Akamai

ARE THE TOP THREE API SECURITY MYTHS PUTTING YOUR ORGANIZATION AT RISK?

API sprawl across commerce organizations is real.
Do you have a clear line of sight into API patterns of abuse?

Overcome the top three myths that may be holding your organization back from delivering safe, engaging digital experiences that drive business – and innovation – forward.

Myth 1

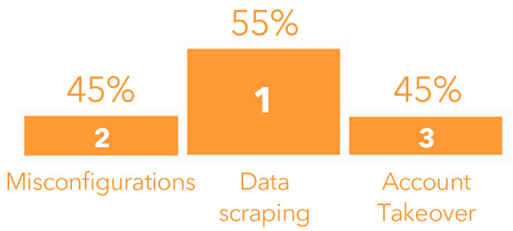
My API gateway is enough to stop API attacks and abuse

Although an API gateway can be effective for authentication, authorization, and even rate limiting of API requests, it falls short of providing the complete visibility and context needed to secure modern API environments. An API gateway – and signature-based defenses like web application firewalls (WAFs) and bot mitigation solutions – act as a proxy at the edge to help stop known bad. Outside of this functionality, they do little to provide defense in depth for keeping back-end API services protected.

The biggest risk? Users and partners who have been authenticated by these perimeter defenses are considered trusted – and assumed safe. Once an authenticated user is inside, it is extremely difficult to detect abuse or anomalous behavior occurring within the APIs – behavior such as excessive scraping, data exfiltration, token reuse, and forms of business logic manipulation. Other types of fraudulent activity include account takeover, which is a major challenge for hospitality, retail, and travel organizations that rely extensively on API integrations for their loyalty or rewards programs and reservation systems.

The bottom line: Just because users are authenticated, doesn't mean they should be trusted. Resource abuse can result from a legitimate API connection, so commerce organizations must be able to detect bad behavior, not just bad signatures.

The top 3 API security concerns among commerce executives:



(Gatepoint Research Pulse Report API Security Strategies, November 2023)

Myth 2

Prioritizing protection for my B2C APIs is enough to mitigate risk

No one will argue against prioritizing the security of revenue-generating business-to-consumer (B2C) APIs. After all, they are public facing and critical to enabling a carefully crafted digital experience across web and mobile applications. And because they are especially vulnerable to bot and other automated attacks, many organizations have deployed first-generation API defenses, bot mitigation, or WAF technologies to help manage access to B2C APIs. But did you know that B2C APIs represent the tip of the iceberg for overall API security needs? That's because significant risk lurks below the surface within an organization's business-to-business (B2B), or partner API, environment.

Many commerce organizations rely on business partners and suppliers to tightly integrate key operational functions through APIs that drive efficiency – and competitive advantage. However, B2B integrations create a complex web of API interconnectivity – and enable direct access to data – which can introduce risk if not properly managed. Although access to data and functionality may be perfectly legitimate for trusted partners, rogue partners and external threat actors could abuse or exploit B2B APIs with damaging consequences. Even worse, a trusted partner could be breached, leaving the organization to deal with the fallout from a ransomware or supply chain attack, which are the two top security concerns of commerce CISOs.

To fully mitigate the risk posed by B2B APIs, organizations need a solution that can monitor API activity coming from sources that were previously assumed safe – such as partners, resellers, and suppliers. Without a visible baseline for normal B2B API activity, it would be almost impossible to determine what abnormal – and therefore compromised – B2B API activity would look as it is infiltrating your organization.

The bottom line: Gaining visibility and a complete inventory of the B2C and B2B APIs exposed by an organization is critical to understanding and mitigating risk across the entire API estate.

85%

of commerce executives rely on their WAF for protection against API abuse – leaving them in a reactive position.

(Gatepoint Research Pulse Report API Security Strategies, November 2023)

Akamai

Myth 3

An advanced API security solution will add too much latency

For commerce organizations, API performance is pivotal to drive revenue and provide an optimal user experience. Slow response times can leave customers frustrated or (worse) drive them to the competition. Akamai's out-of-band API security solution minimizes latency and avoids single points of failure introduced by in-line technologies. Instead of sitting in path, our solution passively ingests copies of API data from an organization's existing in-line security tools or platforms, eliminating the need to reroute or proxy traffic. There are several approaches for conducting advanced behavioral analytics that produce context-rich insights that detect — and stop — API attacks and abuse.

One way of collecting data is through an Akamai custom integration with an existing platform — such as a customer's third-party API gateway, load balancer, proxy, content delivery network, Kubernetes ingress controller, or via packet mirroring. Akamai also offers a zero-touch deployment for customers who are already using the Akamai platform with security configurations so they can take immediate advantage of Akamai API Security. Regardless of the design implementation, sensitive data is anonymized using tokenization, and the API Security cloud operates on the tokenized version of that data to reduce privacy or compliance concerns. Organizations can be confident that the advanced detection and behavioral analytics performed within the API Security data lake are only on the tokenized data.

The bottom line: API security tools must not introduce unnecessary latency or create single points of failure. They also must be able to easily integrate with an organization's existing security ecosystem to reduce operational overhead and complexity for enterprise defenders.

The Akamai API Security software-as-a-service (SaaS)–based data lake is both PCI DSS and SOC 2 Type 2 compliant to meet the stringent customer privacy and security requirements of commerce organizations.

How Akamai can help

Akamai leverages behavioral-based API security protection to help close the visibility gap for commerce organizations. Akamai API Security complements Akamai's flagship web application and API protection (WAAP) offering, Akamai App & API Protector, which secures websites, applications, and APIs by blocking incoming malicious traffic in real time. Together, API Security and App & API Protector deliver the most comprehensive global protection by combining enterprise-wide visibility, behavioral analysis of API activity, and the prevention of attacks and abuse.

Learn how Akamai API Security can help you detect threats that other products miss.

"Akamai's ability to combine anomaly detection with threat hunting brings all of the insights we need to reduce risk together in one place, adding significant value to our organization."

– Yossi Gabay, Vice President of Information Systems, Dan Hotels