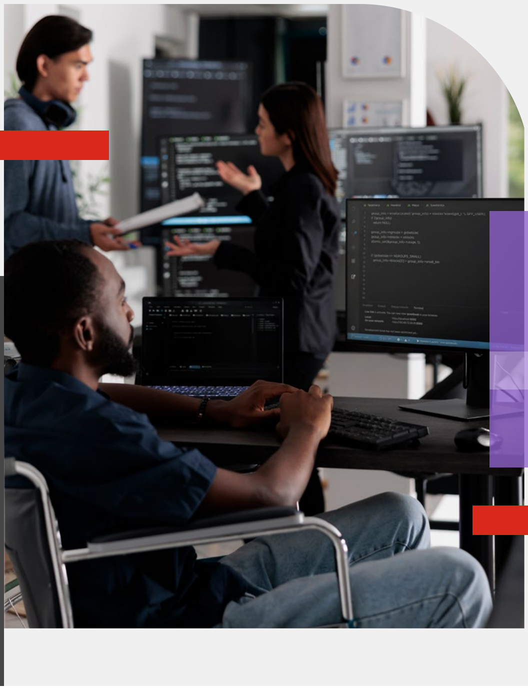
FORTINET

POINT OF VIEW

How Application Security Challenges Could Impact the Business



Evolution of Threats, Development Practices, and Architectures Increase Application Security Complexity. What Can Be Done?

Executive Summary

In today's digital age, web applications have become a business essential for organizations of all types. However, hybrid and multi-cloud environments, emerging architectures, and the need to secure remote working while delivering high service availability to employees, customers, and business partners make securing these applications a major concern. There are multifaceted challenges businesses face when securing web applications and APIs from threat actors and malicious bots. The evolving threat landscape and far-reaching implications of security breaches require organizations to follow best practices to mitigate these challenges.

Despite the many web application security solutions available, businesses still face challenges in securing web applications. Beyond new threats, common failure drivers include resource constraints (budget, skilled experts, or both), complexity of modern applications (microservices, API ecosystem, and frequent changes), as well as false positives (blocking a legitimate user) and false negatives (letting a threat actor in) due to outdated security policies.

Threat Landscape Complicates Web Application and API Protection

The threat landscape for web applications continually evolves, presenting businesses with complex challenges. Key aspects of the threat landscape include:

- **Human threats:** Human threats include hackers, insiders, and other malicious actors who exploit vulnerabilities in web applications.
- **Bot threats:** Bots, both benign and malicious, play a significant role in web application security. Bots are often being used to break into user accounts using stolen credentials. Mimicking real user behavior, they cause tremendous harm at times.
- **OWASP Top 10 risks:** We will introduce the OWASP Top 10, a widely recognized list of the most critical web application security risks. Common attack vectors include SQL injection, cross-site scripting, and other methods to bypass authentication mechanisms or gain unauthorized access.

Why are modern apps difficult to secure?

- Dispersed over data center and cloud infrastructures
- Microservices and API ecosystem complicates data flows
- Frequent changes by dev in CI/CD
- Shortage in skilled experts
- Evolving threats and sophisticated bots

Business Implications

The consequences of failing to secure web applications and APIs extend far beyond technical issues. Some of the business implications of security breaches include:

- **Financial impact:** Security breaches can result in significant financial losses, including direct costs related to breach response and recovery, as well as indirect costs like lost revenue and damage to brand reputation.
- **Reputational damage:** Security breaches can erode customer trust and brand reputation, potentially leading to customer churn and long-term damage to a company's image.
- **Regulatory and legal consequences:** Security breaches can also lead to legal and regulatory repercussions, including hefty fines and penalties for noncompliance with data protection laws.

WAF

Web applications are the most common compromised asset.[1]

A Holistic Application Protection Approach

To address these challenges, businesses can adopt a set of best practices for securing web applications and APIs. Some effective security measures include:

- **Regular vulnerability assessments:** Frequent vulnerability assessments, including automated and manual testing, can help identify and remediate weaknesses in web applications.
- **Patch management:** Keeping software and libraries up-to-date with security patches is crucial in preventing known vulnerabilities from being exploited.
- **Secure coding practices:** Training development and operations teams in secure coding practices can help reduce the introduction of vulnerabilities during the development process.
- **API security:** Given the importance of APIs, a focus on API security is essential, including authentication, authorization, and rate limiting.
- **Incident response plan:** Businesses should have a well-defined incident response plan to mitigate the impact of security breaches when they occur.

Conclusion

Securing web applications is a multifaceted challenge that requires a holistic approach. By understanding the evolving threat landscape, acknowledging the far-reaching business implications of a breach, recognizing the limitations of available solutions, and implementing best practices, businesses can significantly enhance their web application security posture.

[1] 2023 Data Breach Investigations Report (DBIR), Verizon.

FORTINET

www.fortinet.com

Copyright © 2023 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, 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 network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a 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's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.