Comprehensive DDoS Protection

DoS/DDoS Datasheet

Reblaze's DoS/DDoS protection provides multiple benefits: full-scope protection, high levels of accuracy and performance, ease of use, top-tier infrastructure, and autoscaling.

Full-Scope Protection

Reblaze is effective against DoS/DDoS 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.

Reblaze provides full-scope DoS and DDoS protection, defeating attacks across layers 3, 4, and 7 (network, transport, and application). Unlike on-premise solutions, Reblaze blocks attacks in the cloud, before they can affect the incoming Internet pipe.

Many security providers offer layer-3 and (to a lesser extent) layer-4 protection. But even many "DDoS solutions" do not fully protect layer-7. And among those providers which do claim to address this layer, many only protect against the simplest attack types (such as generic HTTP DDoS techniques).

Reblaze is one of the few solutions which can protect against even the most challenging DoS/DDoS attacks: those crafted to exploit vulnerabilities in a specific application or API.

Accuracy and Performance

Along with using proven DDoS mitigation techniques such as syn cookies and connection limiting, Reblaze goes farther and uses adaptive and learning mechanisms to improve the accuracy of its traffic analysis.

Reblaze adapts to traffic characteristics in real time, automatically setting dynamic thresholds according to traffic parameters such as rate and throughput (of packets, requests, messages, HTTP requests, DNS queries per second, etc.), ratios (per protocol for messages, packets, requests, and data types), and more.

Unlike most security solutions, Reblaze's decision-making process is not limited to whatever is currently happening in the traffic stream. The platform uses automated learning processes to continually adapt, not only to variations within a current attack but also to the ever-changing threat environment of the Internet overall. Pattern recognition and behavioral analysis allow Reblaze to successfully identify attacks in their earliest stages, even from traffic flow that otherwise would seem benign. The platform's analysis is fast, accurate, generates minimal false positives, and above all,

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

removes the usual user overhead (of maintenance and ongoing manual fine tuning) required by standard DDoS mitigation products.

Ease of Use

DoS/DDoS protection is an integral part of Reblaze. It is always on, with no need for the user to explicitly invoke it if an attack is suspected.

Reblaze always provides a clear, real-time picture of your traffic. With the click of a mouse, you can switch between data displays of incoming traffic, showing geolocation, source, disposition, targeted URLs, signatures, and more. You can view all stats and analytics over a specific period of time, or drill all the way down into individual requests.

Even in the midst of a massive volumetric attack, you can easily see the attack's scale, characteristics, attributes, and vectors.

Reblaze provides fully automated DoS/DDoS protection. Nevertheless, if additional manual intervention should ever become necessary, you always know exactly what's happening within your applications and APIs, so you can react appropriately.

Infrastructure

Reblaze is integrated with the top-tier cloud providers (AWS, Azure, and GCP. These platforms have invested a combined $75 billion into their infrastructure in recent years). Google Cloud alone has 10x the bandwidth capacity of the entire Internet. Reblaze can run on any of the top-tiers, or on multiple providers simultaneously.

Reblaze makes use of a distributed network, multi-homed to achieve Internet access diversity. The platform scales its resources as needed, leveraging the near-inexhaustible capacity of the global cloud.

Autoscaling

Reblaze can scale from a few concurrent connections up to millions, in a matter of seconds. The platform can handle bandwidth activity larger than the capacity of most ISPs.

Reblaze adjusts and scales its resource usage as needed, leveraging the capacity of the global cloud. Backend instances are created dynamically, to correctly handle current demand conditions.

This allows the platform to handle even massive DDoS assaults, with no impact to the protected network. Scaling occurs automatically, with no user action required.

As with other aspects of Reblaze, load balancing and autoscaling are fully transparent. The Reblaze Console always shows the current deployment and usage of resources, and manual control is available if desired.

Conclusion

DDoS protection is only one part of the Reblaze 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.