APIs provide powerful capabilities for the modern online user experience. This Analyst Connection calls out important factors to consider as businesses plan their API security strategies.

Key API Security Questions to Address for Commerce Organizations

July 2024

Questions posed by: Akamai

Answers by: Christopher Rodriguez, Research Director, Security and Trust

Q. Why are security controls such as web application firewall (WAF), bot management, and API gateways not enough to protect modern APIs?

A. WAF is a foundational technology that offers deep security functionality for web traffic and can extend protections to API traffic as well. However, WAF is a point-in-time inspection point, while APIs are designed to be more dynamic and interconnected. WAF excels at perimeter protection but may not see all API traffic, especially internal, east-west communications between systems. Depending on the configuration, API traffic from an API gateway, as well as shadow API traffic, may not traverse to a WAF either. In IDC's March 2024 *Web Application and Availability Protection Buyer Insights 2024 Survey,* 39% of businesses noted the limitations of existing security tooling such as WAF for fully addressing API security needs.

On the other hand, API gateways are designed to handle API traffic, and they are a natural control point to apply essential security functions such as schema enforcement. However, these platforms are not designed for security — and clever attackers continually probe for weaknesses. IDC's research noted growing success in these attack vectors, as 48.7% of organizations cited the ability for advanced threats to bypass protections included in integration platforms and API gateways as a top API security concern in 2024. In retail/hospitality, this rate rose to 60%.

Dedicated API security solutions are designed to address the security gaps left by WAF and API gateways. These specialized tools are necessary to gain complete inventory of API endpoints and visibility into traffic. They typically provide a range of protections including security testing, threat prevention, and basic bot controls (rate limiting), as well as defenses against API-specific threats. Advanced API security solutions offer API profiling and threat detection to monitor for abuse and fraud.

Q. How can gaining visibility into all API activity help differentiate patterns of abuse from legitimate user behavior?

A. The process of securing websites typically starts with the front end, where users directly interact with applications. These days, a website is made up of a maze of APIs operating behind the scenes to deliver innovative and engaging experiences. Unfortunately, these APIs can be easily discovered by cybermiscreants. Typically, the problem is rooted in ignorance about the API attack surface due to a combination of factors such as lack of documentation, changing development practices, or inadequate tooling. And while existing defenses can protect some API traffic, they may not see all API traffic.

In addition, attackers have started probing for the weaknesses in existing defenses. Static defenses remain a necessary first layer of protection against known attacks. However, smart attackers attempt to exploit the business logic behind APIs for illicit gain. For example, creating a second account to benefit from a discount for new customers may not violate a technical rule, but it would be a violation of the intended purpose of the incentive program. This attack is a manipulation of functionality that is technically operating correctly and therefore requires behavioral analytics to detect. Since attackers do not limit their efforts to known, protected APIs, insight into activity across all APIs is required to pinpoint behavior that veers into abuse.

Q. What types of problems are created by the growing reliance on and proliferation of APIs across the digital estate?

A. APIs are becoming widespread as businesses adopt microservice architecture to create dynamic applications. DevOps teams are under pressure to deliver new features and functionality to the market quickly. Aggressive development practices can lead to skipping security approvals, inadequate documentation, and abandoned/altered efforts. All these actions can lead to "shadow" or "zombie" APIs that are overlooked, forgotten, or otherwise unknown. In IDC's March 2024 *Web Application and Availability Protection Buyer Insights 2024 Survey,* 27.9% of organizations cited an incomplete inventory of APIs as a security concern for 2024; for retail/hospitality, this rate rose to 33.3%.

Security processes that fail to match the pace of development open the door for vulnerabilities to go undetected. The stakes escalate as businesses use APIs to connect not only customer-facing applications but also internal systems. As a result, a simple misconfiguration can expose sensitive data to opportunistic criminals.

Applications and APIs present a more lucrative target to cybercriminals attempting fraud, distributed denial-of-service (DDoS) attacks, and bot attacks as they proliferate and become more important to digital business. APIs must be defended against known general web exploits such as code injection and others represented on the OWASP Top 10 list. However, an array of API-specific threats have emerged as well. OWASP now publishes a list of top API-specific threats such as broken object–level authorization (BOLA) and unrestricted access to sensitive business flows. As a result, businesses must start their API security journey with complete visibility of all APIs, perform proactive testing, and implement active protections.

Q. B2C API security is a priority for retail, travel, and hospitality organizations. Why should security for B2B APIs from suppliers, partners, and resellers also be prioritized in 2024 — and beyond?

A. In IDC's *Web Application and Availability Protection Buyer Insights 2024 Survey,* 40% of retail and hospitality organizations cited a "lack of understanding of the scope/depth of the problem area" as a top challenge in API security compared with 29.5% of other respondents. A common pitfall in a typical API security strategy is to focus on customer-facing applications and APIs while overlooking APIs designed to support business partners. These APIs provide essential data in a readily available, compatible format that allows partner systems to operate with minimal friction. B2B APIs are essential for supporting supply chains and coordinating critical information such as pricing, inventory, and promotions.

However, B2B APIs can also be conduits for threats to propagate. Threat actors often use supply chain attacks targeting B2B APIs to evade the security systems protecting customer-facing applications and APIs. The vulnerability is a logic error on the part of defenders, similar to the challenge driving internal, east-west API risk — excessive implicit trust. The expectation that partner APIs are adequately secured, or that a partner would not willingly engage in a cyberattack, results in excessive levels of implicit trust and inadequate API security. Already, awareness about the risk related to business partner systems has grown, as 17% of businesses cited "business partner requirements" as a top 3 factor for investing in application security in 2023, according to IDC's *Web Application and Availability Protection Buyer Insights 2024 Survey*. However, businesses must be more proactive about addressing B2B API risks as threat actors continually probe for new opportunities to evade existing defenses.

Q. How do specialized API security controls fit into an organization's zero trust security strategy?

A. Zero trust is a modern approach to cybersecurity that promotes key principles of context-based policies, fine-grained access control, strong authentication, and continuous monitoring. Zero trust promotes least privileged access, ensuring that access is established only between an authorized user and the resources required for the task at hand rather than granting broad network access. API security fulfills key zero trust principles through numerous capabilities such as:

- Complete inventorying and continuous detection of new or unsanctioned APIs, combined with continuous monitoring to ensure least privilege access
- Enforcement of API authentication and authorization across all APIs, including internal, "private" APIs
- Continuous, active threat prevention, including the advanced security analytics and automation needed to catch the next generation of threats that target APIs

Although zero trust strategies have traditionally focused on private, internal applications, the reality is that many organizations increasingly rely on web applications and APIs for more than supporting customers' online experiences, including employee access and partner integrations. Zero trust strategies must start to factor in and extend to APIs, given their importance to internal communications between critical business systems.

While WAF is a valuable tool for monitoring and controlling ingress and egress traffic, API security solutions further provide insight and control over "east-west" traffic. This is a necessary capability to prevent the lateral movement between applications that attackers use to gain and maintain persistent unauthorized access to their victims' IT environments.

About the Analyst

Christopher Rodriguez, *Research Director, Security and Trust*

Christopher is a research director in IDC's Security and Trust research practice focused on the products designed to protect critical enterprise applications and infrastructure. IDC's Security and Trust research services to which Chris contributes include Active Application Security and Fraud, where he covers web application firewall, DDoS mitigation, bot management, and API security.

MESSAGE FROM THE SPONSOR

About Akamai API Security

While APIs are essential to drive growth for retail, travel and hospitality organizations, they also drive risk. Improving your security posture means reigning in API sprawl across the digital estate. With Akamai API Security commerce companies can:

- Discover enterprise-wide APIs — including shadow, legacy and rogue — for an accurate inventory
- Identify vulnerable APIs and misconfigurations, including all the OWASP API Top 10
- Detect threats such as excessive scraping, data exfiltration, account takeover, token reuse, and business logic abuse
- Improve compliance to help protect cardholder data required by the PCI DSS v4.0 global standard

To learn more about Akamai API security and detecting threats that others miss, click here.

IDC Custom Solutions

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
blogs.idc.com
www.idc.com