

CHECKLIST

7 Essentials for Securing Modern Applications

Protecting modern applications can be overwhelming for security professionals. Multiple trends that evolve simultaneously increase complexity exponentially: cloud migration and apps dispersed across environments, emerging architectures and practices such as the API ecosystem, microservices and CI/CD, SaaS, and remote work with the risk of supply chain attacks, and, of course, the threat landscape that keeps expanding.

Organizations limited by knowledge, resources, and regulations often settle for suboptimal web application and API protection (WAAP) approaches, making sacrifices and hoping for the best. However, there are a few common objectives to keep in mind when evaluating WAAP solutions to achieve a more secure, efficient, and simple-to-manage WAAP strategy.

7 Business Objectives for Your Web Application and API Protection Strategy



Security Coverage

- OWASP Top 10 risks to web applications: There are various ways to exploit vulnerable applications. At the
 core, a WAAP solution must compensate for these risks (such as SQL injections, XSS, broken access control,
 denial-of-service) including anomaly detection and zero-day protection.
- **Bot management:** Machine learning and behavioral analysis to distinguish bots from human users, and good from bad bots.
- API security: Many interconnected applications rely on APIs for access control and data exchange. As such, APIs are susceptible to a complete set of possible attacks to steal data and disrupt operations. In 2019, OWASP introduced a Top 10 list of risks to APIs, which demonstrates the threats to API-based ecosystems.
- Real-time monitoring: Ensure the solution offers real-time monitoring capabilities to detect and respond to threats as they occur.



Ease of Operation

- User-friendly interface: Ensure the solution offers an intuitive and user-friendly dashboard for easy management and monitoring.
- Centralized control: Seek a solution that provides centralized control over web application and API security policies, allowing for streamlined management.
- **Automation:** Look for automation features, such as rule-based actions and automated incident response, to minimize manual intervention.



TCO Reduction

- **Scalability:** Opt for a scalable solution that can grow with your organization's needs without incurring substantial additional costs.
- **Cloud-native options:** Consider cloud-native or hybrid solutions that eliminate on-premises hardware and reduce maintenance expenses.
- **Licensing model:** Evaluate licensing models that align with your budget and usage requirements, such as subscription-based pricing.

1

\square

Increased Productivity

- **Real-time reporting:** Choose a solution with robust reporting and analytics features that provide insights into security events and trends.
- **Integration capabilities:** Ensure the solution integrates seamlessly with your existing security tools and infrastructure to avoid productivity bottlenecks.
- **Customization:** Look for customization options to tailor the solution to your organization's unique requirements and workflows.

\square

Automation and Integration

- **Incident response automation:** Seek a solution that offers automated incident response workflows, such as blocking malicious traffic or triggering alerts based on predefined rules.
- **Threat intelligence:** Consider solutions that integrate threat intelligence feeds for automated threat correlation and enrichment.
- Policy enforcement: Look for automated policy enforcement based on security best practices and compliance requirements.
- **Platform integration:** Make sure the solution either natively connects to other security solutions and systems in your environment (such as SIEM, SOAR and others), or comes as part of a comprehensive network and application security suite.

abla

Compliance

- **Regulatory compliance:** Ensure the solution assists in meeting regulatory compliance requirements relevant to your industry, such as GDPR, HIPAA, or PCI DSS.
- Audit trails: Verify that the solution provides comprehensive audit trails and reporting to facilitate compliance audits.

Support and Training

- **Vendor support:** Assess the level of support provided by the vendor, including access to technical support, updates, and patches.
- **Training resources:** Look for available training resources and documentation to empower your team in effectively using the solution.

Conclusion

By considering these solution 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. Additionally, don't hesitate to consult with your security team and other stakeholders to ensure that the chosen solution fits seamlessly into your organization's security posture.

Read the solution brief to learn how organizations meet these business objectives with FortiWeb.



www.fortinet.com

Copyright © 2023 Fortinet, Inc., all rights reserved. Fortinet", FortiGate", FortiCare" and FortiGated", and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different networks environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet; and Fortinet, and Fortinet indexionals all warranties, whether express or implied, except to the extent Fortinet enternal contract, signal of the purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet instead in the performance in the same for ideal conditions as in Fortinet instead in the previous of the publication of the publication shall be applicable.