SECURING THE API ATTACK SURFACE

Melinda Marks, Senior Analyst

MAY 2023

Research Objectives

Organizations across industries improve their productivity, innovation, and customer service with an increase in web, mobile, and cloud applications leveraging microservices architectures. But this brings an increase in APIs connecting application components and resources. Organizations rate APIs as the element in the cloud-native stack most susceptible to attack, and attacks stemming from insecure APIs were the most commonly identified cybersecurity incident tied to cloud-native app development over the last 12 months. As the number of APIs continues to grow, security risk increases.

As a result, organizations need effective API security solutions to reduce risk as cloud-native development scales and help their teams discover, manage, configure, monitor, and protect their APIs to keep pace with modern software development. To gain further insight into these trends, TechTarget's Enterprise Strategy Group (ESG) surveyed 397 IT, cybersecurity, and application development professionals at organizations in North America (US and Canada) responsible for evaluating or purchasing cloud security technology products and services.

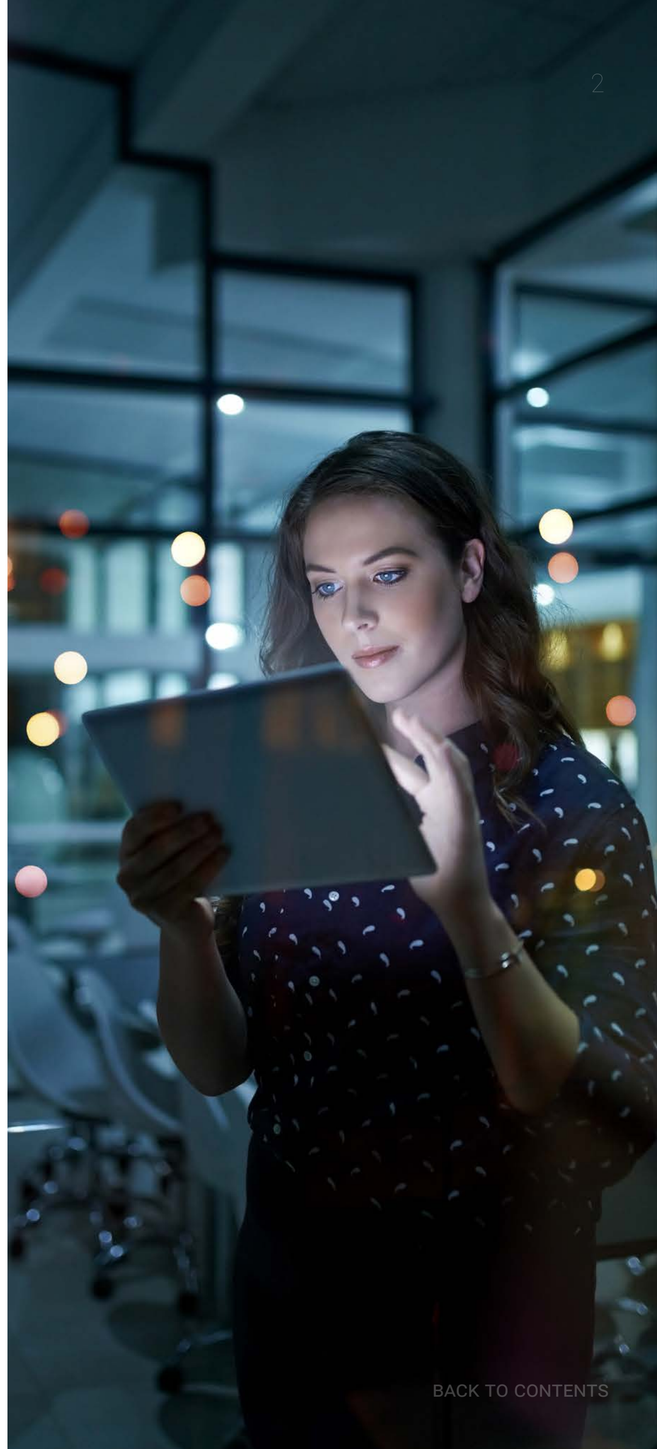
This study sought to:

Validate API usage and growth patterns associated with cloud adoption and digital transformation.

Examine current API security approaches and their effectiveness.

Highlight the challenges security teams face in securing their APIs.

Determine best practices for improving API security.



BACK TO CONTENTS

KEY FINDINGS

CLICK TO FOLLOW

Application Development Modernization Necessitates Cybersecurity Modernization

PAGE 4

API Growth Is Exacerbating Security Risk Levels

PAGE 8

API Security Incidents Are Pervasive, Resulting in Many Challenges and Shortcomings

PAGE 13

Building an Effective API Security Strategy Involves a Variety of Tools and Developer Participation

PAGE 20

Organizations Are Committed to and Investing in Solidifying API Security Posture

PAGE 27

Research Methodology and Demographics

PAGE 31

Application Development Modernization Necessitates Cybersecurity Modernization

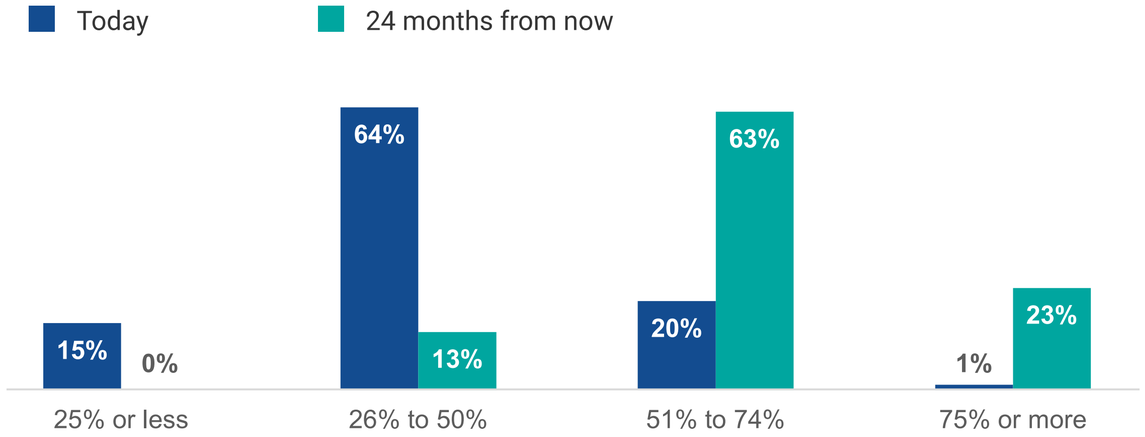
Digital Transformation for Business Applications

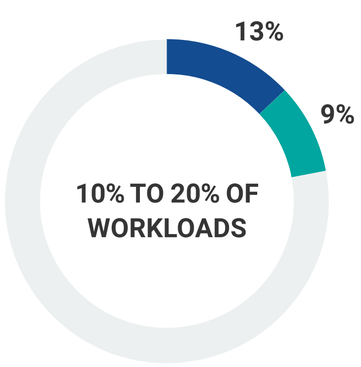
Organizations are increasingly moving their production workloads to public cloud platforms. By leveraging the state-of-the-art technologies and services from cloud service providers (CSPs) and microservices application architectures, they can efficiently build and deploy their applications faster to serve their employees, partners, and customers.

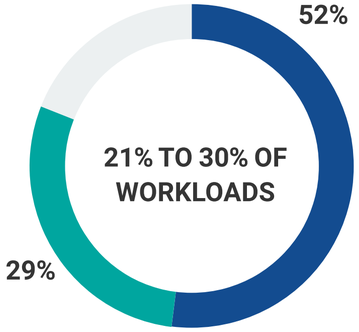
Percentage of production server workloads run on public cloud infrastructure services.

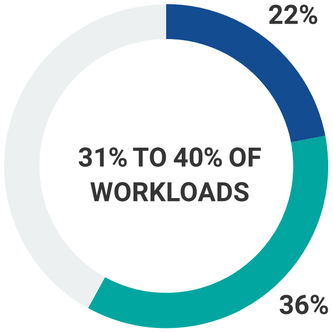
- Percentage of production workloads run on public cloud infrastructure services today
- Percentage of production workloads run on public cloud infrastructure services 24 months from now

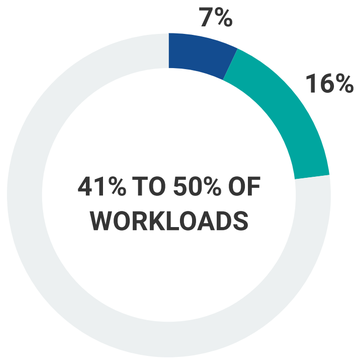
Percentage of public-facing web applications based on a microservices, cloud-native architecture.

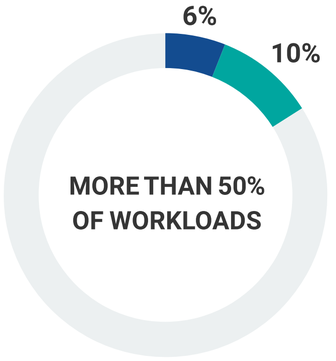








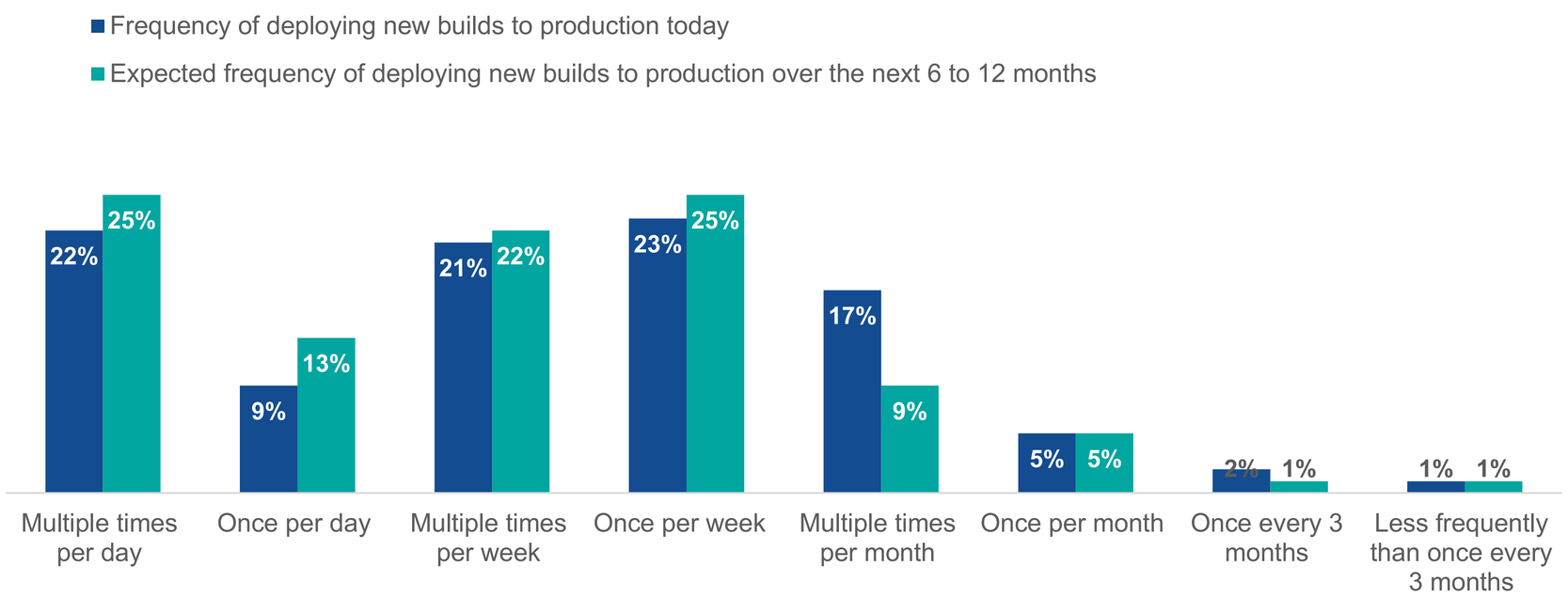




BACK TO CONTENTS

Use of DevOps to automate CI/CD of code and infrastructure.

Frequency with which developers and/or DevOps teams deliver new builds to production.



Increasing Developer Efficiency for Faster Releases

Organizations are also leveraging DevOps methodologies for continuous integration and continuous deployment (CI/CD) of applications. This empowers developers to provision their own cloud infrastructure, collaborate via CI/CD pipelines to efficiently build their applications, and deploy them to the cloud. Many organizations currently release new builds daily, and developers expect to increase the frequency of releases, raising challenges for security to keep up with the rapid pace.

BACK TO CONTENTS

Challenges Incorporating Security to Keep Up with Release Speed

Although cloud-native application development brings efficiency and productivity benefits, security teams are challenged gaining the control they need to ensure that the applications deployed are secure. In addition to citing production builds being deployed with security issues, many organizations report their security teams lack visibility into development processes and/or that developers are skipping security processes.

They need ways to incorporate security into the development processes without slowing operations down.

> “They need ways to incorporate security into the development processes **without slowing operations down.”**
>
> - Melinda Marks, Senior Analyst

Security challenges resulting from the faster development cycles of CI/CD.

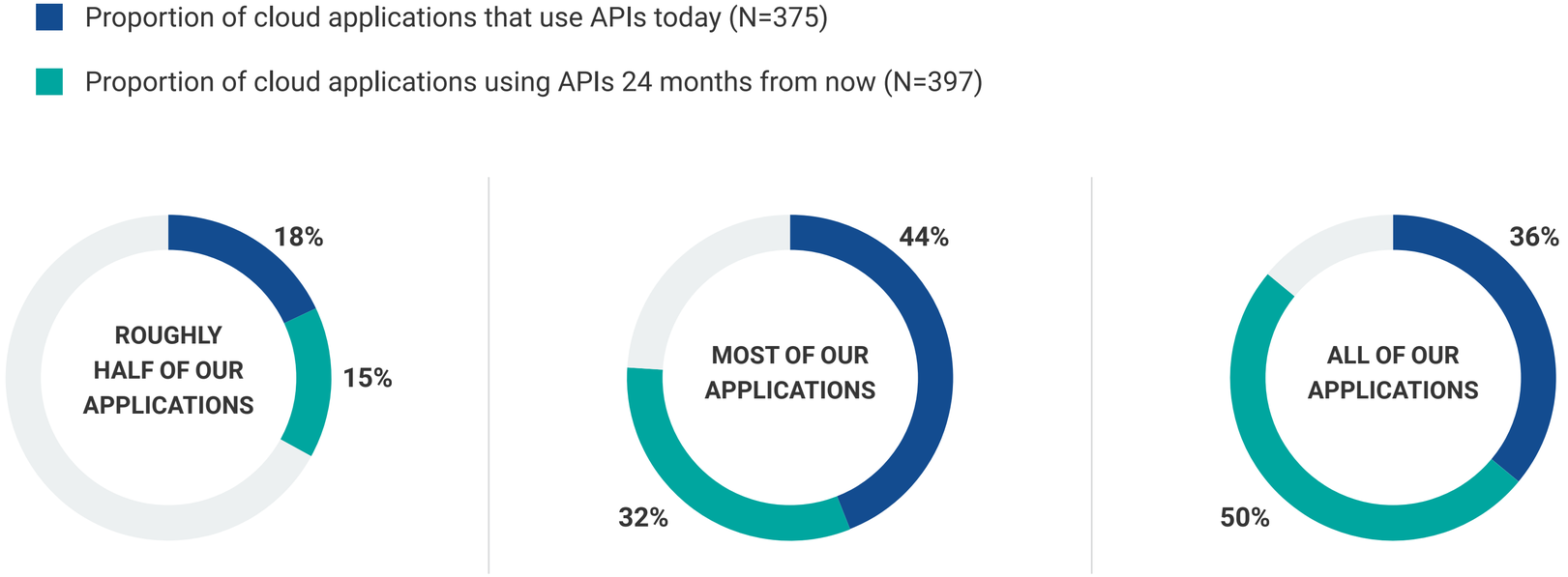
BACK TO CONTENTS

API Growth Is Exacerbating Security Risk Levels

Growing Proportion of Applications Using APIs

As cloud-native development with microservices-based applications continues to grow, those applications require APIs to access services, data, or other applications. As developers create more complex applications, the number of APIs can grow. Indeed, while more than one-third of organizations say all of their applications use APIs today, this is expected to grow to 50% over the next two years.

Proportion of cloud-native applications using APIs.



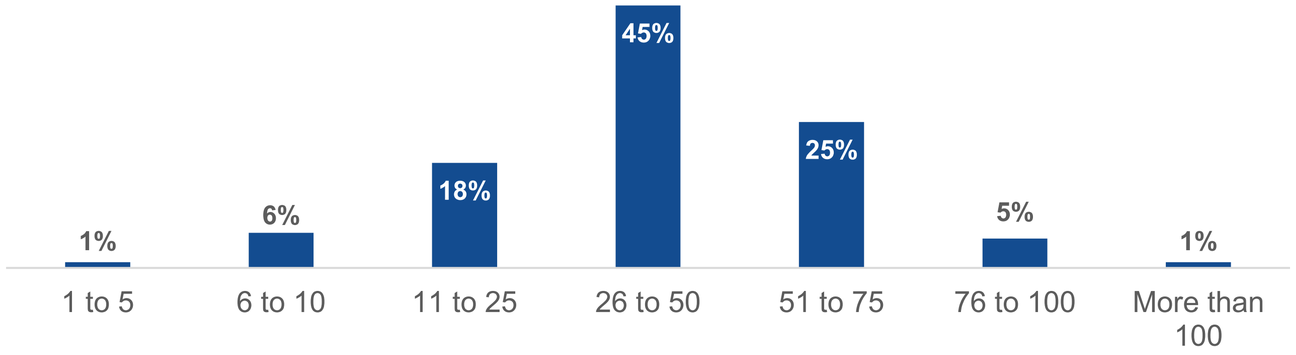
“More than one-third of organizations **say all of their applications use APIs today... this is expected to grow to 50% over the next two years.”**

BACK TO CONTENTS

Security Risk with High Numbers of APIs per Application

More than three-quarters (76%) of organizations report that they have an average of 26 APIs per application deployed. High percentages of organizations are using open APIs for public consumption, connecting applications with partners and connecting microservices. Security teams need to ensure every connection is secure to meet their key business drivers of keeping applications running and secure.

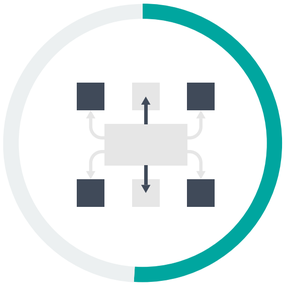
Average number of APIs per application.



How APIs are used.

67%
Open APIs for public consumption

64%
Connecting applications with partners



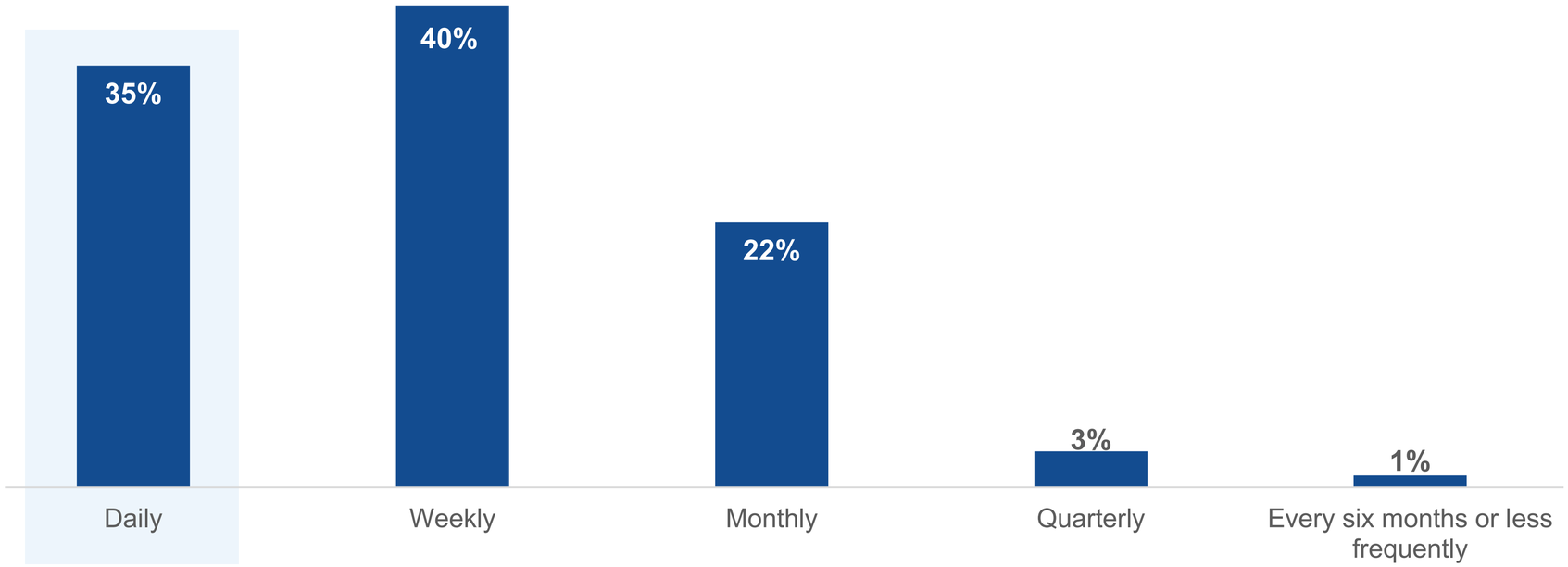
51%
Connecting microservices

BACK TO CONTENTS

Frequency of API Updates

In addition to facing challenges from the rapidly growing number of APIs and their exposures from the associated types of connections, security teams are challenged keeping up with the speed of API updates. More than one-third (35%) of organizations release updates daily, and another 40% update on a weekly basis.

Frequency with which organizations typically change or update APIs.



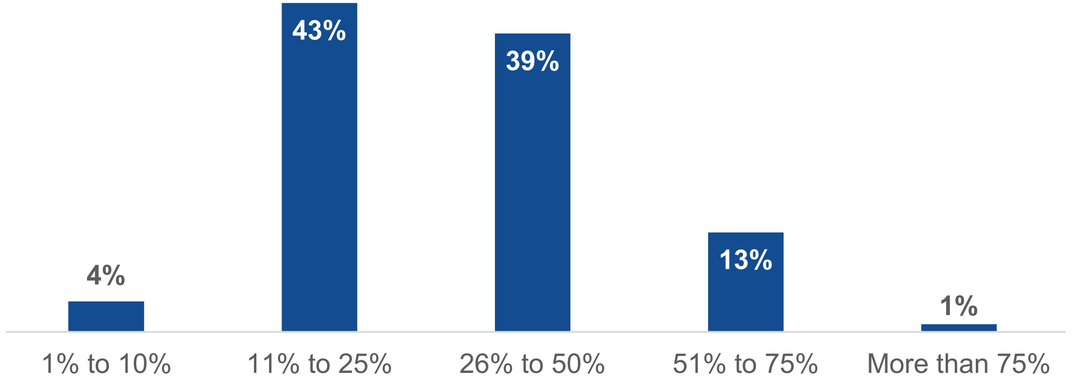
“More than one-third (35%) of organizations **release updates daily.**”

BACK TO CONTENTS

API Exposures and Connections

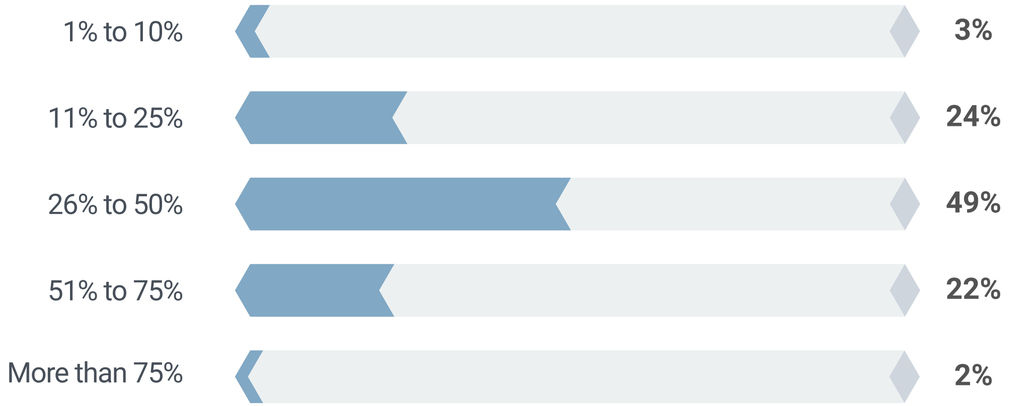
APIs are important for building modern applications that can call other services, applications, or data. Every API or update can add attack surface if it is not secured because of the way that they are connected and the related exposure. While most applications use APIs, the majority of organizations don't have high percentages of internet-facing APIs. This indicates that many are internal-facing, likely for connecting multiple microservices. A high percentage of APIs connect applications to other applications. This reflects the increasing trend of sharing open APIs for integrations, which could be with internal departments within companies or external third-party developers or business partners to connect applications for richer functionality. The data also shows that organizations recognize the growing percentage of cloud/internet traffic that is API traffic, underscoring the importance of API security in their network security strategies.

Percentage of organizations' APIs exposed to the internet.



Percentage of APIs that are third-party APIs connecting to other applications.

Percentage of cloud/internet traffic that is API traffic.



BACK TO CONTENTS

API Security Incidents Are Pervasive, Resulting in Many Challenges and Shortcomings

Security Incidents from Insecure APIs

As the number of APIs continues to proliferate, organizations have suffered from security incidents related to insecure APIs over the past 12 months. Despite having multiple products in place addressing API security, more than half (57%) faced multiple incidents, and 35% faced at least one incident within the last year.

Have organizations experienced a security incident related to insecure APIs in the last 12 months?

We have experienced multiple security incidents related to insecure APIs in the last 12 months,

57%

We have experienced one security incident related to insecure APIs in the last 12 months,

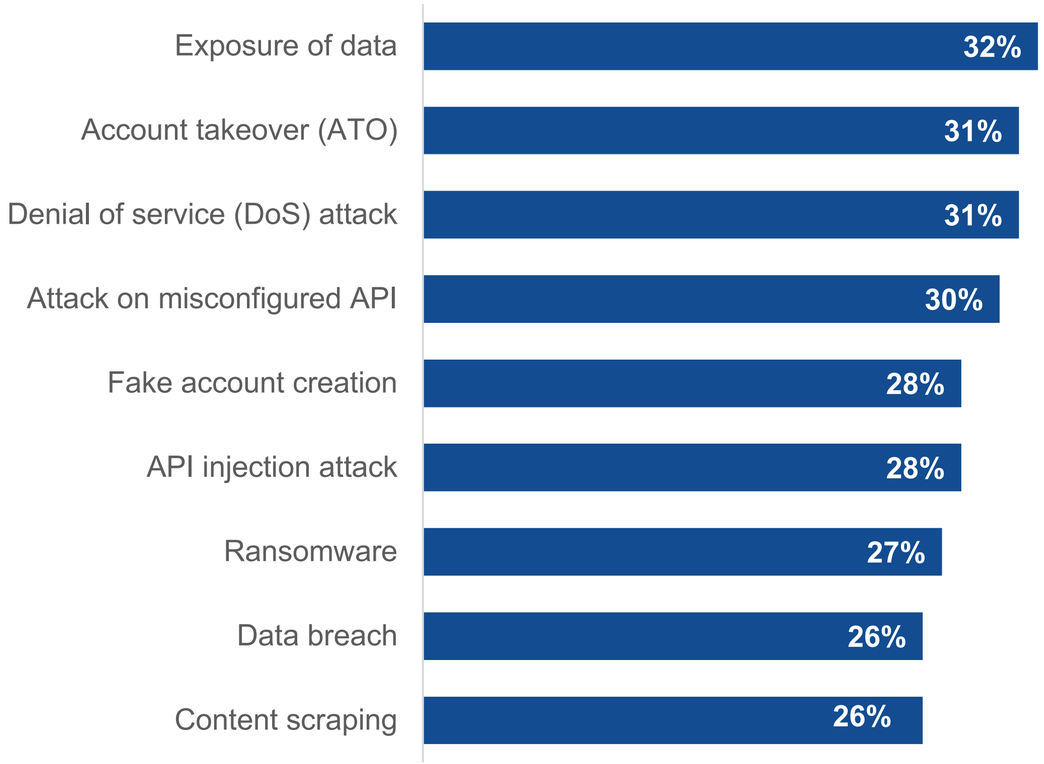
35%

BACK TO CONTENTS

Types of API Security Incidents and Their Impacts

Security teams need effective ways to manage security risk to support the growing usage of APIs because they open them up to exposure to a wide variety of attacks. Organizations have suffered a range of security incidents from insecure APIs, including account takeover, denial of service attacks, and data breaches. These attacks can have serious impacts for organizations, and this impedes them from meeting their top application security drivers for application uptime, customer service, and cost management.

Types of security incidents from insecure APIs.



Impacts of API security incidents.

BACK TO CONTENTS

Attacks Despite Security Solutions in Place

Nearly three-quarters (74%) of organizations believe they have a robust API security program with processes and controls in place for API security. They have multiple web application protection tools in place, including API security tools, web application firewalls (WAFs), and API gateways, as well as distributed DoS mitigation and bot management solutions.

Discrete tools used to protect web applications.

59%
API security tools

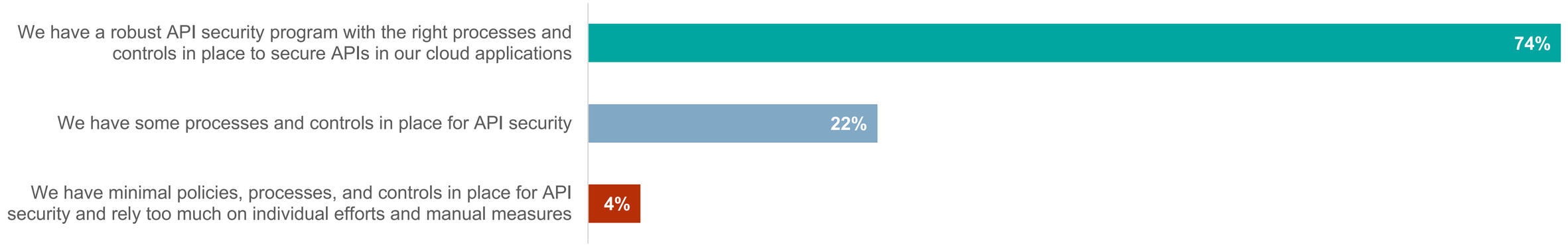
57%
Web application firewall (WAF)

50%
API gateways

48%
Distributed denial of service mitigation

42%
Bot management

Status of API security capabilities.



BACK TO CONTENTS

Top API Security Challenges

Despite having robust API security programs with multiple tools in place, organizations face many challenges across application security. These are challenges managing multiple tools and gaining visibility into and control over elements that are scaling rapidly with cloud-native development. For APIs, they are particularly challenged with inventories that would enable them to consistently apply security processes and policies.

Biggest challenges organization have faced with API security.

29%
Using multiple API management tools

28%
Lack of control over/visibility into deployment of APIs

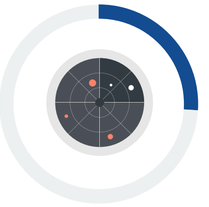
27%
Accurately inventorying third-party APIs used by our applications

27%
Inconsistent adoption of API specifications

27%
Enabling developers to perform API security testing before deploying applications

26%
Data governance and/or data exposure issues as a result of insecure APIs

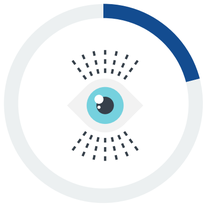
26%
Discovering and remediating misconfigured APIs



26%
Keeping pace with the threats targeting our APIs

25%
Accurately inventorying APIs used in our organization

24%
Using application security tools not purpose built for API security



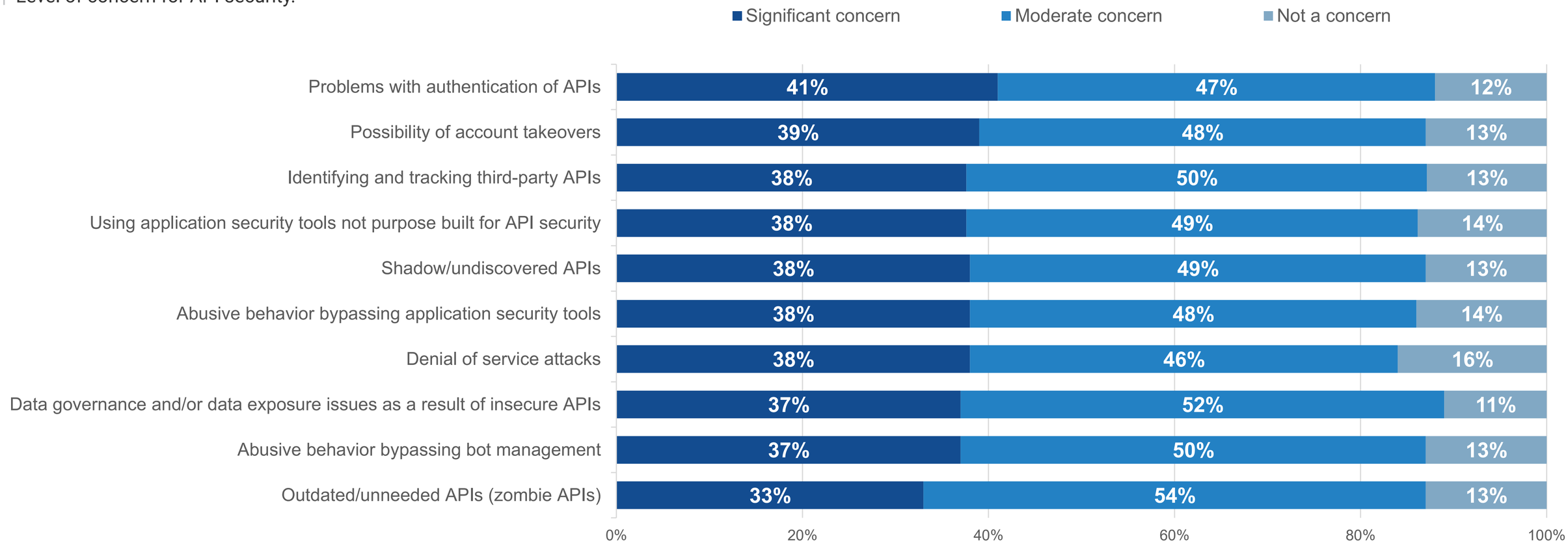
21%
APIs possibly exposing sensitive data

BACK TO CONTENTS

API Security Concerns

Knowing how the numbers of APIs are increasing, the wide variety of security concerns shows the urgency in addressing them to effectively manage cloud security risk. The top concern is around authentication, which is alarming because every connection needs effective authentication to be secure. There are also many visibility concerns, including identifying and tracking APIs, discovering shadow APIs, and zombie APIs. The range of concerns underscores the need for organizations to find a better approach to securing their APIs.

Level of concern for API security.



BACK TO CONTENTS

Types of API vulnerabilities that are of greatest concern.

34%
Sensitive data exposure

31%
Attribute-based access control vulnerabilities

31%
API business logic flaws

30%
Distributed denial of services attacks

29%
Code injection attacks

28%
Privilege escalation attacks

27%
Man-in-the-middle attacks

26%
Parameter tampering

23%
Cross-site request forgery attacks

Wide Range of API Vulnerabilities Causing Concern

APIs play such an important role in modern applications by connecting them to other services, applications, and data, which makes them vulnerable to a range of attacks.

Organizations are concerned about the wide range of API security susceptibilities that could expose them to serious attacks, including sensitive data exposure, access control vulnerabilities, and API business logic flaws.

BACK TO CONTENTS

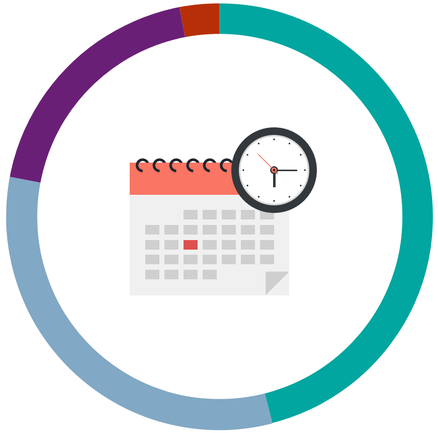
Building an Effective API Security Strategy Involves a Variety of Tools and Developer Participation

The Need to Drive Remediation Efficiency

For security to support the scale and speed of growing APIs, they need tools to help drive efficient remediation so they can respond quickly to vulnerabilities. The data shows that more than two-thirds can respond within a day, with 39% reporting the ability to do so within hours. When vulnerabilities expose sensitive data, that time is precious.

The data also shows organizations are relying more on manual testing and review versus automated alerting to protect their sensitive data. As organizations scale with increasing product releases and higher numbers of APIs to add functionality and services to their applications, this is not sustainable. Security teams need fewer tedious manual tasks and solutions that can automate alerting to drive efficient actions that remediate vulnerabilities exposing them to risk.

| Time it typically takes to remediate an API vulnerability.



46% Hours

32% One day

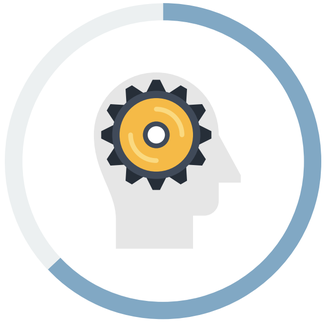
19% One week

2% Several weeks

| Methods of ensuring APIs do not expose sensitive data.

79%

Manual testing and review



63%

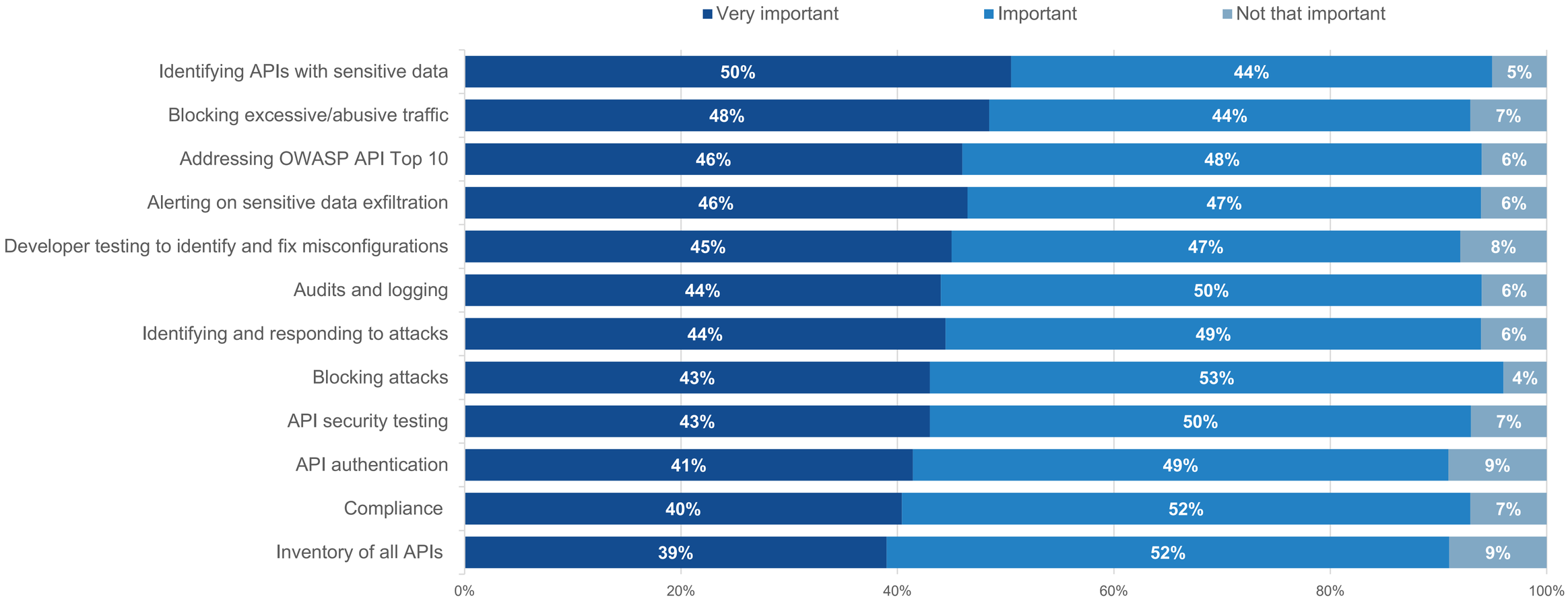
Automated alerting

BACK TO CONTENTS

Key API Security Capabilities

Organizations are looking for API security solutions with a comprehensive set of features, rating a wide range of capabilities as important or very important. Many important capabilities are related to the security concerns mentioned earlier, including identifying and tracking APIs, API authentication, and ways to block attacks or excessive traffic. Identifying APIs with sensitive data, which would help provide context to prioritize actions for better protection, was identified as a very important capability of an API security offering.

Importance of API security capabilities.

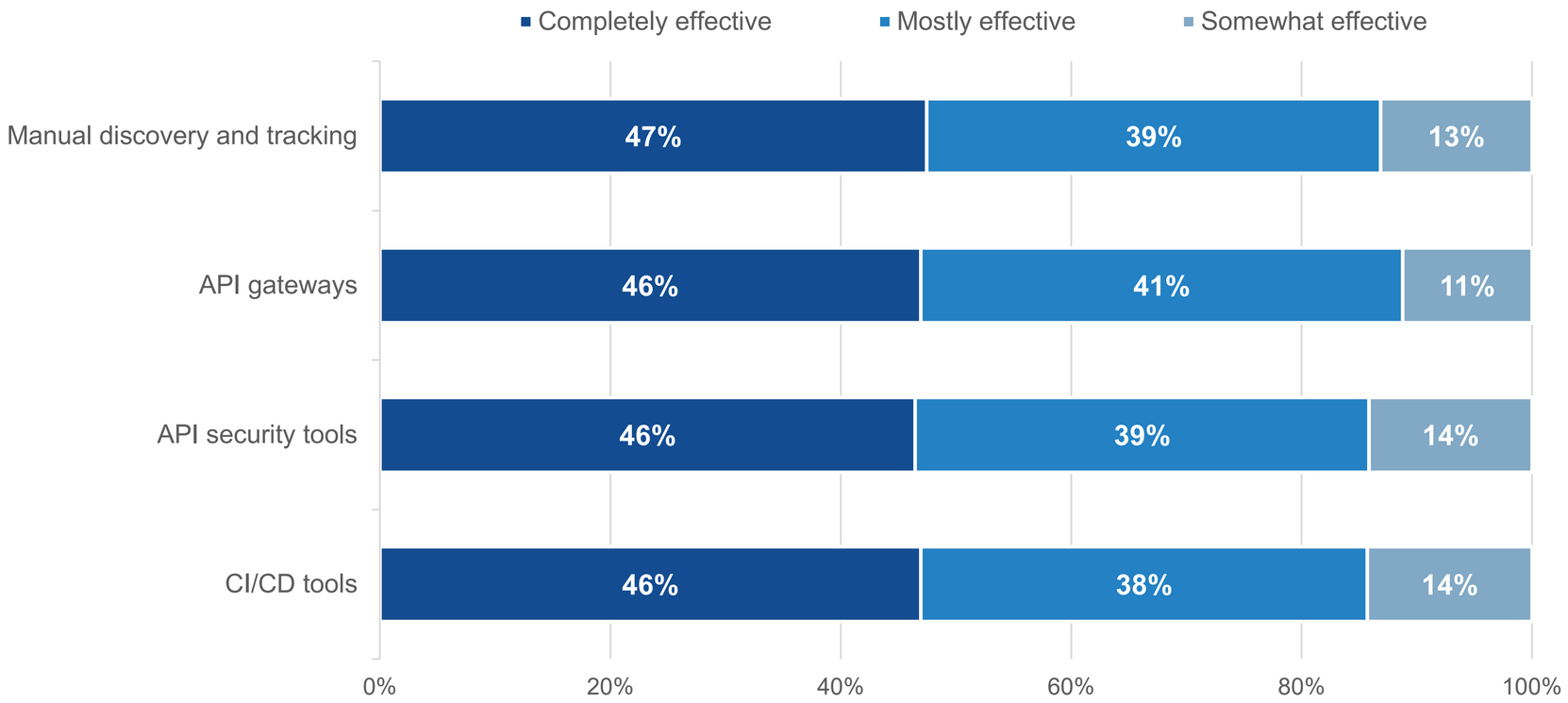


BACK TO CONTENTS

Effectiveness of Discovery and Tracking Processes and Tools

Inventory and discovery of APIs are foundational to an effective API security program. Many organizations are using some combination of API gateways, API security tools, and CI/CD tools, and the majority rate them as mostly effective for API discovery and tracking. However, it is worth noting that despite the fact that they are using multiple tools, manual discovery and tracking is also seen as mostly effective.

Tools or processes used to **discover and track** APIs.



Many organizations are using some combination of API gateways, API security tools, and CI/CD tools."

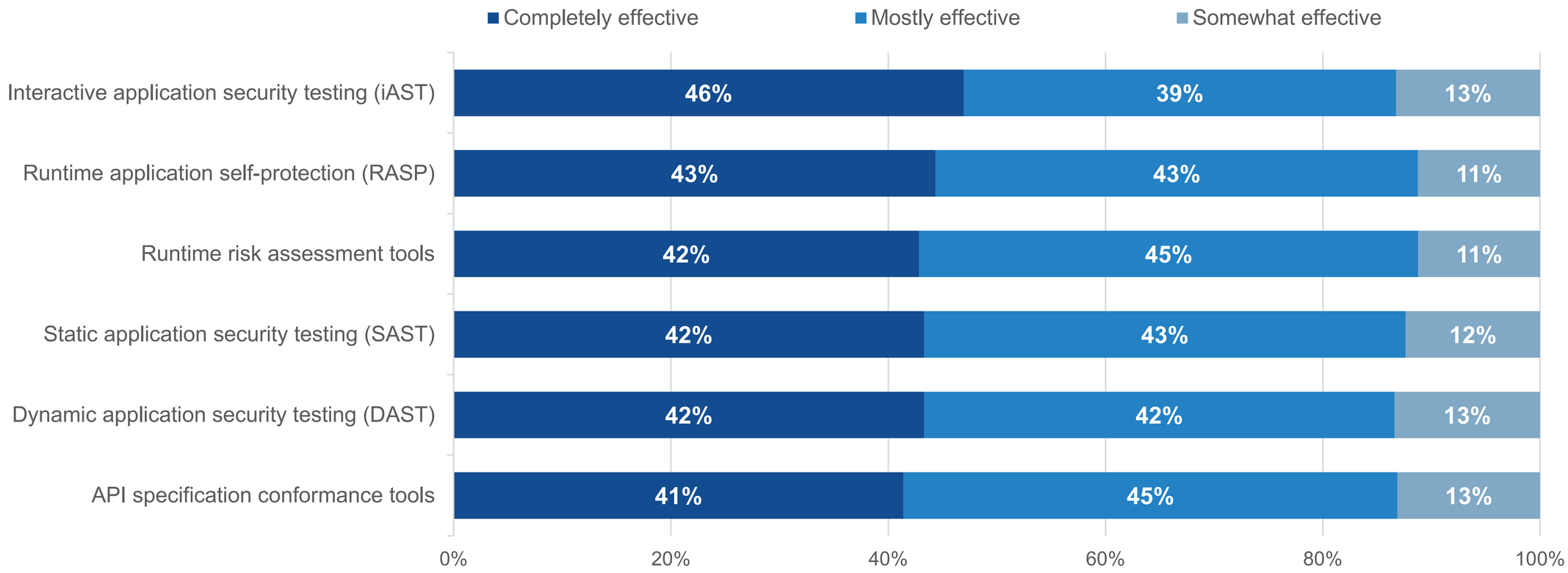
BACK TO CONTENTS

NEARLY HALF
classify iAST tools as
completely effective.

API Code Remediation with Application Security Tools

For remediating API coding issues, organizations are typically utilizing their multiple application security tools, including testing tools, runtime application self-protection, runtime assessment tools, and API specification conformance tools. As was the case with discovery and tracking API tools and processes, these tools were most rated as completely or mostly effective, with nearly half classifying iAST tools as completely effective.

Tools used to **discover and remediate** APIs.

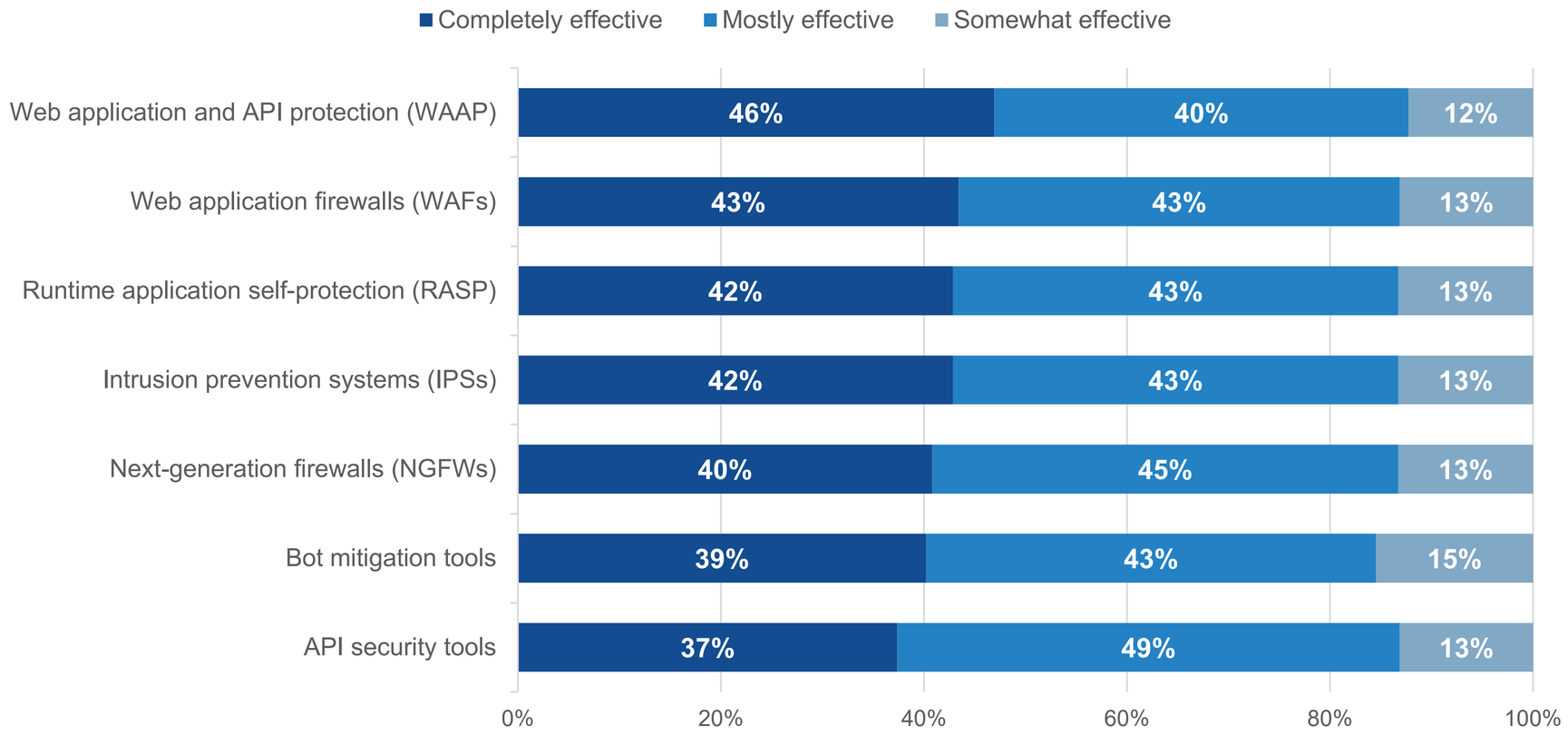


BACK TO CONTENTS

Effectiveness of Tools in Stopping or Blocking Attacks

Organizations are also using a plethora of tools to stop or block attacks on APIs. In terms of their efficacy, as was the case with other tools and processes in place to secure APIs, the majority rated tools such as web application and API protection (WAAP), web application firewalls (WAFs), and runtime application self-protection (RASP) tools as mostly or completely effective.

Tools used to **stop or block** attacks on APIs.



> **Organizations are using a plethora of tools** to stop or block attacks on APIs.”

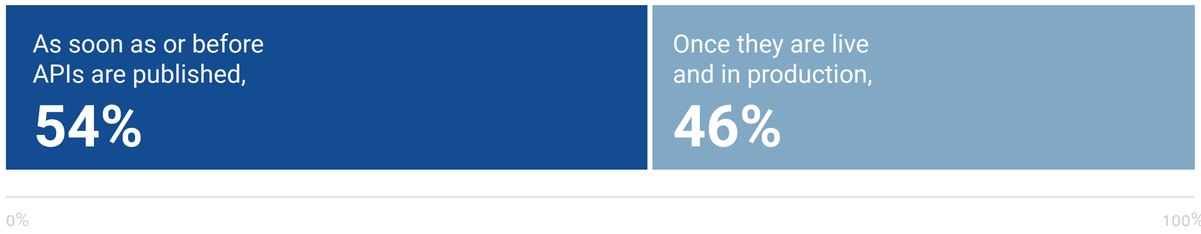
BACK TO CONTENTS

Increasing Cooperation between Security and Development

To mitigate risk, security should be involved in securing APIs before they are deployed. More than half (54%) of teams responsible for securing APIs are involved with development as soon as or before they are published, so there is still a lot of room for improvement. However, it is promising that organizations rate a high percentage of developers as having either a good (22%) or high (71%) level of API security knowledge. Overall, 89% of organizations provide formal API security training to their development teams, which jumps to 96% among those reporting their developers have a high level of knowledge about API risk.

Developer understanding of API risk.

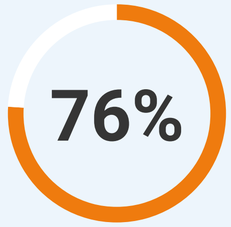
When security becomes involved in API publication process.



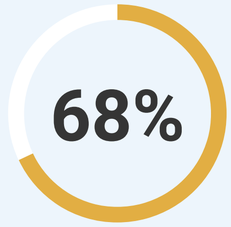
89%
of organizations provide **formal API security training** to their development teams.

Percentage of organizations that provide formal API security training to development teams based on API security risk knowledge of development teams.

HIGH level of knowledge for API security risks



GOOD level of knowledge for API security risks



LIMITED level of knowledge for API security risks

BACK TO CONTENTS

Organizations Are Committed to and Investing in Solidifying API Security Posture

API Security Investments and Future Plans

Organizations are prioritizing investing in API security because of its importance in enabling digital transformation. The data shows that most organizations have dedicated budget for API security, and most expect to increase their investments in API security solutions over the next 12-18 months. The areas in which organizations expect to focus their increased spending include API security tools, with many looking for API security capabilities in other tools like cloud-native application protection platforms (CNAPPs), application security tools, API management tools, WAFs, bot management, and DDoS mitigation tools.

Source from which API security is funded.

60%
A dedicated API security budget

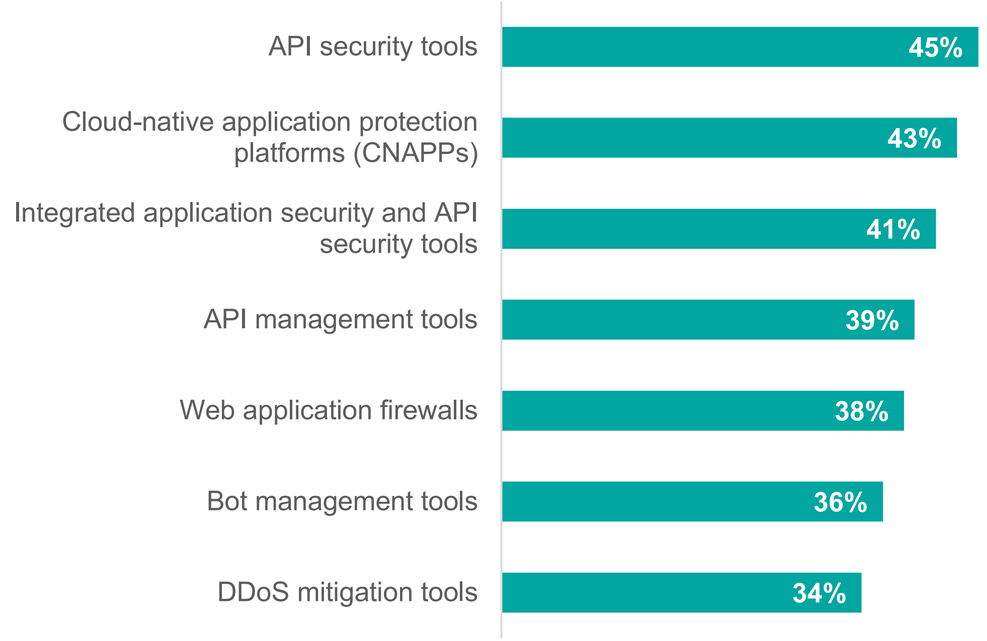
30%
Discrete web application and API protection budget within other security program budgets, such as network security or application security

8%
Discrete web application and API protection budget within other non-security IT or line-of-business program budgets

3%
Discrete web application and API protection budget within cloud services program budgets

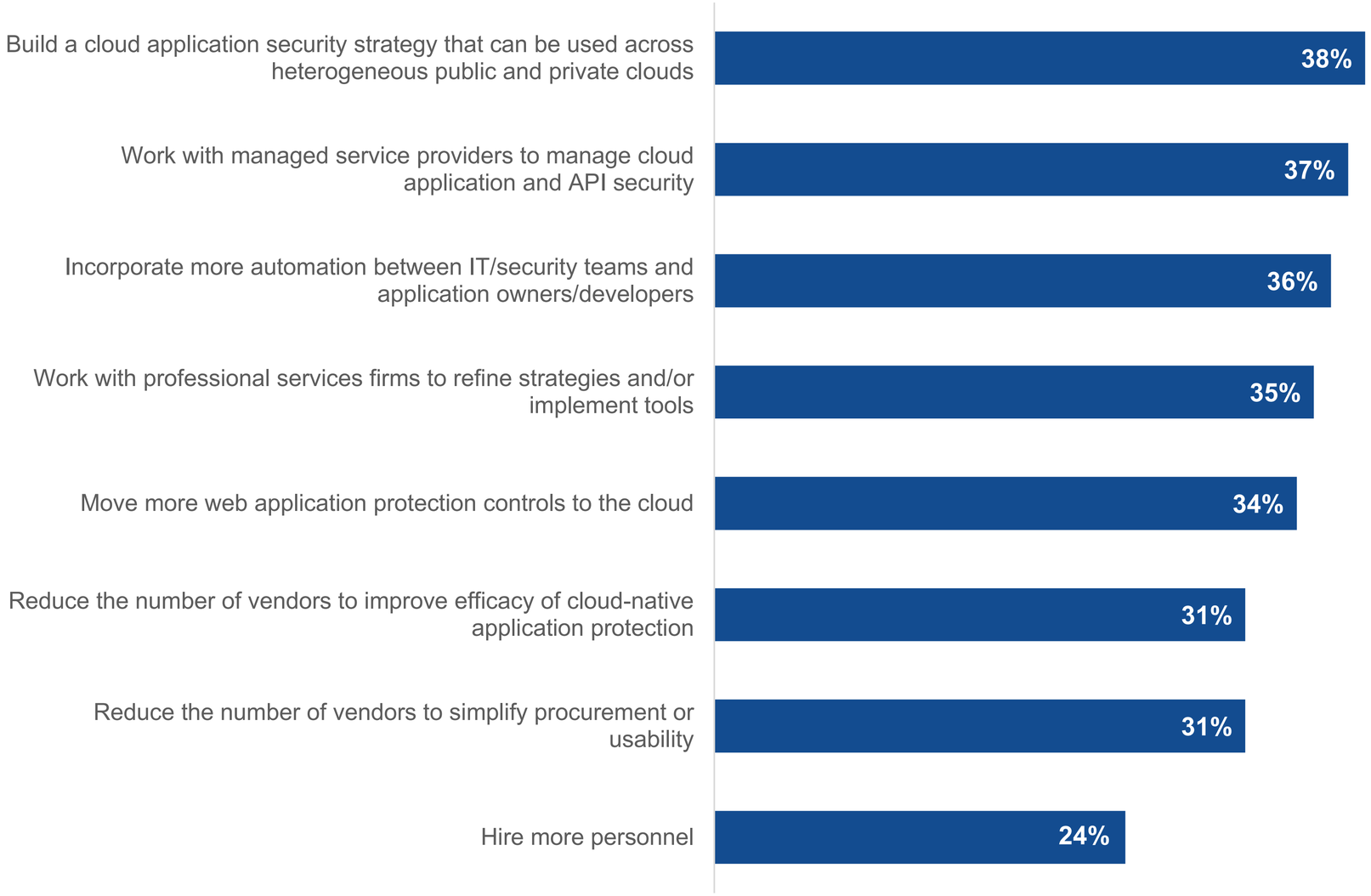
Expected change in API security spending over the next 12-18 months.

Areas of expected increased API security spending.



BACK TO CONTENTS

Plans for optimizing API security with cloud-native security strategies.



The Importance of API Security for Cloud Security Optimization

Organizations should look for API security solutions that fit well into their overall cloud security strategy to support digital transformation.

As a key element of cloud-native development, gaining control of securing rapidly growing APIs will have a high impact on effectively managing security risk to enable the business to scale.

Organizations indicated their strategies for optimizing their programs to scale security with modern application development.

BACK TO CONTENTS

Prisma Cloud Prisma® Cloud is a comprehensive cloud-native security platform with the industry's broadest security and compliance coverage—for applications, data, infrastructure, workloads, APIs, and the entire cloud-native technology stack—throughout the development lifecycle and across hybrid and multi-cloud deployments. Prisma Cloud's integrated approach enables security operations and DevOps teams to stay agile, collaborate effectively, and accelerate cloud-native application development and deployment securely.

Prisma Cloud analyzes more than 10 billion events every month. By proactively detecting security and compliance misconfigurations as well as triggering automated workflow responses, Prisma Cloud helps ensure you continuously and securely meet the demands of your dynamic cloud architectures. To get started with Prisma Cloud, request your free trial today.

LEARN MORE

ABOUT ENTERPRISE STRATEGY GROUP

TechTarget's Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm providing market intelligence, actionable insight, and go-to-market content services to the global technology community.

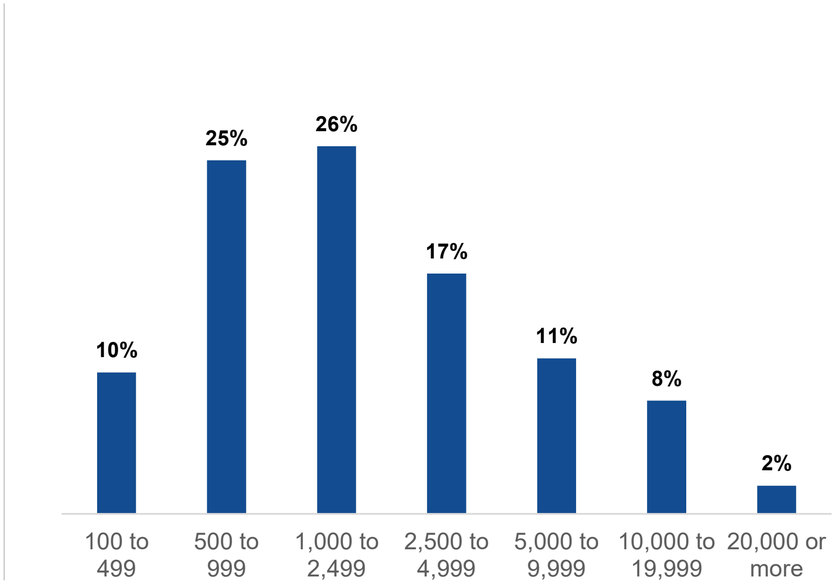
BACK TO CONTENTS

Research Methodology and Demographics

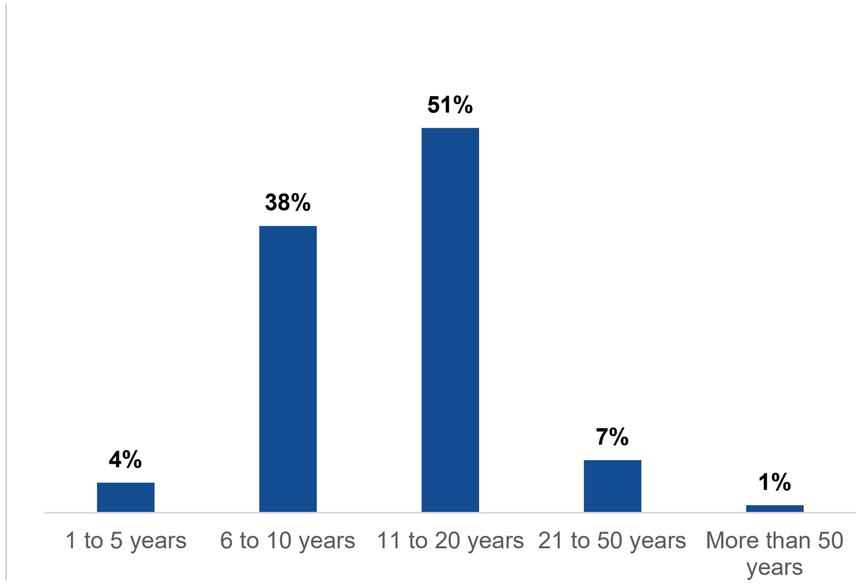
To gather data for this report, TechTarget's Enterprise Strategy Group conducted a comprehensive online survey of IT, cybersecurity, and application development professionals from private- and public-sector organizations in North America between March 9, 2023 and March 14, 2023. To qualify for this survey, respondents were required to be responsible for evaluating or purchasing cloud security technology products and services. All respondents were provided an incentive to complete the survey in the form of cash awards and/or cash equivalents.

After filtering out unqualified respondents, removing duplicate responses, and screening the remaining completed responses (on a number of criteria) for data integrity, we were left with a final total sample of 397 IT, cybersecurity, and application development professionals.

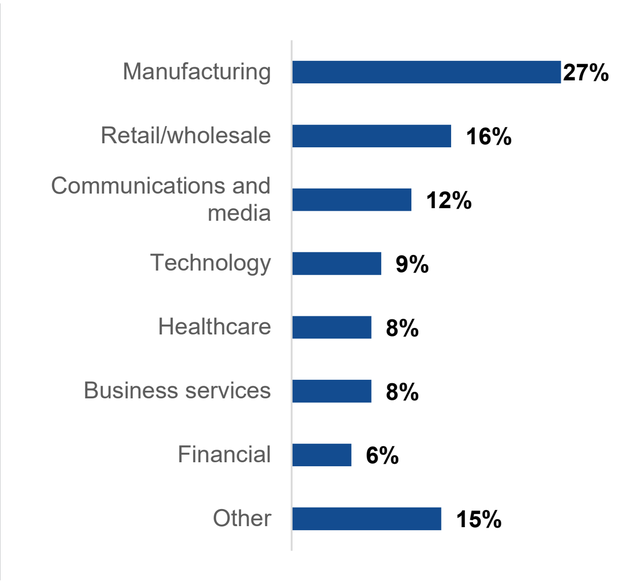
RESPONDENTS BY NUMBER OF EMPLOYEES



RESPONDENTS BY AGE OF ORGANIZATION



RESPONDENTS BY INDUSTRY



BACK TO CONTENTS

Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm providing market intelligence, actionable insight, and go-to-market content services to the global technology community.