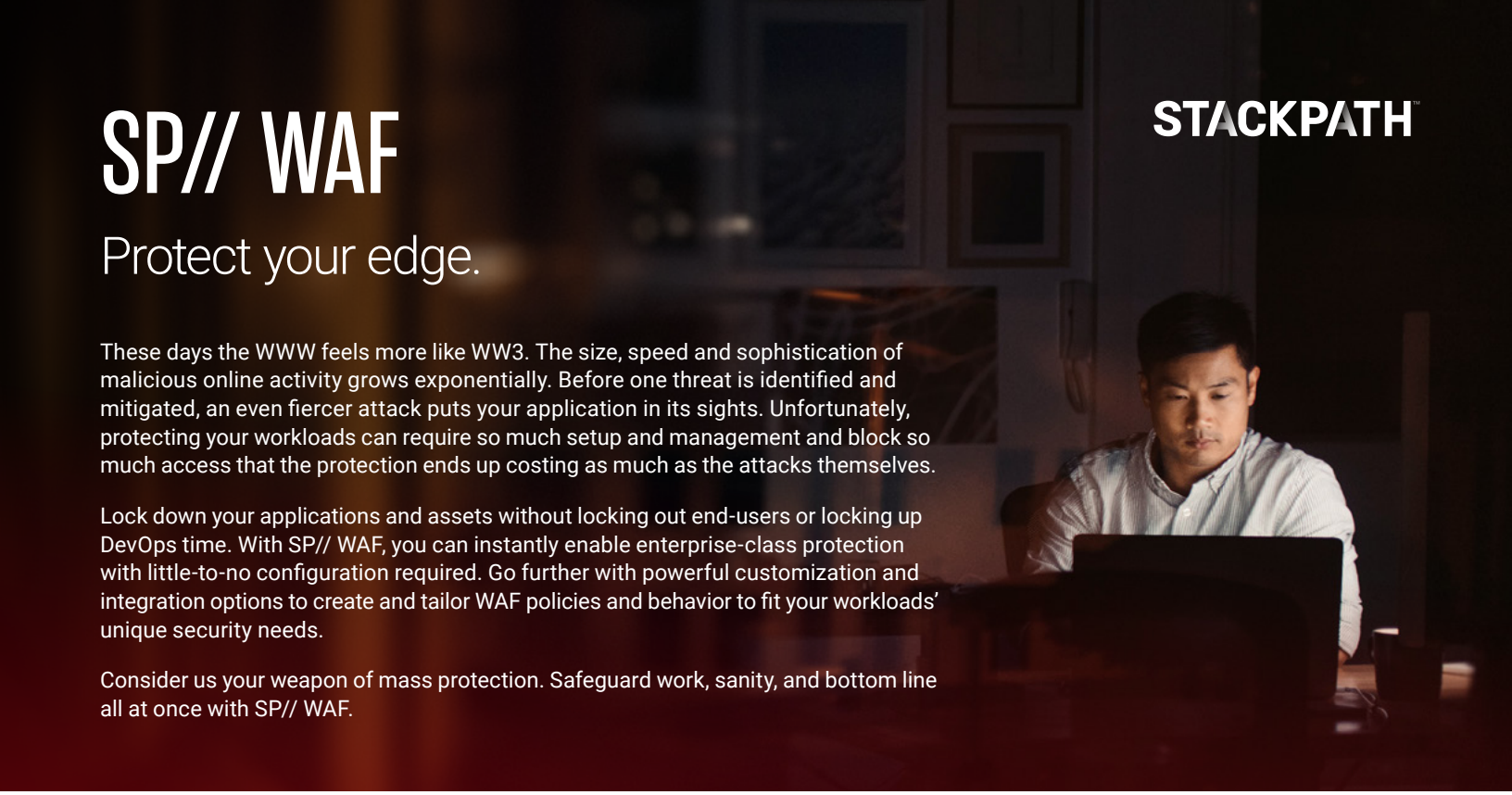
SP// WAF

Protect your edge.

STACKPATH



These days the WWW feels more like WW3. The size, speed and sophistication of malicious online activity grows exponentially. Before one threat is identified and mitigated, an even fiercer attack puts your application in its sights. Unfortunately, protecting your workloads can require so much setup and management and block so much access that the protection ends up costing as much as the attacks themselves.

Lock down your applications and assets without locking out end-users or locking up DevOps time. With SP// WAF, you can instantly enable enterprise-class protection with little-to-no configuration required. Go further with powerful customization and integration options to create and tailor WAF policies and behavior to fit your workloads' unique security needs.

Consider us your weapon of mass protection. Safeguard work, sanity, and bottom line all at once with SP// WAF.

Use Cases

Application Protection
Protect internet-connected applications, including websites, online games, APIs and SaaS products, with little to no additional performance overhead or impact to legitimate traffic.

Content Protection
Control access to and protect the value of the content you sell or deliver, such as photography, video streams and files, audio streams and software packages.

Layer-7 DDoS Attack Mitigation
Block and resolve application-layer DDoS attacks of any size, with unique and comprehensive identification technologies and techniques.

Virtual Patching
Quickly and easily protect newly identified application vulnerabilities that have not yet been patched in your application source code.

Benefits

High-Precision Threat Identification
Unique device-level fingerprinting, diverse DDoS attack profiling, and globally synchronized threat detection and mitigation reduces false-positives and catches sophisticated and emerging threats.

Instant and Easy Setup
Built-in policies created by our expert security team mitigate the most common and dangerous threats, including OWASP Top 10, right out-of-the-box, requiring little-to-no configuration.

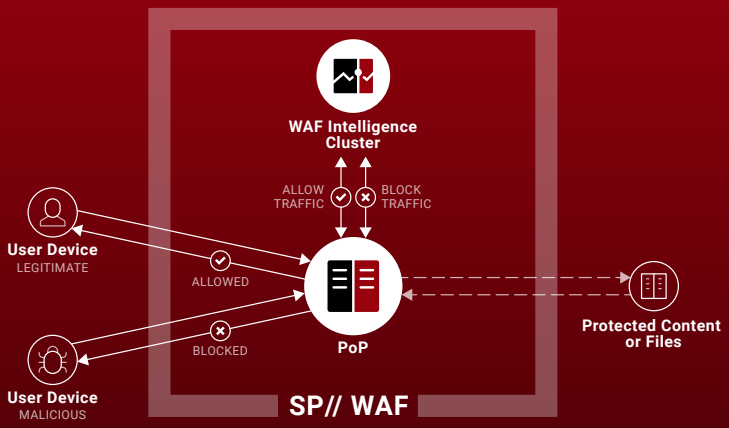
Always Up to Date
Allow our around-the-clock security experts update built-in policies in real-time to address emerging or increasing threats identified anywhere in the world, requiring no action on your part.

Total Customization and Control
Built-in policies are easy to toggle on/off or further customize. An easy-to-use custom rules engine and robust API make it simple to create unique security policies and system integrations.

How it Works

Deliver your content and use the power of SP// WAF to get to your end users securely without comprising on speed.

Filter, monitor, and block any malicious traffic instantly with our continuously updated built-in policies through the WAF Intelligence Cluster. Allow valid traffic to be sent straight to the originating source.



Features

Built-in Policies

Powerful WAF policies created by our expert team are automatically activated for each WAF site you create—with no action needed from you or additional cost required—addressing vulnerabilities related to:

- **OWASP Top 10 Threats**
- **CSRF Attacks**
- **User Agents**
- **Traffic Sources**
- **Automation and Bot Protection**
- **Spam and Abuse**
- **Irregular Traffic Behavior**
- **CMS Protection**
- **Known and Unknown Bots**
- **Brute-force Attacks**

Customized Rules Engine

An easy-to-use rules editor lets you create EdgeRules™ that enforce your own policies and automate protection behaviors, including:

- **Rate Limiting**
- **Block List IP Addresses and Ranges**
- **Allow List IP Addresses and Ranges**
- **Perform CAPTCHA**
- **Browser Validation**
- **Monitoring**

Device-level Fingerprinting

Patented device-level fingerprinting technology distinguishes individual devices—not just individual IP addresses—to take a better look at suspicious traffic and reduce false or missed positives from situations, like bad devices using different IPs or good devices using “bad” IPs.

Anti-Automation Suite / Bot Traffic Protection

Patented technology stops malicious activities—like inventory lockups, scraping and price stealing—from automated tools and bots, identifying and covering tactics and threats including:

- **Common Traffic Anomalies**
- **Domain-specific Traffic Anomalies**
- **Automated Clients**
- **Headless Browsers**

Layer-7 DDoS Attack Mitigation

Overlapping layers of threshold rules (domain, burst, sub-second) recognize application layer DDoS attacks and activate the protection of individual or clustered resources, while machine-learned models of normal traffic allow good traffic through even while DDoS attacks are being mitigated.

Data & Analytics

Built-in monitoring and reports provide real-time visibility of WAF activity, with all the details of any security event available including:

- **Rule triggered**
- **Action Taken**
- **Source IP**
- **Source Country**
- **User Agent**
- **Client (application)**
- **Client Type**
- **Request Headers**