

Web Application and API Protection Capabilities Checklist



Deploying a web application and API security solution while planning, implementing, or optimizing your information security strategy will provide your organization with the ability to understand your unique risks, target security gaps, and detect threats. You need a web application and API protection (WAAP) solution that provides continuous visibility with comprehensive insights, and the full capability to identify and stop the most sophisticated attacks.

This checklist can be used to assess vendor capabilities or as a list of requirements needed to implement an effective WAAP solution.

CATEGORY 1: PLATFORM REQUIREMENTS

Organizations come in all shapes and sizes with varying degrees of requirements. Your web application security solution should be flexible, scalable, and easy to administer.

Scalability to match traffic demands and provide continuous protection without loss of performance

Architecture that can overcome the challenges of geographically dispersed applications

Audit log capabilities to ensure proper usage

Protection of on-premises, private, or public cloud (including multi-cloud or hybrid-cloud) site origins

Network layer [L3/4] distributed denial-of-service (DDoS) mitigation with a zero-second service-level agreement

Visibility into who is attacking, the frequency of attacks, and the severity of attacks with crowd-sourced attack intelligence across the platform

Reverse proxy with web traffic via ports 80 and 443

Network privacy protections with SSL/TLS encryption

Web Application and API Protection Capabilities Checklist

CATEGORY 2: ADAPTIVE WEB APPLICATION AND DDoS PROTECTION

Your web application security must go beyond traditional signature-based detection to more advanced forms of adaptive web application and DDoS protection for the most accurate and reliable security outcomes.

Detection beyond signature-based attacks with anomaly and risk-based scoring

Machine learning, data mining, and heuristics-driven detection capabilities to identify rapidly evolving threats

Automatic web application firewall (WAF) rule updates with continuous real-time threat intelligence from security researchers

Ability to test new or updated WAF rules against live traffic before deploying to production

Protection (at a minimum) against SQL injection, XSS, file inclusion, command injection, SSRF, SSI, and XXE

Fully customizable predefined rules to meet specific customer requirements

Protection from application layer [L7] volumetric DoS attacks designed to overwhelm web servers with recursive application activity

Fully managed WAF rules to eliminate the need for continuous configuration and updates

Client reputation scoring and intelligence for both individual and shared IP addresses

Custom rules to quickly protect against specific traffic patterns (virtual patching)

Request rate limits to protect against automated or excessive bot traffic

Protection from direct-to-origin targeted attacks

IP/Geography controls via multiple network lists to block or allow traffic from specific IP, subnet, or geographic areas

Protection from automated clients, such as vulnerability scanning and web attack tools

Web Application and API Protection Capabilities Checklist

CATEGORY 3: API VISIBILITY, PROTECTION, AND CONTROL

API protections have become a critical part of web application security. You need a WAAP solution with robust API discovery, protection, and control capabilities to mitigate API vulnerabilities and reduce your surface area of risk.

Automatic discovery and profiling of unknown and/or changing APIs (including API endpoints, characteristics, and definitions)

Automatic inspection of XML and JSON requests to detect API-based attacks

Custom API inspection rules to meet specific user requirements

Ability to predefine acceptable XML and JSON object formats that restrict the size, type, and depth of API requests

Protection of API back-end infrastructures from low and slow attacks designed to exhaust resources (e.g., Slow Post, Slow Get)

Real-time alerts, reporting, and dashboards at the API level

Rate controls (throttling) for API endpoints based on API key

API network lists (allowlists/blocklists) based on IP/Geography

API lifecycle management with versioning

Secure authentication and authorization via JSON Web Token (JWT) validation

Definition of allowed API requests by key (quota for each key defined independently) for full control over consumption

API onboarding using standard API definitions (Swagger/OAS and RAML)

Web Application and API Protection Capabilities Checklist

CATEGORY 4: FLEXIBLE MANAGEMENT

You need simple and automated workflows to maximize your investment and improve operational efficiencies. Whether protecting new or changing applications, adopting new WAF rules, or extending protections to APIs, the process must be seamless and intuitive.

Open APIs and the CLI to integrate security configuration tasks into CI/CD processes

Integration with on-premises and cloud-based security information and event management (SIEM) applications

Full staging environment and the ability to implement change control

Self-tuning security protections that automatically adapt to your traffic

Real-time dashboards, reporting, and heuristics-driven alerting capabilities

Centralized user interface (UI) to access detailed attack telemetry and analyze security events

Flexibility to manage WAAP via high-touch controls and/or fully automated protections

Fully managed security services to offload or augment your security management, monitoring, and threat mitigation

The Akamai Intelligent Edge Platform gleans insight from millions of web application attacks, billions of bot requests, and trillions of API requests every single day. This level of insight, coupled with advanced machine learning and threat research, allows us to constantly improve, catch new threats, and develop innovative capabilities.

Akamai's web application and API security solutions will secure your organization against the most advanced forms of web application, DDoS, and API-based attacks. Contact us today to learn more about our WAAP solutions and to schedule a demonstration.



Akamai secures and delivers digital experiences for the world's largest companies. Akamai's intelligent edge platform surrounds everything, from the enterprise to the cloud, so customers and their businesses can be fast, smart, and secure. Top brands globally rely on Akamai to help them realize competitive advantage through agile solutions that extend the power of their multicloud architectures. Akamai keeps decisions, apps, and experiences closer to users than anyone – and attacks and threats far away. Akamai's portfolio of edge security, web and mobile performance, enterprise access, and video delivery solutions is supported by unmatched customer service, analytics, and 24/7/365 monitoring. To learn why the world's top brands trust Akamai, visit akamai.com, blogs.akamai.com, or @Akamai on Twitter. You can find our global contact information at akamai.com/locations. Published 11/20.