INDUSFACE™

An Increase in API Use Leads to API Risks Concerns

74% of developers are using APIs for internal applications. Among them, 49% are working on third-party APIs, with 44% working on partner-facing APIs. This's up from 35% a year ago.

Source: A Global Annual Survey, RapidAPI

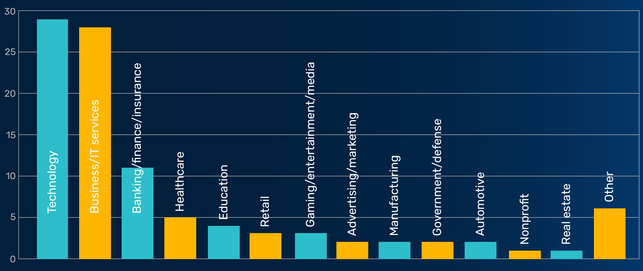
2022 and the years to come are going to be the time of the API (Application Programming Interface), as businesses shift to new operating models to accelerate digital transformation.

The API management market is projected to be worth $5.1 billion by 2023, at a CAGR of 32.9%.

Source: Marketsandmarkets.com

API Adoption Is on The Rise Across All Industries

Industries that work with API



Source: Postman.com

APIs Growing in The Time of Covid

- APIs supported pandemic response: 51%
- APIs did not support response: 49%

Were your organization's changes supported by APIs?"

- More time and resources on APIs: 56%
- Same time and resource on APIs: 38%
- Less time and resource on APIs: 7%

Organizations will continue investing in APIs as a key part of their business strategies

Source: 2021 State of the API Report, Postman.com

Healthcare APIs Are Growing By 6.3% CAGR

The global healthcare API market size was valued at $210.9 million in 2019 and is expected to grow at a CAGR of 6.3% from 2020 to 2027.

Source: Grandviewresearch.com

Increase in API Security Breaches

API investment and adoption aren't the only things rising quickly in the digital ecosystem. So are issues related to cybersecurity.

By 2022, API abuses will be the most-frequent attack vector resulting in data breaches for enterprise web applications.

Source: Gartner

The average API has nearly 27 serious vulnerabilities.

Source: techbeacon.com

41% of organizations had an API security incident in the last year.

63% of those observed that the incident involved a data loss or data breach.

Source: The 2022 API Security Trends Report, nonamesecurity.com

2/3rd of the incidents analyzed engaged improperly configured APIs – according to the analysis of X-Force Incident Response data of impacted clients.

Source: 2021 IBM Security X-Force Cloud Threat Landscape Report

Major API Data Breaches

1 Venmo
Venmo's API allowed one to scrape millions of transactions that users didn't realize were public.

2 Facebook
Facebook photo API exposure exposed private data in a breach affecting up to 6.8 million users and 1,500 apps

3 USPS
Corporate's insecure Web API allowed an attacker to query the USPS website and scrape a database of over 60 million corporate users.

4 Parler
The major security flaws in Parler's API-enabled attackers to easily scrape over 60 terabytes of data on the site's 10 million users.

5 NoxPlayer
Threat actors compromised the company's official API using a sophisticated technique, which exploited insufficient API response validation.

Clearly, API security is an issue we all need to be keeping an eye on in 2022!

Stop a Wide Range of API Attacks with AppTrana

Gartner Peer Insights Customers' Choice 2022

Indusface is the Only Vendor To Be Named Gartner® Peer Insights™ Customers' Choice in All the 7 Segments of Voice of Customer WAAP 2022 Report.

Protect Your Digital Assets

indusface.com

Get Started for Free