Reblaze | Cloud Native Web Application & API Protection (WAAP)

ATO PREVENTION

Account Takeovers (ATOs) are one of the broadest and most serious threats to web applications today. A successful ATO campaign can compromise a large number of accounts; this will anger customers and users, create a PR nightmare, trigger compliance audits, elicit punitive fines from privacy regulators, and more. Unfortunately, ATO attacks are one of the most difficult threats to defend against, because hackers have many different ways to wage them.

Reblaze includes ATO prevention as an important part of its all-in-one web security platform, protecting customer and user accounts against takeover attacks in all of their forms. Other features include OWASP Top 10 (WAF) protection, content filtering, multi-layer DDoS mitigation, bot management, precise ACL, real time reporting, and more, all in a fully managed solution. Reblaze runs natively on the top-tier cloud platforms, and also in containers, hybrid architectures, and service meshes.

PROTECTION FROM ACCOUNT TAKEOVERS

Reblaze excludes malicious traffic sources that attempt to compromise accounts:

CREDENTIAL THEFT

Reblaze prevents code and command injection, SQL injection, and other techniques for retrieving credential sets and other data from your backend.

CREDENTIAL STUFFING

Reblaze includes advanced rate limiting to defeat "stuffing": the mass submission of stolen credential sets into other web applications and APIs.

CREDENTIAL DISCOVERY

Reblaze blocks brute-force attempts to discover valid credentials, even when hackers attempt to evade detection (e.g., by rapidly rotating IPs/geolocations/etc.)

CREDENTIAL ABUSE

When threat actors steal credentials from elsewhere (other sites, social engineering, etc.), Reblaze's user/behavioral profiling detects the anomalous attempted usage.

SESSION ATTACKS

Reblaze shuts down attempts to compromise active user sessions via MitM attacks, XSS, CSRF, session side jacking, session fixation, and more.

OTHER THREATS

Reblaze prevents vulnerability scans, API and app abuse, form manipulation, out-of-limit arguments, malicious payloads, protocol exploits, and much more.

Reblaze | Cloud Native Web Application & API Protection (WAAP)

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.

reblaze.com | hello@reblaze.com | 408.907.7712

aws partner network | Google Cloud Partner | DigitalOcean Partner | Microsoft Partner