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.

“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
How it works

Wallarm Cloud Engine
Metadata (async) → App specific security rules

Wallarm filtering nodes
Normal & malicious traffic → Lumen edge container

Cloud Console & integration
Dashboard → Alerts → Triggers
Scanner → Metrics → Dev tools

Customer app and APIs
Legitimate requests

Features and specs

| App / API protection | • Complete protocol support (JSON, XML, WebSocket, gRPC, 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.

Why Lumen?

At Lumen, we understand the security pressures our customers face. We offer a holistic and comprehensive approach to security. Lumen provides the flexibility your DevSecOps team requires for rapid, agile deployment – delivered via our common automation and orchestration platform: Lumen Application Delivery Solutions.