DDoS Protection and Mitigation

Powerful, real-time DDoS protection and mitigation

DDoS attacks growing in size

Distributed denial of service (DDoS) attacks are getting bigger and more disruptive. These attacks can outstrip aggregate bandwidth and computing resources of any data center serving critical users. With the increasing size of the average DDoS attack, on-premise DDoS solutions no longer suffice and are generally not practical or cost effective. CDNs offer a powerful and scalable alternative due to their robust networks, high capacity, and distributed application resources.

Fastly DDoS mitigation

Fastly's edge cloud offers a **multi-terabit-per-second**, globally distributed network to absorb even the largest DDoS attacks. Our DDoS mitigation service protects against highly disruptive Layer 3 and Layer 4 DDoS attacks, as well as more complex Layer 7 attacks. Fastly's edge cloud platform is built on a flexible Varnish open source software, allowing us to make configuration changes on the fly, responding to attacks in real time and filtering out malicious requests at the network edge. With our Origin Cloaking capabilities we are able to hide the origin IP, forcing all attack traffic through our edge cloud platform, where we apply DDoS mitigation rules. We connect directly with your origin server using private network interconnections, hiding the IP address from the public internet.

Always-on DDoS mitigation

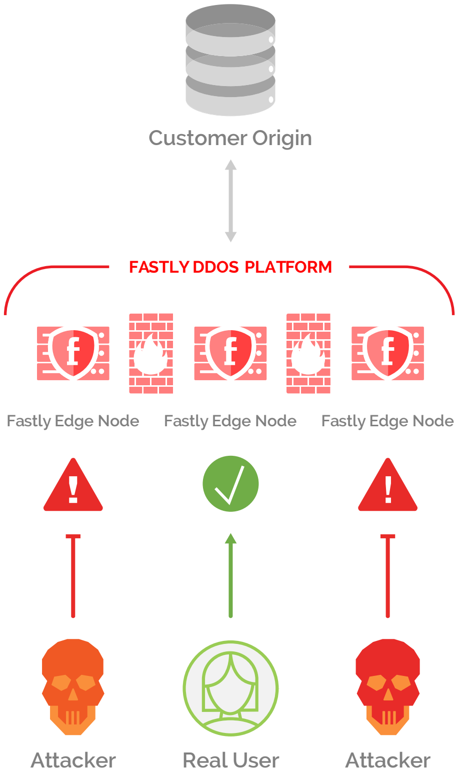
Fastly's DDoS mitigation service provides an always-on security solution. This approach uses in-line scrubbing to monitor traffic and remove suspicious requests at the point of presence (POP). We don't reroute traffic through a separate sub-optimal network introducing latency and more IT complexity. Instead, our entire network acts as a scrubbing center for DDoS attacks, offering you the same level of DDoS mitigation for both encrypted and unencrypted traffic.

Superior protection at all layers

Our edge-based filtering technology provides broad DDoS protection, automatically blocking all types of highly disruptive Layer 3 and Layer 4 attacks at the edge before they hit your origin. To protect your network from complex application (Layer 7) attacks, our edge cache nodes act as enforcement points. Our security experts can apply rules using Varnish Configuration Language (VCL) to inspect the entire HTTP/HTTPS request, and block based on criteria (headers, cookies, request path, client IP, geo location etc.). We also give you the option to customize rules to fit your security needs.

1stdibs®

> "Fastly's technology allows us to handle attacks better than anything else while still giving us control. With Fastly, we have an edge cloud platform that gives us the ability to provide uninterrupted service in the event of another attack."
>
> *Ross Paul, CTO*
> *1stdibs*



Real-time visibility and control

Fastly provides real-time access to data logs and historical statistics. You can identify suspicious activity, such as unusual traffic spikes from a DDoS attack, and troubleshoot right away. We empower you to make real-time configuration changes using Varnish Configuration Language (VCL). With our highly modified and improved Varnish, we enable you to apply custom DDoS rules in under a second globally for powerful and rapid mitigation. With full access to HTTP requests, VCL can be used to create rules based on any attribute of the request or response.

A comprehensive solution

Our 12 month DDoS Protection and Mitigation service is an add-on to your Fastly edge cloud service. We provide layer 3, 4, and 7 DDoS mitigation support of HTTP (port 80) and HTTPS (port 443, TLS). You are also covered for unlimited overage protection, irrespective of attack size. Our security support team is available 24/7.

Key capabilities

- **High-network capacity:** Multi-terabit-per-second network capacity at the edge with large transactional capacity per identical cache node.
- **Broad DDoS protection:** Secure your origin server from multi-layer attacks.
- **Real-time control:** Custom DDoS rules can be crafted with VCL to force a particular client to be served from cache during a DDoS attack.
- **Origin Cloaking:** Hides customer origin IP address forcing traffic through our network for DDoS mitigation.
- **Highly automated:** 80% of configurations can be done via API, unlike most security systems that rely on CLI.
- **High-performance:** Security is tightly integrated with our edge cloud, so performance is never compromised.
- **Dedicated security team:** 24x7 cyber security expertise and support.

Comprehensive DDoS protection

- DNS flood
- HTTP flood
- UDP
- ICMP (NTP, SSDP, etc.)
- IGMP
- Layer 7 DNS
- Mixed flood (SYN + UDP or ICMP + UDP)
- Ping of Death
- Pulse Waves
- Slowloris
- Smurf
- TCP SYN+ACK
- TCP FIN
- TCP Reset
- TCP ACK
- TCP Fragment
- Reflected ICMP + UDP
- Teardrop
- And more...