**Google Cloud Armor**

Help protect your applications and websites against denial of service and web attacks.

* Benefit from DDoS protection and WAF at Google scale
* Detect and mitigate attacks against your [Cloud Load Balancing](https://cloud.google.com/load-balancing) workloads
* [Adaptive Protection](https://cloud.google.com/armor/docs/adaptive-protection-overview)  ML-based mechanism to help detect and block Layer 7 DDoS attacks
* Mitigate OWASP Top 10 risks and help protect workloads on-premises or in the cloud
* [Bot management](https://cloud.google.com/armor/docs/bot-management) to stop fraud at the edge through native integration with[reCAPTCHA Enterprise](https://cloud.google.com/recaptcha-enterprise)

BENEFITS

### **Enterprise-grade DDoS defense**

Cloud Armor benefits from our experience of protecting key internet properties such as Google Search, Gmail, and YouTube. It provides built-in defenses against L3 and L4 DDoS attacks.

### **Mitigate OWASP Top 10 risks**

Cloud Armor provides [predefined rules](https://cloud.google.com/armor/docs/rule-tuning) to help defend against attacks such as cross-site scripting (XSS) and SQL injection (SQLi) attacks.

### **Managed protection**

With [Cloud Armor Managed Protection Plus](https://cloud.google.com/armor/docs/managed-protection-overview) tier, you will get access to DDoS and WAF services, curated rule sets, and other services for a predictable monthly price. [Learn more](https://cloud.google.com/armor#section-7).

## **Key features**

### **Adaptive protection**

Automatically detect and help mitigate high volume Layer 7 DDoS attacks with an ML system trained locally on your applications. [Learn more](https://cloud.google.com/armor/docs/adaptive-protection-overview).

### **Support for hybrid and multicloud deployments**

Help defend applications from DDoS or web attacks and enforce Layer 7 security policies whether your application is deployed on Google Cloud or in a hybrid or multicloud architecture.

### **Pre-configured WAF rules**

Out-of-the-box rules based on industry standards to mitigate against common web-application vulnerabilities and help provide protection from the OWASP Top 10. Learn more in our [WAF rules guide](https://cloud.google.com/armor/docs/rule-tuning).

### **Bot management**

Provides automated protection for your apps from bots and helps stop fraud in line and at the edge through native integration with reCAPTCHA Enterprise. [Learn more](https://cloud.google.com/armor/docs/bot-management).

### **Rate limiting**

Rate-based rules help you protect your applications from a large volume of requests that flood your instances and block access for legitimate users. [Learn more](https://cloud.google.com/armor/docs/rate-limiting-overview).

### **All features**

|  |  |
| --- | --- |
| Pre-defined WAF rules to mitigate OWASP Top 10 risks | Out-of-the-box rules based on industry standards to mitigate against common web-application vulnerabilities and help provide protection from the OWASP Top 10. |
| Rich rules language for web application firewall | Create custom rules using any combination of L3–L7 parameters and geolocation to help protect your deployment with a flexible rules language. |
| Visibility and monitoring | Easily monitor all of the metrics associated with your security policies in the Cloud Monitoring dashboard. You can also view suspicious application traffic patterns from Cloud Armor directly in the [Security Command Center](https://cloud.google.com/security-command-center) dashboard. |
| Logging | Get visibility into Cloud Armor decisions as well as the implicated policies and rules on a per-request basis via [Cloud Logging](https://cloud.google.com/logging). |
| Preview mode | Deploy Cloud Armor rules in preview mode to understand rule efficacy and impact on production traffic before enabling active enforcement. |
| Policy framework with rules | Configure one or more security policies with a hierarchy of rules. Apply a policy at varying levels of granularity to one or many workloads. |
| IP-based and geo-based access control | Filter your incoming traffic based on IPv4 and IPv6 addresses or CIDRs. Identify and enforce access control based on geographic location of incoming traffic. |
| Support for hybrid and multicloud deployments | Help defend applications from DDoS or web attacks and enforce Layer 7 security policies whether your application is deployed on Google Cloud or in a hybrid or multicloud architecture. |
| Named IP Lists | Allow or deny traffic through a Cloud Armor security policy based on a curated Named IP List. |