DDOS PROTECTION

Reblaze provides full-scope, multi-layer protection from DDoS attacks. It leverages underlying cloud infrastructure to defeat assaults on layers 3 and 4 (network and transport), while adding sophisticated detection and mitigation for layer 7 (application layer) attacks. Reblaze adjusts and scales its resource usage as needed, leveraging the capacity of the global cloud. Backend instances are created dynamically, to correctly handle current demand conditions.

Reblaze is effective against DoS/DDoS at all scales, from massive botnet assaults to single malformed-packet DoS attempts. It defends against the full spectrum of attack vectors, including protocol exploits, amplification and reflection, volumetric flooding, malicious inputs, resource depletion & exhaustion, slow-rate, application-layer vulnerabilities, DNS abuse, combination attacks, and more.

Unlike many web security solutions, Reblaze is not limited to geolocation and IP to identify hostile traffic sources. Modern threat actors often use cellular gateways, IoT botnets, and other resources to access millions of IP addresses, continually switching their IPs to defeat rate limits. Reblaze uses a variety of mechanisms that can identify, track, and block malicious requestors, even when they use a different IP for every request.

AUTOMATED & ALWAYS-ON DDOS DEFENSES

TOP-TIER INFRASTRUCTURE

Reblaze is integrated with the top-tier cloud providers, uses a distributed network multi-homed to achieve Internet access diversity, and leverages the near-inexhaustible capacity of the global cloud.

INSTANT AUTOSCALING

Reblaze can scale from a few concurrent connections up to millions, in a matter of seconds. It can handle bandwidth activity larger than the capacity of most ISPs. Backend instances are created dynamically in response to demand.

UNMATCHED VISIBILITY

Reblaze's dashboard provides a clear view of incoming traffic. Even in the midst of a massive volumetric attack, you can easily see the attack's scale, characteristics, attributes, targeted URLs, vectors, and more, all in real time.

MACHINE INTELLIGENCE

Along with using proven DDoS mitigation techniques such as syn cookies and connection limiting, Reblaze goes farther and uses adaptive and learning mechanisms to improve the accuracy of its traffic analysis.

SOPHISTICATED PROTECTION

Reblaze defeats even advanced threats such as yo-yo DDoS and other attacks that are designed to exploit the victim's cloud infrastructure, business processes, and other characteristics and practices.

DONE FOR YOU

Reblaze is maintained by a team of security professionals. Full management includes a 24×7 SOC that monitors your platform, notifies you about anomalies and incidents, and proactively addresses them immediately.

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