

CHECKLIST

7 Essentials for Multi-Cloud Application Security and Delivery

Protecting modern applications can be overwhelmingly complex. Organizations also contend with trends such as cloud migration, dispersed apps, emerging architectures, the API ecosystem, microservices and continuous integration and continuous delivery practices (CI/CD), SaaS, remote work, supply chain attacks, and the expanding threat landscape. In addition, cloud providers often have their own tools, which can create availability, performance, and user experience challenges.

Web Application and API Protection Strategy Objectives

Hybrid and multi-cloud security and management must be consistent. Still, lack of knowledge, resources, and regulations often create challenges, so organizations settle for suboptimal web application and API protection (WAAP) approaches. When evaluating vendors and solutions, consider the following capabilities to achieve a more secure, efficient, and simple-to-manage WAAP strategy.



Comprehensive Security

- **OWASP Top 10 risks to web applications:** Vulnerable applications can be exploited in many ways, and a WAAP solution must compensate for risks such as SQL injections, XSS, broken access control, and distributed denial-of-service (DDoS). It also should include anomaly detection and zero-day protection features to identify unknown threats.
- **Bot management:** An effective solution should incorporate machine learning (ML) and behavioral analysis to distinguish bots from human users and good bots from bad bots.
- **API security:** Many interconnected applications rely on APIs for access control and data exchange, so the solution must be able to secure APIs that are susceptible to various attacks that steal data and disrupt operations.
- **DDoS protection:** Network and application-layer attack mitigation should feature real-time customizations, automation, and, ideally, a 24x7 security operations center (SOC).



Environment-Agnostic Traffic Management

- **Global server load balancing:** The ability to dynamically share workloads across cloud-hosted servers and locations based on traffic volumes, network, or server performance requires dynamic traffic distribution features.
- **Availability:** Solutions should ensure business continuity when local network disruptions occur.
- **Content routing:** Layer 7 traffic should be routed to the back-end server pool to simplify front-end coding of webpages and obfuscate sensitive configuration.



Performance Optimization

- **Content Delivery Network (CDN):** A distributed network of images should be used to minimize latency and match local regulatory requirements.
- **Resource utilization:** Solutions should deploy redundant resources globally to ensure the uptime of critical apps.
- **Health checks and monitoring:** A solution must be able to validate the performance of cloud resources and server responsiveness continuously and act in real time if needed
- **Caching:** Solutions should have high-speed data storage to improve application performance.



✓ Unified Management

- **Environment-agnostic:** Organizations should be able to roll out policies and traffic to applications controlled across environments without adapting to each cloud provider's requirements and tools.
- **Observability:** Solutions must be able to monitor and control service disruptions and application-layer attacks from a single, centralized interface.
- **Real-time reporting:** Solutions should include robust analytics that provide insight into security events and priorities in addition to remediation guidance to ensure productivity.

✓ Compliance

- **Regulatory compliance:** Solutions must be able to assist in meeting industry regulatory compliance requirements, such as GDPR, HIPAA, and PCI DSS.
- **Granular reporting:** Dashboards and reports should be available to help you monitor the effectiveness of your application security policies and connect configurations to industry standards.
- **Audit trails:** A solution must be able to provide comprehensive audit trails and reporting to facilitate compliance audits.

✓ Reduce Total Cost of Ownership

- **Scalability:** A solution should be scalable so it can meet changing needs without incurring substantial additional costs.
- **Cloud-native integrations:** Consider cloud-native or hybrid solutions to eliminate on-premises hardware and reduce maintenance expenses.
- **Licensing model:** Look for licensing models that align with budget and usage requirements, such as subscription-based pricing or flexible programs that allow transferring resources to optimize investments.

✓ Support and Training

- **Vendor support:** When comparing vendors, assess the level of vendor support, including access to technical support, updates, and patches.
- **Training resources:** Look for available training resources and documentation to help ensure a smooth transition.
- **Experts on demand:** Consider solutions that include access to experts or a dedicated SOC with monitoring, triage, and remediation guidance if your organization anticipates needing support.

Make an Informed Decision

By considering these requirements and thoroughly evaluating potential vendors and solutions against them, you can make an informed decision that aligns with your business goals and cybersecurity needs. Don't hesitate to consult with your security team and other stakeholders to ensure that your selected solution will integrate seamlessly into your organization's security. Learn more in the [FortiAppSec Cloud solution brief](#).