Fastly Secure packages

Right-sized protection for the digital experiences that power your business

Fastly's Secure packages are designed to help you confidently protect your web apps and APIs in any environment — on premise, cloud, or hybrid — with the right level of support to meet your needs. Each package features our next-gen WAF, which offers multiple layers of protection and is so effective that more than 90% of our customers use it in full blocking mode. Fastly delivery customers can also take advantage of additional security features such as our comprehensive DDoS protection and TLS encryption.

Secure packages summary

- **Essential:** Ideal for small- to mid-sized companies looking for effective app and API protection, our essential package includes our award-winning next-gen WAF, along with DDoS protection and TLS encryption.
- **Professional:** Our professional package is designed for mid-market and larger organizations looking for effective app and API protection but with more custom security requirements.
- **Premier:** Our premier package is ideal for large, global organizations with advanced security requirements and a need for enhanced customization, visibility, control, and elevated support.

Features by package

Features	Essential	Professional	Premier
Workspace and RPS	1 Workspace 25 RPS included	Various Workspace and RPS options available	Various Workspace and RPS options available
Fastly next-gen WAF	✓	✓	✓
Deploy anywhere: cloud, datacenter or hybrid	✓	✓	✓
DDoS protection*	✓	✓	✓
TLS encryption*	✓	✓	✓
Custom signals		✓	✓
API and ATO protection rules		✓	✓
Rate limiting			✓
Eligible to purchase Response Security Service			✓
Support	By email and docs with next business day response SLA	By email, docs, or support portal. 1-hour response time for urgent issues via portal.	By email, docs, or support portal. 1-hour response time for urgent issues via portal.

*Customer must separately purchase a Fastly delivery product to leverage DDoS and TLS capabilities.

Features and capabilities

Fastly next-gen WAF

Our next-gen WAF is designed to detect and stop OWASP Top 10 attacks like SQL injection and cross site scripting (XSS). We protect against advanced web-layer attacks like account takeover (ATO) via credential stuffing, API abuse, shopping cart ID enumeration, malicious bots, and more — all in one solution.

Deploy anywhere: cloud, datacenter, or hybrid environments

With a flexible software agent-module pair, our next-gen WAF is designed for rapid deployment in any environment. No matter where you operate your apps and APIs, you'll quickly gain protection and visibility across your entire application footprint.

API and ATO protection rules

We provide dedicated API and Account Takeover (ATO) rules to help surface security telemetry for advanced attack scenarios, like user ID enumeration, credit card validation flow abuse, and password reset attempts. With dedicated visual dashboards, your security, development, and operations staff can quickly gain granular visibility into Layer 7 attacks with minimal effort.

Custom signals

Our custom signals provide increased visibility into rules and how they automatically block or allow web requests. Rules can be configured with custom signals to show why requests were blocked. Signals can be created on individual Workspaces or organization-wide so you can easily use them in multiple workspaces.

Rate limiting

Our next-gen WAF provides rate limiting capabilities that include intelligent controls to reduce the number of requests directed at key web application functions. By utilizing application-specific rate limiting rules, we can detect and mitigate fraudulent abuse of apps and APIs.

Workspace

Our Workspace feature gives you the ability to manage and access security metrics for a discrete collection of apps and APIs in our next-gen WAF management console. You can group apps and APIs to suit your business requirements, like grouping apps and APIs for a specific business unit or production environment.

Requests per second (RPS)

RPS is a measure of the web requests our next-gen WAF inspects per second to detect and stop malicious traffic. Small organizations with few apps in production benefit from our default 25 RPS, while mid-sized and larger organizations with many apps will have higher traffic volumes. We'll work with you to ensure you have adequate request inspection volume to suit your traffic.

DDoS protection

Available to Fastly delivery customers, our DDoS Protection blocks volumetric attacks at Layer 3 and 4. Additionally, our next-gen WAF provides application-layer DDoS prevention. When unexpected web request traffic exceeds your pre-defined thresholds, excessive request volumes are automatically blocked to keep your apps and APIs available to legitimate customers.

TLS encryption

Available to Fastly delivery customers, Platform TLS provides a simple way for you to configure TLS on our network using a web API. It's fast, easy to manage, and highly scalable.

Getting started today

Reach out to our team to learn more about our secure packages and how quickly you can protect the digital experiences that drive your business.

Contact Sales