

LevelB/ue



PRODUCT BRIEF

# Secure Your Web Properties and APIs Using a Single Platform with LevelBlue App and API Protector



## Take Your Security Strategy to the Next Level with an Adaptive Self-Tuning Solution that Keeps Critical Web Applications and Data Safe and Secure.

Web applications and APIs make it easy to conduct transactions and connect with third-party partners. To make sure your websites, applications, and APIs remain trusted and secure, you need a web application and API protection (WAAP) solution that automatically learns, adapts, and defends against new and existing threats across all your attack surfaces.

LevelBlue App and API Protector strengthens your security strategy with a single WAAP solution that monitors and inspects incoming traffic at the edge to halt attacks before they happen.

### Why Choose LevelBlue App and API Protector

With so many applications and APIs to keep track of, it's hard to identify every loophole or vulnerability. LevelBlue App and API Protector is purpose-built to address this evolving application landscape. We combine advanced automation, machine learning, and adaptive self-tuning to protect against volumetric distributed denial of service (DDoS), automated botnet, injection, and API-based attacks to defend your network and applications.

### Features

- Adaptive self-tuning security offers precise, accurate, threat-based detection
- Extensive security controls detect and stop unwanted bots
- Security policies stay up to date
- Seamless protection scales to meet traffic demands with accelerated performance

### Benefits

- Single solution protects websites, apps, and APIs from a broad range of threats including DDoS, botnets, injection, and API-based attacks
- Frictionless maintenance
- Significantly reduces API attack surfaces
- Optimizes spending

## Security That is Adaptive and Self-Tuning

Modern applications and APIs use lots of moving parts, shared components, and third-party services. To prevent unauthorized access, LevelBlue App and API Protector checks every web and API request against the latest threat intelligence to identify attacks and reduce false positives that need to be investigated. Adaptive decision-making capabilities monitor inbound network traffic to guard against a wide range of common and targeted attacks. From there LevelBlue App and API Protector uses machine learning to analyze each threat and make policy recommendations that can be added to your existing protocols, quickly and easily.

## Advanced API Detection

The best offense is a lockdown defense. That's why LevelBlue App and API Protector scans all APIs in your web traffic by default and inspects them for errors, changes, and harmful code. It also collects information related to unexpected updates. And registering new APIs is done in just a few clicks. Our optional Advanced Security Management tool provides additional protection at the network edge to secure against unauthorized or suspicious API behavior.

## Real-Time Bot Visibility and Mitigation

Using a directory of thousands of known bots, LevelBlue App and API Protector detects, monitors, and defends against harmful bots and DDoS attempts without impacting the work of registered bots that make life easier for your users.

"LevelBlue is my first stop for security and technology."



**Stephen Locke**  
Chief Information Officer,  
NHS Management, LLC







### DevOps Integration and Collaboration

LevelBlue App and API Protector includes programmable APIs and security information and event management (SIEM) integration to speed software development, IT operations, and policy decision making. It also improves collaboration across teams and workflows to ensure your security keeps pace with the changing threat landscape.

### Optimal Performance, Maximum Protection

Your website is essential to the success of your agency. LevelBlue App and API Protector scales to meet your traffic demands, monitoring and adjusting central processing unit (CPU) and memory resources to keep you protected during times of peak activity. Cached content is delivered to the edge, along with image and video optimization, API acceleration, and edge computing capabilities to ensure your applications always perform at their best.

### Advanced Security Management

Our optional Advanced Security Management module offers flexibility and control when customized security measures are needed. A manual update

option lets you review new updates alongside existing protections, so you understand what is being updated and how you'll benefit. It also includes additional tools to manage web and API protections, including access to internet protocol (IP) threat intelligence data to verify the authenticity of the requests you're receiving.

### Additional Capabilities

- Automatic updates
- DoS/DDoS protection
- Network lists block malicious requests from specific IPs or traffic
- Custom rules
- Hostname evaluation
- Response actions
- Site Shield
- Dashboard, alerting, and reporting tools
- Simplified onboarding

# About LevelBlue

We simplify cybersecurity through award-winning managed security services, experienced strategic consulting, threat intelligence and renowned research. Our team is a seamless extension of yours, providing transparency and visibility into security posture and continuously working to strengthen it.

We harness security data from numerous sources and enrich it with artificial intelligence to deliver real-time threat intelligence. This enables more accurate and precise decision making. With a large, always-on global presence, LevelBlue sets the standard for cybersecurity today and tomorrow. We easily and effectively manage risk, so you can focus on your business.

**Cybersecurity. Simplified.**

To learn more, contact your LevelBlue representative or visit [LevelBlue.com](https://www.LevelBlue.com)