Next-Gen Web Application Firewall

WAF/IPS Datasheet

A comprehensive, robust Web Application Firewall and Intrusion Prevention System (WAF/IPS) is one of the core technologies of the Reblaze web security platform. When you protect your web assets with Reblaze, you get an advanced WAF with a unique combination of benefits.

Reblaze protects against all the vulnerabilities in the OWASP Top 10, and many more. Its multivariate approach (explained below) is effective not only against known threat vectors, but also in blocking zero-day attacks.

Approach

The Reblaze WAF/IPS uses a multivariate, multidimensional approach with a variety of techniques to accurately identify and block malicious traffic. This includes Application Whitelisting, Blacklisting, Granular ACL, and Behavioral Analysis & Machine Learning.

Application Whitelisting

This is an automatic mechanism (which can be set in a supervised mode); it yields a fine-grained application rule-set that defines the allowed headers, HTTP methods, resources, content types, encoding, languages, forms, input fields, etc. within an application. Once this set is defined, it is virtually impossible for an attacker to inject code of any kind.

Blacklisting

Reblaze maintains a database of virtually all the web-related vulnerabilities ever published. As soon as a new threat is discovered, the database is updated with the solution that neutralizes it, and the changes are pushed immediately to all deployments of Reblaze, worldwide.

Granular ACL (Access Control Lists)

Reblaze's Web Application Firewall (WAF) works in conjunction with an unparalleled Access Control technology that filters traffic in three different forms and levels:

1. Static Lists
2. Semi-Dynamic
3. Dynamic

Static ACL

Static lists are straightforward. Access is allowed or denied according to IP address, ranges of IP addresses, organization, ISP, or geolocation.

(over, please)

PREVENTS:

- Code and SQL injection
- Cross-site scripting
- Form manipulation
- Protocol exploits
- Session tampering
- Malicious payloads

USES:

- Advanced bot detection
- Field policy enforcement
- HTTP error triggering
- ISON and XML schema validation
- Content evaluation
- Argument limitations
- RFC compliance
- Nested encoding detection
- Method filtering
- Signatures
- Payload inspection
- Consumption thresholds
- And more.

PROVIDES:

- Full support for DevSecOps. Reblaze automatically recognizes and adapts to new deployments, has a full API, and has other features for supporting agile workflows.
- Full API protection via its client-side SDK. Reblaze rejects automated usage, enforces schemas, blocks reverse-engineering attempts, reports changes in usage patterns, and more.
- Full reporting, streamed into virtually any destination.
- Full integration with top-tier cloud security frameworks such as AWS WAF and Google Cloud Armor.

Semi-Dynamic ACL

Semi-Dynamic ACLs are datasets which Reblaze updates periodically. These include lists such as TOR networks, anonymous proxies, VPN providers, and other managed lists such as cloud infrastructures and various blacklists. Reblaze refreshes these lists and updates the platform at various intervals. For example, TOR is updated every 30 minutes, while lists of cloud providers and proxy servers are updated every 24 hours.

Dynamic ACL

As the name suggests, Dynamic ACLs are rulesets and logic defined by the user and platform itself. Reblaze dynamically applies them automatically (per behavior and activity) with no need for user intervention. Examples of dynamic ACLs are Bots, Unknown Proxies, Brute Force, and others.

Reblaze's ACLs are easy to setup and activate, and they provide granular, separate security policies for the protected platform: from a globally applied ACL down to specific clusters of sites, or individual sites or applications, or even individual URLs.

The platform's combined ACL capabilities are among the most powerful in the industry. They can be fine-tuned to whatever degree of precision you need.

Behavioral Analysis and Machine Learning

Every Reblaze deployment anonymizes and streams its incoming traffic requests to a central Big Data trove that contains all requests that every deployment worldwide has ever received. Machine Learning continually analyzes this data, identifying new traffic and behavioral patterns (both legitimate and hostile), and updating all deployments appropriately. Thus, even as new web threats arise, Reblaze hardens itself against them.

Machine Learning is also applied on a local scale. For each application and API that 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 (mouse clicks, screen taps, zooms, scrolls, etc.) they usually generate, 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 access.

Conclusion

Reblaze's WAF is only one part of the complete platform (a comprehensive, dynamic, intelligent security and control solution for web applications and services). See the other Reblaze Data Sheets for more information on its other capabilities.

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.