Ultimate WAF Evaluation Checklist

A tool to find the right solution for your application and API security needs

Simplify your search for the right web application firewall (WAF) or web application and API protection (WAAP) vendor. Use this comprehensive checklist to evaluate WAF and WAAP providers, ensuring that the solution meets your security, performance, financial, and operational needs.

Security capabilities

Application security

- Ensure **coverage against the OWASP Top 10 vulnerabilities**, such as SQL injection, XSS, LFI, and SSRF. Confirm whether protection can be customized and automatically deployed.
- Assess whether your solution proactively controls traffic from **IPs with bad reputations** and warns you if a previous **exception is being abused**.
- Assess the **flexibility of allowlists and blocklists** — can you correlate attributes like IP, Geo, ASN, and TLS fingerprints to create effective policies?

DDoS protection

- Validate that the vendor offers **multilayer DDoS protection** for applications and APIs, including DNS, Layer 3/4, and Layer 7.
- Confirm that the solution offers **behavioral DDoS detection** for application security.
- Determine the granularity of **rate limiting** controls. Are these automatic or manually configured? Can these measures protect against both volumetric and slow-post attacks?
- Review the capabilities that **reduce load** during DDoS attacks and enhance performance.
- Understand potential **additional costs** from increased traffic during DDoS events.
- Ensure that **L7 DDoS protection is automated** to save your team time and expertise. Are the **protections adaptive** to your specific traffic profile or risk tolerance?

Zero-day exploit protection

- Confirm that the WAF has **existing protections for known CVEs** and can rapidly adjust to defend against new zero-day exploits. Investigate the solution's **zero-day defense track record** and response times.
- Determine whether you have **protections against specific CVEs** as a customer.

API protection

- Ensure the solution **protects API endpoints** from injection attacks, DoS, and specification violations.
- Check for **API discovery** — can it detect new and modified APIs automatically? How easily can you apply protection to them?
- Confirm **PII detection and alerts** to safeguard sensitive data and prevent data breaches.

Bot protection

- Confirm whether the WAF **detects and mitigates automated threats** by using a bot directory and definitions. How expansive is the bot directory? How often is it updated with new and modified bots?
- Determine what **bot definitions** exist in the tool. Can you **create your own** bot definitions?
- Check whether the solution includes a **CAPTCHA or human verification mechanism** that doesn't disrupt the user experience. Does the CAPTCHA/verification require your end users to interact with it before moving forward?

Threat intelligence and automation

Threat intelligence

- Ensure the provider uses **first-party data** for threat intelligence, avoiding third-party delays and potential data tampering.
- Verify the size of the provider's **threat hunting team** and the global network of security experts who monitor emerging risks.
- Assess the **volume and relevance of data** processed by the intelligence database. Does it include data from industries similar to yours or from organizations frequently targeted by cyberattacks?

Automation

- Check whether the WAF relies on **outdated ruleset technology**. Does it use advanced, modern technologies such as automated updates via advanced heuristics and machine learning?
- Ensure that rulesets are automatically updated to **eliminate manual intervention**. Are automatic updates applied on a global level? What are your options to remove a previously applied update or **test it on live traffic**?
- Determine whether the solution customizes protections to your environment without intervention. Does the solution **self-tune** security policies continuously based on your org's live traffic profile?
- Evaluate how the solution controls for **false positives**. How does it balance reducing false positives with minimizing the **disruption of valid traffic**?

Visibility and reporting

Granular visibility

- Ensure the WAF provides **detailed visibility into threats** and performance, with customizable dashboards and reporting that cover multi-solution environments.
- When operating a WAF, security teams spend most of their time in the data console. Explore the **customizations**, proactive analysis features, and **granularity of reporting** you will have access to.
- Evaluate the solution's ability to **monitor API traffic** and application traffic effectively, detect abuse, and provide detailed insights into API sprawl.

Real-time alerts and proactive analysis

- Check for near–**real time alerting** capabilities that notify your team of critical threats. Alerts should be customizable based on specific criteria such as severity, source, or attack type for ease of understanding and rapid response.
- Look for the solution to deliver **pre-analyzed insights** into where, when, and how attacks occur to reduce the burden on your security team. The solution should also **recommend next steps** to improve your security stance.

Platform and architecture

Global reach

- Confirm whether the WAF provides access to a global network edge or CDN services for enhanced performance and security. Research the solution's **global availability** to ensure coverage for your primary locations and those of your customers.

Cloud and hybrid support

- Verify that the solution is **cloud agnostic** and capable of supporting your multicloud, hybrid, and on-premises environments. If CDN based, ensure the solution can extend protection beyond CDN for off-edge security.

Resiliency and failover

- Assess the **solution's resiliency** — can it failover automatically to maintain protection during outages or disruptions?
- Review the provider's **recent service interruptions and response**.
- Determine if the **service-level agreements** (SLAs) meet your business needs.

Support and managed services

Included support and access to services

- Determine the **levels of support included** and available at a cost with the WAF solution.
- Check whether **24/7 incident response** is available and whether you will have direct access to the security operations center (SOC) during attacks.
- Ensure the vendor offers **fully managed security services** to cover potential gaps in your internal resources, including expertise for handling attacks, configuration, or staff turnover.

Integration and DevSecOps compatibility

APIs, CLI, and infrastructure automation

- Check for **APIs, CLI, and Terraform** integration to automate and embed security into your development workflows. Support for GitOps and other infrastructure-as-code frameworks is crucial for consistent security enforcement across environments.

SIEM integration

- Ensure the WAF **integrates seamlessly with SIEM** tools like Splunk or QRadar for enhanced monitoring, reporting, and incident response.

Business outcomes and efficiency

Scalability and performance

- Confirm the solution's ability to **scale automatically** to handle large volumes of traffic without degrading performance. At what point does the solution introduce latency or become vulnerable under heavy load?
- Ensure there's a **100% availability** SLA and assess whether the solution can also provide performance enhancements such as caching and traffic acceleration to improve your applications.

Unified management

- Evaluate whether the provider offers a single-pane-of-glass interface to **manage security policies across all environments** — cloud, on-premises, and hybrid. Ensure that the solution is integrable with your current stack and provides a frictionless experience for both security and development teams.

Cost effectiveness

- Assess the solution's ability to **unify WAF, DDoS, bot management, and API protection** under a single vendor, reducing complexity and management costs. Evaluate the balance between security effectiveness and operational cost to determine overall value.

Akamai

Trust and vendor reliability

Service and stability history

- Review the provider's **outage and service disruption history** for the past 5 years.
- Verify that the company is **financially stable**. Is it profitable? How long has it been in business? What sizes and types of customers does it serve?

Reputation and reviews

- Research verified reviews and customer testimonials to see if similar organizations in your industry **trust the vendor**. Do the use cases of current customers align with your needs?
- Check whether it is **recognized by industry analysts** like Gartner and Forrester for its application and API protection solutions.
- Ensure that after discussions with the vendor, **you feel confident** in its responsiveness and support should issues arise once you become a customer. Ask about who will support your account after initial onboarding.