Reblaze

Web Application & API Security

Keeping Bots Out

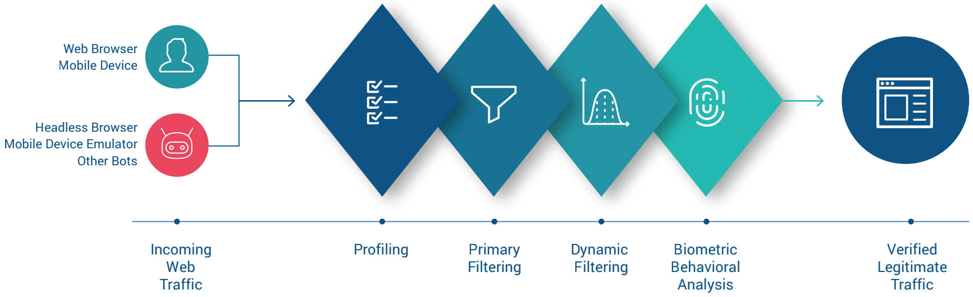
Bot Management Datasheet

Reblaze includes robust bot management in its comprehensive web security platform. Hostile traffic is blocked in the cloud, before it reaches the protected API or application. (Processing latency is minimal: ~0.5 ms.) Web applications and API servers receive only legitimate requests. They remain secure, responsive, and performant.

Exclude Hostile Bots From APIs and Web Applications

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.

Incoming web traffic is subjected to a series of increasingly stringent challenges. Failure of any challenge results in that requestor being immediately blocked.



Step 1a: Profiling ACLs

Reblaze offers the most precise ACL capabilities in the industry. Requests can be filtered based on geolocation, network usage (VPN, proxy, TOR, cloud platform, etc.), and more. Out of the box, Reblaze detects 75-80 percent of bot traffic. (The rate improves further once it is customized for the web apps and APIs it is protecting.) Reblaze's ACLs eliminate the majority of bots with minimal processing workload, before deep packet inspection begins.

Step 1b: Profiling Browser Environments

Incoming HTTP requests must pass a full stack of inspections and challenges in order

COMPLEX THREATS WITH SERIOUS CONSEQUENCES

Bots are an integral part of modern web attacks. Failing to fully control bots creates numerous vulnerabilities.

Site Downtime
when DDoS attacks exhaust its resources.

Data Theft
via scraper bots.

Site Breaches
via recon bots and pen tests.

Inventory Hoarding
prevents legitimate customers from buying.

Account Theft
via credential stuffing.

Degraded Experience
for customers when bots consume bandwidth and add latency.

TRADITIONAL BOT DETECTION IS NO LONGER EFFECTIVE

Most bot mitigation solutions use tools such as reCAPTCHA, IP checking, signature detection, and Javascript injection to identify and exclude non-human traffic.

These methods cannot detect the latest bots. CAPTCHA and reCAPTCHA challenges can be solved automatically more than half the time. Blacklists and rate limiting are evaded by rotating IP addresses. Signature detection is defeated by spoofing. Javascript injection can be processed correctly by modern bots.

to be validated. Then, headless browsers are detected. Reblaze goes beyond legacy techniques such as agent validation or Javascript injection. The platform subjects the requestor to a battery of advanced challenges, enabling Reblaze to detect even the most sophisticated headless environments.

Step 2: Primary Filtering

Primary traffic filtering begins with blacklisting, rate limiting, and signature detection. These legacy methods will not detect the newest bots, but they eliminate another tranche of older bots with minimal workload.

The platform then continues with more stringent tests. Data integrity is ensured by Layer 7 inspection, including JSON payloads. Reblaze includes a full positive security model, and ingests web and API schemas for enforcement. A full API provides programmatic control, allowing rapid schema additions or revisions in DevOps and DevSecOps environments.

Step 3: Dynamic Filtering

Reblaze blocks requestors that have anomalous usage patterns over time, by monitoring consumption of resources in terms of quantity, pace, rhythm, types & methods, etc.

Most platforms track requests only by IP address. Reblaze identifies attackers using multiple identifiers: IP, headers, cookies, even POST body arguments. Thus, Reblaze can detect and block abuse even when an attack is performed simultaneously across multiple addresses.

The platform's ruleset capabilities provide powerful, granular filtering. This includes:

- **Dynamic rate limiting**. (Example: too-frequent calls to a login URL.)
- **Network anomaly tracking**. (Example: excessive per-request data consumption in a specified time.)
- **Layer 7 anomaly detection**. (Example: number of requests per MIME type per minute.)

Step 4: Biometric Behavioral Analysis

For each application it protects, Reblaze builds a sophisticated, comprehensive behavioral profile of legitimate users.

It learns and understands how legitimate users interact with each app: device and browser statistics, typical analytics and metrics of each session, the interface events they usually generate (mouse clicks, screen taps, zooms, scrolls, etc.), and much more.

By definition, every hostile user (whether bot or human) must, at some point, deviate from legitimate user behavior. As soon as it does, Reblaze detects it and blocks it from further network access.

Additionally, Reblaze uses Machine Learning to learn and develop over time. Even as hackers develop new attack techniques, the platform becomes more sophisticated, always adapting to the ever-changing Internet environment.

Learn More

www.Reblaze.com. Contact hello@reblaze.com. International: +972 (73) 200-5200. U.S./Canada office: Reblaze Technologies, 940 Stewart Dr., Sunnyvale, CA 94085. **(408) 907-7712**.

OTHER BENEFITS

FAST DEPLOYMENT

There's nothing to install; a DNS change is all that's required.

FLEXIBILITY

Reblaze works for any web platform, and runs natively on popular cloud platforms such as AWS, Azure, and GCP.

PRECISION

You can define separate security policies for sites, clusters of sites, subnets, IP ranges, or even for individual URLs.

DEDICATED VPCs

Dedicated Virtual Private Clouds for each customer ensure near-zero latency, and eliminate the multi-tenancy vulnerabilities that other cloud solutions have.

COMPREHENSIVE

Reblaze includes a next-gen WAF, DDoS protection, advanced bot management, API security, a client-side SDK, and more.

MANAGED SERVICE

Reblaze is managed by a team of security experts. As new threats arise, Reblaze is updated immediately and automatically to defend against them.

COMPLIANT & 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 is a PCI DSS Certified Level 1 Service Provider.