okta

What Does an Effective API Strategy Look Like?

Okta Inc.
80 Pacific Hwy, Level 13
North Sydney, NSW 2060

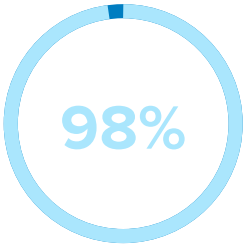
info@okta.com
+61 (2) 8310-4484

Table of Contents

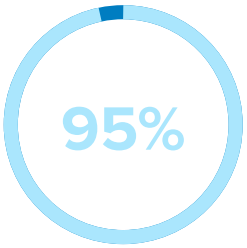
Introduction to the API Landscape

APIs are transforming how we conduct business—they're improving the speed and quality of software development and data integration—and they're a growing phenomenon. In the last eight years, the number of public APIs has gone from less than 2,000 to more than 50,000, and that growth is driving increased investment across multiple industries. According to Okta's Executive Survey on API Strategy, 98% of respondents said they had some sort of API strategy in place and 95% are planning to invest in APIs in the near future. APIs are here to stay.

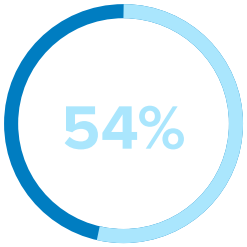
Alongside the rise of investment in the sector, API-centric breaches are also developing in scale and both Gartner and OWASP identify these types of attacks as the next major security vector. In an environment where tech integration is becoming the norm, organizations need to understand the risks of implementing an API strategy and be equipped to manage and secure their APIs effectively.



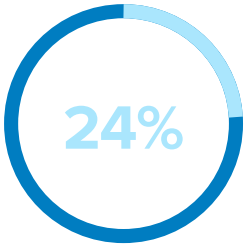
of respondents said they had some sort of API strategy in place



are planning to invest in APIs in the near future



of respondents feel that their strategies are likely to succeed



indicated that their strategies were already successfully planned and implemented

Why Invest in an API Strategy?

As organizations continue to uncover their value, APIs are becoming an integral part of how business is conducted. Respondents to Okta's survey believe a strong API strategy enables them to create integration tools that drive adoption, integrate effectively with partners, and scale internal operations, while also lowering total cost of ownership (TCO) and maintenance costs.

Overall, organizations are feeling optimistic about this investment in strategies: 54% of respondents feel that their strategies are likely to succeed, and 24% indicated that their strategies were already successfully planned and implemented. Regardless, we can't let this optimism blind us to the new and different landscape that comes with API adoption.

Risks of API Adoption

Despite the drastic growth of APIs, corresponding security practices have not developed at the same pace and are often a secondary consideration for the developers shipping applications. Currently development teams work independently of their security teams, making it difficult for the latter to effectively test or validate API security policies, leaving their organization vulnerable to an attack.

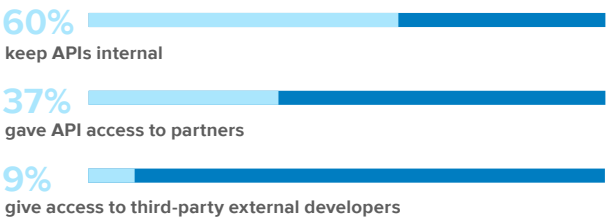
API-based data breaches present an ongoing threat to organizations that host large amounts of customer information. According to Gartner, they will be the largest source of data breaches by 2022. We're already seeing early examples, with Facebook having over 50 million accounts compromised as a result of an attack on their API, and other big name breaches such as Equifax and T-Mobile. For organizations that host a wealth of personally identifiable information (PII), including names, credit card details, or even social security numbers, data breaches can be catastrophic. Not only do they pose a massive security risk, they also compromise the organization's reputation, impact the confidence of stakeholders, and create legal liability and attract the attention of regulatory agencies. As such, companies that offer customers omni-channel experiences must secure their customer data as they plan their API strategy.

One of the primary risks associated with API development comes down to conflicting motivations of IT administrators versus developers. While IT focuses on managing secure enterprise applications, developers are encouraged to innovate with new features that drive user growth and retention. Effectively one group wants stability and reliability while the other must constantly experiment and grow to gain an edge.

Further, only 8% of respondents to Okta's survey said they had input from all stakeholders (i.e. IT teams, Product Management, Engineering and Development, and Information Security teams) when it came to API development. For organizations that are dependent on collaboration and coordination to succeed, this is a recipe for disaster. To bridge these gaps, all stakeholders should be engaged early to make API security a team effort from the beginning.

Best Practices for Creating a Secure API Strategy

The key to deploying a secure organization-wide API strategy is to understand the full API lifecycle. Currently 60% of respondents said APIs were purely internal, while 37% also gave access to partners and 9% also gave access to third-party external developers. This reflects of the lifecycle as successful APIs are usually developed internally, then rolled out across the organization, and finally introduced to partners and external users. Success might drive failure here—if security considerations aren't applied at the beginning with the end in mind, it becomes time-consuming and costly to implement changes once the API has reached external partners and end users.



To effectively secure their API strategy throughout the lifecycle, organizations should consider security from Day One, and maintain strict standards like only exposing interfaces as needed, only collecting and sharing essential data, and only granting access to the key users and systems that require the API. In addition, organizations should have plans for both responding to problems that might arise in the API development—such as data breaches—and for communicating with users on policy changes and more. Understanding and adopting specific API access management guidelines and implementing standards like OAuth 2.0 and OpenID Connect is also key.

How Okta's API Solutions Can Help You Win

Organizations want to offer omnichannel digital experiences to customers, but often lack the strategic and technical knowledge to properly secure their APIs. Okta can help our customers create secure and seamless user experiences, and scale as users and requirements change over time. Okta's API Access Management protects APIs by providing secure and developer-friendly solutions such as:

1. Authentication: Creates improved login procedures to verify a user's identity
2. Authorization: Controls which users and developers can access APIs using granular authorization policies based on application type, user group membership, and permissions requested
3. User management: Keeps all users, groups, devices, and policies centrally located within the Okta Identity Cloud to create a single source of truth
4. Lifecycle management: Automates onboarding and offboarding to APIs in the same way as for all other applications
5. B2B integrations: Securely integrates with API gateways

Okta's API Access Management works with Okta's Universal Directory and allows for Single Sign-On and centralized authorization monitoring that controls API access based on a user's profile, device, network, and group membership. It also provides token revocation and introspection, integration with API Gateways, customizable authorization policies, and a real-time dashboard to flag abnormal behavior and token-related events.

By working with Okta, you can outsource time – and resource-intensive compliance requirements – allowing your developers to create the best services for your customers. Okta also provides a range of flexible tools, templates, and libraries and enables your team with examples ranging from simple how-to guides to detailed use cases.

To learn more about API access management with Okta, refer to the API Access Management datasheet.