Reblaze

Web Application & API Security

Comprehensive. Intelligent. Automated. Effective.

COMPREHENSIVE PROTECTION

NEXT-GEN WAF

Reblaze defeats SQL injection, XSS, form manipulation, protocol exploits, session poisoning, malicious payloads, and other attacks.

DDOS PROTECTION

The platform provides full multi-layer DoS/DDoS protection, blocking attack traffic before it can affect your incoming Internet pipe.

BOT MANAGEMENT

Advanced human behavioral analysis and bot detection algorithms allow you to exclude unwanted bots.

MACHINE INTELLIGENCE

Reblaze continually analyzes global traffic data, using machine learning to identify and harden itself against new attack vectors.

FULLY MANAGED

The platform is maintained remotely by Reblaze personnel. Your security is always up-to-date and always effective.

CDN & LOAD BALANCING

Global CDN integration and load balancing increase your site's availability and accelerate its perceived responsiveness to your users.

AUTOSCALING

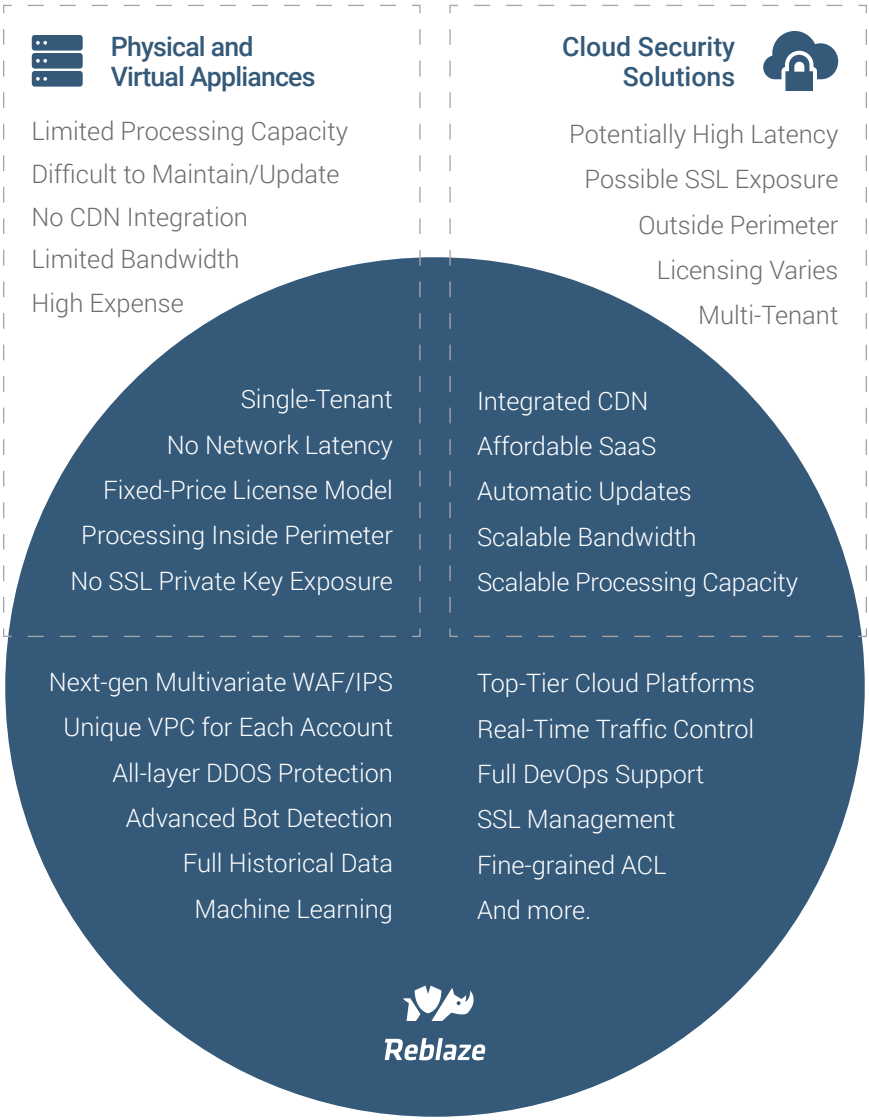
As traffic demands change, Reblaze scales resources automatically, immediately (with no pre-warming required), and efficiently.

REAL-TIME CONTROL

Full details of all requests are available, both in real time and in historical logs. You always know what's happening within your site.

THE ADVANTAGES

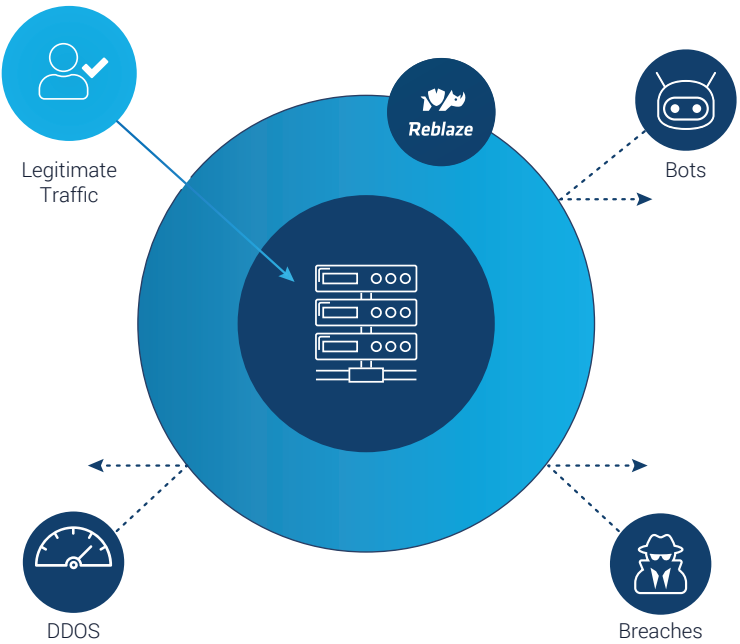
of appliances and cloud solutions, without their drawbacks.



UNIQUE PRIVATE CLOUDS

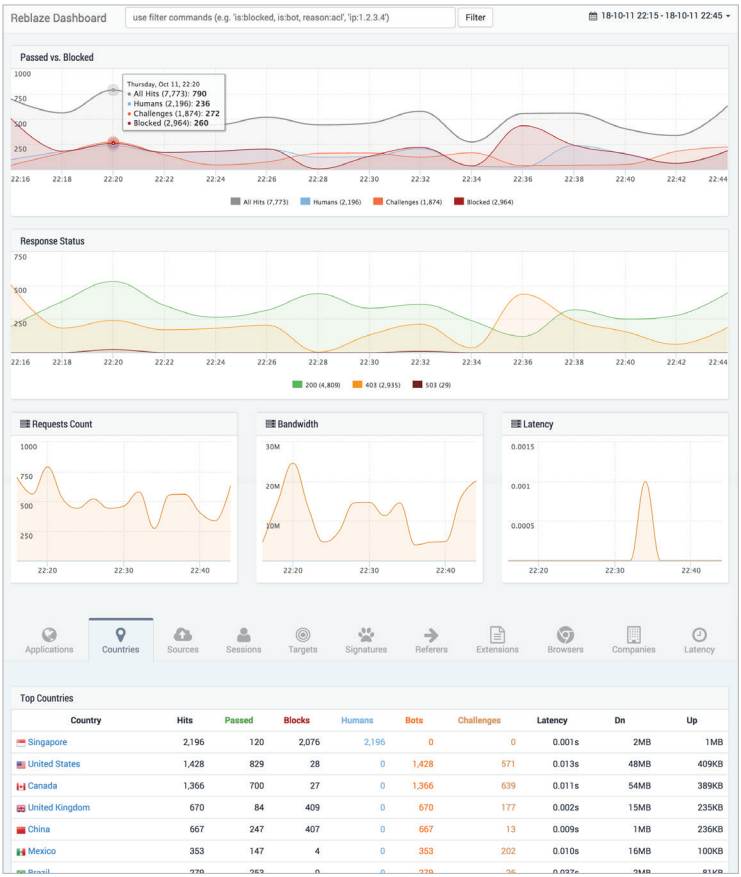
Reblaze deploys a unique VPC (Virtual Private Cloud) for each customer: an entire dedicated stack for each protected web platform, geolocated immediately in front of it.

- All incoming traffic is routed through the VPC and scrubbed as it passes through. Latency is negligible (generally 1.5 milliseconds or less).
- Hostile traffic is blocked before it reaches the protected network. Legitimate traffic has normal access.
- Attackers cannot reach the targeted web platform.
- Bandwidth, instance groups, and other resources scale automatically as needed, limited only by the capacity of the global cloud.



REAL TIME TRAFFIC CONTROL

With Reblaze, you can watch and control your traffic in real time. The Dashboard provides an intuitive overview of all your traffic (whether legitimate and hostile), with the ability to quickly drill down into individual requests to see their full details (headers and payloads). Even during DDoS attacks, you always know what's happening within your site.



MULTIVARIATE WAF

Provides next-generation threat detection

Reblaze's WAF is effective against the full spectrum of intrusion techniques:

- Code and SQL injection
- Cross-site scripting
- Form manipulation
- Protocol exploits
- Cookie and session poisoning
- Malicious payloads
- And more.

The Reblaze WAF detects malicious traffic using a multivariate approach, including not only signature detection but also:

- Content evaluation
- Field policy enforcement
- HTTP error triggering
- ISON/XML schema validation
- Argument limitation
- RFC compliance
- Nested encoding detection
- Blacklisting
- Method filtering
- Consumption thresholds
- Payload inspection
- And more.

DDOS PROTECTION

Adaptive shielding across all layers

Reblaze includes full-spectrum protection against DoS/DDoS, defeating attacks across network, transport, and application layers. Resources scale automatically as needed.

The platform is effective at all scales, from single malformed-packet DoS attempts to massive DDoS botnet assaults. It defends against the full spectrum of attack vectors:

- Protocol exploits
- Amplification and reflection attacks
- Volumetric flooding
- Malicious inputs
- Resource depletion & exhaustion
- Application-layer vulnerabilities
- And more.

Reblaze is uniquely adaptive. Its Machine Learning capabilities provide optimized Layer 7 protection, customized for each one of your web applications. The platform continually conforms and reshapes itself to your specific needs. As your web apps evolve, so does Reblaze.

BOT MANAGEMENT

With advanced biometric detection

Bots are used for a variety of modern web attacks:

- Application-layer DoS and DDoS
- Credential stuffing
- Dictionary attacks
- Vulnerability scanners
- Scraping & data theft
- And more.

Modern bots have become quite sophisticated; many can credibly mimic human visitors, sending keystrokes, mouse movements, and click events to the targeted site. Few web security products have kept up with these advances.

Reblaze's industry-leading biometric bot detection goes far beyond traditional methods such as browser authentication. The platform uses Machine Learning to construct and maintain behavioral profiles of legitimate human visitors. For each user, Reblaze continually gathers and analyzes stats such as client-side I/O events, triggered by the user's keyboard, mouse, scroll, touch, zoom, device orientation, movements, and more. Therefore, Reblaze understands how actual humans interact with the web apps it is protecting. Continuous multivariate analysis verifies that each user is indeed a legitimate human.

INTEGRATES WITH YOUR SIEM/SOC/COMMAND CENTER

Reblaze works seamlessly with your existing reporting and response solutions. All incidents, metrics, and other data are instantly passed through to your security platforms, integrated into the business processes and policies you already have in place.

Your SIEM/SOC

Reblaze integrates fully with a wide range of SIEM and SOC solutions, including ArcSight, RSA, IBM, and Splunk.

Azure and Google command centers

Reblaze integrates with cloud command and control solutions such as Azure Security Center and Google Cloud Security Command Center. Traffic data and events from Reblaze are streamed into these platforms, with the ability to quickly drill down and display granular details.

Other security platforms

If you use a popular security product, it is probably already supported. If not, an engineering team from Reblaze will assist you in integrating it. Reblaze is designed for flexibility and interoperability, to work well with the portals and platforms that you are already using.

CDN INTEGRATION

Reblaze integrates seamlessly with virtually every CDN provider.
Or use Reblaze's out-of-the-box CDN solution shown here.

North America

Ashburn
Atlanta
Boston
Charleston
Chicago
Council Bluffs
Dallas
Denver
Hayward
Hillsboro
Houston
Jacksonville
Los Angeles
Miami
Minneapolis
Newark
New York City
Palo Alto
Philadelphia
Phoenix
San Jose
Seattle
San Francisco
South Bend
The Dalles
Washington D.C.
Montréal
Toronto
Mexico City
Puebla
Querétaro

South America

Barranquilla
Bogotá
Buenos Aires
Lima
Medellin
Quito
Rio de Janeiro
São Paulo
Santiago
Valparaiso

Europe

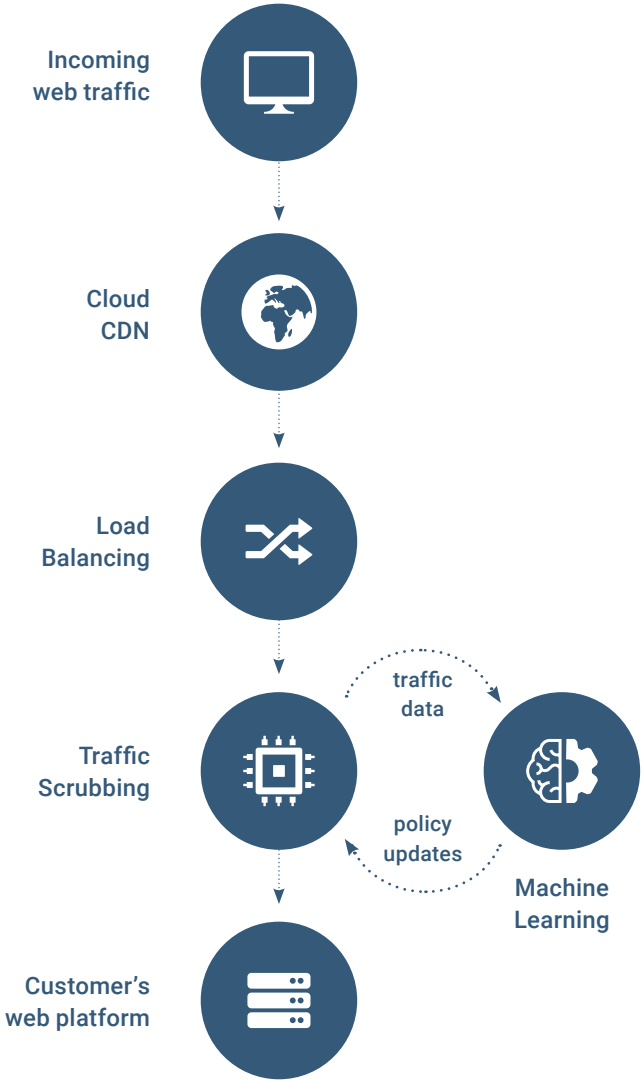
Amsterdam
Berlin
Bucharest
Budapest
Copenhagen
Dublin
Frankfurt
Groningen
Hamburg
Hamina
Helsinki
Kiev
Lisbon
London
Madrid
Manchester
Marseille
Milan
Moscow
Munich
Oslo
Palermo
Paris
Prague
Riga
Rome
Sofia
St. Ghislain
St. Petersburg
Stockholm
Vienna
Warsaw
Zagreb
Zurich

57
Tbps Capacity

525
Points of Presence

3.1K+
Interconnects

ARCHITECTURE

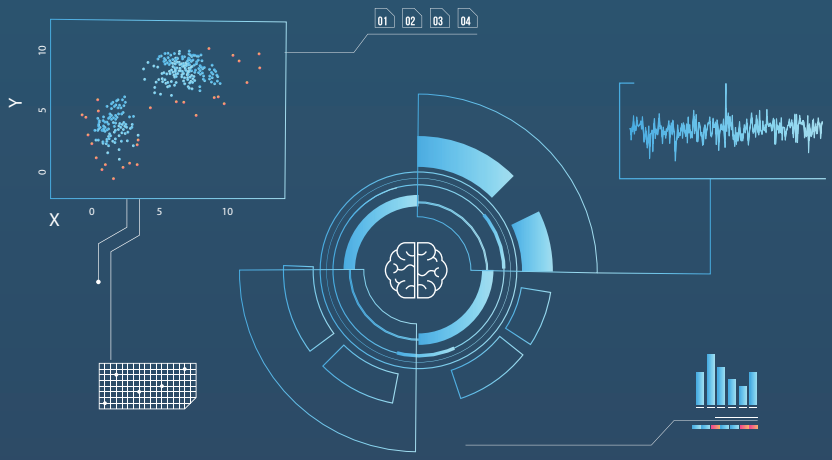


MACHINE LEARNING

Continual Analysis. Continual Adaptation.

Reblaze continually collects and analyzes global traffic data, applying machine learning to identify trends in traffic patterns, user behavior, etc. The platform reshapes its security posture in response to current conditions, ensuring maximum accuracy in threat detection. As soon as a new attack pattern is encountered, Reblaze learns from it, adapts to it, and immediately updates all worldwide deployments, hardening them against it.

Even as new web threats arise, Reblaze remains effective.



DYNAMIC AND ADAPTIVE THREAT IDENTIFICATION

AUTOMATED SECURITY

Autonomous:

Automatic cloud load-balancing distributes loads globally as needed. When an attack occurs, Reblaze blocks the hostile traffic automatically, immediately, and appropriately. Resources autoscale as needed, with no pre-warming required.

Fully managed service:

Reblaze is managed and kept up-to-date remotely by a team of security experts. As new threats are identified, all global Reblaze deployments are upgraded immediately and automatically to defend against them. You always have the latest protection.

"The reason I chose Reblaze is because I do no work at all. That's very important to me. It just works."

Bonnie Grossman, CTO, AllJobs

"Reblaze allows us to do more than just block attackers. Now we're converting data scrapers into paying customers."

Livne Niv, Head of Operations and IT, mySupermarket

"Reblaze was the only solution that could support us at a reasonable price."

Aviram Radai, Sr. Director of Engineering, Samanage

TOP-TIER CLOUDS

Reblaze is fully integrated with the top-tier cloud providers: AWS, Azure, and Google. (Other cloud solutions use self-owned infrastructure, which can't match the top-tiers for performance and reliability.)

AWS WAF • AZURE WAF GOOGLE CLOUD ARMOR

Google, Microsoft, and Amazon all provide cloud security frameworks: GCP Cloud Armor, Azure WAF, and AWS WAF. These require user intervention to define their security rules and keep them updated. This can be very challenging, especially under the stress of an attack.

Although Reblaze is a full-featured cloud security solution, some customers prefer to use these policy enforcement modules from their cloud providers. Reblaze's next-generation threat detection is fully integrated with all of these platforms, converting them into autonomous systems which react immediately to every type of attack. Reblaze identifies hostile traffic, and the cloud providers immediately block it at the edges.

FULL DEVOPS SUPPORT

Most WAFs hinder DevOps, but Reblaze supports it. A full API allows you to configure security profiles programmatically, so that every app or service you deploy or modify is protected immediately.

MAXIMUM PRIVACY

Reblaze scrubs your traffic exclusively within *your* clouds: the clouds you already trust for your other business processes. (Other cloud solutions decrypt, and usually store, your data on their servers.)

UNPARALLELED ACL

Reblaze's fine-grained ACL capabilities allow you to precisely control your traffic. You can allow or exclude traffic by IP address, URL, organization, user behavior, geolocation (country, state, and/or city), platform (cloud, anonymous proxies, TOR, etc.), data payload, and more.

"Because Reblaze deploys a dedicated cloud for each data center, if one data center suffered a massive attack, it wouldn't affect the others. But I have no experience with that, because I've never seen any attacks getting through Reblaze to any of my data centers."

Roger Tan, Systems Manager, Reebonz

OUR CUSTOMERS

200+
Global customers

25K+
Web applications

3B+
HTTP(S) transactions daily

Many Verticals

Including airlines and other transportation, e-ticketing, hospitality, government, defense, aerospace, ecommerce, technology, gaming, banking, finance and payments, healthcare, SaaS, and more.

COMPLIANCE

Reblaze's clouds are fully compliant with GDPR, SOC 1/SSAE 16/ISAE 3402, FISMA Moderate, PCI DSS, ISO 27001, FIPS 140-2, HIPAA, CSA (Cloud Security Alliance), and other standards and certifications.

CERTIFICATIONS

Reblaze Technologies is ISO 27001 Certified, AICPA SOC 2 Certified, and is a PCI DSS Certified Level 1 and Level 2 Service Provider.

PARTNERSHIPS

aws partner network
Advanced Technology Partner

Google Cloud Partner

Microsoft Partner

OUR LOCATIONS

TRY REBLAZE RISK-FREE.

- No contract. No obligation.
- No installation: As a cloud platform, Reblaze deploys in minutes. Only a DNS change is required.
- No risk: You can add Reblaze to your existing security in "report only" mode. (Reblaze will not filter any traffic; it will merely report on what it would have filtered in active mode.)
- Guarantee: Try Reblaze for 30 days. If you aren't delighted with the results, your account will be cancelled and you'll owe nothing.
- Get started: email us at **hello@reblaze.com**, or call our U.S. office at **(408) 907-7712**.

Reblaze

940 Stewart Dr, Sunnyvale CA 94085