A Superior Protective Shield

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 the most advanced WAF available today, with a unique combination of benefits.

Keeps Hackers Out

The Reblaze WAF (Web Application Firewall) provides a complete protective shield for websites, web based apps, and web services. Malicious traffic is blocked before it reaches your ISP, while legitimate requests pass through to your network as normal.

The Reblaze WAF is effective against the full spectrum of hacking and intrusion techniques: code and SQL injection, cross-site scripting, form manipulation, protocol exploits, cookie and session poisoning, malicious payloads, and much more.

Reblaze maintains a comprehensive database of known web-related vulnerabilities. As soon as a new threat is identified on the Internet, the database is immediately updated with the solution that neutralizes it.

Zero-day exploits are defeated by denying all traffic which does not conform to a strict, fine-grained set of application specifications. This makes it virtually impossible for hackers or intruders to inject code of any kind. Reblaze also uses advanced behavioral analysis to detect and deny network reconnaisance, pen tests, reverse-engineering attempts on pages or application protocols, and other probing.

As a cloud-based service, Reblaze provides superior WAF protection when compared to previous-generation technologies. (See “How It Works” on the next page for more.)

The Superior Cloud Solution

Reblaze gives you many advantages over competing “cloud” security products. For example, Reblaze provides the most powerful ACL capabilities in the industry. You can allow or deny access from specific countries, states, cities, networks, companies, anonymizer networks, cloud and data-center networks, platforms, and more.

Additionally, other cloud solutions have a serious flaw; they require you to share resources with their other users. As a result, your site’s availability and/or security can be compromised by attacks on those other users.

Conversely, Reblaze deploys an exclusive Virtual Private Cloud (VPC) around your network. You get an entire dedicated stack (including DNS servers, load balancers, logs, database, etc.) for your use alone. As a result, your site remains immune to whatever attacks might be occurring elsewhere.

PROTECTING YOUR WEB ASSETS

To accurately identify hostile traffic, Reblaze uses a wide variety of analysis methods, including:

- Threat blacklisting
- Bot identification algorithms
- Header, form, and field policy enforcement
- HTTP error triggering
- Resource consumption thresholds
- Schema validation
- Content evaluation
- Minefields and honeypots
- Signatures
- IP address allocation maps
- TOR network mapping
- Progressive challenge mechanisms
- Argument limitations
- RFC compliance
- Nested encoding detection
- Method filtering
- Payload inspection
- Behavioral analysis
- And much more.

As traffic patterns change, Reblaze learns and adapts. This ensures that diagnostic analyses remain accurate, with a near-zero rate of false positives.

As new attack techniques arise, Reblaze is upgraded immediately to defeat them. The result: your protection is always on, always up-to-date, and always effective.

Reblaze is a PCI DSS Certified Level 1 Service Provider.

How It Works

Reblaze is always on, and always protecting your web assets. Attack detection and mitigation occur 24/7, automatically.

All incoming traffic passes through your Virtual Private Cloud for scrubbing, before being allowed to access your network. Dynamic DNS allocation prevents attackers from reaching (or even finding) the targeted data centers. Meanwhile, legitimate traffic is allowed through as usual, with little if any additional latency. Indeed, most Reblaze-shielded sites are more responsive to their users than they were previously, thanks to Reblaze's global load balancing and CDN integration.

Network reconnaissance attempts are automatically detected and denied. This mitigates many attacks before they even begin.

Multidimensional analysis accurately identifies hostile traffic. Reblaze analyzes multiple traffic dimensions, including content, rate (the throughput of packets, requests, messages, etc.), and ratio (a per-protocol assessment of messages, packets, requests, and data types). Malicious packets are precisely identified, with a minimum of false positives.

Hostile traffic is blocked, and its source is banned. Reblaze tracks the amount of hostile traffic originating from each IP address. When an IP exceeds specified thresholds, that address is banned as a traffic source for a configurable amount of time. Reblaze does this automatically, with no user intervention required.

Bandwidth scales automatically as needed. As resource requirements increase, Reblaze automatically brings more bandwidth online. Reblaze can access higher levels of bandwidth than even many ISPs, limited only by the capacity of the global cloud.

Reblaze learns and adapts to changing traffic patterns. This maintains a high level of accuracy for attack detection. In addition, this saves the user from the usual overhead and ongoing manual fine-tuning required by standard security products.

Immediate upgrades protect against new forms of attack. Your Reblaze deployment is maintained and upgraded automatically by Reblaze's team of security experts. Even as new attack vectors arise, Reblaze is updated immediately. You always have the latest protection against the full breadth of Internet threats.

About Reblaze

Reblaze is the comprehensive, cloud-based, robust protective shield for your web assets. Core technologies include: WAF/IPS, Multilayer DoS/DDoS protection (network, transport, and application), Anti-Scraping, High-level ACL, Advanced Human Detection and Bot Mitigation, Advanced Management Console, and Real-time Traffic Analysis. Added value services include: Layer 7 Load Balancing, Global Secured CDN, and a complete DNS solution. For more information, visit www.Reblaze.com. Contact Reblaze via email (info@reblaze.com) or by phone: International +972 (73) 252-7007, U.S./Canada (786) 509-6401.

OTHER BENEFITS

FAST DEPLOYMENT

Shielding your network with Reblaze requires only a simple DNS change. As propagation occurs, any ongoing attacks are shut down immediately.

FLEXIBILITY

Reblaze works for any web platform, at any scale. It also integrates seamlessly with popular cloud services such as Amazon, Microsoft, and Google.

PRECISION

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

RISK-FREE

Reblaze can act as an additional layer of protection to existing solutions.

COMPREHENSIVE

Reblaze is effective against all forms of Internet attack. Organizations with web assets no longer need to assemble a solution from multiple products and vendors; Reblaze does it all.

RELIABLE

The SLA includes 24/7 support and 99.999% uptime.

COMPLIANT & CERTIFIED

Reblaze's clouds are fully compliant with SOC 1/SSAE 16/ ISAE 3402, FISMA Moderate, PCI DSS Level 1, ISO 27001, FIPS 140-2, HIPAA, and CSA. Reblaze is a PCI DSS Certified Level 1 Service Provider.