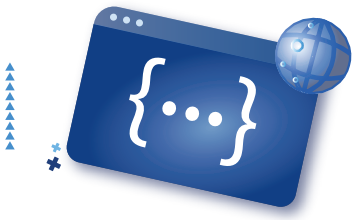

API SECURITY

Protecting an API is one of the most challenging tasks in cybersecurity. Today's threat environment includes a wide variety of methods for compromising systems via their APIs. Meanwhile, as microservices and mobile application APIs become more widely used, hackers are more motivated to attack them. Worst of all, many security solutions cannot fully protect APIs; for example, many solutions exclusively use headless browser detection to identify hostile bots, but for incoming API traffic, there is no browser environment to verify.

Reblaze protects APIs with its comprehensive suite of security technologies, including OWASP Top 10 (WAF) protection, multi-layer DDoS mitigation, bot management, precise ACL, real time reporting, rate limiting, and more.

As a fully managed solution, Reblaze is maintained for you by a team of security professionals; it is always up-to-date and always effective. Reblaze runs natively on the top-tier cloud platforms, and protects all modern architectures: any combination of private/public cloud, single/multi-cloud, hybrid, on-prem, containers, service meshes, and serverless.

PROTECTION FROM CYBERTHREATS

APIs can be vulnerable to a wide range of attacks. Reblaze excludes malicious traffic from endpoints:

DISTRIBUTED DENIAL OF SERVICE

Reblaze mitigates DDoS attacks, autoscaling resources to absorb volumetric assaults and keep your platform available and performant to your customers.

INJECTION ATTACKS

Reblaze includes a variety of protective mechanisms to sanitize and validate requests (headers & payloads), blocking attempted injection of SQL, code, commands, and more.

API-SPECIFIC ATTACKS

Reblaze includes specific protection for APIs: reverse-engineering prevention, schema enforcement, automated recognition of new functions, and more.

HOSTILE BOTS

Reblaze blocks input fuzzing, vulnerability scans, payment card fraud, inventory denial, scraping & data theft, content spam, application abuse, and more.

ACCOUNT TAKEOVERS

Reblaze defeats ATO attacks, including credential stuffing, brute-force credential discovery, compromise of user sessions, and more.

OTHER THREATS

Reblaze defeats XSS, form manipulation, out-of-limit arguments, malicious payloads, protocol exploits, cookie and session poisoning, and much more.

Reblaze

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.

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.

reblaze.com | contactus@reblaze.com | +1 408 907 7712