Wallarm on Lumen

End-to-end API Security and WAF right at the edge

Modern organizations need to support more diverse environments. There is a wide array of highly sophisticated threats targeting your applications and API portfolio: injection attacks, DDoS, account takeover (ATO), brute force, credential stuffing, as well as API-specific threats. Legacy web applications firewalls (WAFs) fall short in delivering the breadth, accuracy and speed needed to keep up with today's high-impact and multi-vector attacks.

Wallarm on Lumen offers an end-to-end solution to discover all applications and APIs, protect them against emerging threats, and streamline your incident response. All of which can be deployed and configured quickly and easily on the Lumen global edge - for many use cases within 60 minutes.

Protection against new and existing threats

Wallarm on Lumen secures applications and APIs from OWASP Top 10, bots and application abuse with no manual rule configuration and minimal false positives.

Real-time alerting and rapid response

Monitor your threats with complete visibility and easily drill down into malicious requests to block them before they harm your systems. Leverage Wallarm's 24/7 SOC to get quick response protocols whenever you're under attack.

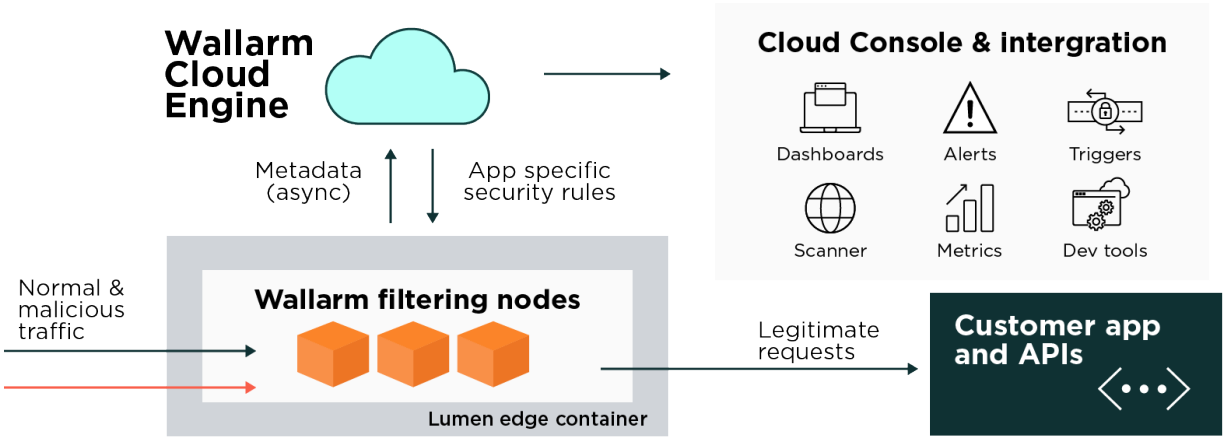
Understand your attack surface

You can't protect what you don't know. API Discovery will help to understand your attack surface and shadow resources to track changes. Identify misconfiguration issues and vulnerable applications and resources.

> **By 2022, API attacks will become the most-frequent attack vector, causing data breaches for enterprise web applications."**
>
> — **Gartner. API Security:** What You Need to Do to Protect Your APIs

LUMEN® TECHNOLOGIES

How it works



Features and specs

App / API protection	• Complete protocol support (JSON, XML, WebSocket, gRCP, GraphQL, REST, SOAP) • Robust protection for the entire application including OWASP Top 10 (injections, XXE, RCE, etc.), API abuse, credential stuffing, bots, account takeover • No API specs required
API discovery	• Discovers API endpoints and parameters; API inventory (legacy, zombie, and shadow APIs) • Track changes in APIs • No manual configuration, no schema uploading
DevOps / integrations	• Ready for CI/CD; doesn't rely on API specifications. • Set up cross-team workloads via your existing DevOps and security tool chain (SOARs, SIEMs). • Set up triggers and noise-free alerts in Slack and other messengers, PagerDuty and more. • Native support of Kubernetes and containers, and seamless deployment on Lumen CDN edge
Automation	• Wallarm's libDetection and core signature-less attack detection encourage low false positives. • Automated incident response reduces manual analysis and noise level. • Automated threat verification dissects potentially harmful attacks from millions of random scans and report vulnerabilities.

Wallarm's end-to-end API security solutions provide enterprise-class protection for APIs, microservices, and serverless workloads running in cloud-native environments. Hundreds of Security and DevOps teams from organizations including the Fortune 500, rely on Wallarm to get unique visibility into malicious traffic, robust protection across the whole API portfolio and automated incident response.

wallarm

Why Lumen?

It's all about the experience. Lumen helps enterprises accelerate development workflows, optimize performance and secure applications through containerized modules designed to power and protect the digital interactions your customers demand.

lumen.com | application.delivery@lumen.com

LUMEN® TECHNOLOGIES