

Akamai API Security for Online Gaming

In modern gaming environments, every interaction is powered by APIs, from gameplay and in-game purchases to player authentication and partner integrations. As platforms grow more complex, driven by AI automation and real-time services, the volume and speed of these interactions continue to increase.

This shift is changing how attacks happen. Instead of breaking into systems, threat actors now operate within them, using legitimate API calls to manipulate outcomes, exploit workflows, and scale fraud. Without the ability to evaluate API behavior and usage patterns, organizations lack control over the interactions that directly impact revenue, gameplay integrity, and player trust.

How API sprawl expands the gaming attack surface

Online gaming platforms rely on APIs to power real-time gameplay, transactions, player authentication, and third-party integrations. As these environments scale, API ecosystems are growing quickly, often faster than security teams can track or govern.

This growth is happening alongside a measurable rise in application-layer and API attacks. In 2025, the average number of API attacks per enterprise **increased by 113%** year over year. Gaming platforms remain heavily targeted by application-layer attacks, particularly during peak events when performance, availability, and player experience are directly tied to revenue.

As API ecosystems expand through rapid feature releases, partner integrations, and live services, older endpoints often remain active and unmanaged. Organizations that lack a complete and accurate inventory of their APIs often can't identify which ones expose sensitive player data or financial logic. The result is a fragmented environment with limited visibility into how the connections are being used and where risk is concentrated.

For online gaming operators, that gap isn't just technical. APIs are directly tied to revenue, gameplay integrity, and player trust. Without a clear understanding of which APIs exist, how they behave, and which interactions carry financial or competitive risk, organizations are left with an expanding attack surface and limited ability to control it.

Why legacy security controls fail modern gaming APIs

Legacy security controls are designed to detect and block known threats at the edge. They focus on signatures, anomalies, and unauthorized access. That approach is effective against volumetric attacks and common exploits, but it breaks down in modern API environments. Attackers have taken advantage of this shift. Web-application attacks in the gaming industry **surged 94%** between Q1 2023 and Q1 2024, showing how aggressively attackers continue to target the digital systems behind player experiences.

Benefits for your business

Comprehensive API visibility

Continuously discover APIs, including shadow and unmanaged endpoints, and understand how they support gameplay, transactions, and integrations across your platform.

Risk-based prioritization

Identify which APIs expose sensitive data or critical functionality, and focus security efforts on the interactions that carry the highest financial and operational risk.

Early fraud detection

Detect bot activity, credential abuse, and gameplay manipulation within legitimate API traffic before it can scale into financial loss or player disruption.

Strong player trust

Detect manipulation of gameplay systems, and protect account integrity, helping maintain fair experiences and long-term player confidence in your platform.



In 2025, **61% of API attacks** involved unauthorized workflows and abnormal behavior, highlighting how often threat actors are targeting API behavior rather than simply trying to break through infrastructure. In gaming environments, this can include credential stuffing, and manipulation of gameplay systems — all executed through requests that may appear legitimate.

Industry guidance from the OWASP Foundation reinforces this trend, identifying business logic abuse and **broken authorization** as leading API risks. These attacks don't trigger traditional defenses because they use valid credentials and expected workflows.

The result is a combination of direct financial loss from degraded gameplay and erosion of player trust.

Without the ability to detect and mitigate abuse at the API level, these risks compound as platforms grow.

Gain control of API-driven gaming environments

Understanding the API environment is only the first step. Preventing abuse requires the ability to detect and respond to malicious activity. **Akamai API Security** helps protect gaming APIs against both known threats and emerging abuse patterns, delivering a framework for resiliency in the AI-driven gaming era.

It starts with discovery. Akamai identifies APIs across environments using both traffic analysis and code-based discovery, including known, shadow, and dormant endpoints. This creates a continuously updated inventory and provides visibility into how APIs are used, including which are tied to gameplay, transactions, and other high-risk interactions.

With that foundation, organizations can govern API risk based on business impact. Akamai helps security teams identify which APIs may expose sensitive data or critical functionality and map vulnerabilities to established frameworks such as OWASP. This allows teams to prioritize the interactions that matter most, rather than applying the same controls across all endpoints.

At the same time, Akamai uses behavioral analysis to identify patterns associated with fraud, automation, and abuse, even when requests appear legitimate.

Enabling secure growth in competitive gaming markets

As digital services continue to expand, APIs increasingly connect gameplay systems, partners, payment processors, and player-facing applications. Security teams need the ability to evaluate new integrations quickly without introducing new vulnerabilities.

Akamai API Security provides the visibility and protection required to support that growth. By understanding API behavior and detecting abuse early, organizations can adopt new technologies and AI-enhanced experiences while maintaining strong security governance.

This visibility also helps organizations understand how APIs are used to access and exchange player data, enabling stronger compliance and fair-play standards. In an industry where trust is the ultimate currency, this allows gaming operators to expand capabilities while protecting revenue, gameplay integrity, and long-term player confidence.

APIs run every bet, every match, and every moment of player trust on your platform. Attackers don't break in anymore — they game the system from the inside using normal traffic. Behavioral protection at the API level is what keeps gameplay fair and revenue secure.

The future of gaming security

Gaming platforms will continue scaling as live services, partner ecosystems, and AI-powered experiences become the new normal. APIs remain at the center of every real-time interaction.

Operators who can see their API landscape and identify and respond to abuse quickly will win on two fronts: protecting revenue and keeping players coming back.

Akamai API Security helps gaming organizations transform fragmented environments into secure, observable, and resilient platforms that are ready for the speed, scale, and threats of tomorrow.

Trusted by organizations across highly regulated, high-stakes sectors, Akamai delivers the scale, intelligence, and operational reliability needed to secure modern digital ecosystems.



Secure your gaming APIs

Identify APIs, prioritize high-risk interactions, and reduce abuse across your platform before it impacts revenue, gameplay integrity, or player trust.

To learn more, talk to an Akamai expert or **request a personalized demo** of Akamai API Security.