Datasheet

Next-Gen WAF

Get advanced protection for your applications, APIs, and microservices, wherever they live, from a single unified solution.

Smarter, easier security

- ✔ Defeat advanced threats
- ✔ Visibility for faster remediation
- ✔ Protection everywhere you operate

~90%

of customers in full blocking mode

Traditional WAFs rely on regex pattern-matching rules that are difficult to manage and require constant tuning to avoid false positives that block legitimate traffic. Fastly's Next-Gen WAF effectively detects and blocks malicious traffic without tuning, so your AppSec teams can focus on bigger problems. Use sophisticated techniques like deception easily to frustrate attackers without custom development.

Contextual detection

- Our Next-Gen WAF uses SmartParse, a highly accurate detection method, to evaluate the context of each request and how it would execute, to determine if there are malicious or anomalous payloads in requests. SmartParse enables near-zero tuning and the ability to start detecting threats immediately.

Preemptive security

- NLX is a trusted IP reputation feed based on anonymized, confirmed malicious activity collected from tens of thousands of Fastly customers. It uniquely recognizes attack patterns across our customer network, then alerts upon and preemptively defends your web apps and APIs.

Flexible Deployment

- Our hybrid SaaS WAF quickly installs via an agent-module software pair or via edge or cloud-based options that require no software installation.

Learn more at
https://www.fastly.com/products/web-application-api-protection