

Managed Web Application and API Protection (WAAP)

Comprehensive threat detection and response in one managed solution.

Web applications and APIs drive innovation and growth but expand the attack surface. LevelBlue Managed WAAP unifies protection to simplify security, prevent breaches, and scale with your business.

LevelBlue Managed Web Application and API Protection

LevelBlue Managed WAAP services are designed to help organizations secure their digital environments without adding operational burden. By combining Akamai's industry-leading App and API Protector platform with expert-led management, LevelBlue enables customers to protect critical applications and APIs, reduce risk, and maintain performance at scale. Our services are delivered by experienced security specialists to drive measurable outcomes:

Stronger Security Posture

Stay ahead of attackers with real-time threat detection. LevelBlue delivers 24x7 protection through a team of experts in web application and API security. Our AI-powered threat detection and edge-based controls identify and neutralize threats early — keeping your environment resilient and adaptive.

Reduced Risk and Downtime

With 24x7 monitoring, behavioral traffic analysis, and expert-led incident response, LevelBlue helps minimize the impact of attacks including API abuse, bot-driven fraud, and denial-of-service disruptions. Rapid threat identification and mitigation help maintain uptime and business continuity.

Operational Simplicity

Managing WAAP solutions can be complex and resource intensive. LevelBlue eliminates this burden by providing a fully managed service that handles policy tuning, threat response, and optimization. This reduces false positives, closes internal skill gaps, and frees security teams to focus on strategic priorities.

Improved Performance

Protect users without degrading experience. LevelBlue ensures applications remain fast and responsive through adaptive mitigation and optimized policy enforcement even during peak traffic or active threats.

Better Visibility

Gain actionable insights into traffic patterns, threats, and API behavior through continuous discovery, real-time analytics, and detailed reporting. LevelBlue enables faster, more informed security decisions.

Why LevelBlue Managed WAAP?

- Protect web apps and APIs with integrated WAF, DDoS defense, bot mitigation, and comprehensive threat detection and response in one managed solution.
- Leverage behavioral analysis and AI to gain critical insights into your evolving threat landscape, anticipating and neutralizing attacks ahead of impact.
- Built on the globally recognized Akamai App and Protector platform, trusted by enterprises worldwide for high-performance, edge-based protection.
- Take advantage of flexible service tiers and scalable protection that can grow with your organization.
- Deploy quickly with onboarding support for security policy and configuration setup, tailored tuning, and integration.
- Discover and catalog apps and APIs across your network and address risks.
- Benefit from global threat intelligence to improve security outcomes.
- Access 24x7 help desk, dedicated collaboration spaces, and strategic guidance to keep your defenses sharp.

Service tiers

LevelBlue Managed WAAP is available in two service tiers, Essentials and Advanced, designed to meet the needs of organizations at different stages of digital maturity. Both tiers include the full suite of WAAP service components, with the Advanced tier offering deeper protection, proactive management, and enhanced support.

Discover

Continuously maps your web apps and APIs including shadow assets using AI-driven analytics to uncover vulnerabilities and misconfigurations.

Simplify

Centralized visibility, auto-updating policies, and seamless integration with development pipelines reduce complexity and accelerate response.

Defend

Blocks threats in real time with adaptive WAF rules, bot mitigation, API protection, and layer 7 and layer 3/4 DDoS defense.

Optimize

Continuously refine protections based on traffic behavior and threat patterns to reduce false positives and improve performance.

Service Component	Essentials	Advanced Essentials capabilities plus
Deployment and Onboarding	<ul style="list-style-type: none"> Initial setup and policy deployment 	<ul style="list-style-type: none"> Includes advanced tuning and multi-environment support
WAF Policy Management	<ul style="list-style-type: none"> Baseline rules with automatic updates 	<ul style="list-style-type: none"> Custom rules and as-needed tuning
API Protection	<ul style="list-style-type: none"> API discovery and basic controls 	<ul style="list-style-type: none"> Parameter validation, rate limiting group policies
Bot Mitigation	<ul style="list-style-type: none"> Baseline detection and blocking 	<ul style="list-style-type: none"> Behavioral analysis and custom mitigation
DDoS Protection	<ul style="list-style-type: none"> Always-on edge-based protection 	<ul style="list-style-type: none"> Adaptive mitigation, fine-tuned thresholds and Slow POST protection
Tuning and Optimization	<ul style="list-style-type: none"> Self-service tuning via portal 	<ul style="list-style-type: none"> Expert-led, behavior-informed tuning
Traffic Monitoring	<ul style="list-style-type: none"> Self-monitoring via portal 	<ul style="list-style-type: none"> 24x7 monitoring, anomaly detection, and traffic forensics
SIEM Integration	<ul style="list-style-type: none"> Prebuilt connectors 	<ul style="list-style-type: none"> Managed integration with USM Anywhere
Threat Intelligence	<ul style="list-style-type: none"> Access to standard curated feeds via portal 	<ul style="list-style-type: none"> Direct access to Threat Team and tailored threat reports
Threat Management	<ul style="list-style-type: none"> Customer-managed via portal 	<ul style="list-style-type: none"> 24x7 monitoring, incident notification and root cause analysis
Attack Support	<ul style="list-style-type: none"> Business-hour support (limited) 	<ul style="list-style-type: none"> 24x7 real-time support and coordination Post-incident analysis
Incident Response	<ul style="list-style-type: none"> Business-hour phone support only 	<ul style="list-style-type: none"> 24x7 triage, investigation, and coordinated response
Support and Escalation	<ul style="list-style-type: none"> 24x7 support via phone/email/ticketing 	<ul style="list-style-type: none"> 24x7 support via phone/email/ticketing Quarterly operational reviews
Reporting	<ul style="list-style-type: none"> Self-service reports via portal Basic quarterly reports 	<ul style="list-style-type: none"> Quarterly reports with attack trends and expert recommendations
Customer Portal	<ul style="list-style-type: none"> Access for administration, analytics, reporting, and more 	<ul style="list-style-type: none"> Access for administration, analytics, reporting, and more