REBLAZE TECHNOLOGIES LTD.

A New Approach to Web Security

Next-generation protection for web apps, services, and sites

Tzury Bar Yochay
Founder and CTO
Reblaze Technologies

Reblaze

Reblaze is a new approach to web security. As an intelligent, cloud-based platform, Reblaze has many advantages—not only over legacy technologies such as appliances, but also over other cloud security platforms as well.

A WAF is not enough

Other security solutions are passive filters, built on some variation of the following approach: a WAF sits in front of the protected network, receiving a continual stream of traffic. For each incoming packet, the WAF has only a few milliseconds to decide if it should be blocked or allowed through. Signature detection is the primary technique used.

Incoming requests are received and processed one-by-one as they arrive. No broader context is available for the threat-identification process, although even a single incorrect decision could have significant implications for the targeted organization. Worse, the WAF must do this in the midst of an increasingly hostile Internet. State-sponsored DDoS attackers, Russian and Eastern European organized-crime rings, South American financial cybercriminals, and other threat actors are constantly mounting assaults from around the world. And each WAF must try to defeat them all, despite being outgunned, isolated, and alone. Such is the situation for almost every security solution today.

But Reblaze is different.

A New Approach

Consider the threat environment on today's Internet. Now imagine the ideal defense.

The ideal security solution would be comprehensive. It would protect against all forms of web threats: intrusions and breaches, DoS and DDoS, bots and scrapers, and more.

It would use next-generation threat identification, far beyond merely detecting known signatures within incoming requests. In fact, it wouldn't even be limited to the requests themselves. This solution would understand that requests which are benign in themselves can nevertheless be part of a larger attack. So it would not merely block specific requests—it would block all incoming traffic from users who have hostile intent.

How would user intent be evaluated? The security solution would maintain a full history of all the traffic it had ever received. Thus, new requests would not be analyzed in isolation, but all would be understood within the broader context of everything that user had ever done, compared to all traffic received to date.

Continual analysis would reveal if attack patterns were developing within each user's behavior. Moreover, user intent would not be evaluated as a binary allow/block decision. Instead, users with a higher number of potentially questionable characteristics (for example, use of an anonymizing network) would receive more scrutiny, be treated with more suspicion, and be cut off from network access more quickly.

Nor would this process be confined to each local network. All global deployments of this solution would add to, and read from, a common Big Data trove of historical data. Each current user (encountered by any deployment) would be analyzed and compared to all previous users (of all deployments), whether legitimate or illegitimate.

Further, built-in machine learning would ensure that over time, the security solution would grow ever-more sophisticated in its abilities to identify and block illegitimate users.

Thus, the solution would not be dependent on recognizing historical attack signatures. Instead, as it continued to receive and analyze traffic, it would always be learning and adapting to current conditions. Even as new threats developed, the solution would remain effective against them.

Also, as machine intelligence identified new traffic patterns, they would be communicated among all global deployments. Thus, any individual deployment would not be limited to what it had encountered locally: instead, it would remember everything ever seen by the entire global network.

Therefore, a deployment of this solution would not be an isolated element on the Internet, attempting to fight global threats by itself. Instead, each would be a node in a worldwide system—a ***globally distributed machine-intelligent security network*** that would:

- Continually monitor and analyze traffic, from all around the world.
- Learn from and adapt to new traffic patterns as soon as they were seen anywhere.
- Harden itself immediately against new threats as they arose.

And as you might have guessed, everything described above exists today.

This solution's name is Reblaze.

Many Additional Advantages

In addition to the above, Reblaze is distinct from other security solutions in many additional ways.

Design

Holistic Web Security: Reblaze is not a collection of security modules (WAF, DDoS protection, etc.) It is a unified, proactive, intelligent software platform that detects and defeats all forms of illegitimate traffic, with one easy-to-use interface.

Runs On *Your* Clouds: Reblaze can run on private clouds, public clouds, or a combination of both. It integrates fully with AWS, Google, and Azure, which have invested a combined $65 billion into perfecting their platforms. Compare this to other cloud web security solutions, which use self-owned infrastructure and cannot match the performance or reliability of the industry leaders, especially during the stress of an attack. As a Reblaze customer, your data will be processed on a smarter, faster, larger, and more secure foundation—the clouds you already trust for your other business processes.

Superior Architecture: Reblaze deploys Virtual Private Clouds for every customer. The platform's architecture ensures that your network is isolated from Internet threats, with autoscaling bandwidth and the ability to run on multiple cloud providers. Global CDN integration and flexible geographic deployment options keep your sites and applications fast and responsive to your users, worldwide. (Other cloud solutions only provide shared environments, which expose their customers to outages as a result of attacks on others, and often have additional multi-tenancy vulnerabilities.)

Effectiveness and Performance

Accuracy: Reblaze monitors and tracks dozens of traffic parameters, using multivariate analysis to identify traffic patterns for both legitimate and illegitimate users. This goes far beyond typical security solutions. Example: for all incoming requests, Reblaze reaches out to detect the 'man in the browser', collecting and analyzing anonymized data about user devices (their computers, phones, and tablets), the browsers used, how people interact with the protected website, and so on.

Precise Traffic Control: Reblaze has the most powerful and finest-grained ACL in the industry. You can allow or deny access based on any parameter you can think of: specific countries, cities, networks, companies, and more.

Industry-Leading Bot Detection: Other solutions try to exclude bots by identifying and allowing humans. This is inadequate and ineffective. (For example, click farms are made up of humans.) Reblaze does not merely evaluate user *identity*—it discovers user ***intent***.

Real-Time Behavioral Analysis: Reblaze is optimized for near-instantaneous threat identification and traffic scrubbing. Latency is less than two milliseconds.

Automation and Ease of Use

Autoscaling: In only a few seconds, Reblaze can scale from zero to millions of concurrent connections. When attacks or other traffic spikes occur, load-balancing and other resources scale as needed, automatically.

Fully Managed: The platform is maintained remotely by Reblaze personnel. It is always up-to-date, with no effort required from your staff.

Other Capabilities and Benefits

Fully Extensible: Reblaze is not just SaaS, it's PaaS. A full API allows you to roll your own analytics, or use Reblaze as a machine learning engine, or extend and leverage many of Reblaze's other capabilities.

Full Support for DevOps: Most web security solutions hinder DevOps: their WAFs require hours, or even days, of reconfiguring every time a new app is introduced. Not so with Reblaze: whenever you deploy a new app or service (or change an existing one), they are protected immediately. The platform is continuously adaptive, so whenever something new is deployed, it quickly recognizes it, adapts to it, and starts protecting it. Reblaze also has an API for programmatic control.

Full Real-Time Traffic Visibility: When attacks occur, other solutions leave you wondering what is going on. Reblaze always shows you exactly what is happening within your site. An intuitive dashboard gives you a real-time overview of your traffic, with the ability to quickly and easily drill down into individual requests. You can always see **full details** (headers and payloads) of **all requests in real time**. And full historic data is always available, with high-performance forensic tools to help you get security intelligence and business-related insights from your traffic.

Customer Experience

Unique SLA: Reblaze is provided month-to-month, with no on-boarding fee, no contractual lock-in, and no long-term commitments.

Risk-Free Offer: Reblaze can be tried completely risk-free. The platform can be deployed as an additional layer of security, on top of existing security solutions. There's nothing to install: a simple DNS change can activate Reblaze for any site or web application in minutes. And there's no obligation. If after one month, you aren't delighted with Reblaze, you can cancel your account, and you'll owe nothing.

More Information

To get a no-obligation demo of Reblaze in the U.S. or Canada, call **(408) 907-7712**. In the United Kingdom, call (0161) 711 0103 or (0845) 154 1110. International inquirers should call +972 (73) 252-7007. Or, send an email to info@reblaze.com for a prompt response.

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. More information: www.Reblaze.com. Reblaze's clouds are fully compliant with 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.

Reblaze is a PCI-DSS Certified Level 1 Service Provider.