fastly

WHITE PAPER

10 Key Capabilities of the Fastly Next-Gen WAF with AWS Cloud

aws

10 Key Capabilities of the Fastly Next-Gen WAF with AWS Cloud

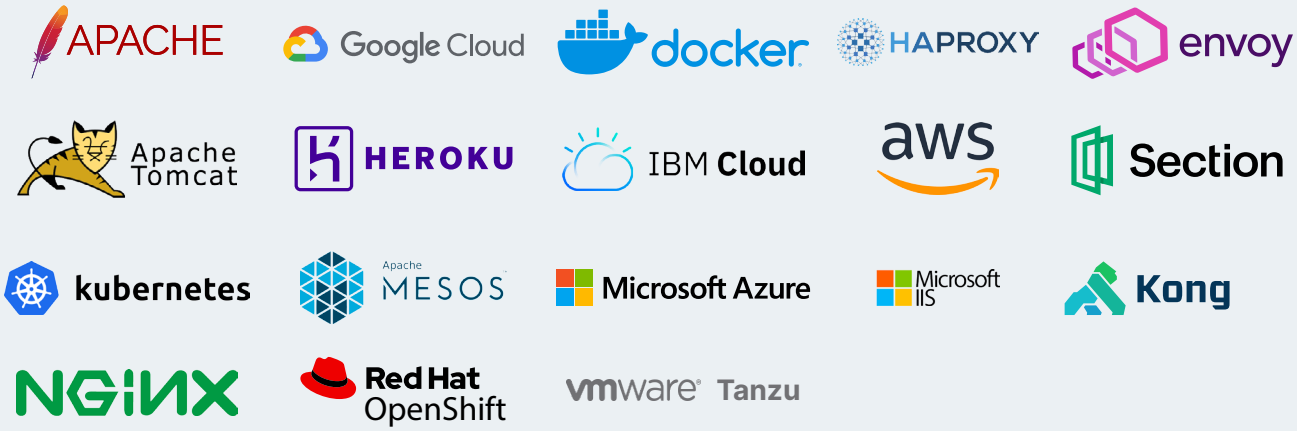
As the application development landscape evolves with faster feature release cycles and the adoption of new and modern languages and cloud platforms, software teams are struggling to secure their rapidly growing web attack surface. The Fastly Next-Gen WAF (powered by Signal Sciences) is designed to work 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.

Fastly's Next-Gen WAF is the ideal web application security technology for modern software teams leveraging AWS Cloud. Providing seamless integration with AWS services, we work closely with our joint customers to enhance their security posture and navigate the complexities of modern application security. There are several vendors claiming to provide effective and scalable offerings to protect applications and APIs, so we will dig into exactly what makes us the WAF technology of choice for modern development and security teams.

1. Flexible Deployment Options for Any Architecture–Now and in the Future

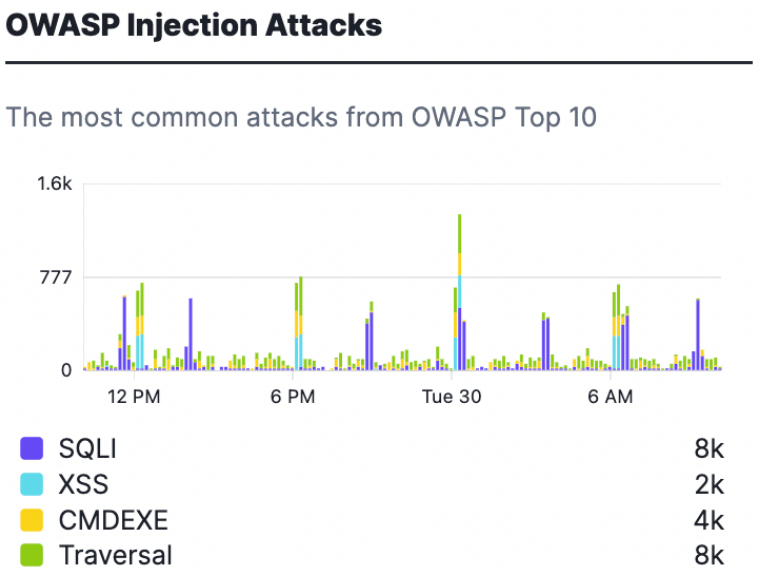
Modern software teams deploy applications everywhere: in containers, on multi- and hybrid clouds, load balanced across multiple CDNs, and everything in between. Whether your apps live on market-leading cloud services providers like AWS, other platforms, some combination of these, or something altogether different, the Fastly Next-Gen WAF protects your Layer 7 assets with the widest deployment options on the market. Additionally, to protect legacy applications, we can operate as a reverse proxy. Security teams also have the option to deploy on our Fastly edge cloud to add more layers of defense using the Fastly global network and 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 and tomorrow.

Supported Platforms



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.



Our Next-Gen WAF can install on the Fastly edge, or behind your existing technologies, to identify and block threats that other security tools might miss. Attacks like credential stuffing or account takeover rely on a "low and slow" method to bypass volumetric-based signatures maintained by traditional WAFs. Instead, Fastly blocks attacks based on content analysis of executable code and ensures that even drip-fed attacks are blocked.

For teams that want an all-in-one solution, deploying the Fastly Next-Gen WAF on our Edge Cloud Network can prevent attacks from reaching your origin, allowing you to realize the performance benefits of Fastly's CDN while simultaneously securing your traffic.

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: Nearly 90 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.

Gartner Peer Insights Customers' Choice 2023

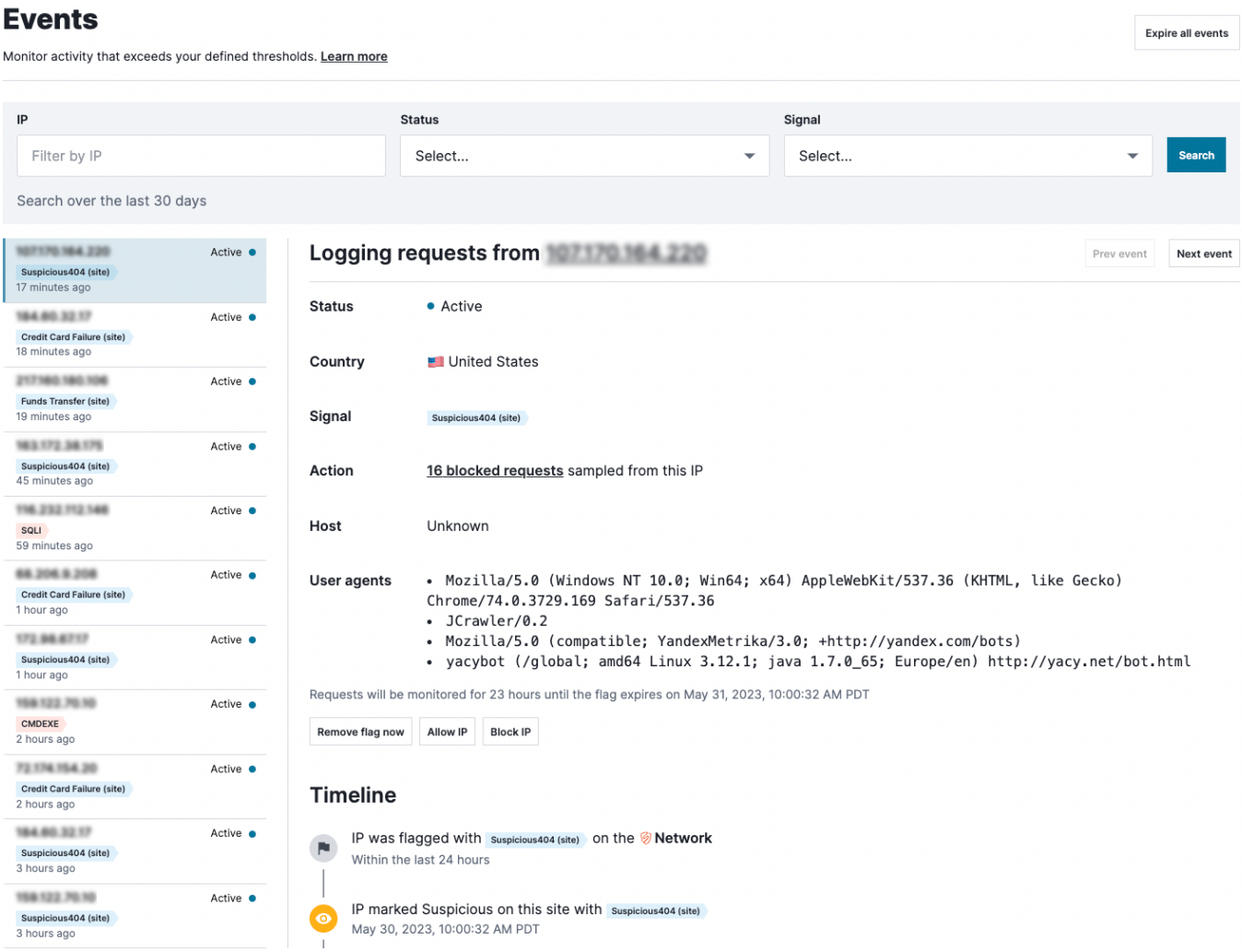
Customers deploy us in blocking mode because they love our efficacy and protection, helping us maintain our Gartner Peer Insights Customers Choice for WAAP 5 years in a row.

fastly

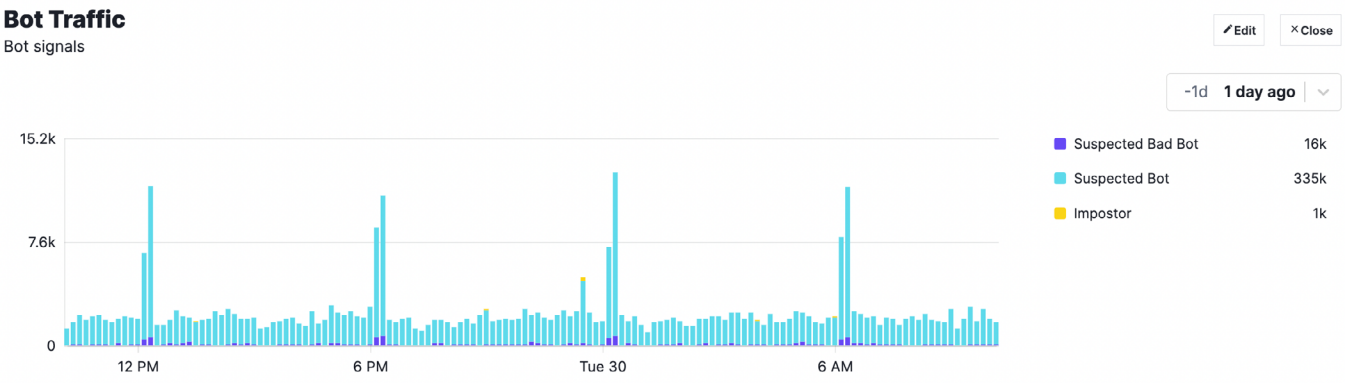
4. Identifies and Blocks Bots and Scrapers to Protect Your Resources

Attackers use automation and botnets to acquire valuable data, especially from content-rich sites in 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.



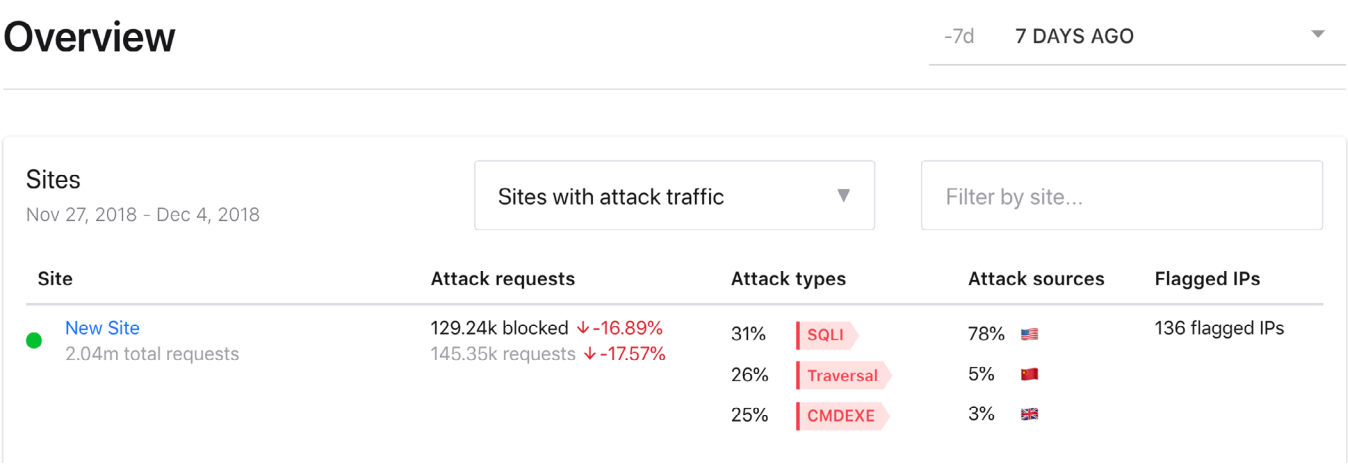
A 30-Day Events report summarizes attacks blocked (left column) and the volume of malicious requests blocked from a flagged IP address (upper right). Our Timeline view shows why the IP was flagged as malicious as well as current status (active or past event).



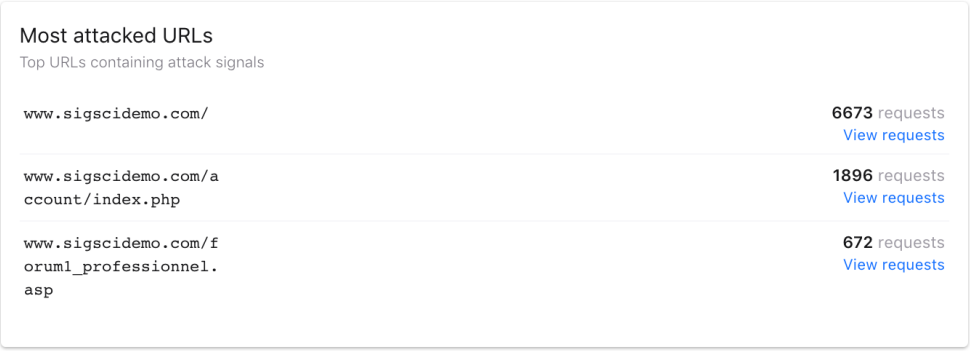
With rate-limiting rules enabled, Fastly blocks high-volume malicious bot requests.

5. Serverless protection with native integrations in AWS Lambda functions

Serverless architectures are quickly becoming a popular way to deploy and manage applications in the cloud, especially since it provides scaling and cost efficiencies. But they still require protection from Layer 7 threats. Fastly's native integration of our Next-Gen WAF into AWS Lambda functions helps provide comprehensive security for serverless architectures. Our agent can be invoked within a Lambda function itself to minimize latency and increase performance, or can be made into a Lambda layer allowing for easy integration into all of your functions. Our solution ensures consistent protection, features, and performance across distributed architectures, safeguarding your Layer 7 assets from both OWASP-style incidents and advanced attacks.



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.

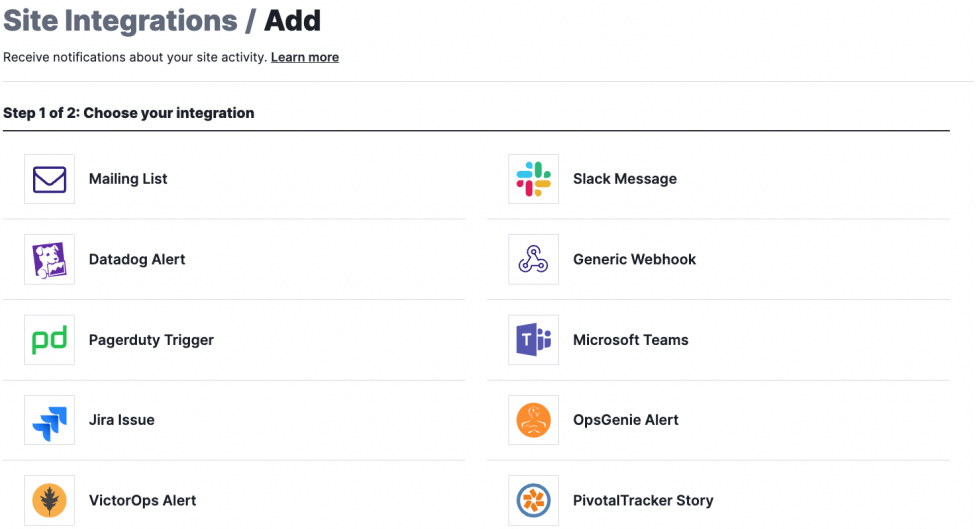


Example of specific URLs receiving the most malicious requests. Your team can get more context by drilling down to a "Requests" report for each attacked URL.

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 could 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

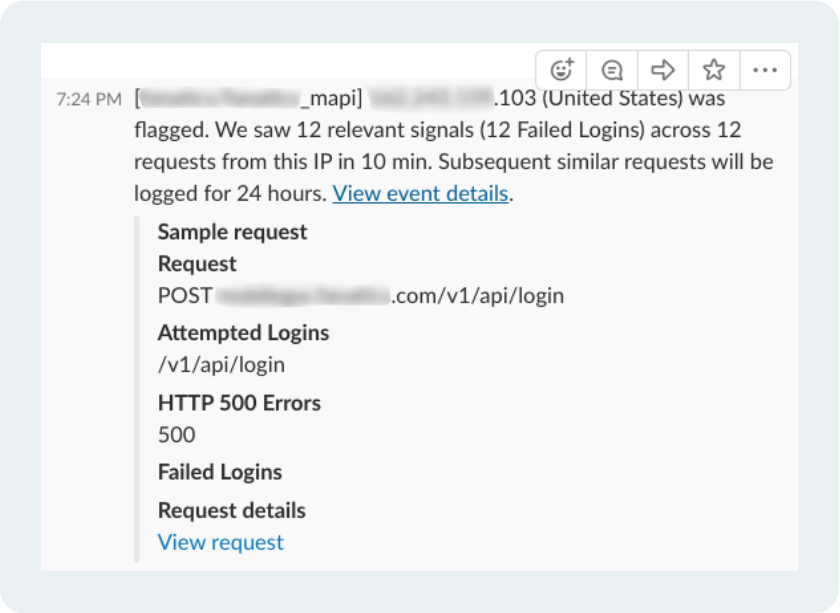
The Fastly Next-Gen WAF provides the broadest coverage against real threats and attack scenarios across any modern architecture, including the mobile apps that empower your customers to access your products and services anywhere. As mobile applications rely on APIs to transfer critical data from application 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.

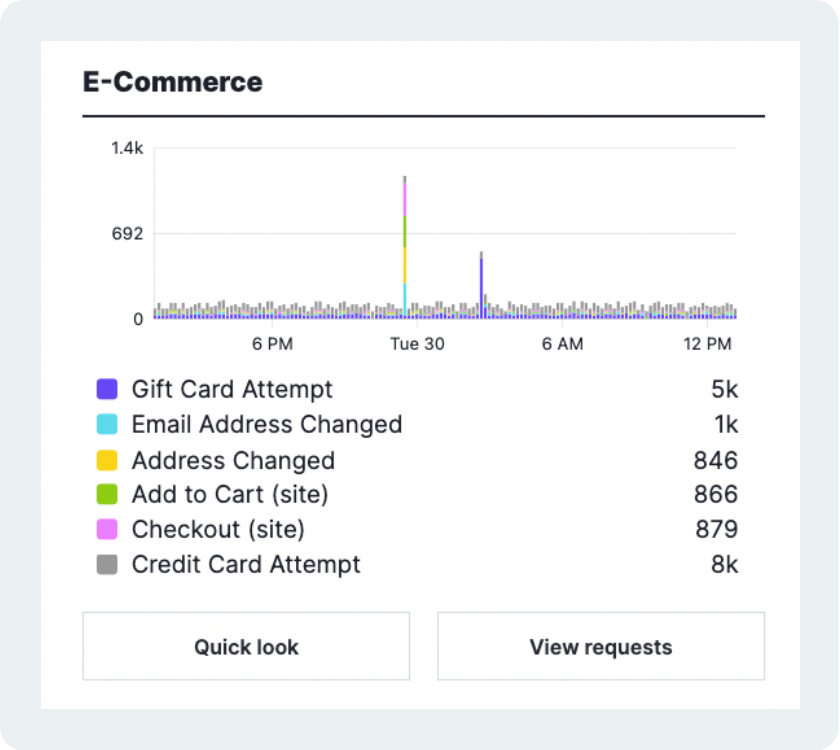
For example, you can view the number of transactions per minute, checkouts per hour, discount codes used, and so on.

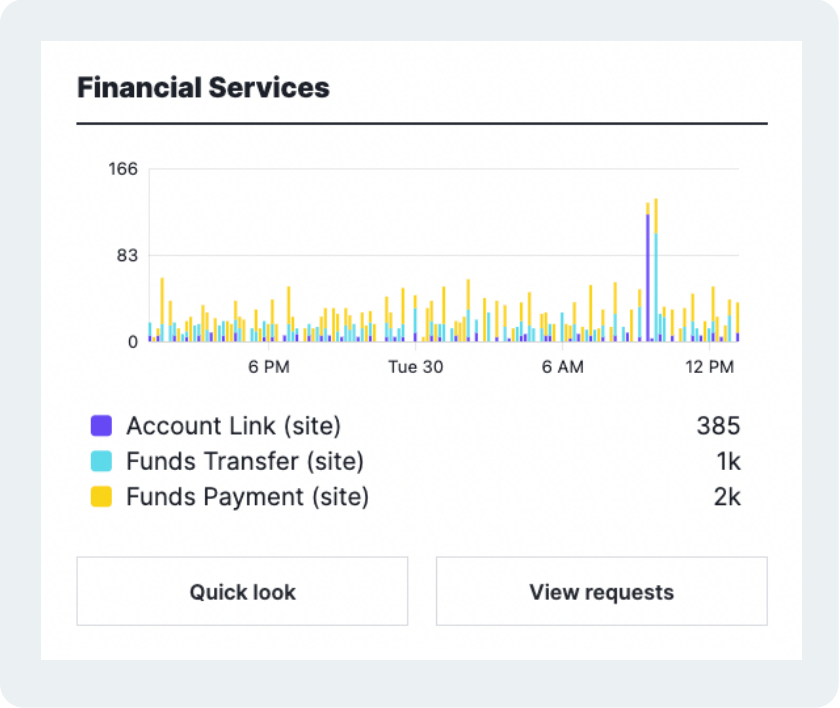
With added visibility that doesn't impact the performance and user experience of your mobile app, your teams can gain insight into particular use and abuse patterns (that were formerly difficult to find) buried in log data.

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.

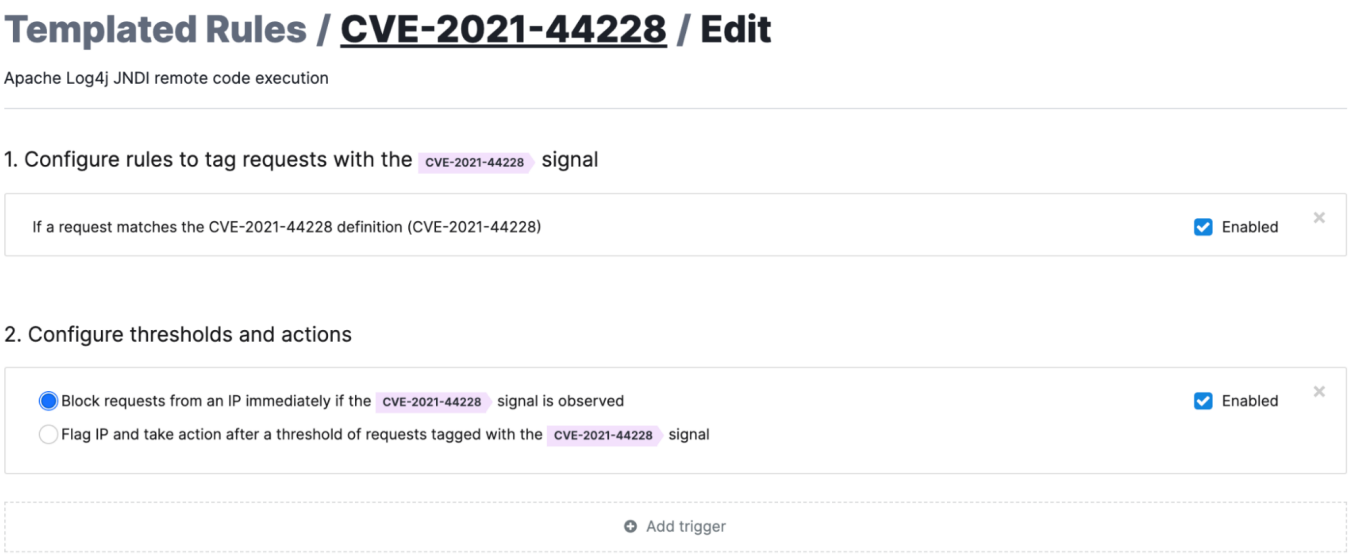
8. Addresses Vulnerabilities with Virtual Patching

Software creates new vulnerabilities that attract attackers who unleash payloads to exploit its 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. This 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. It connects asynchronously with our powerful cloud-hosted analytics backend: Cloud Engine. Net result? Almost zero latency and minimal impact to your applications' uptime and customer experience. We built our agent to expose metrics that operations teams rely on, from CPU and memory usage to how much delay the 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 vendors don't have APIs for these metrics and provide little detail in their UI.



This example 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.

Agents

Agents and modules work together to analyze and take action on malicious web traffic. Learn more

Manage alerts | View agent keys

Agents		Module		Status	
All	5	All	5	All	5
Online	5	Detected	5	Host clock skew	0
Offline	0	Undetected	0		
Outdated (How to update)	5	Outdated (How to update)	5		

Overview | Metrics

5 agents

Filter by agent name, IP address...

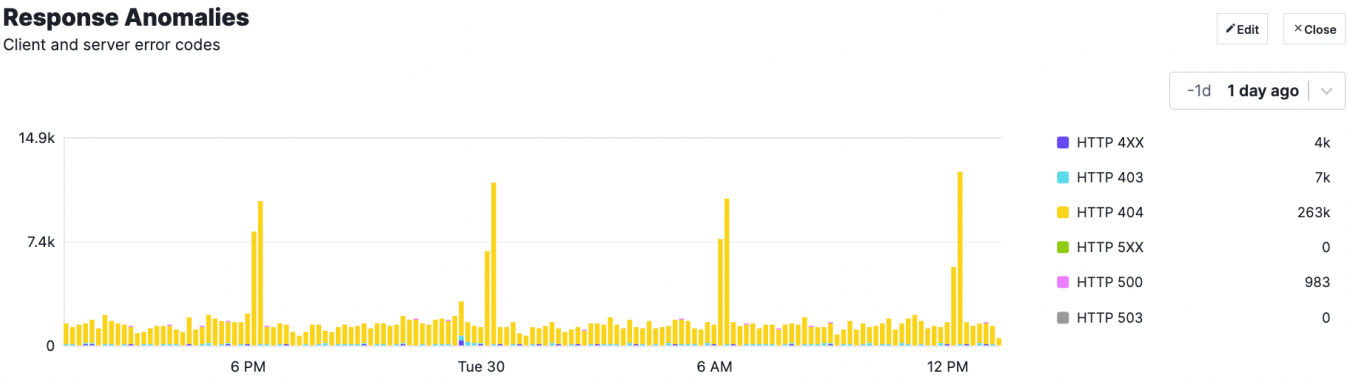
AGENT ▲	CURRENT REQUESTS	CONNECTIONS TOTAL	CONNECTIONS OPEN	CONNECTIONS DROPPED	MEMORY CONSUMED	UPTIME	HOST CLOCK SKEW	DECISION
demo-site-759df9f74b-6w9jj	10	2m	0	0	74.3MB	11 d, 2 h, 32 min, 22 sec	1 sec	5.29468
demo-site-759df9f74b-dswch	10	2m	0	0	60.3MB	11 d, 2 h, 35 min, 25 sec		4.97828
demo-site-759df9f74b-h2dlq	11	2m	0	0	74.4MB	11 d, 2 h, 35 min, 22 sec		6.25097

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.

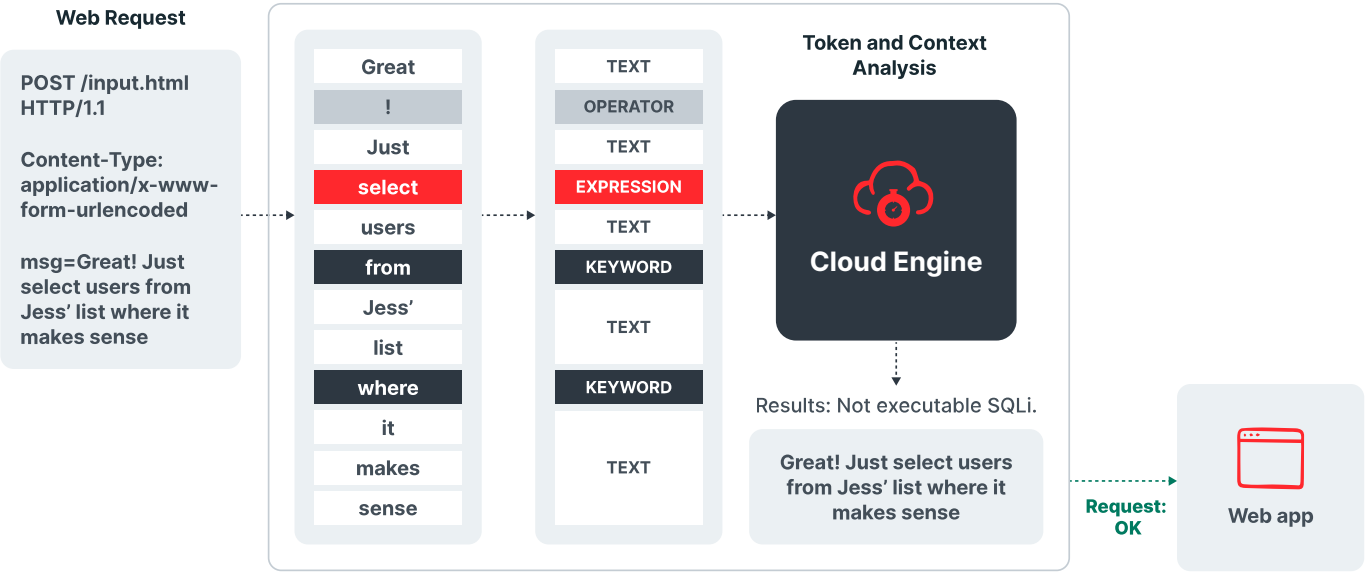
10. Automated Blocking that Scales with Rules Tuning

Legacy WAFs were created when waterfall development (long, sequential release cycles) and homogeneous environments defined the software development lifecycle. Today they require learning mode and constant signature tuning to rule out false positives, and 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 Fastly 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

The AppSec Solution for Modern Development Teams

Fastly's Next-Gen WAF combines essential capabilities to meet the needs of modern development, operations, and security teams, ensuring quick and secure software iteration and release. With easy installation, comprehensive coverage, seamless AWS integration, and support for AWS services, Fastly ensures application reliability, simplified management, and enhanced cloud security. On top of all this, Fastly has achieved AWS Security Competency status as a proven AWS Partner with validated technology and deep security expertise, offering comprehensive web app and API protection. Together with AWS, Fastly's Next-Gen WAF protects against advanced threats, delivers rapid time to value, and enables scalable business growth.

Contact us to learn more.