Comprehensive DDoS Protection

DoS/DDoS Datasheet

Multi-layer DoS/DDoS protection is a core technology of the Reblaze web security platform. Reblaze intercepts and mitigates threats far away from your data center, ensuring that your site continues to operate at high performance levels. Your users won't even notice that an attack is occurring.

Defeats All Forms of DoS/DDoS

Reblaze protects your web assets from DoS/DDoS across layers 3, 4, and 7 (network, transport, and application). It is effective at all scales, from massive DDoS botnet assaults to single malformed-packet DoS attempts. It defends against the full spectrum of attack vectors, including protocol exploits, amplification and reflection attacks, volumetric flooding, malicious inputs, resource depletion/exhaustion, application-layer vulnerabilities, and more.

Automated Protection

DoS/DDoS detection and mitigation are always on, and occur automatically. Bandwidth scales dynamically as needed, with no user intervention required. Reblaze can access near-inexhaustible bandwidth, limited only by the capacity of the global cloud.

The Reblaze Advantage

Reblaze offers many advantages over previous-generation security solutions.

- Reblaze is upgraded automatically as new threats arise. Your protection is always up-to-date, and always effective.
- Reblaze scrubs your traffic before it even reaches your ISP. Your Internet pipe and data center remain unaffected by DoS/DDoS attacks.
- Reblaze protects against all forms of Internet threats. Also, as an integrated platform, Reblaze can perform more sophisticated traffic analyses than those available from single-purpose security products.

The Superior Cloud Solution

Many competing "cloud" security products offer some of the benefits described above. Unfortunately, these other 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.

SCOPE

Reblaze is effective against all forms of DoS/DDoS, including:

- Chernobyl packets
- Christmas trees
- Connection flooding
- DNS exploits
- DNS flooding
- Fraggle
- HTTP exploits (GET, POST, etc.)
- HTTP flooding
- ICMP
- IGMP
- Malformed/fragmentary packets
- NTP exploits
- NTP flooding
- Ping flooding
- Ping of Death
- ReDOS
- RUDY
- Shrew
- Slow Read
- SlowDroid
- Slowloris
- Smurf
- Spoofing
- TCP exploits (ACK, ACK+PSH, FIN, LAND, RESET, SYN, SYN-ACK, etc.)
- Teardrop
- Twinge
- UDP exploits
- UDP flooding
- XDoS/XMLDoS
- XML Bombs
- Combination attacks, e.g. Mixed SYN+UDP
- Attacks against specific OS vulnerabilities
- Attacks against specific server vulnerabilities
- Attacks against specific app vulnerabilities

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 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.