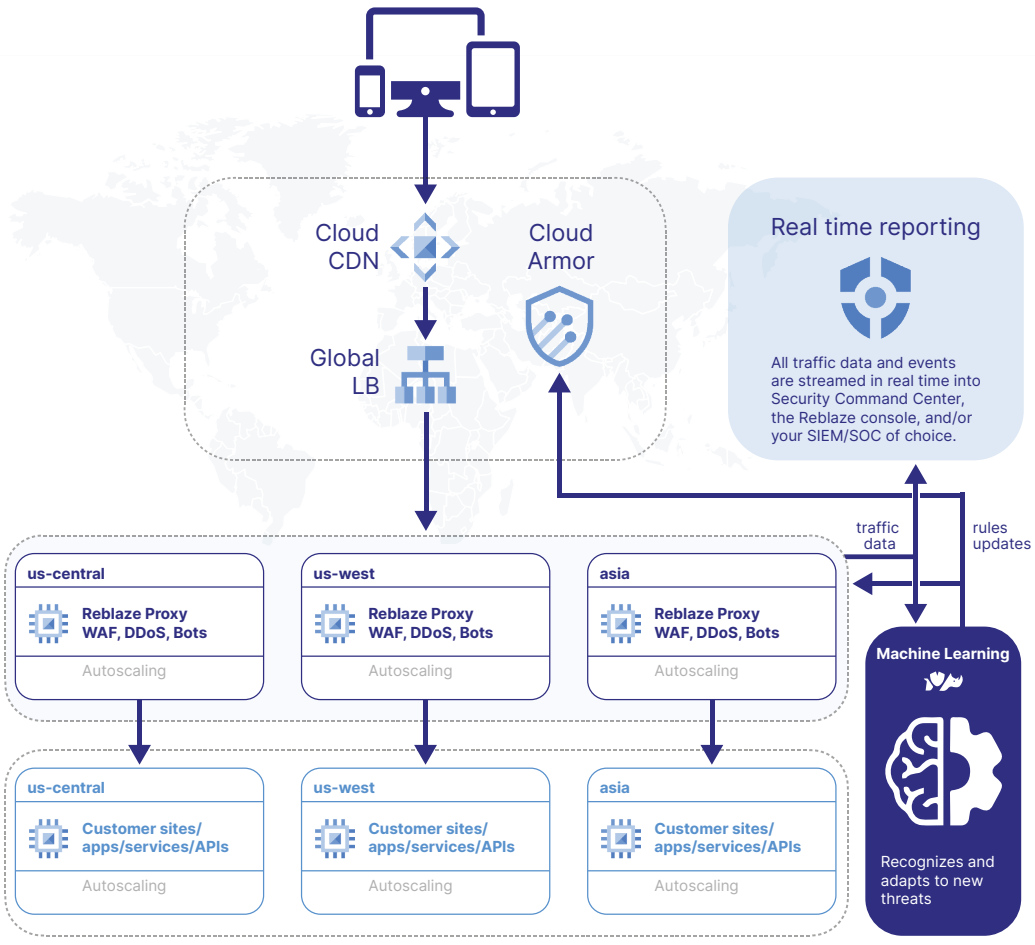
SECURE YOUR GCP WORKLOADS

Reblaze provides automated, turn-key web security for Google Cloud Platform.

Cloud Armor is a robust distributed security framework built into Google Cloud Platform, blocking hostile traffic in the cloud before it can reach the protected sites and web applications. On its own, Cloud Armor requires its users to define and maintain its security rules. This is time-consuming, complicated, and can be very challenging.

Reblaze's next-generation threat detection is fully integrated with Google Cloud. It converts Cloud Armor into an autonomous system which reacts immediately to every type of attack: Reblaze identifies hostile traffic, and Cloud Armor blocks it at the edges. Reblaze extends GCP's native security capabilities, and adds many more: next-generation WAF, multi-layer DDoS protection, bot management, precise ACL, real time reporting, full traffic transparency, API security, ATO (account takeover) prevention, mobile app security, and more.

As a fully managed solution, Reblaze is maintained for you by a team of security professionals. It is always up-to-date and always effective. Reblaze provides protection for all modern architectures: any combination of private/public clouds, single- and multi-cloud, hybrid, on-prem, containers, service meshes, and serverless.



Reblaze

About *Reblaze*

Reblaze is a cloud-based, fully managed protective shield for sites and web applications. The platform is a comprehensive web security solution, providing a next-gen WAF, DoS and DDoS protection, bot management, scraping prevention, CDN, load balancing, and more.

Reblaze offers a unique combination of benefits. Machine learning provides accurate, adaptive threat detection. Dedicated Virtual Private Clouds ensure maximum privacy. Top-tier infrastructure assures maximum performance. Fine-grained ACLs enable precise traffic regulation. An intuitive management console provides real-time traffic control. Full integration with top-tier cloud platforms provides a turn-key web security solution.

NEXT-GENERATION WAF/IPS

Reblaze defeats breach attempts, code and SQL injection, cross-site scripting, form manipulation, protocol exploits, session poisoning, malicious payloads, and other forms of attack.

DOS/DDOS PROTECTION

Reblaze is effective against DoS across layers and at all scales: from single malformed-packet DoS attempts to massive DDoS botnet assaults.

BOT MANAGEMENT

Reblaze prevents data theft & scraping, credential stuffing, brute force attacks, application abuse, vulnerability scanners, inventory denial, and more.

ATO PREVENTION

Reblaze prevents ATO (Account Takeover) attacks, and keeps user & customer accounts secure.

API SECURITY

Reblaze provides full protection for web services, microservices, mobile/native APIs, and more.

REAL TIME TRAFFIC CONTROL

Reblaze provides full real-time traffic analytics and statistics, even during large-scale attacks.

FULLY MANAGED SAAS

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

MACHINE INTELLIGENCE

Reblaze uses Machine Learning to recognize new threats as they arise, and hardens itself against them.

DEPLOYS ANYWHERE

Run Reblaze as SaaS, or in your own cloud, container, hybrid/multi-environment, or service mesh.

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 Technologies is a PCI DSS Certified Level 1 Service Provider.

reblaze.com | contactus@reblaze.com | +1 408 907 7712

Google Cloud Partner