HOSTILE BOT MANAGEMENT

Bots are an integral part of modern web attacks: they perpetrate pen tests, scraping and data theft, brute-force login attempts, fraudulent account creation, and more. Reblaze includes robust bot management in its comprehensive web security platform. Hostile traffic is blocked in the cloud, before it reaches the protected APIs or applications. Web applications and API servers receive only legitimate requests, and remain secure, responsive, and performant.

Multidimensional and multilayer bot protection mechanisms are built into the core of Reblaze. The platform continuously analyzes each session's requests, packets, and bidirectional data transfer, to accurately identify the nature of each user. Reblaze inspects the full spectrum of layer 7 context, including headers, cookies, application flow, MIME types, and communication pace, combining these data points with additional parameters such as the user's source network, platform, behavior, and resource consumption. Most of this analysis is done server-side, ensuring that the protected client-side applications do not have their performance affected.

EXCLUDING UNWANTED BOTS

from your sites, services, web applications, and APIs

FLEXIBILITY AND CONTROL

Select the bots to allow (such as search engine spiders), and exclude the rest. Configure actions according to the bots' nature and sources: you can allow, block, issue custom responses, flag for dashboards and logs, and more.

GRANULAR ACLS

Fine-grained Access Control Lists eliminate many bots with minimal processing, before deep packet inspection begins. Requests can be filtered based on geolocation, network usage (VPN, proxy, TOR, cloud platform, etc.), and more.

THREAT INTELLIGENCE FEEDS

Another mechanism for low-overhead bot filtering, based on feeds containing current known sources of hostile automated traffic. Threat intelligence feeds are auto-updated regularly and frequently with the latest data.

CLIENT VERIFICATION

Reblaze detects and excludes headless browsers and emulators, going beyond legacy techniques such as agent validation and Javascript injection, and using a battery of advanced challenges to ensure users are legitimate.

BIOMETRIC BEHAVIORAL ANALYSIS

Reblaze uses Machine Learning to construct behavioral profiles, learning and understanding how legitimate users interact with protected apps and APIs. Anomalous requests and misbehaving traffic sources are flagged and blocked.

CONFIGURED BEHAVIORAL ENFORCEMENT

Along with its automated Behavioral Analysis, Reblaze also allows admins to define and configure a variety of additional behavioral enforcement mechanisms, including advanced rate limiting, session flow control, and 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.