SPOTLIGHT
Sponsored by: Broadcom

Organizations are using more APIs than ever before, and many have started adopting tools to better manage and observe the function of APIs. But they often stop short of utilizing full API security, leaving the organization at risk.

Securing the API Economy: How API Management and API Security Must Coexist

June 2023

Written by: Christopher Rodriguez, Research Director, Security & Trust, and Shari Lava, Research Director, Automation Within the AI and Automation Group

Introduction

The use of application programming interfaces (APIs) is exploding as organizations digitize, connect, and share data. According to IDC's January 2022 *Future Enterprise Resiliency and Spending Survey, Wave 12,* 54% of respondents were relying on APIs to enable easy integration with other applications, as well as with new products and features. APIs power most digital and mobile experiences, making them a cornerstone of a digital business. They provide the capability to connect systems and data inside the organization and beyond its four walls with business partners and customers.

This speedy adoption of APIs has led to much digital innovation, but it has also created some organizational risks. Some APIs used or deployed by organizations are unmanaged, redundant, or developed with inadequate risk management considerations. Left unmanaged, such software can create both inefficiencies and security vulnerabilities that could impact the very business outcomes companies hope to achieve.

AT A GLANCE

KEY STAT

54% of organizations cited microservices and APIs as key for enabling easy integration for new products and features and with other applications (source: IDC's *Future Enterprise Resiliency and Spending Survey, Wave 12,* January 2022).

KEY TAKEAWAY

API use is growing quickly. While management capabilities are important for governing the organization's APIs, security is critical to protecting them.

In response, many organizations have begun to implement API management solutions. *Worldwide Integration and API Management Software Forecast, 2022-2026* (IDC #US45898420, June 2022) predicted strong growth for API management with the market doubling in size by 2026. IDC forecasts that organizations worldwide will spend $4 billion in standalone API management software by 2026, not including software that is fully embedded in iPaaS platforms. Organizations are taking the right steps to manage their APIs from a development and observability perspective.

API management solutions are a critical component for protecting the organization from duplication of effort as well as from unintentional development and change control issues that lead to poor performance of the API or poor user experience. However, they are only one layer of protection in de-risking APIs. API gateways, which are often a runtime component of an API management solution, provide an additional layer of security at runtime. They handle authentication and access control, as well as routing and filtering capabilities that ensure requests and responses are routed correctly. API gateways are a critical part of the infrastructure, but there are additional risks such as vulnerability

exploitation that require additional security capabilities. This is where API security solutions can offer an added layer of protection.

Organizations need to understand that despite their utility, APIs are a net-new threat vector. They also can represent a means for threat actors to access data that they may not otherwise be able to reach. Threat actors are always searching for new entry points and defensive gaps, and APIs may introduce new vulnerabilities and add complexity that weakens security posture. While API management offers useful security functionality, these capabilities should be considered table stakes for enabling API integration, rather than a security end state. A complete API security architecture requires comprehensive visibility and inventory, assessment, runtime protection, policy enforcement, and behavior monitoring.

Definitions

- **Application programming interfaces (APIs) —** APIs are software components that can access other systems, applications, and data stores to request data and respond back to the requester without needing to understand the entire data structure behind the system being accessed. APIs power many of the experiences that consumers have today with online banking, social media, and other online activities.
- **API gateway –** This runtime proxy engine oversees API requests to manage authentication, enable load balancing, and request routing. It is often the control plane component of API management software.
- **API management –** This software manages the API life cycle, including the import, creation, and publishing of APIs.
- **API security –** This is the practice of protecting API communications from misuse, abuse, and exploits, through secure design, testing, identity management, policy enforcement, and threat detection. Some functions are aspects of established practice areas and technologies such as application testing, identity management, web application firewalls, and API management. However, specialized solutions exist to fully address the unique security requirements of APIs.
- **Web application firewalls (WAF) –** This specialized security gateway protects web application traffic against a variety of attacks, including automated bots, code injection, and application-layer denial of service. WAF leverages various techniques to protect applications including positive and negative security models, access policies, behavioral analytics, and client/IP reputation. WAF solutions are offered in a variety of form factors including hardware appliances, virtual appliances, and SaaS.

Benefits

At first glance, API management, WAF, and API security tools offer value in drastically different ways. However, these solutions share a common goal to reduce risk and enable the organization to pursue the digital transformation initiatives required to succeed in the modern business environment.

These technologies can also offer varying degrees of overlap in terms of security functionality. API management platforms, WAFs, and standalone security tools can be leveraged as security control points, inspecting traffic and enforcing a positive security model such as schema validation and enforcement. In addition, the functions provided by each solution are often complementary. For example, API management solutions can be used to enforce rate limits to mitigate DDoS attacks, and WAFs offer analytics-based detections to defuse more sophisticated layer 7 DDoS tactics. Given the nature of DDoS threats, more and varied options for attack detection and mitigation are always welcome.

The combination of these technologies offers a step-up approach to achieving holistic API security. Therefore, it is important to consider each solution with an understanding of the role it plays in the broader API security architecture, as well as respective areas of strength, benefits, overlap, and complementing functionality.

API management solutions provide an important base level of security for all known API endpoints. WAF solutions extend essential protections to all application and API traffic traversing an established perimeter. Dedicated API security solutions are also available to provide specialized protections to defend applications against more intentional and sophisticated efforts as theft, fraud, and manipulation, including advanced attacks such as broken object-level authorization and business logic abuse.

API management, API security, and WAF technologies support the broader goal of risk reduction, with WAF and API security offering the benefits of cybersecurity protection spanning availability, integrity, and confidentiality.

As such, 60% of organizations report adoption of some form of API security tooling, with another 8% planning to adopt in the coming year, which trails WAF adoption rates only slightly, according to IDC's April 2022 *DevSecOps Adoption, Techniques, and Tools Survey*. Overall, a robust API security program spanning built-in management capabilities and purpose-built API security is key to fulfilling the promise of the API economy. Ideally, these capabilities will complement and extend each other, reducing the trade-offs between the platforms and cross-pollinating feature functionality when possible.

Trends

An understanding of API security has slowly built up over the years through both security research and real-world lessons. However, many organizations continue to underestimate or misunderstand the risks of APIs. API-related data breaches dominated headlines in 2022 as multiple large international companies fell victim to data breaches caused by simple misconfigurations or lack of basic security visibility. 2023 has already started off with a similar pattern.

This relatively low security maturity level is to be expected as APIs introduce unanticipated challenges. APIs may be designed for public or private access, and a late change in plans or simple miscommunication can introduce a security gap. They may be abandoned or forgotten, leading to concerns of "zombie APIs." Unprotected/under-protected APIs may be unintentional mistakes driven by version control or poor documentation practices, but security researchers have also noted the possibility of rogue APIs for nefarious purposes by insider threats. Either way, unprotected APIs are easily discovered by threat actors and bots as they scan for new vulnerabilities to exploit.

As IT organizations address these low-level security requirements, more complex challenges await. APIs expose functionality that can be abused in unexpected ways such as business logic attacks that exploit approved functionality for unapproved purposes. Furthermore, threat actors may employ evasion techniques that bypass basic access controls provided in API management solutions or perimeter WAF protections, such as authorized sessions and conforming object payloads.

Notably, while API management platforms provide valuable and necessary functionality, they lack the comprehensive visibility or advanced detection capabilities needed to stop sophisticated API-based attacks. As a result, specialized API security solutions have emerged that provide complete visibility and inventory of APIs and related vulnerabilities, protection against top API-specific threats, behavior-based runtime protection, and advanced business logic protection. These solutions address a growing need, and as a result, IDC research shows the market for API security solutions

reaching $700 million by 2026 (see *Worldwide API Security Forecast, 2022–2026: Purpose-Built Security Fills the Gap,* IDC #US49427622, August 2022).

Considering Broadcom API Security

Broadcom offers solutions for API management, including a hardened API gateway, API security capabilities, and a separate dedicated WAF solution. Broadcom leverages its robust visibility into API communications and endpoints, as well as deep security expertise through its WAF solution to deliver a complete API security offering.

Broadcom API management offers essential security functionality such as:

- Schema enforcement
- Input validation/sanitization
- Rate limiting/quotas per API
- Identity and access management, SSO
- Extensible OAuth/OIDC implementation
- End-to-end encryption
- Threat detection, leveraging Broadcom's expertise in WAF to protect against OWASP Top 10 threats, including code injection and layer 7 DDoS

Broadcom also offers its Symantec WAF, a proxy solution for securing application and API traffic, available as appliances or virtual appliances. The solution offers advanced protections including:

- Known threat detection including OWASP Top 10 threats
- Signatureless, behavior-based threat detection
- IP reputation
- Malware detection including signatures, sandboxing, and static code analysis
- Layer 7 DDoS protection
- Transparent authentication or challenges
- Granular policy enforcement across users, groups, geolocation, user agent, headers, browsers, and other variables

As a dedicated proxy, the Broadcom WAF can also perform caching of content for performance optimization, as well as SSL termination, compression, and decompression.

Challenges

One key challenge faced by those investigating API security solutions can often be in understanding and explaining the limits of the protection provided by API management solutions. If organizational awareness of the risks of APIs is low, companies may not be implementing API security solutions proactively, waiting instead until a threat has been realized.

A second key challenge faced by those investigating Broadcom's API security solutions includes concerns about adopting solutions outside of core infrastructure providers. Many organizations choose to adopt API management solutions of cloud-based infrastructure providers. That said, Broadcom offers strong capabilities for hybrid infrastructure environments that provide a great deal of flexibility.

Conclusion

IDC believes businesses will continue to invest heavily in APIs for the many benefits they offer that support digital enablement. The importance of a holistic approach to both API management and security is gaining recognition as a critical success factor for these API strategies. There is no magic pill solution for API security, however, as a complete API security solution requires a coherent, cooperative approach between API management and application security solutions. Technology buyers should consider solutions that can address both the management and the security challenges in this paper to address the critical needs of the API security journey.

There is no magic pill solution for API security.

About the Analysts

Shari Lava, *Research Director, Automation Within the AI and Automation Group*

Shari Lava is Research Director, Automation Within the AI and Automation Group. Ms. Lava's core research coverage includes the fast-changing automation and API management software space. Based on her background in enterprise applications and data integration, Ms. Lava's research also includes an emphasis on the market understanding and adoption of these key technologies that are integral to business productivity and success.

Christopher Rodriguez, *Research Director, Security & Trust*

Christopher is a Research Director in IDC's Security & Trust research practice focused on the products designed to protect critical enterprise applications and infrastructure. IDC's Security & Trust research services to which Chris contributes include Active Application Security and Fraud, where he covers web application firewall, DDoS mitigation, bot management, and API security.

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com