December 2023

API Security Solution Evaluation Guide

Tari Schreider

Commissioned by F5 Networks

Table of contents

List of figures

List of tables

© 2023 Datos Insights or its affiliates. All rights reserved.

Summary

The global digital economy requires application programming interfaces (APIs) to connect application-based services to customers, consumers, partners, and employees. Legacy, modernized, and new applications are built with APIs to advance the state of application development and reduce time-to-market. Moving application functionality closer to the customer to reduce friction is the genesis of decentralized architectures and the API-first movement. Unfortunately, the efficiencies gained through APIs in application development are becoming overshadowed by the risk they introduce to an IT enterprise. Hackers have learned compromising APIs is easy when they are lightly protected. No one would argue that APIs require secure practices; however, there is debate on the best way to secure APIs. This API security solution evaluation guide describes the various approaches to securing APIs and the important considerations buyers of API security solutions should consider. The foundation of deciding to acquire a security solution is to understand:

- **API sprawl is shockingly pervasive:** Today, the average number of APIs organizations use is over 20,000. Lack of API management and oversight leads many organizations to promote APIs to production with known security issues. API sprawl creates a target-rich attack surface, motivating hackers to develop an increasing number of zero-day API attacks. APIs will approach 2 billion by 2030,[1] further exacerbating the problem.

- **Compromised APIs have led to over 1 billion stolen records:** API exploitation is growing in frequency and sophistication, accounting for many compromised records. Zero-day attacks where a web-facing server vulnerability is exploited to achieve remote code execution to allow lateral movement to databases have led to single-event compromises of tens of millions of records.

- **Regulations drive the need for API security:** Regulators have taken notice of the risk introduced by APIs and encouraged companies to mitigate their risk throughout their IT enterprises, including third parties.

[1] Rajesh Narayanan, Mike Wiley, Continuous API Sprawl, F5, November 4, 2021, https://www.f5.com/company/news/press-releases/api-sprawl-threat-business-economy.

© 2023 Datos Insights or its affiliates. All rights reserved.

- **API gateways are no longer sufficient to manage the scale and complexity of API ecosystems:** Operating in a distributed cloud environment is the norm today. However, using a dedicated API gateway as a single entry point to control security has limitations, including single points of failure and performance degradation. Overcoming these limitations has given rise to the use of multiple gateways, leading to API gateway sprawl.

- **Web application firewalls (WAFs) only partially protect APIs:** Next-generation WAFs provide robust protection and some level of security for API protocols, including GraphQL and gRPC, but do not offer advanced API security management or the necessary behavioral observability of APIs to detect advanced threats. Many WAFs lack dynamic API discovery, threat mitigation, testing, and OpenAPI document specification automation capabilities.

- **Architectural planning is required to deploy API security solutions effectively:** Deploying an API security solution requires infrastructure integration and connectors, some custom to deploy in an IT estate properly. Understanding the intricacies of deployment requires architectural planning. Selecting a solution that operates out of the box within an existing IT enterprise architecture reduces deployment time.

- **Privacy must be considered when securing APIs:** Personal data is the property of the individual, not an application or service provider. The digital economy fuels open data sharing. APIs enable private, public, partner, and third-party data and services. APIs need to have privacy-preserving technologies applied to comply with data privacy regulations.

- **APIs suffer the same risk as applications:** Hackers have long realized that APIs suffer the same security maladies as web applications, including weak authentication and authorization controls. They have become adept at exploiting API vulnerabilities, abusing business logic, and creating zero-day exploits to access IT enterprises with little resistance. The intended audience for the guide includes enterprise architects, DevOps and SecOps managers, and CISOs.

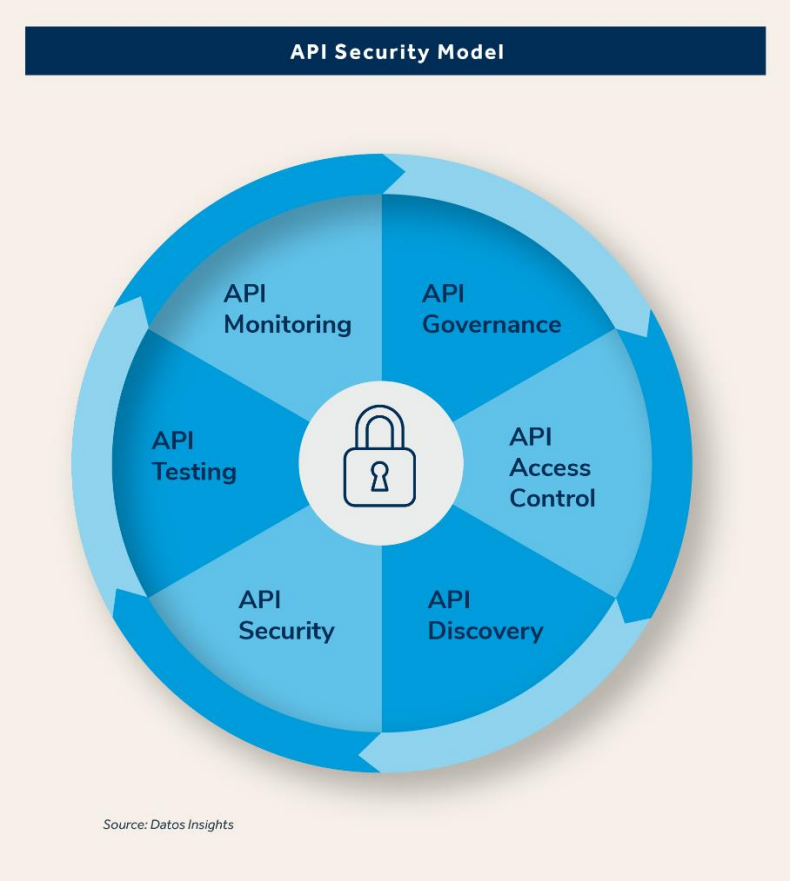
The guide highlights important considerations when acquiring an API security solution and helps you avoid overspending for a solution that is over- or under-engineered for your needs.

© 2023 Datos Insights or its affiliates. All rights reserved.

Introduction

This guide strips away the veneer of industry hype and takes a realistic look at what buyers of API security solutions should look for when performing a product evaluation. Dozens of product features are touted as the best, but do you know what matters most when protecting APIs? Should you select a product with the most bells and whistles, which few may apply, or begin with a security model and select an API security solution commensurate with your API risk profile? The answer begins with a solution that addresses your API risk profile. APIs are exposed to the same threats and vulnerabilities as other components of an attack surface, but the context is different. The starting point of a secure API journey begins with an API security model. Technology alone cannot solve the API security problem. However, the technology must integrate with the model. An API security model typically includes six core components. Figure 1 presents a security model offering a balanced approach to protecting APIs.

Figure 1: API Security Model



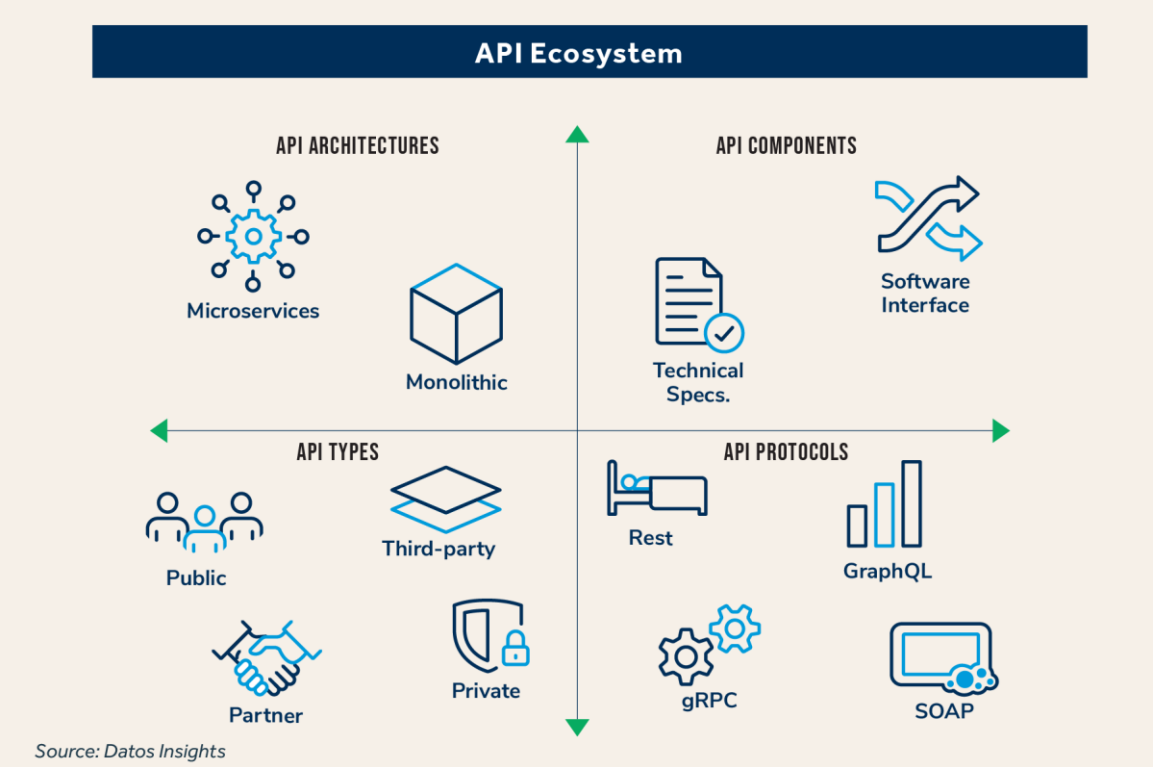
© 2023 Datos Insights or its affiliates. All rights reserved.

API Ecosystem

APIs operate in a complex ecosystem comprised of architectures, components, types, and protocols. The API ecosystem represents the attackable surface area of APIs. Organizations inadequately protect APIs mainly due to a lack of understanding of the API ecosystem.

Figure 2 is an abstract view of the API ecosystem.

Figure 2: APIs Ecosystem



© 2023 Datos Insights or its affiliates. All rights reserved.

The Problems With APIs Today

Hackers know that APIs connect valuable applications, so why expend the effort to infiltrate a single application when they can infiltrate an API library and get access to core applications? APIs have many of the same inherent risks as applications; however, the ever-changing nature of APIs opens the potential for more zero-day attacks. APIs require a holistic approach to protection, such as offered by the multidimensional security provided by a Web Application and API Protection (WAAP) solution. Table A discusses the problems inherent with APIs today and their implications for an IT enterprise.

Table A: API Problems

Problem	Implications
API vulnerabilities are largely unaddressed by organizations.	• A growing number of significant security breaches owing to poor API visibility and security occur and will continue for the foreseeable future.[2] • The race toward digitizing organizations will put more rushed and poorly designed APIs into production. • Many organizations will attempt to solve API vulnerabilities through better design and coding, only to realize the same security failings as applications in general, partly because security is not a core competency for a typical application developer.
Organizations are pushing the envelope in their desire for advanced API security functionality.	• Security information event management (SIEM) and security orchestration automation and response (SOAR) product integration detect and respond to API security incidents. • API security management is evolving. • It is increasingly clear that dynamic discovery and automated protection using machine learning is the only way to maintain resilience when protecting API-driven architectures.
Proliferation of API endpoints	• The core of API sprawl is the lack of a holistic strategy that includes governance and best practices. • Agile application development has led to multiple versions of the same API without the benefit of API version control. • The move to microservices results in an application comprising many dozens of APIs. • Unmanaged APIs create rogue, shadow, and zombie APIs.

[2] Ian Dinno, Lesson Learned (So Far) from the T-Mobile breach, F5, February 8, 2023, https://www.f5.com/company/blog/lessons-learned-so-far-breach-t-mobile.

© 2023 Datos Insights or its affiliates. All rights reserved.

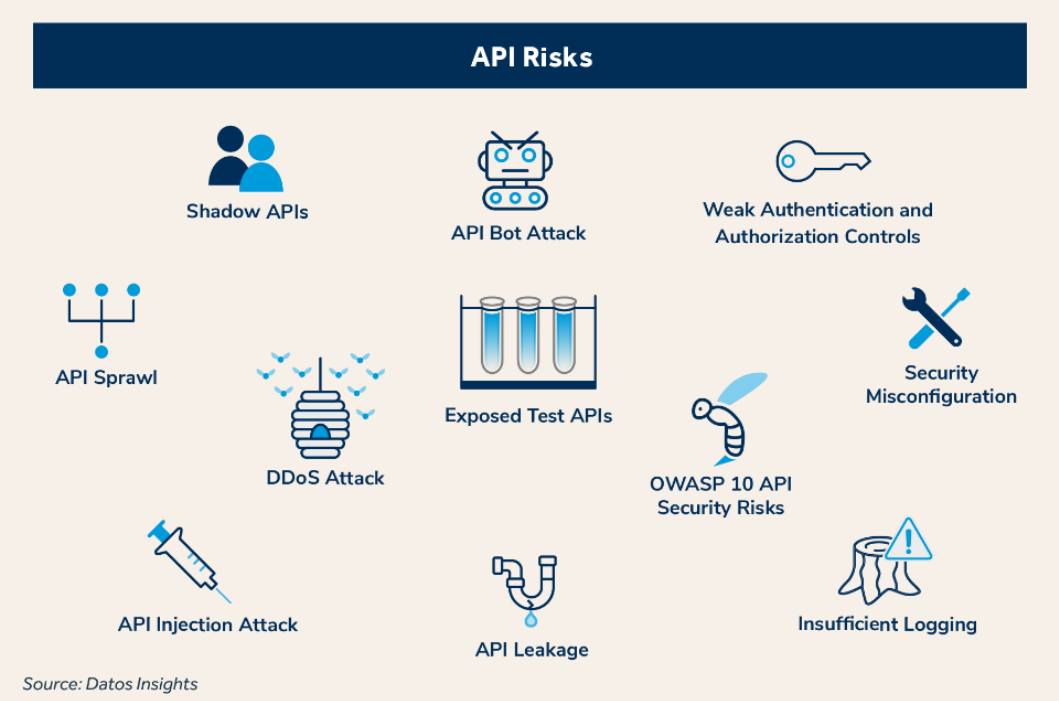
Problem	Implications
Hackers increased the level of sophistication and focus on APIs.	• Attackers reverse engineer APIs to understand their structure and business logic, mostly missed by gateways as the activity looks like normal traffic. • API attacks have many zero-day exploits due to their wide variety of design, use, and controls. • Hackers know many APIs are not protected against the OWASP Top 10 API risks, most notably those related to access control, authentication, and authorization.

Source: Datos Insights

Threats to APIs

API security is directly related to application security; subsequently, APIs have many of the same frailties of compromise as applications. APIs are critical because they transfer data between clients and servers connected over public networks. There are many points of potential weakness in that process requiring security safeguards. Dozens of threats exist that hackers can leverage to compromise APIs. Figure 4 presents the most common API threats.

Figure 3: API Risks



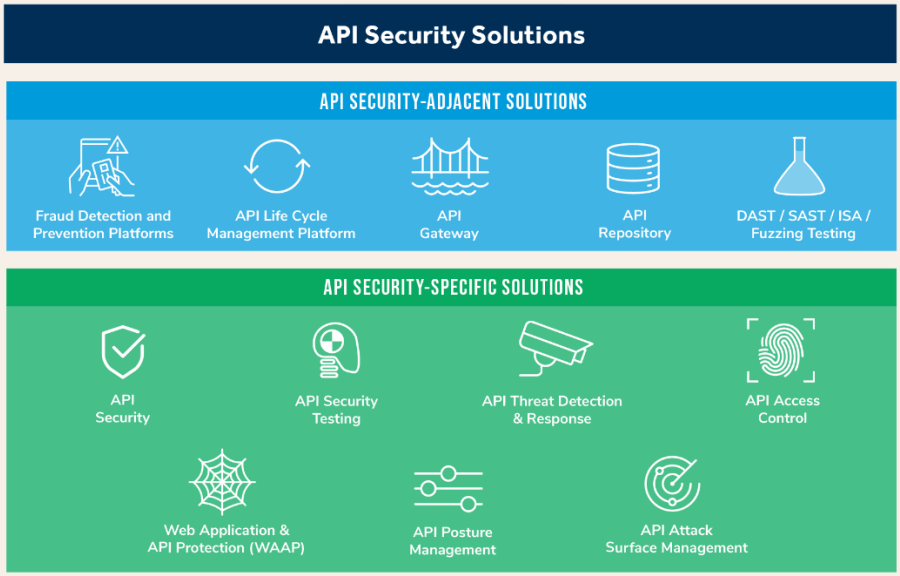
© 2023 Datos Insights or its affiliates. All rights reserved.

Solutions to Secure APIs

> *Enterprises benefit most from comprehensive solutions that consolidate functionality across an entire API ecosystem.*
>
> **Tari Schreider,**
> Strategic Advisor, Datos Insights

Many API security solutions are available, but only web application and API security (WAAP) solutions and API security platforms offer integrated API security solutions. It is important to note that although a category of API security product may have similar functionality, how that functionality is provided, its context, and the depth and breadth of security coverage must be considered before making a buying decision. Figure 4 shows security solutions currently available.

Figure 4: Available API Solutions



Source: Datos Insights

WAAPs have the added functionality of an integrated platform that protects web applications and APIs, detects and deters bad bots and malicious automation, defends against denial-of-service attacks, and serves as a firewall to APIs and web applications to enforce protocol compliance, validate schema, and control access through granular authentication and authorization. This defense-in-depth approach is designed to provide optimum API protection and speed remediation across hybrid and multi-cloud architectures.

© 2023 Datos Insights or its affiliates. All rights reserved.

Essential Capabilities

APIs allow disparate applications to work together; compromising an API can open access to the whole of an enterprise. Subsequently, APIs require an enterprise-class solution offering the same protection afforded to web applications. Table B overviews the top 16 capabilities an API security solution should provide.

Table B: Essential Capabilities of an API Solution

Capability	Overview
Flexible deployment models	The solution should provide maximum flexibility to deploy within an IT enterprise, including as an on-premises hardware or virtual appliance, an as-a-service platform, and a managed service. A hybrid approach to deploy at the true edge is essential for broad-based API discovery, detection, and attack remediation.
Architecture integration	The solution must secure APIs at scale across tiered data centers or cloud architectures. API security policies must follow APIs across multi-cloud, distributed, shared, or app service, management, and operations tier environments. The solution should conform to an existing architecture.
API discovery and mitigation	Dynamic API inventory discovery to catalog all internal and external APIs used within an enterprise is critical, without which unseen and unknown APIs represent a risk to the organization. Knowing the shadow and zombie APIs communicating with endpoints is fundamental to securing APIs. Mitigation must be tightly aligned to discovery to complete the API protection loop.
OpenAPI (OAS) support	Provides a consistent means to extend information through all stages of the API lifecycle. With OAS, the solution can discover how an API works and understand its service capabilities. The APIs' design contract can be compared to its behavior. The solution should auto-generate documents to support security testing, ensuring insecure APIs don't reach production.
API observability	The solution must be able to passively collect an API's events, traces, and metrics to observe its behavior. Understanding how the solution listens to APIs through agents, libraries, or detectors to capture and analyze telemetry is important to deploying the solution.
Comprehensive API visibility	Identify all enterprise API endpoints, map them to applications, monitor for malicious activity and shadow APIs, and observe global API metrics from a centralized user interface.

© 2023 Datos Insights or its affiliates. All rights reserved.

Capability	Overview
Security posture management	API posture management involves inventorying APIs, assessing their vulnerabilities, scoring their risk, and remediating detected vulnerabilities.
Strong API access control	Augment API gateway functionality, delivering enhanced visibility, oversight, and control over API authentication and access while helping to identify gaps in API authentication, control access, and stop unauthorized attempts to exploit APIs.
Positive security API model	Automatically deliver a positive security model with existing OpenAPI spec (OAS) to enforce desired API behavior through valid endpoint, parameter, method, authentication, and payload details.
Sensitive data detection and masking	Provides visibility into endpoint details, including the detection and flagging of PII that is being exposed, with capabilities to mask sensitive data or block endpoints distributing sensitive data.
API authentication state discovery	Identifies and baselines the authentication state of all APIs within an environment, allowing for automatic discovery with views into authentication status, details, and the risk score of APIs.
API risk identification	Identify the most used and attacked API endpoints, usage patterns, correlate good and bad actor activity, plus sensitive data, including PII, to optimize and tune protection policies for APIs.
API security testing	API Security solutions should integrate with dynamic and static security testing (DAST/SAST) to quickly incorporate stopgaps for vulnerabilities discovered during penetration testing. The solution should also provide dynamic API discovery and schema validation, which can be used to enforce contract testing for APIs.
Runtime protection	Provide a real-time protection environment post-development, countering attacks using behavioral analytics by blocking attacks related to malicious users, insiders, malware infections, and malicious rootkits. Apply behavior management to detect abnormal API activities while operating or making requests.
Threat intelligence	API security solutions should be backed by an API threat intelligence service that provides intel on threats and contextual information about the nature and purpose of the active threat campaign. In contrast, a WAF may detect a suspicious pattern in a web application form; without threat intelligence, it cannot have combinations of identifiers that form part of a current, sophisticated threat campaign.

Source: Datos Insights

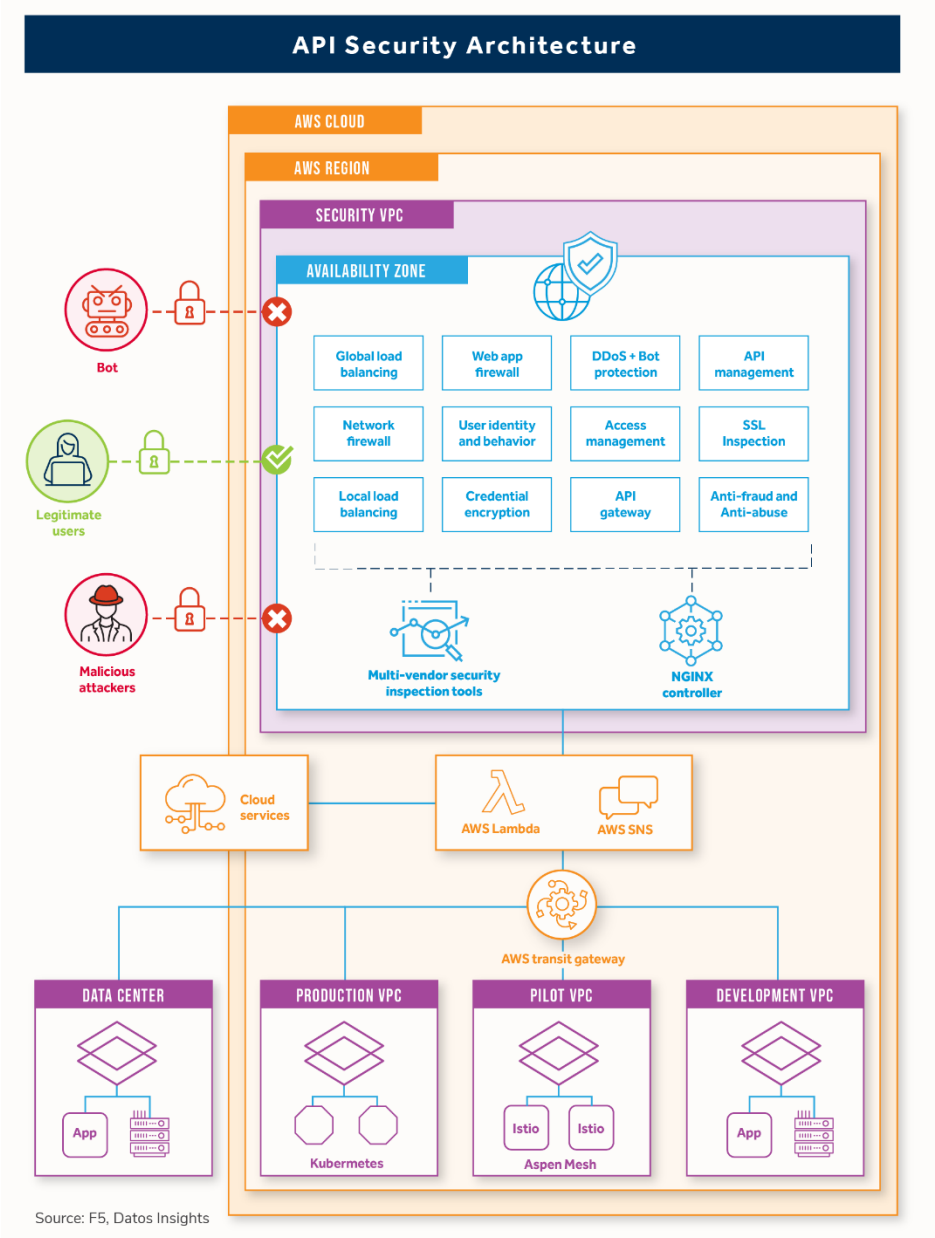
© 2023 Datos Insights or its affiliates. All rights reserved.

API Security Architecture

An API security architecture must consider integrating with a distributed IT enterprise, including multi-cloud, regional edges, and service tiers. The solution should be deployable to any hardware, virtualized environment, docker, Kubernetes, etc. The solution must allow security policies to follow the API through its ecosystem.

Figure 4 presents an API security architecture to aid buyers of API security solutions with visualizing the end-state API protection requirements.

Figure 5: API Security Architecture

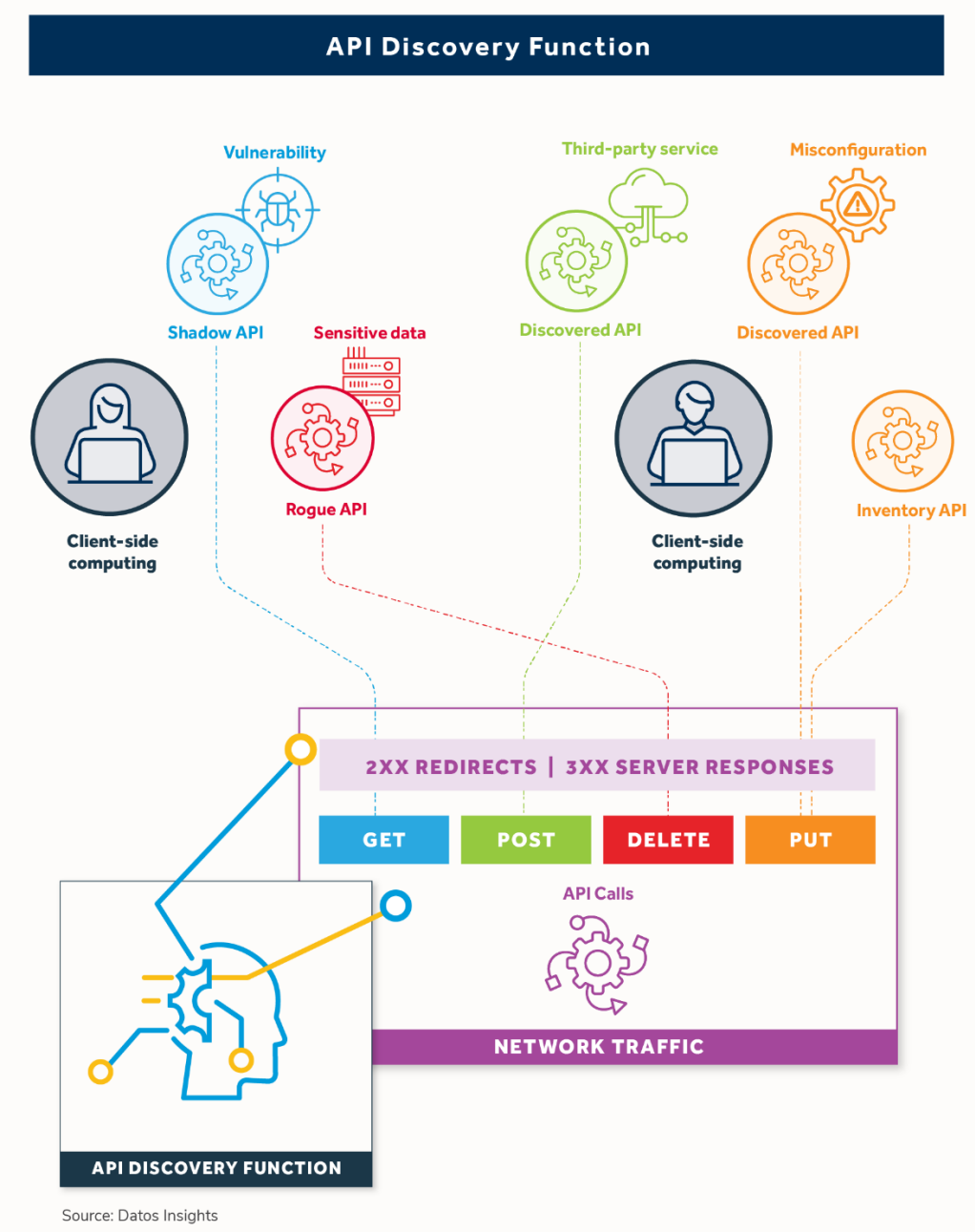


Source: F5, Datos Insights

© 2023 Datos Insights or its affiliates. All rights reserved.

One of the essential elements of an API security solution is how it discovers rogue, zombie, and third-party APIs. The API discovery function listens to network traffic to detect API calls. The API path leads to the API, which is identified and inspected for misconfigurations and vulnerabilities. Figure 6 is an abstract view of the API discovery process.

Figure 6: API Discovery Function



Source: Datos Insights

© 2023 Datos Insights or its affiliates. All rights reserved.

Conclusion

- Understanding the API ecosystem of the organization is the first step in defining API protection strategies and choosing an API security product to enforce those strategies.
- APIs operate in a multi-cloud environment and require a protection architecture that detects vulnerabilities and business logic abuse and automatically remediates and reacts to anomalous behavior.
- API security must be tightly integrated with DevSecOps; the CISO must be engaged to have visibility to the extent of the API problems faced by the organization.
- The enumeration of the API attack surface is essential to securing APIs. CISOs cannot protect what is not known. API discovery is needed to identify shadow, orphan, out-of-version, and dated APIs.
- WAFs and API Gateways are important in protecting APIs but stop short of providing full-featured security of APIs in today's complex IT enterprises and rapidly developing API threat landscape.
- Not all API security products are created equally. Products that understand API context dynamically discover and visualize API dependencies, score risk factors, provide runtime protection, and work effectively in a distributed cloud environment provide the most value.
- The litmus test in API security solutions is the unburdening of security teams by vetting and suppressing false positives that needlessly consume valuable cybersecurity and resources.
- Nearly 90% of IT decision-makers cite regulations as a key driver for securing APIs, according to a September 2023 research study conducted by Datos Insights.
- The looming consolidation of the API security market will require a deeper analysis of vendors to determine market staying power. Buying decisions must consider the stability of the solution provider.

© 2023 Datos Insights or its affiliates. All rights reserved.

About Datos Insights

Datos Insights is an advisory firm providing mission-critical insights on technology, regulations, strategy, and operations to hundreds of banks, insurers, payments providers, and investment firms—as well as the technology and service providers that support them. Comprising former senior technology, strategy, and operations executives and experienced researchers and consultants, our experts provide actionable advice to our client base, leveraging deep insights developed via our extensive network of clients and other industry contacts.

Contact

Research, consulting, and events:

sales@datos-insights.com

Press inquiries:

pr@datos-insights.com

All other inquiries:

info@datos-insights.com

Global headquarters:

6 Liberty Square #2779
Boston, MA 02109

www.datos-insights.com

Author information

Tari Schreider

tschreider@datos-insights.com

© 2023 Datos Insights or its affiliates. All rights reserved. This publication may not be reproduced or distributed in any form without Datos Insights' prior written permission. It consists of information collected by and the opinions of Datos Insights' research organization, which should not be construed as statements of fact. While we endeavor to provide the most accurate information, Datos Insights' recommendations are advisory only, and we disclaim all warranties as to the accuracy, completeness, adequacy, or fitness of such information. Datos Insights does not provide legal or investment advice, and its research should not be construed or used as such. Your access and use of this publication are further governed by Datos Insights' Terms of Use.