Reblaze and Google Cloud Platform Architecture

Leveraging the Full Power of the Cloud

Reblaze provides industry-leading web security technologies in a single easy-to-use platform, integrating seamlessly with Google Cloud Platform (GCP). It shields your web apps, services, and sites by protecting them within a Virtual Private Cloud. Incoming traffic is scrubbed as it passes through the cloud; hostile traffic is blocked, while legitimate traffic passes through. Typical latency is two milliseconds or less. Global CDN integration ensures accelerated site responsiveness for legitimate visitors.

Comprehensive Web Security

Reblaze protects against all forms of web threats. Its next-generation WAF (Web Application Firewall) provides a protective shield for your web assets and data. Robust DDoS protection defeats DoS/DDoS across layers 3, 4, and 7 (network, transport, and application) before the attack traffic reaches your ISP. Advanced bot detection and human behavioral analysis prevent data scraping, mass account creation, click fraud, and other malicious activities.

Fully Integrated with Google Cloud

Reblaze can be deployed from Google's Cloud Console with just a few clicks. This includes dynamic load balancing, full CDN integration, and other GCP features, all created and set up automatically in a matter of minutes. Reblaze can run exclusively on GCP, or across the customer's choice of cloud platforms.

The combination of Reblaze and Google Cloud Platform provides all the benefits of SaaS (including easy setup, automatic updates, modest monthly pricing, and more), along with the privacy, power, and control usually available only from appliances.

Harness the Full Power of GCP

As do many other "cloud security" solutions, Reblaze runs in the cloud, rerouting incoming traffic dynamically, and scaling bandwidth automatically as needed.

But unlike other solutions, Reblaze takes full advantage of Google Cloud Platform's capabilities. Reblaze does not analyze incoming traffic on a request-by-request basis, as other solutions do. Instead, Reblaze treats each requestor holistically, understanding that individual requests are only part of the larger picture of that user's intent.

Harnessing Big Data: Reblaze builds and refines a pattern analysis of each user's behavior, comparing it to a data trove maintained in Google BigQuery Datastore. This

MORE BENEFITS

FULL SUPPORT FOR DEVOPS
Reblaze is continuously adaptive. Whenever you deploy or change an app or service, Reblaze recognizes it and protects it immediately. The platform also has an API for programmatic control.

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

PRECISE
You can allow or deny access from specific countries, cities, networks, companies, & more. You can define separate security policies for sites, subnets, IP ranges, even individual URLs.

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

COMPLIANT & CERTIFIED
Reblaze's clouds are fully compliant with GDPR, 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.**

Google Cloud Partner

is a comprehensive record of user behavior parameters, going back years—not only for the protected domain, but of all traffic the platform has ever encountered. This massive data set can be accessed in an instant, thanks to Google Cloud DataFlow.

This enables Reblaze to instantly recognize any attack vector that it has seen in the past, even in the attack's earliest stages. And if the attack vector is new, Reblaze will adapt to it and counter it.

Harnessing Machine Learning: Reblaze uses Google Cloud Machine Learning to adapt and learn over time. Even as hackers develop new attack techniques, the platform becomes more sophisticated, staying effective and adapting to the ever-changing Internet environment.

With other security solutions, a would-be intruder usually only needs to outwit a WAF, or some similar device.

But with Reblaze, he must contend with the computing capacity of the entire global cloud, which can marshal years of data and analytics against him, instantly recognizing if his behavior is legitimate or not.

Superior Design

Reblaze deploys Virtual Private Clouds for every customer: a full dedicated stack for each protected network. Other cloud solutions only provide shared environments, which expose their customers to outages as a result of attacks on others.

Resources scale automatically to handle volume spikes. Bandwidth is limited only by the capacity of the global cloud.

Fully Extendable via API

Reblaze is more than just SaaS—it is PaaS (Platform as a Service).

As a fully automated system, Reblaze can be deployed and maintained entirely via its API. It is straightforward to integrate Reblaze with existing deployment processes.
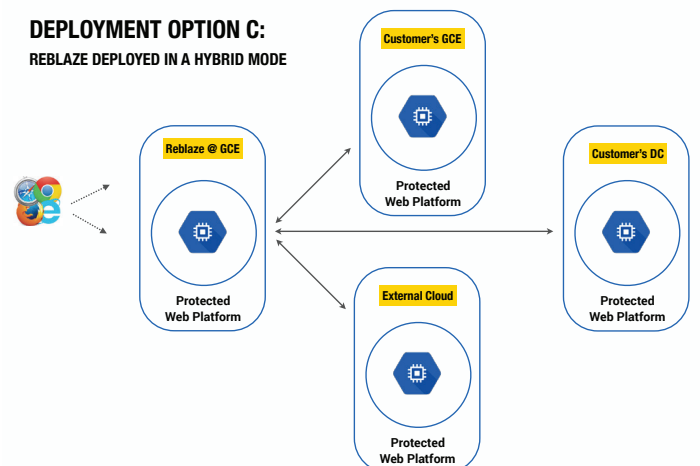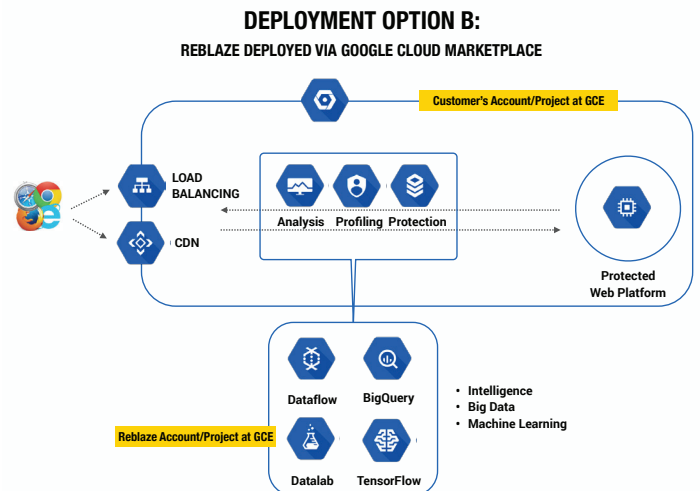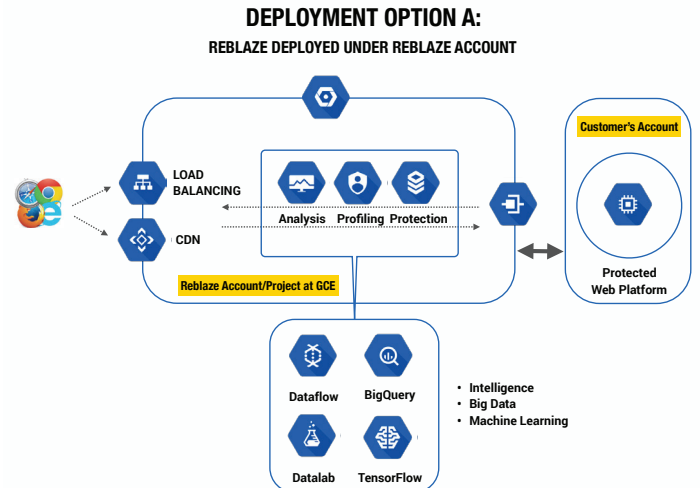
Developers can easily extend its system, security, and traffic profiles. Data scientists can analyze and understand their networks' data, create TensorFlow model graphs, train their models, and analyze model quality.

Reblaze's API is versatile, providing capabilities beyond web security alone. For example, you could roll your own analytics solution, using Reblaze's trove of historical traffic data stored in Google BigQuery.

Always Effective, Always Up-to-Date

All Reblaze deployments are maintained and upgraded automatically by Reblaze's team of security experts. Whenever new attack vectors arise, Reblaze is updated immediately. You always have the latest protection against the full breadth of Internet threats.

Flexible Deployment Options

DEPLOYMENT OPTION A:
REBLAZE DEPLOYED UNDER REBLAZE ACCOUNT

DEPLOYMENT OPTION B:
REBLAZE DEPLOYED VIA GOOGLE CLOUD MARKETPLACE

DEPLOYMENT OPTION C:
REBLAZE DEPLOYED IN A HYBRID MODE

Got Questions? We've Got Answers.

More info: www.reblaze.com. Email us: **hello@reblaze.com**. Reblaze Technologies, 940 Stewart Dr, Sunnyvale CA 94085. Phone: **(408) 907-7712.**