) attacks, which can make the system unavailable to legitimate users. Such exploitations can have serious business implications, resulting in loss of service availability, customer dissatisfaction, and potential revenue losses, depending on the length and range of the outage. It is critical to have measures in place that limit the rate of API requests and the size of data returns to prevent loss of service.

How Akamai can help

Akamai secures your APIs from unrestricted resource consumption threats by:

- Identifying at-risk endpoints and providing real-time alerts on attempted volumetric attacks
- Spotting excessive errors, login attempts, or atypical behavior indicating risk

Akamai mitigates this risk by:

- Identifying API endpoints that are lacking rate limits or are under attack through large volumetric dictionaries or credential stuffing attacks
- Initiating workflows to slow down or block volumetric attacks
- Generating alerts on attempted volumetric attacks

API5:2023 — Broken Function Level Authorization

Broken function level authorization (BFLA) can occur when access control models for API endpoints are incorrectly implemented. Incorrect or outdated access control methods can fail to adequately restrict unauthorized access — allowing attackers to access sensitive information or the system as a whole. To mitigate this risk, organizations can adopt the principle of least privilege, ensuring that all functions, particularly administrative functions, are only accessible to users with appropriate permissions.

How Akamai can help

By tracking behavioral timelines, applying security policies to sensitive functions, managing key rotation and revocation, and prompt alerting of any suspicious attempts, Akamai can help to fortify organizations' BFLA prevention and response strategy.

Akamai mitigates this risk by:

- Identifying behavioral timelines on API endpoint access through capturing users, API keys, access tokens, session IDs, etc.
- Applying key rotation or exposed key revocation through Akamai API Gateway
- Generating alerts on suspicious attempts to access administrative functions

API6:2023 — Unrestricted Access to Sensitive Business Flows

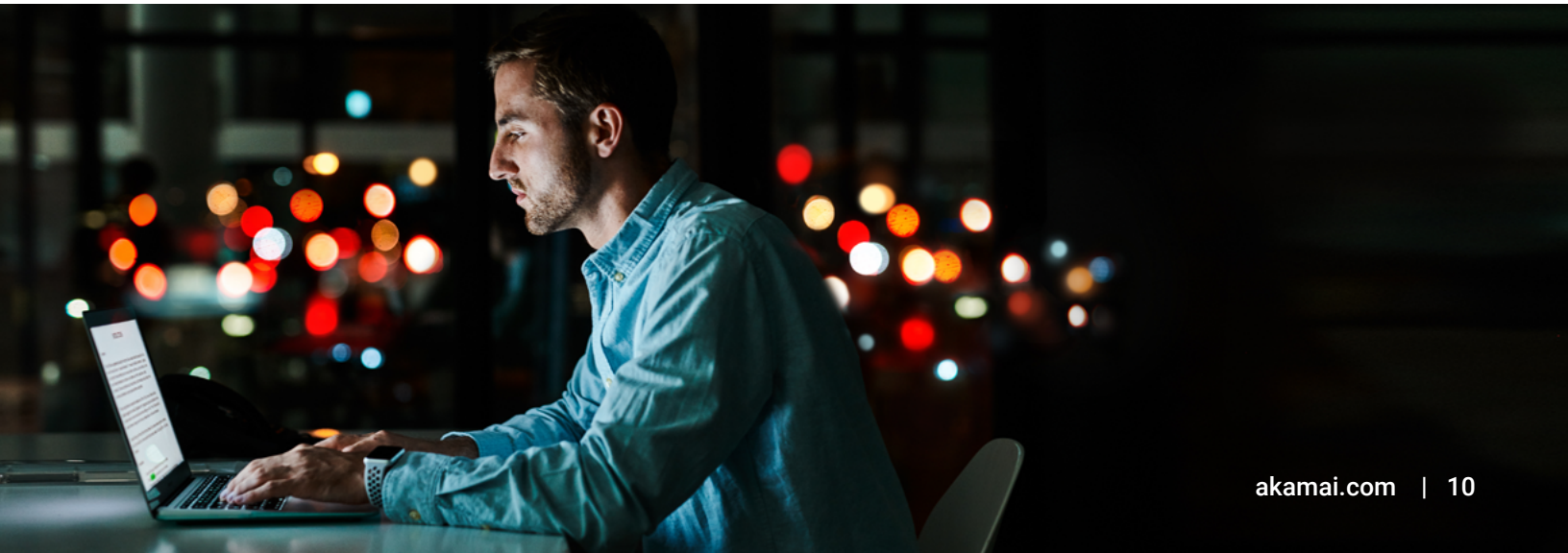
Unrestricted access to sensitive business flows arises when an API exposes critical operations like business logic without sufficient access control. This can lead to unauthorized access and exploitation, causing significant harm to an organization. Exploitation typically involves understanding the business model backed by the API, identifying sensitive business flows, and exploiting loopholes to these flows. This can lead to impacts like preventing legitimate users from purchasing a product.

How Akamai can help

Secure your business with Akamai's comprehensive API protection solutions, offering sensitive endpoint identification, real-time exploitation alerts, and expert consultancy to safeguard your critical data and operations.

Akamai mitigates this risk by:

- Identifying sensitive API endpoints, such as payment flows or endpoints handling PII
- Generating alerts on a variety of potential exploitations ranging from data exfiltration to data manipulation and suspicious attempts on these sensitive API endpoints



API7:2023 — Server-Side Request Forgery

Server-side request forgery (SSRF) allows an attacker to induce the server-side application to make HTTPS requests to an arbitrary domain of the attacker's choosing. In a typical SSRF attack, the attacker tricks the server into making a request to internal resources, thereby bypassing firewalls and gaining access to internal services, which can lead to data exposure or remote code execution. To mitigate this risk, it's crucial to validate, filter, or sanitize user input and limit the outbound connections your server can make, ensuring that it only communicates with critical services.

How Akamai can help

Strengthen your security posture with Akamai, delivering anomaly detection in trusted API connections, effective key management, and immediate notifications on SSRF exploitation attempts.

Akamai mitigates this risk by:

- Applying protection through web application and API protection policies targeting SSRF attacks
- Applying key rotation or exposed key revocation through API Gateway

API8:2023 — Security Misconfiguration

Security misconfiguration refers to the improper setup of security controls, which can leave a system vulnerable to attacks. This could include insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP(S) headers, and verbose error messages containing sensitive information. To mitigate risks, it's vital for organizations to ensure they have correctly configured their security controls across all aspects of their applications and APIs. This involves regular updates, thorough testing, and continuous monitoring to identify and rectify any misconfigurations promptly.

How Akamai can help

Enhance your insights as Akamai helps you identify shadow, rogue, or zombie API endpoints, align with security best practices, achieve robust HTTPS implementation, and receive instant alerts on security misconfigurations.

Akamai mitigates this risk by:

- Identifying shadow API endpoints that might expose low-level environments (e.g., testing and staging environments)
- Identifying and matching API endpoints, objects, and properties against security configuration best practices and standards
- Applying security policies through API security best practices, such as well-formed HTTPS requests and responses, configuring or removing correct HTTP headers, and ensuring full control over cross-origin resource sharing (CORS) and cache control headers
- Applying proper HTTPS implementation through SSL/TLS, including correct and secure cipher suites
- Generating alerts for misconfiguration or noncompliance with API security best practices and standards

API9:2023 — Improper Inventory Management

Improper inventory management is a challenge for every organization managing APIs. API security solutions can protect known APIs, but unknown APIs — including shadow APIs — may be left unpatched and vulnerable to attack. This can lead to outdated components, unused pages or APIs, and unnecessary exposure of sensitive information. Unmaintained service management can make systems vulnerable to threats, and attackers can potentially gain access to sensitive data or even the server through unknown APIs that are connected to the same database. Access controls and regular audits are essential to avoiding constantly changing components of an organization's services.

How Akamai can help

Akamai persistently oversees API traffic to help discover hidden API endpoints and APIs with potential risks, providing organizations secure data storage, advanced threat analysis, and immediate alerts on potential exploitations.

Akamai mitigates this risk by:

- Continuously monitoring exposed API traffic flowing through your environments, including north-south API endpoints targeting publicly accessible APIs and east-west internal API endpoints
- Identifying shadow API endpoints that might expose low-level environments (e.g., testing and staging environments) or undocumented and/or deprecated API versions
- Creating an up-to-date API inventory based on risk scoring and data classification
- Generating alerts on a variety of potential exploitations ranging from data exfiltration to data manipulation and suspicious attempts on these sensitive API endpoints

API10:2023 — Unsafe Consumption of APIs

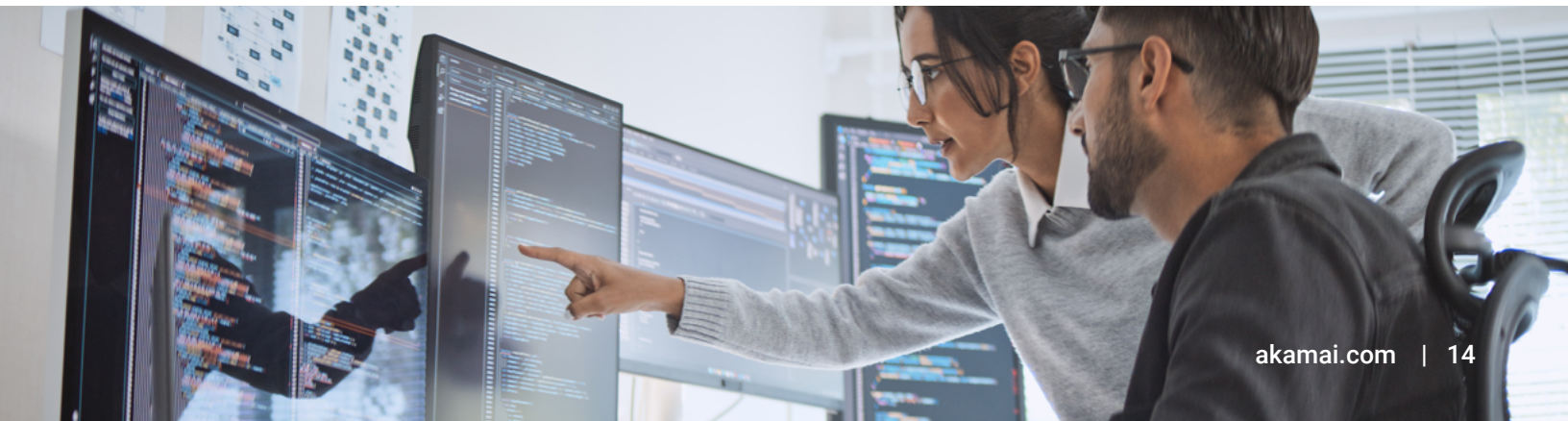
Unsafe consumption of APIs refers to the risks associated with the use of third-party APIs without proper security measures in place. Organizations are increasingly reliant on third-party APIs to extend services and functionality, so these APIs are often trusted by default. This can lead to significant security vulnerabilities. Not implementing proper encryption, data validation, sanitization, and resource consumption limits can open organizations to significant vulnerabilities. To mitigate these risks, organizations can implement encryption for all data transmitted over the network, validate and sanitize all data inputs, and set reasonable limits on resource consumption.

How Akamai can help

Continuously protect your systems by monitoring and validating your services to ensure security with Akamai's monitoring, alerting, and consulting services.

Akamai mitigates this risk by:

- Monitoring continuously on all exposed API traffic flowing through your environments, including east-west and outbound APIs that facilitate B2B and/or third-party integrations
- Generating alerts on a variety of potential exploitations ranging from data exfiltration to data manipulation and suspicious attempts on these sensitive API endpoints
- Applying protection through web application and API protection policies targeting a variety of API attacks collected in attack groups



Additional security risks from OWASP

The OWASP Top 10 API Security Risks of 2023 were the nonprofit organization's first major update to its list since 2019. It's worth looking back, however, at the original list, which discusses additional security risks, such as injection attacks, that still are relevant in today's landscape.

Akamai can help with this security risk by:

- Identifying API injection–vulnerable endpoints and injection attempts by matching on signatures and detecting anomalies
- Applying security policies through JSON and XML inspection of API requests and scanning for a variety of injection attacks such as SQLi, XSS, CMDi, RFI, and LFI
- Generating alerts on injection exploitation

OWASP has also released other lists of top 10 security risks, such as the OWASP Top 10 Web Application Security Risks. Akamai's security portfolio can help with mitigating these security risks as well.

We are here to help!

Organizations and their security vendors must work closely together, aligning across people, processes, and technologies to institute a solid defense against the security risks outlined in the OWASP Top 10 API Security Risks.

Akamai provides industry-leading security solutions, highly experienced experts, and a platform that gleans insight from millions of web application and API attacks, billions of bot requests, and as many as trillions of API requests every single day.

Akamai's web application and API security solutions will help secure your organization against the most advanced forms of web application, DDoS, and API-based attacks. Additionally, Akamai Managed Security Service provides 24/7 monitoring, security management, and threat mitigation.

To learn more about Akamai's security portfolio, please take a look at our website. If you would like to discuss and explore in more detail how we can partner to build the best protection for your business, please reach out to your Akamai sales representative today.

Akamai Security protects the applications that drive your business at every point of interaction, without compromising performance or customer experience. By leveraging the scale of our global platform and its visibility to threats, we partner with you to prevent, detect, and mitigate threats, so you can build brand trust and deliver on your vision. Learn more about Akamai's cloud computing, security, and content delivery solutions at akamai.com and akamai.com/blog, or follow Akamai Technologies on X, formerly known as Twitter, and LinkedIn. Published 09/24.