WEB SECURITY FOR ONLINE GAMING PLATFORMS

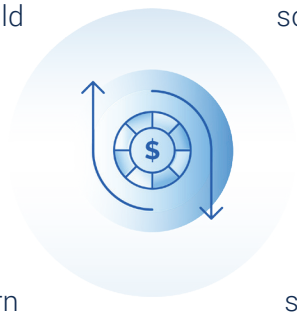
Gaming sites and applications are popular targets for cybercriminals. Reblaze provides robust web security for gaming sites, APIs, and applications. Each customer receives a dedicated Virtual Private Cloud, eliminating multi-tenancy vulnerabilities. Multivariate threat detection, behavioral analysis, and machine learning ensure accurate, adaptive security. All customers enjoy full protection, without having to purchase premium tiers or subscribe to additional services.

Reblaze is a comprehensive web security solution, providing a next-generation WAF, multi-layer DoS and DDoS protection, industry-leading bot management, precise ACL, real time reporting, full traffic transparency (even headers and payloads of individual HTTP requests), and more. Reblaze runs natively on the top-tier cloud platforms or in hybrid architectures, and is also available as a plugin in a service mesh.

UNIQUE SECURITY CHALLENGES

Reblaze provides robust protection against the threats faced by the online gaming industry, including:

Distributed Denial of Service: DDoS attacks on gaming platforms are rampant, including extortion attempts (sites are attacked until ransom demands are paid) and attacks from competitors to knock down a platform right before important events (when a rush of last-minute bets would otherwise be coming in). Reblaze provides DDoS mitigation to keep your platform available and performant to your customers, autoscaling bandwidth and other resources as needed to absorb even massive volumetric assaults.



ATO (Account Takeover) attacks: Modern threat actors use a variety of sophisticated tactics to compromise customer accounts. Reblaze protects against them all: it prevents credential theft, credential discovery, session attacks, the abuse of valid credentials, and other forms of ATO.

API Abuse: Cybercriminals are increasingly attacking APIs, since many security platforms have difficulty securing them. Reblaze provides complete protection for API endpoints: reverse-engineering prevention stops API attacks in their earliest stages, API schema enforcement rejects illegitimate requests, a client-side SDK hardens and authenticates mobile/native application traffic, and more.

Hostile Bots: Automated traffic can contain a variety of threats against gaming platforms, including vulnerability scans, breach attempts, injection attacks, and less hostile (but still unwelcome) traffic such as poker bots. Reblaze blocks unwanted bots using multivariate analysis, including whitelisting, blacklisting, anomaly detection, environmental verification, biometric behavioral analysis, and more.

Reblaze | Web Application & API Security

ABOUT REBLAZE

Reblaze is a cloud-based, fully managed protective shield for sites and web applications. The platform is a comprehensive web security solution, providing a next-gen WAF, DoS and DDoS protection, bot management, scraping prevention, CDN, load balancing, and more.

Reblaze offers a unique combination of benefits. Machine learning provides accurate, adaptive threat detection. Dedicated Virtual Private Clouds ensure maximum privacy. Top-tier infrastructure assures maximum performance. Fine-grained ACLs enable precise traffic regulation. An intuitive management console provides real-time traffic control. Full integration with top-tier cloud platforms provides a turn-key web security solution.

NEXT-GENERATION WAF/IPS

Reblaze defeats breach attempts, code and SQL injection, cross-site scripting, form manipulation, protocol exploits, session poisoning, malicious payloads, and other forms of attack.

DOS/DDOS PROTECTION

Reblaze is effective against DoS across layers and at all scales: from single malformed-packet DoS attempts to massive DDoS botnet assaults.

BOT MANAGEMENT

Reblaze prevents data theft & scraping, credential stuffing, brute force attacks, application abuse, vulnerability scanners, inventory denial, and more.

ATO PREVENTION

Reblaze prevents ATO (Account Takeover) attacks, and keeps user & customer accounts secure.

API SECURITY

Reblaze provides full protection for web services, microservices, mobile/native APIs, and more.

REAL TIME TRAFFIC CONTROL

Reblaze provides full real-time traffic analytics and statistics, even during large-scale attacks.

FULLY MANAGED SAAS

The platform is maintained remotely by Reblaze personnel. Your web security is always up-to-date.

MACHINE INTELLIGENCE

Reblaze uses Machine Learning to recognize new threats as they arise, and hardens itself against them.

DEPLOYS ANYWHERE

Run Reblaze as SaaS, or in your own cloud, container, hybrid/multi-environment, or service mesh.

ISO 27001 Certified | PCI DSS Certified

Reblaze's clouds are fully compliant with GDPR, SOC 1/ SSAE 16/ ISAE 3402, FISMA Moderate, ISO 27001, FIPS 140-2, HIPAA, and CSA. Reblaze Technologies is a PCI DSS Certified Level 1 Service Provider.