fastly

DDoS Mitigation

Powerful, real-time DDoS 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 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. Our network 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 CDN, 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 and thwarting any attempts to bypass the CDN.

Always-on DDoS mitigation

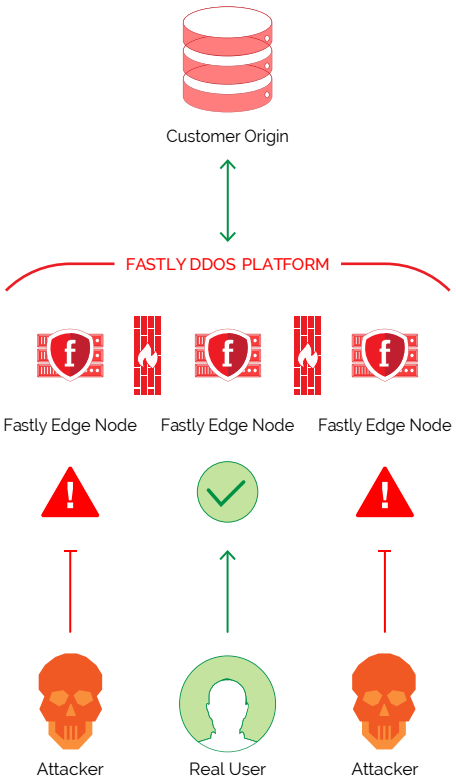
Fastly's DDoS mitigation service provides an always-on security solution. This approach uses in-line scrubbing to monitor traffic and remove suspicious requests at the point of presence (POP) without routing through specialized servers. Our entire network acts as a scrubbing center for DDoS attacks, 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.

Business benefits

- **Safeguard your website**
  Reduce downtime and risk to brand damage with rapid response to DDoS threats and events
- **We help you first**
  Decide later on payment model
- **Overage protection**
  Unlimited overage protection always included
- **Cost-effective solution**
  Single vendor for DDoS protection and CDN services



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.

We help you first

We give our customers flexibility and control in making an economic decision after an attack. If you are under attack we will help you, no questions asked. Afterwards you can choose to enroll in our DDoS Mitigation service or pay for CDN overages — based on what the actual billing is rather than pressuring you to select upfront and to try to predict the more cost-effective option.

Flexible service options

To take advantage of our powerful DDoS mitigation, you can choose one of our two options as an add-on to your CDN service. Both plans provide DDoS protection of HTTP (port 80) and HTTPS (port 443, TLS) services with unlimited overage protection.

- **DDoS protection and mitigation service:** Fastly offers a 12-month service commitment for customers who want to minimize their risks with continuous protection on an annual basis.
- **DDoS threat response service:** Fastly also offers a month-to-month DDoS protection of HTTP and HTTPS services. This mitigation service is available for immediate response to a DDoS threat or ongoing DDoS attack.

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 CDN, 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
- Slowloris
- Smurf
- TCP SYN+ACK
- TCP FIN
- TCP Reset
- TCP ACK
- TCP Fragment
- Reflected ICMP + UDP
- Teardrop
- And more...