Predicts 2022: APIs Demand Improved Security and Management

Overview

Key Findings

- Organizations are adopting diverse types of APIs — internal APIs to represent coarse- and fine-grained service interfaces, data elements, and private and public APIs — at an expedited rate. Software engineering leaders are thus tasked with managing the explosion of both known and shadow APIs.

- API security challenges have emerged as a top concern for most software engineering leaders, as unmanaged and unsecured APIs create vulnerabilities that could accelerate multimillion dollar security incidents.

- While APIs have tremendously improved access to applications and services in software architectures, the use of third-party APIs introduces dependencies and failure risks, especially for mission-critical applications.

Recommendations

Software engineering leaders responsible for API technologies should:

- Manage and govern all APIs by investing in discovery, cataloging and automatic validation and by using an adaptive governance approach to manage a wide range of use cases and API types.
- Improve API security posture by developing a security strategy for threat protection, API security testing and API access control that leverages newer approaches and vendor solutions.

- Improve architectural resiliency by actively managing the consumption of APIs — that is, the use of both internal APIs and third-party APIs.

**Strategic Planning Assumptions**

By 2025, less than 50% of enterprise APIs will be managed, as explosive growth in APIs surpasses the capabilities of API management tools.

By 2025, more than 50% of enterprises will use GraphQL in production, up from less than 10% in 2021.

By 2025, the percentage of third-party APIs used in applications will average 30%, up from less than 10% in 2021, complicating dependency management.

By 2024, 25% of all insurance transactions involving new ecosystem partners will require open and public APIs, up from less than 5% in 2021.
Analysis

What You Need to Know

APIs are now at the core of digital business, as organizations of all sizes have adopted APIs to improve connectivity and to build composable architectures. API requests comprise 83% of all hits, according to an analysis by Akamai, with API hits growing by 30% year over year and expected to reach 42 trillion hits by 2024. Furthermore, infrastructure and security vendor CloudFlare found that API traffic grew 300% faster than web traffic in 2020. Gartner client inquiries related to APIs, including API security and API management, have increased by 33% year over year. In short, APIs are here to stay.

The explosive growth of APIs is driven by two key trends:

- Organizations are rapidly adopting APIs to deliver services and data, both internally and externally, due to their simplicity and increased access to technology and standards.
- New approaches and use cases involving APIs are emerging, especially as regulations and mandates force API adoption in industries such as banking and healthcare.

The proliferation of APIs is poised to continue for the foreseeable future. While the benefits of an API-driven future are clear, APIs also present significant risks:

- Most organizations are likely to be net consumers of APIs. Outages of these APIs or, worse, security incidents have an impact on the applications using them.
- Unmanaged and unsecured APIs are easy targets for attacks, increasing vulnerability to security and privacy incidents.
- Many SaaS vendors, including new startups, provide services via APIs. The widespread use of third-party APIs brings dependency risks.
- Industry regulations for access to data are adding new requirements to API initiatives.

Like the two sides of a coin, APIs provide software engineering leaders with key enabling capabilities to improve their technical posture and business models; but on the flip side, APIs create management and security challenges (see Figure 1).
In this research, our analysts offer top predictions about the future of APIs and provide guidance on how to maximize the benefits of APIs while mitigating the risks.
Strategic Planning Assumptions

Strategic Planning Assumption: By 2025, less than 50% of enterprise APIs will be managed, as explosive growth in APIs surpasses the capabilities of API management tools.

Analysis by: Jeremy D’Hoinne, Mark O’Neill

Key Findings:

- Enterprises are producing and consuming an exponentially growing number of APIs.
- API discovery is challenging; organizations struggle to manage a wide number of API initiatives (reproducing patterns observed in the early years of cloud infrastructure).
- Security controls are not maturing fast enough to match the rapid pace of API adoption.

Market Implications:

Enterprises are producing a massive number of APIs at a rate that far outpaces the maturity of network and application security practices. Newly created APIs are supported by emerging architectures and are frequently hosted in cloud environments. This situation resembles the early days of infrastructure as a service (IaaS) deployment, as ungoverned API usage is on the rise. As the architecture and operational technologies continue to mature, security controls try to apply old paradigms to new problems. These controls can be a temporary solution, but it will take a long time for security controls and practices to catch up with the new architecture paradigm.

Although specialized security controls exist, their API discovery features are limited in scope and lack the application logic awareness to enable the creation of relevant security policies. For APIs, this means that application security teams will deploy perimeter controls with threat inspection capabilities, but will be limited to generic policies and detection signatures. Further, building a business case for API security can be difficult for software engineering leaders. The business importance of APIs is evolving quickly, and many organizations continue to believe that general-purpose API management tools sufficiently address API security. By the time the security team gets funding and builds an RFP for a product, hundreds of APIs might already be in production.
Strong inventory and real-time discovery are both necessary to gain enough visibility into all APIs that the organization produces. Inventory can happen during the API development, which will require software engineering leaders to help build collaboration and mutual trust between the API product team and the security teams.

**Recommendations:**

- Lead with collaboration between the API product team and the security teams. Don’t treat API security as a problem that technology will solve entirely, and instead include secure coding practices in your API development.
- Prioritize API discovery and categorization at runtime and during API development.
- Plan for improvements and evolution in API security during the next several years, as both attacks and security controls are nascent.

**Strategic Planning Assumption:** By 2025, more than 50% of enterprises will use GraphQL in production, up from less than 10% in 2021.

**Analysis by:** Mark O’Neill

**Key Findings:**

- GraphQL APIs are growing in importance, as more development teams rapidly adopt them to expose back-end data and functionality with greater flexibility than REST APIs.
- GraphQL APIs are beginning to be published in API marketplaces, which will further drive usage.
- Vendor support for GraphQL APIs is nascent but growing, as it has expanded from specialists such as Apollo and Hasura to now include API gateway vendors and API design tooling vendors.

**Market Implications:**
GraphQL APIs are gaining in importance because developers benefit from the ability to control the data content of API responses. Consumer needs drive user experiences to evolve and adapt in multiple unpredictable ways. These changes can affect how an application interacts with back-end services and data. REST APIs tend to be opinionated in how response data is presented, and changing needs of the UI result in changes to the API. The flexibility of GraphQL APIs allows UI developers to be less dependent on back-end changes to meet their needs, helping them deliver value more quickly. As adoption of GraphQL APIs continues to grow, software engineering leaders will require tooling to support API discovery, governance and integration.

GraphQL APIs will also expand into data sharing and integration-centric use cases, driving demand for better native GraphQL support from business intelligence (BI), self-service analytics, integration platforms and low-code application platforms (LCAPs). For data-centric use cases, software engineering leaders must be wary that while GraphQL APIs are easy to use, they also have limitations. Furthermore, badly designed GraphQL APIs can introduce performance issues. They are neither a true “graph data” technology, nor a general-purpose query language like SQL, Apache Gremlin or Cypher.

The growth of GraphQL will drive the need for tools to secure, manage and deliver GraphQL APIs at scale and will drive the market for GraphQL skills in the developer community.

**Recommendations:**

- Consider GraphQL as an alternative for dedicated “experience APIs” or backend for frontend (BFF) APIs to API consumers to flexibly tailor API interactions to their needs.

- Adopt a “community of practice” approach to share GraphQL skills and experience across the organization. Include architects and integrators to help them better understand GraphQL capabilities and constraints.

- Ensure that your organization’s API security strategy applies GraphQL security and authorization best practices to GraphQL APIs, as security controls for REST APIs are not sufficient for detecting attacks or threats on GraphQL APIs.

*Special thanks to Gary Olliffe for his substantial contributions to this research.*
**Strategic Planning Assumption:** By 2025, the percentage of third-party APIs used in applications will average 30%, up from less than 10% in 2021, complicating dependency management.

**Analysis by:** John Santoro

**Key Findings:**

- The number of third-party APIs used by enterprises is exploding, including APIs for employee background checks (e.g., Checkr), payments (e.g., Stripe), marketing data enrichment (e.g., Clearbit), video (e.g., api.video) and a huge variety of other purposes.

- An outage by a third-party API impacts any application that uses that API. For example, Auth0's outage in April 2021 impacted all organizations that used Auth0's APIs to authenticate their users. ⁴

- Applications that use third-party APIs introduce availability, networking and security concerns, which software engineers must address.

**Market Implications:**

Developers create composite applications by combining existing functionality with new functionality to support new user experiences and business opportunities. This new functionality increasingly comes from third-party APIs that provide a wide range of business capabilities, including search (e.g., Algolia) and sentiment analysis (e.g., Nylas), or from other cloud-provided services. It also includes APIs provided by business partners, such as in supply chain or retail, or even within the company from other business units or product teams. Since these APIs must be licensed from and operated by the provider, composite applications are vulnerable when the APIs experience outages, suffer security breaches, increase their prices significantly or discontinue product support.

---

Most organizations are likely to become net consumers of APIs.
IT departments evaluate and manage SaaS applications with a concern for the provider’s ability to honor service-level agreements, secure customer data and reliably invest in product improvements (see How to Evaluate SaaS Providers and Solutions by Developing RFP Criteria). However, they appear to have somewhat of a blind spot when it comes to third-party APIs, which are also a form of SaaS that Gartner terms “API-centric SaaS.” Applications that consume third-party APIs must apply the same rigor to enforcing providers’ uptime, performance, security, licensing terms and product roadmaps, as they do for traditional SaaS services.

In addition to treating third-party APIs as products that are consumed, software engineering leaders must ensure that policies for end-user access to an application are consistent with the policies for communications among application components, including these third-party APIs. Ideally, the mapping between the two sets of policies should be stored in a single repository that can be accessed by all elements that provide communications and security. These technologies include SD-WAN, API gateways, ingress controllers and application delivery controllers. We call this nascent solution “composite application secure connectivity environment” (CASCE) — the convergence of application and network security to build a comprehensive policy configuration and enforcement model.

**Recommendations:**

- Create an inventory of the third-party APIs used by your organization. Use this to understand the impact if a third-party API — such as a payment API or an API used to authenticate customers — suffers an outage or, worse, a security breach.

- Manage the consumption of third-party APIs the way that you should manage SaaS applications: Negotiate and enforce SLAs, security compliance, licensing terms and continuity of service.

- Ensure secure connectivity across application components by using the concept of CASCE, distributed API gateways and private networks to enforce policies with fewer points of contact and more complete control.

**Strategic Planning Assumption:** By 2024, 25% of all insurance transactions involving new ecosystem partners will require open and public APIs, up from less than 5% in 2021.

**Analysis by:** Sham Gill

**Key Findings:**
Market Implications:

Public and open APIs represent a long-term strategic enabler for an insurer's digital business technology platform that will underpin the development of new business models, products and services:

- Public and open APIs hold the potential to expand an insurer's reach to a broader audience. They will enable insurers to increase distribution partnerships beyond traditional insurance agents and brokers. For example, Wakam (an insurtech) now offers all of its insurance products as APIs. This has enabled it to work with more than 200 partners to create new products and distribution channels including vehicle manufacturers, credit card fintechs and nonprofit organizations; see Case Study: Insurance API-Driven Digital Ecosystem Transformation (Wakam).

- Open and public APIs will also play a vital role in digital optimization and business transformation. For example, a European life insurer has exposed a set of public APIs that enable member data to be updated directly from the employer's HR systems to drive cost optimization.

- Most insurance companies are likely to be net consumers of APIs — for example, leveraging open banking APIs to validate a consumer's identity or to prefill data for quotation and new business stages (see Top Cross-Industry Open API Trends for Insurance CIOs to Track in 2021).
Recommendations:

- Accelerate the creation of public and open APIs in your digital business platform by identifying common interactions with partners to promote and co-create APIs that provide mutual business value.

- Run purposeful pilot projects using public and open APIs offered by other industries, with a focus on learning rather than performance.

- Build on the initial pilot by leading increasingly sophisticated projects that represent the organization's most likely public and open API use cases.

- Track volume trends and API usage frequency by analyzing the data provided by API management tools to build the business case for future value-creation opportunities.

- Safeguard your organization against problems that could arise when partners withdraw public/open API services by defining an exit strategy that outlines key dependencies and decisions.

A Look Back

In response to your requests, we are taking a look back at some key predictions from previous years. We have intentionally selected predictions from opposite ends of the scale — one where we were wholly or largely on target, as well as one we missed.

On Target: 2017 Prediction — By 2022, API abuses will be the most-frequent attack vector resulting in data breaches for enterprise web applications.

In 2017, attacks on APIs had not reached mainstream awareness. It was rare for a data breach to come via an API because little critical business data was publicly available through APIs.
This prediction was based on our analysis of the growing number of APIs, which increase the attack surface for organizations and consequently become a threat vector that attackers frequently exploit.

As 2022 approaches, this prediction could arguably be counted as “missed” — but only because we underestimated the steep rise in attacks on APIs. By 2020, more than half of all data thefts were traceable to unsecure APIs. This upward trajectory has continued in 2021, with IBM Security X-Force reporting that two-thirds of its analyzed incidents are due to unsecure APIs. Attacks on APIs happen on a regular basis, as documented by APIsecurity.io.

**Evidence**

1. [The State of the Internet](#), Akamai.
2. [Protecting Your APIs From Abuse and Data Exfiltration](#), CloudFlare.
3. Gartner client inquiry volume related to APIs increased steadily from 2019 to 2021, at an average increase of 33% year over year.
4. [Auth0 Outage April 20, 2021 — 3 hours](#), APImetrics.
5. [2021 IBM Security X-Force Cloud Threat Landscape Report](#), IBM.

**Recommended by the Authors**

Some documents may not be available as part of your current Gartner subscription.

- Top Cross-Industry Open API Trends for Insurance CIOs to Track in 2021
- Top Trends in Financial Services Product Reinvention for 2021
- API Security: What You Need to Do to Protect Your APIs