

# 10 Key Capabilities of the Fastly Next-Gen WAF

A look at specific areas on why Fastly is the web application security technology of choice for modern software teams.

# The Top 10 Capabilities of the Fastly Next-Gen WAF

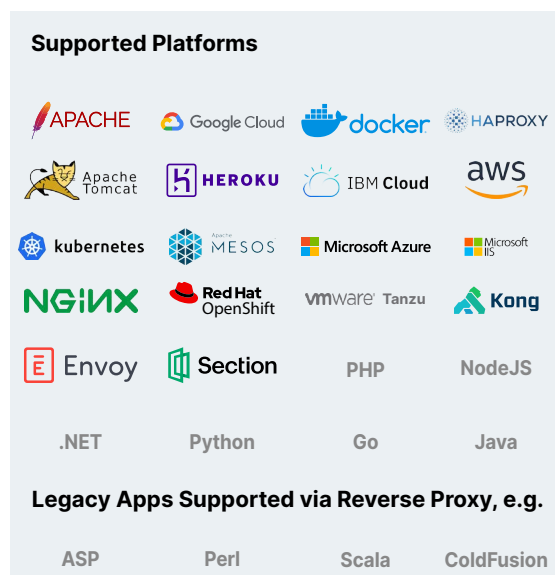
As the application development landscape evolves with faster feature release cycles and the adoption of new and modern languages and cloud platforms, software teams are struggling to secure their rapidly growing web attack surface.

The Fastly Next-Gen WAF is designed to work quickly and effectively, enabling application developers and operations teams to deliver modern, business-critical web applications and APIs that are well protected and running performantly.

There are many vendors claiming to provide effective and scalable offerings to protect applications and APIs, so we want to dig into exactly what makes us the next-gen WAF and RASP technology of choice.

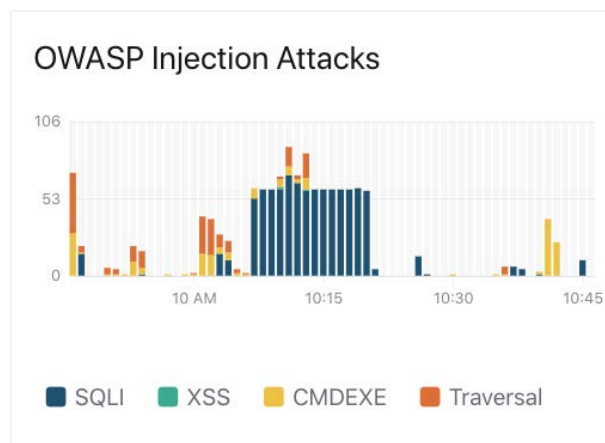
## 1. Flexible Deployment Options for Any Architecture—Now and In The future

Modern software teams deploy applications everywhere: in containers, on multi- and hybrid clouds, load balanced across multiple CDNs, and everything in between. Whether you're using Amazon Web Services (AWS), Microsoft Azure, Google Cloud, some combination of these, or something altogether different, with the Fastly Next-Gen WAF you gain visibility and protection wherever your apps, APIs, and microservices live—and in whatever language they're written. Additionally, to protect legacy applications, we can operate as a reverse proxy. Security teams also have the option to deploy our Fastly edge cloud to add more layers of defense using the Fastly global network with the programmability of the edge. Providing the widest range of installation options in the industry and a single control pane to monitor all your apps, our Next-Gen WAF is a foundational piece of a future-proof strategy that supports your architecture today, in addition to where and how you run your apps in the future.



## 2. Installs Easily Behind Existing Edge Security Tools to Catch Missed or Unknown Attacks

Your organization may have made a substantial investment in a CDN, and that's not uncommon. Putting a WAF on the edge network makes sense to many operations engineers since that's where cached content is utilized to remove the load from web and application servers and brings protection closer to end users and shields origin systems from abusive traffic. It also allows engineers to easily check the "compliance" box for security audits. But in practice, customers have requested more specific application-level attack and behavior detail than what these products were designed to provide.



Fastly can augment existing WAF investments and identify and block unique threats while providing protection against the OWASP Top 10 and beyond.

Our Next-Gen WAF can install on the Fastly edge or behind your existing technologies to identify and block unique threats they cannot. For teams that want an all-in-one solution, deploying the Fastly Next-Gen WAF on the Fastly CDN edge enables organizations to realize the performance benefits of Fastly's

CDN while simultaneously securing your traffic, without having to install agents, or deploy and manage.

### 3. Protects Your Apps Without Breaking Them

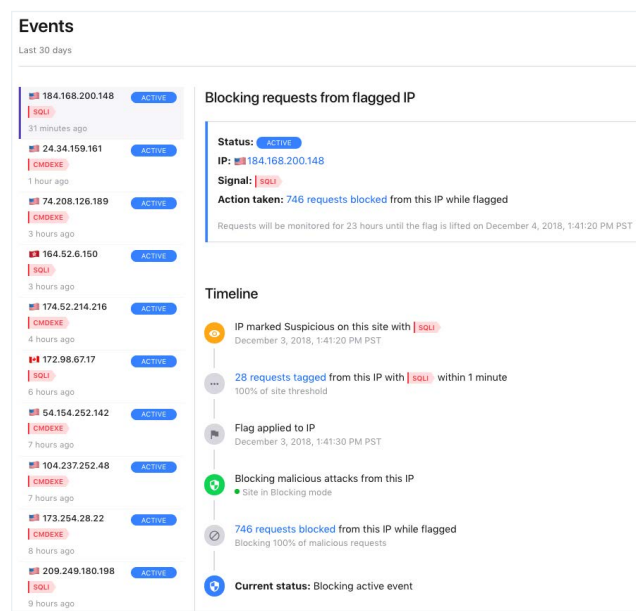
The Fastly Next-Gen WAF takes a threshold approach to blocking so you can run our solution in full, automated blocking mode in production with virtually no false positives: 95 percent of our customers trust us to do just that. With threshold blocking, we don't make a decision on each request like other WAFs, but we instead look at suspicious payloads over time and with context to determine whether an actual attack is occurring. Our patented approach analyzes production requests from over 90,000 app deployments with no noticeable performance impact on the applications and APIs we help our customers protect.

### 4. Identifies and Blocks Bots and Scrapers to Protect Your Resources

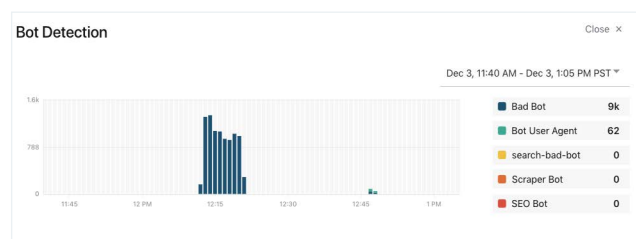
Attackers use automation and botnets to acquire valuable data, especially from content rich sites in the media, e-commerce, and technology businesses. With Fastly, you can enable rate-limiting rules around abusive behavior such as content scraping and eliminate serving up content and resources to malicious users, potentially saving on infrastructure costs.

With rate-limiting rules enabled, you can block high-volume, malicious requests without a single false positive. You can use the same threshold-based approach to prevent malicious automated attacks via bots

deployed to perpetrate application DDoS and account takeovers. Lastly, you can also utilize whitelisting and blacklisting for known good and bad sources to allow or deny requests as necessary, reducing noise in your environment.



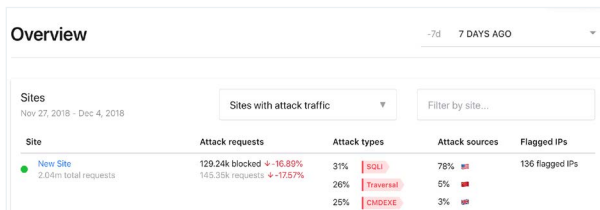
A 30-Day Events report summarizes attacks blocked (left column) and the volume of malicious requests blocked from a flagged IP address (upper right). Our Timeline view shows why the IP was flagged as malicious as well as current status (active or past event)



With rate-limiting rules enabled, Fastly blocks high-volume malicious bot requests.

## 5. Guides Engineers to Fix the Right Things

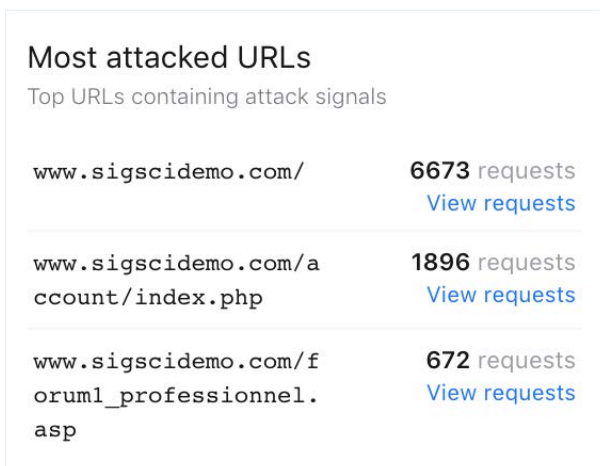
Engineers never have a shortage of bugs to fix, but the challenge is understanding which ones to prioritize. The Fastly Next-Gen WAF provides clear reports on the most common attack types to help your teams focus on what exactly is under attack. Engineering and security managers use this real-time data to best utilize their resources, including what types of training needs to be reinforced depending on the attack tactics used against their apps and APIs in production. Developers and security engineers are able to self-serve data to get a better understanding of the bigger picture of attacks against their code.



The screenshot shows the 'Overview' section of the Fastly dashboard. It displays a table with columns for Site, Attack requests, Attack types, Attack sources, and Flagged IPs. The data is for a site named 'New Site' from Nov 27, 2018, to Dec 4, 2018. The table shows 129,246 blocked requests (16.89% increase) and 143,336 requests (17.87% increase). The attack types listed are SQLi (31%), XSS (26%), and CMDXSS (25%). The attack sources are 78% from the Internet, 5% from CloudFront, and 3% from other sources. There are 136 flagged IPs.

Site	Attack requests	Attack types	Attack sources	Flagged IPs
New Site Nov 27, 2018 - Dec 4, 2018 2,041m total requests	129,246 blocked +16.89% 143,336 requests +17.87%	31% SQLi 26% XSS 25% CMDXSS	78% Internet 5% CloudFront 3% Other	136 flagged IPs

An example overview report shows the volume, types and sources for attacks against a single site: this key information helps your team focus their resources.



The screenshot shows the 'Most attacked URLs' section of the Fastly dashboard. It lists the top URLs containing attack signals. The first URL is www.sigscidemo.com/ with 6673 requests. The second URL is www.sigscidemo.com/account/index.php with 1896 requests. The third URL is www.sigscidemo.com/forum1\_professionnel.asp with 672 requests. Each URL has a 'View requests' link.

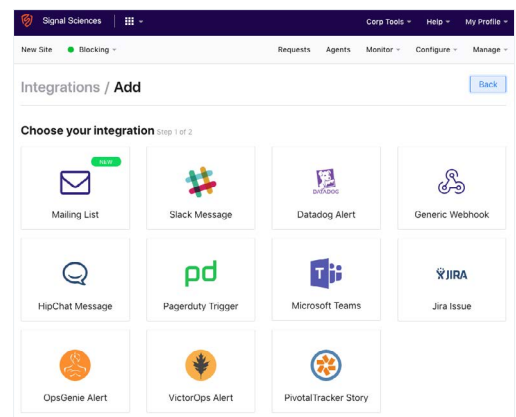
URL	Requests
www.sigscidemo.com/	6673 requests
www.sigscidemo.com/account/index.php	1896 requests
www.sigscidemo.com/forum1_professionnel.asp	672 requests

Example of specific URLs receiving the most malicious requests. Your team can get more context by drilling down to a "Requests" report for each attacked URL.

## 6. Brings Dev and Ops to the Security Party with Actionable Data

Security cannot be an afterthought. Aligning security, dev, and ops teams is crucial for all three groups to understand the requirements of security in the development lifecycle before issues arise that impact you and your bottom line. The Fastly Next-Gen WAF shows all stakeholders how requests are impacting their app or service and provides the self-service data to prove it. Data around application attacks, anomalies, and behavior is available via customizable dashboards and APIs, as well as through the toolchain products your teams are already using. Teams can easily create alerts when critical thresholds are triggered, sending messages through to the systems they use. Examples of how we enrich your current toolset include:

- **SIEM integrations** into Splunk, ArcSight, Sumo Logic, and others with fully documented REST/JSON APIs
- **Webhooks to common DevOps tools** like Slack, PagerDuty, Datadog, and Jira provide full event details of alerts



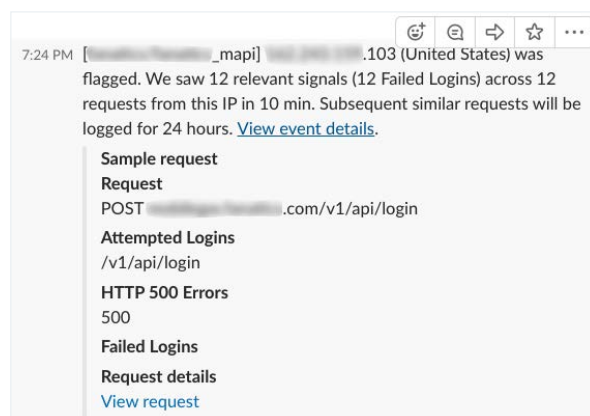
Data that Fastly surfaces can be utilized to create alerts broadcast via several devops tools.

## 7. Defends Mobile Apps with the Same Powerful Capabilities

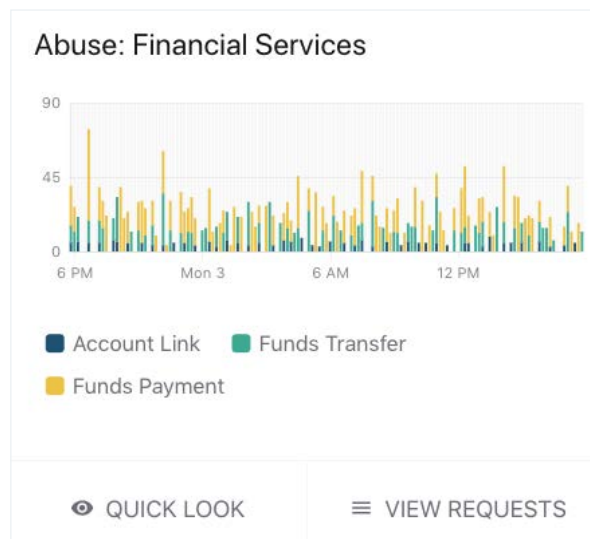
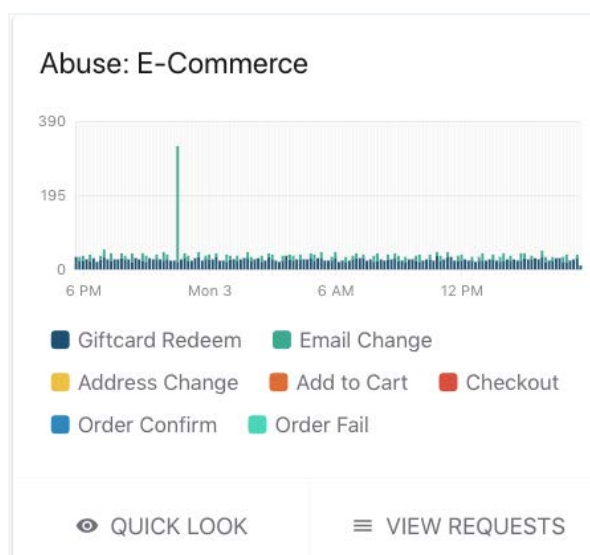
The Fastly Next-Gen WAF provides the broadest coverage against real threats and attack scenarios across any modern architecture, including the mobile apps that empower your customers to access your products and services anywhere. As mobile applications rely on APIs to transfer critical data from application servers, our solution provides you with visibility by installing after the traffic is decrypted at the web server or code layer. Without performance impact, you can leverage us to optimize and secure your mobile app experiences.

Through templated rules, you can monitor any business logic that is unique to your mobile application. For example, you can view the number of transactions per minute, checkouts per hour, discount codes used, and so on. With added visibility that doesn't impact the performance and user experience of your mobile app, your teams can gain insight into particular use and abuse patterns that were formerly difficult to find, buried in log data.

Fastly also defends the authentication flows in any mobile app by detecting and blocking requests from known bad IPs that abuse authentication events like account creation, password reset, or other brute force or account takeover attempts. And because we are able to block with virtually zero false positives, legitimate users will not be denied access to your mobile app—so your business continues uninterrupted.



Example alert from Fastly sent to Slack that highlights a dozen failed logins from the same IP address.



With Fastly you can monitor key application events in your apps and mobile APIs for potential misuse and abuse.

## 8. Addresses Vulnerabilities with Virtual Patching

Software creates new vulnerabilities that attract attackers who unleash payloads to exploit the weaknesses. Because the vulnerability-to-exploit cycle occurs in hours, you need proactive defense against attacks to buy time while fixing the underlying systems. This is exactly what Fastly provides through virtual patching enabled by templated rules you can apply virtual patches that address various Common Vulnerability and Exposures (CVEs) and immediately block requests containing the CVE exploit. Within the console, customers can use templated templated rules that cover various CVEs in a default list.

The example above right displays a templated rule that applies a virtual patch to address the Apache Log4j JNDI remote code execution vulnerability, which allows an attacker who can control log messages to execute arbitrary code loaded from attacker-controlled servers.

## 9. Provides Operations with Data to Ensure Site Uptime and Performance

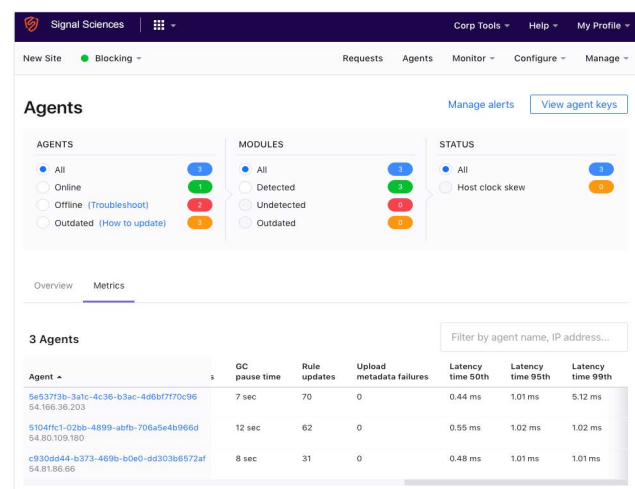
The Fastly Next-Gen WAF's patented module-agent architecture was designed to fail open so legitimate users are never blocked, and connects asynchronously with our powerful cloud-hosted analytics backend: Cloud Engine. Net result? Your applications' uptime, availability, and communication function as if we weren't even there. We built our agent to expose metrics that operations teams rely on,

from CPU and memory usage to how much delay the agent adds to each request (no more than one to three milliseconds).

We also built our API so these metrics pull into the systems your operations teams already use. Many other WAF and RASP vendors don't have APIs for these metrics and provide little detail in their UI.



In this example templated rule, Fastly will apply a virtual patch that will block requests that attempt to leverage CVE-2018-9206, a vulnerability that can lead to remote code execution.



Agent health and KPIs, such as latency, can be easily monitored within the Fastly Console.



In addition, Fastly can surface metrics that are meaningful to operations teams—things like client-side and server-side errors, large response times, sizes, errors, even broken links in the code. These data points can point to critical issues either in your application’s business logic or server configuration and helps teams triage issues faster.

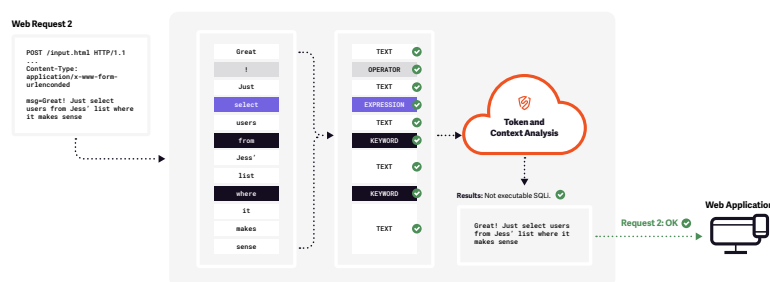
## 10. Automated blocking that scales without rules tuning

Let’s be frank about the effectiveness of other WAFs within the context of multi-cloud and rapid development cycles and releases: they don’t stand a chance. With other WAFs, which require learning mode and constant signature tuning to rule out false positives, the aggressiveness of blocking rules gets turned down or completely turned off for fear of breaking the application. We’re able to block anomalous traffic without breaking the application or blocking legitimate users with SmartParse, our proprietary detection method created by Signal Sciences. SmartParse was designed to make instantaneous decisions in line to determine if there are malicious or anomalous payloads present in requests.



A “Response Anomalies” chart is an example of how Signal Sciences provides visibility into operational data points like anomalies and application behavior that comes enabled right out of the box.

By evaluating the context of the request and how it would actually execute, SmartParse makes highly accurate detections. Designed to run at scale, our detection approach requires no tuning or configuration, and virtually eliminates false positives so you can scale protection without dealing with the maintenance overhead that other WAFs require.



Fastly’s SmartParse detection methodology improves accuracy by tokenizing key value pairs and using big data analytics to determine how likely the request is to be malicious. Dashboards and APIs show request-level details when IPs are flagged to ensure transparency and confidence in detections and decisions.

## The AppSec Solution for Modern Development Teams

These key capabilities are essential to ensuring that a web application security solution meets the needs of modern development, operations, and security teams looking to iterate and release software quickly and securely. The Fastly Next-Gen WAF has deployment options that are both easy to install and provide complete coverage.