axway

FLYER

Take command of your APIs with Amplify Engage and Traceable

Deliver the ironclad security insights and management capabilities you need to protect your digital assets

The growing risk of unmanaged APIs

Did you know that an estimated 20%[1] of the APIs within an organization's ecosystem remain unmanaged and that this number is expected to grow by double digits in the next few years?

Unmanaged APIs create critical security blind spots, leaving your business vulnerable to a range of threats, including:

- **Unintentional exposure of sensitive data.** Sensitive data, proprietary algorithms, or internal financial information can be inadvertently exposed through forgotten or poorly secured APIs. This can lead to data breaches, reputational damage, and significant regulatory fines.
- **Undocumented endpoints open to attack.** Undocumented APIs are a hacker's dream. They're often poorly secured and lack the scrutiny of managed APIs, making them easy targets for exploitation and opening the door for hackers to gain unauthorized access, launch denial-of-service attacks, inject malicious code, and more.
- **Inconsistent access controls leading to compliance gaps.** Without a centralized solution, access controls are fragmented and inconsistent. This makes it difficult to enforce security policies, track user activity, or demonstrate compliance with industry regulations like GDPR, HIPAA, or PCI DSS.
- **Operational inefficiencies and wasted resources.** Unmanaged APIs also create operational headaches. Developers waste time searching for and trying to understand undocumented endpoints. Maintenance is difficult and it's impossible to track API usage. This leads to wasted resources, delayed projects, and increased development costs.
- **Difficulty in evolving your digital strategy.** Unmanaged APIs create a drag on innovation, making it difficult to integrate new services, launch new products, or respond to changing market demands.

57% of organizations experienced API-related data breaches in the past two years, with 73% of these organizations reporting three or more such incidents,[2] so implementing robust API security measures is critical. Besides, data breaches can cost businesses up to 2-5% of global annual revenue in the EU,[3] Brazil, and China, with varying fines in the U.S. and South Africa.

[1] The state of enterprise API maturity, Vanson Bourne Research sponsored by Axway

[2] CMS, GDPR Enforcement Tracker Report

[3] Traceable AI's 2025 State of API Security Report

Amplify Engage and Traceable: A unified approach to API security and governance

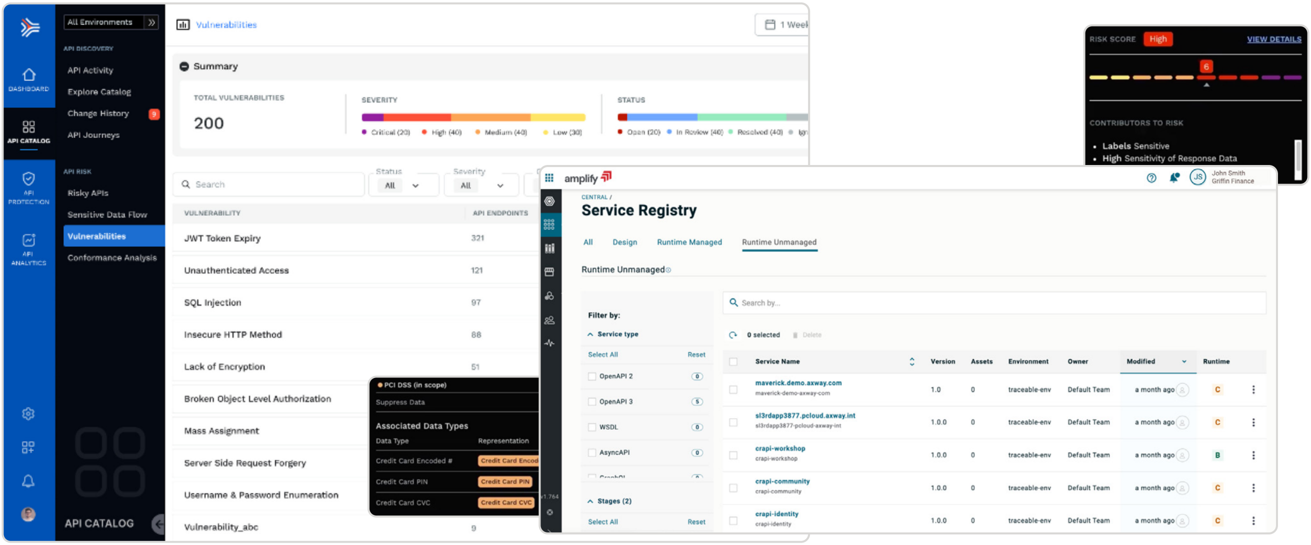
To address the growing risks of unmanaged APIs, organizations need a comprehensive approach that provides broad API visibility, proactive security, and effective governance. Amplify Engage and Traceable work together to deliver a powerful solution that combines federated API management with advanced API security, allowing you to not only identify any issues, but also get them under control.

Extensive API discovery and security posture analysis. AI-driven API discovery, monitoring, and threat detection ensure that all APIs, including shadow, lost, and unmanaged APIs, are identified and secured.

Standardized and secure API access. Organizations can curate and productize their APIs, enforce consistent API policies, automate API lifecycle management, and prevent security misconfigurations across all environments.

Regulatory compliance and risk mitigation. Businesses can assess their security posture, detect vulnerabilities and anomalies, and ensure compliance with global regulatory standards through detailed auditing and reporting.

Governance and business growth. By enabling secure API consumption, organizations can expose, reuse, and monetize APIs, accelerating innovation and driving new revenue streams while maintaining security and control.



VULNERABILITY	API ENDPOINTS
JWT Token Expiry	321
Unauthenticated Access	121
SQL Injection	97
Insecure HTTP Method	88
Lack of Encryption	51
Broken Object Level Authorization	
Mass Assignment	
Server Side Request Forgery	
Username & Password Enumeration	
Vulnerability_abc	9

PCI DSS (in scope)

Suppress Data

Associated Data Types

Data Type	Representation
Credit Card Encoded #	Credit Card Encod
Credit Card PIN	Credit Card PIN
Credit Card CVC	Credit Card CVC

- Labels Sensitive
- High Sensitivity of Response Data

CENTRAL /

Service Registry

All | Design | Runtime Managed | Runtime Unmanaged

Runtime Unmanaged

Filter by:

Service type — Select All — Reset

- ☐ OpenAPI 2 (0)
- ☐ OpenAPI 3 (5)
- ☐ WSDL (0)
- ☐ AsyncAPI (0)

Stages (2) — Select All — Reset

Search by...

0 selected Delete

☐	Service Name	Version	Assets	Environment	Owner	Modified	Runtime
☐	maverick.demo.axway.com maverick-demo-axway-com	1.0	0	traceable-env	Default Team	a month ago	C
☐	sl3rdapp3877.pcloud.axway.int sl3rdapp3877-pcloud-axway-int	1.0.0	0	traceable-env	Default Team	a month ago	C
☐	crapi-workshop crapi-workshop	1.0.0	0	traceable-env	Default Team	a month ago	B
☐	crapi-community crapi-community	1.0.0	0	traceable-env	Default Team	a month ago	C
☐	crapi-identity crapi-identity	1.0.0	0	traceable-env	Default Team	a month ago	C

Together, Axway Amplify Engage (formerly Axway Amplify Enterprise Marketplace) and Traceable provide the complete solution for secure, managed APIs, driving business growth and unlocking the full potential of your API strategy. With universal discovery, curation, productization, access control and deep threat detection at runtime, you are always in complete control.

Want seamless API governance, security, and threat detection with Amplify Engage and Traceable?

Contact Us →

|