edgescan™

FEATURE OVERVIEW

AI-Powered WAF Rule Generation

Accelerate virtual patching with AI-assisted WAF rule generation.

WAF 2.0 extends the value of validated vulnerabilities by generating vendor specific Web Application Firewall (WAF) rules directly from trusted findings. Review, refine and deploy WAF rules faster while maintaining expert oversight and existing remediation processes.

Manual WAF rule creation can slow down protection

When a critical vulnerability is identified, security teams often need to manually create WAF rules, coordinate with infrastructure teams and validate syntax before protection can be applied.

The process takes time, time that can increase exposure while permanent remediation is being planned.

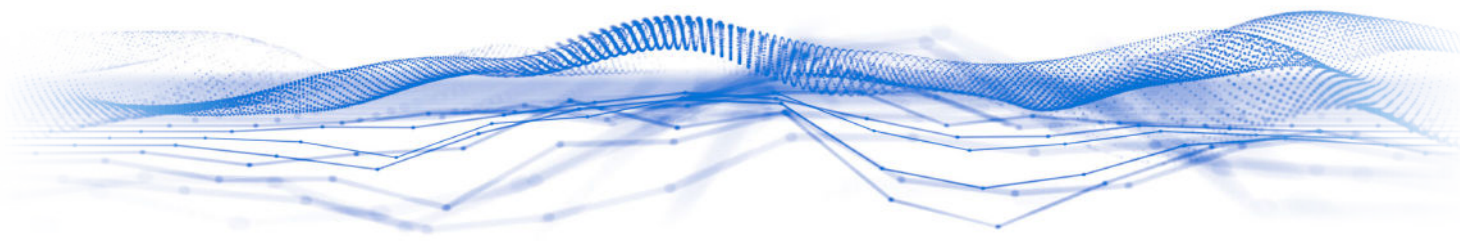
Traditional Patch Generation	WAF 2.0 Patch Generation
✘ Manual WAF rule creation	✔ AI-assisted rule generation
✘ Time spend writing code	✔ Generated rules in moments
✘ Multiple handoffs	✔ Streamlined collaboration
✘ One firewall format	✔ Vendor-specific rule generation
✘ Manual translation	✔ Rules generated from validated findings

Extend the value of every validated vulnerability

Validated Vulnerabilities already provide the confidence needed to make informed remediation decisions.

Edgescan's AI-powered WAF Rule Generation extends that value by helping organisations generate vendor-specific WAF Rules in just a few clicks, reducing manual effort while supporting existing remediation workflows.

WAF 2.0 provides another way to reduce exposure while permanent fixes are planned, tested and deployed.



How It Works

Validate

Every workflow starts with a validated vulnerability within Edgescan.

Generate

Select WAF Virtual Patch from the vulnerability page.

Choose

Select your WAF technology. The rule automatically regenerates to match the selected platform.

Review and Deploy

Review the script and share with your team to support virtual patching while permanent remediation progresses.

Key Benefits

Accelerate Virtual Patching: Generate WAF rules directly from validated vulnerabilities to reduce the time between identifying a risk and implementing protection

Reduce Manual Effort: Remove repetitive WAF rule creation and allow security teams to focus on higher value security decisions

Support Existing Workflows: Integrates naturally into your existing remediation process without changing operational workflows

Vendor specific Rule Generation: Generate rules tailored to supported WAF technologies with a single click

Extend Validated Vulnerabilities: Built on trusted findings with another practical layer of remediation support

Ideal For

- Security teams managing application security
- Organizations using Web Application Firewalls
- Teams looking to accelerate virtual patching
- Enterprises reducing manual remediation effort

For more information on how Edgescan can help secure your business, contact: *sales@edgescan.com*

edgescan

IRELAND | Unit 701 Northwest Business Park, Ballycoolin, Dublin 15, D15 CH26
UNITED STATES | 445 Park Avenue, 9th Floor, New York, NY 10022