Radware API Protection

APIs are integral to all aspects of modern business operations. Keeping them secure has become more important—and more difficult. With a growing number of exploits of business logic vulnerabilities posing a significant challenge to businesses, more attackers can manipulate legitimate API calls for malicious purposes. Radware's AI-powered API protection solution can help your organization by providing complete API visibility with continuous detailed API discovery coupled with auto-learning of business logic. It uses fully automated, real-time protection to accurately secure organizations from the most sophisticated attacks and provide them with comprehensive coverage of the OWASP Top 10 API Security Risks for 2023.

The API Problem

As the API threat landscape continues to expand, APIs have become the primary attack surface for organizations, and API attacks are increasingly sophisticated. Hackers can use AI tools to generate a series of legitimate-looking API calls that manipulate the application's business logic. While some solutions already use auto-learning to understand application business logic, they rely on logs of past attacks and offer only remediation recommendations, failing to provide real-time detection and mitigation. Additionally, any auto-learning algorithm can generate false positives, inadvertently blocking legitimate users. Addressing this issue is crucial for any effective real-time mitigation of such API attacks.

Solution Overview

Real-Time Defense Against Embedded Threats

Continuous detailed auto-discovery translates APIs into tailored positive security policies, ensuring real-time protection against embedded attacks.

Immediate Protection against Business Logic Attacks

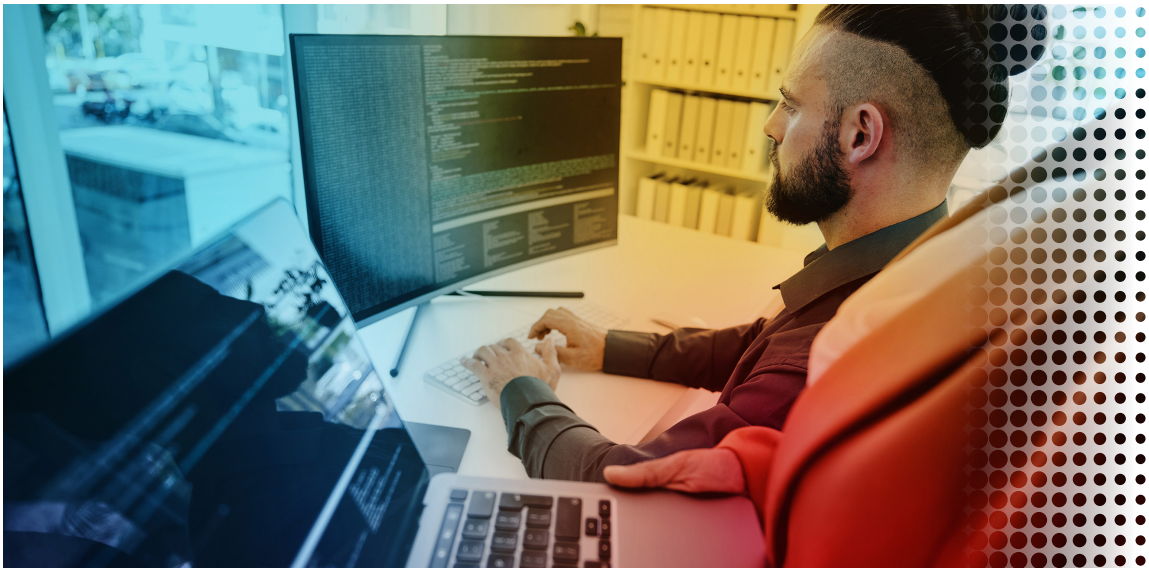
Continuously learns API business logic from real-time transactions to identify and block malicious activities without disrupting legitimate operations.

Accurate Protection Lowering False Positives

Delivers accurate protection with reduced false positives, suitable for production environments, enabling immediate automated action against attacks.

Blocking of Unauthenticated API Use

Enforces token validation to ensure only authenticated users can access and perform authorized operations on your APIs.



Real-time Automated Protection for Any Type of API Attack

Effective API protection starts with an intimate familiarity with all APIs of the application. This is why continuous auto-discovery of APIs is essential. Our solution generates a detailed schema file that is automatically converted into accurate and up-to-date positive security policies. This process enables real-time protection of your APIs against embedded attacks, which is crucial for detecting threats hidden within API calls.

Seamless authentication and authorization enforcement are also key components of our solution. We ensure that only API calls with a validated token are allowed. However, many attacks are carried out by authenticated users who discover loopholes in the business logic, allowing them to perform unauthorized API calls.

Radware's API protection solution addresses these business logic vulnerabilities with unparalleled real-time detection and immediate mitigation of business logic attacks. Our AI-driven protection engine goes beyond analyzing logs of past attacks by continuously learning the API's business logic directly from real-time transactions. This enables the detection of malicious API calls as they occur. Our solution takes immediate action by automatically generating and applying security policies in real-time to block business logic attacks, ensuring comprehensive protection for your APIs.

Multi-Layered Detection and Mitigation of Business Logic Attacks

Continuous Real-Time Learning of the APIs' Business Logic

Learns directly from real-time transactions, unlike others that rely on historical logs, allowing for immediate and accurate detection of malicious API calls.

Immediate Mitigation

Automatically generates and applies security policies in real time to block business logic attacks as they occur.

Accurate Bad Actor Identification

Goes beyond simple IP blocking to surgically identify and block the specific malicious user or client responsible for the attack. This prevents false blocking of legitimate users sharing the same IP.

Unmatched detection and mitigation accuracy

Uses real-time AI-driven context analysis of security policies to ensure only the most reliable policies are applied and significantly enhances the protection accuracy.

Enables PCI DSS Compliance For Your APIs

Radware's API protection solution ensures PCI DSS 4.0 compliance by addressing the requirement to detect and protect against business logic vulnerability-based attacks. Our AI-driven engine continuously auto-discovers APIs and learns their business logic in real-time, providing immediate detection and mitigation of malicious API calls. This proactive approach secures your APIs and sensitive payment card information, meeting the stringent standards of PCI DSS.

Conclusion

Radware's API protection solution offers unparalleled security for your APIs by leveraging AI to provide real-time, accurate protection. It ensures compliance with standards like PCI DSS 4.0 and delivers comprehensive protection against sophisticated API-based attacks, making it an indispensable component of any robust security strategy.

RWI 285 | 06.28.2024