Cloud DDoS

Summary

Signal Sciences Cloud DDoS is integrated in our Cloud WAF infrastructure with global points of presence to examine traffic before it reaches app or API endpoints.

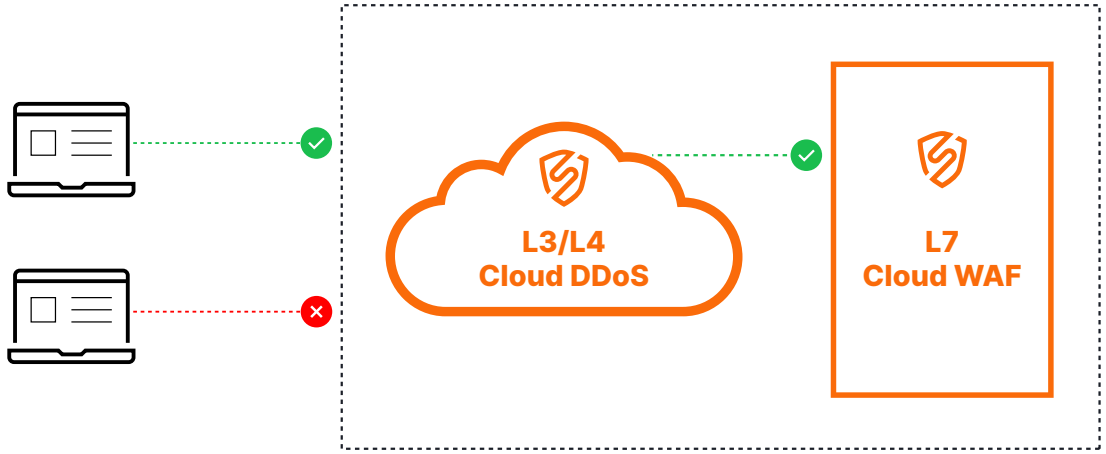
Protect applications and APIs against network and application layer attacks.

Attackers flood a target application or API with malicious requests at the network or transport layer to overwhelm that resource so legitimate users cannot use it. Threat actors can also stage denial of service attacks at the web application layer with the same goal: make your site unreachable.

If your company website or web-based service is not available, both your customer experience and company's ability to generate revenue are negatively impacted. Signal Sciences Cloud DDoS protection prevents network-based attacks, while our patented web protection technology detects and stops application layer denial of service attacks.

Excessive web requests can negatively impact application and API performance, but Signal Sciences Cloud DDoS prevents those attacks by blocking volumetric requests that could take a website or key APIs offline, ensuring optimal customer experience and availability of your organization's business-critical applications and APIs. Signal Sciences Cloud WAF customers are automatically protected by default with Signal Sciences Cloud DDoS.

Signal Sciences Cloud DDoS is an always-on service that monitors and inspects web request traffic in real-time to detect and stop DDoS attacks with a combination of traffic signatures, anomaly algorithms and other analysis techniques to block malicious traffic. It requires no additional installation, maintenance or related costs as part of the Signal Sciences protection platform.



Our Cloud WAF architecture protects the applications and APIs operating behind it.

Features

- **Detects and stops common DDoS attacks:** Automated mitigation techniques stop common network protocol-based floods including SYN floods and reflection attacks using UDP, DNS, NTP, and SSDP.
- **Automatic mitigation:** Applied inline for fast prevention before volumetric traffic can reach the app or API endpoint
- **Integrated DDoS attack detection:** protects against common infrastructure attacks. Automatic mitigations are applied inline to protect your applications without latency impact.

Benefits

- **Cost effective:** Cloud DDoS protection is automatically enabled for all SigSci customers at no additional cost.
- **Seamless integration and deployment:** Signal Sciences Cloud WAF customers are automatically protected from frequently occurring network and transport layer DDoS attacks.
- **Managed protection and attack visibility:** Always-on, heuristics-based network flow monitoring and inline mitigation against network and transport layer DDoS attacks.
- **Requires no additional training** or resources to implement.
- **Scales automatically as applications scale** in complexity to meet demand.

Cloud DDoS Use Cases

Network/Transport Layer Attacks

UDP Reflection and SYN Floods

Attackers use these methods to generate large traffic volumes that inundate a server to overwhelm it. Signal Sciences Cloud DDoS service filters out malicious traffic so your application can respond to legitimate customer traffic.

Application Layer Attacks

HTTP of DNS Floods

Attackers send HTTP requests that appear to be from a real user of the web application. HTTP floods can target a specific resource, while complex HTTP floods attempt to emulate human interaction with an app. Threat actors also use well-formed DNS queries to exhaust DNS server resources. Signal Sciences was purpose built to detect and stop application layer attacks.

Any Application

Kubernetes	Microsoft .NET
AWS	Apache
AWS Lambda	Java
VMWare Tanzu	Section
NGINX	Kong

Any Attack

OWASP Top 10	Rate Limiting
DDoS	ATO
Brute Force Attack	Bad Bots
App Abuse and Misuse	CVEs

Any DevOps Toolchain

Slack	Microsoft Teams
Datadog	JIRA
Splunk	Generic Webhooks
PagerDuty	Restful JSON API