Enterprise Strategy Group™ by TechTarget

API Security From Development to Runtime

John Grady | Principal Analyst

Melinda Marks | Practice Director

ENTERPRISE STRATEGY GROUP

OCTOBER 2024

Research Objectives

Every API is a potential attack vector, and adversaries have a variety of avenues to compromise endpoints at their disposal. Attacks on availability, exploitation of weak authentication, and the abuse of shadow APIs are all common and can easily lead to sensitive data loss. The breadth of tools used to secure APIs and issues with collaboration across personas responsible for ensuring secure development, deployment, and operation of APIs may be creating more challenges than organizations realize. Success requires security operations and tools spanning the software development process, from development to runtime, to help teams discover, manage, configure, monitor, and protect APIs. Leaders need to understand the behaviors that forward-thinking organizations have undertaken and how to properly assess solutions to secure APIs from development to runtime.

To gain insights into these trends, TechTarget's Enterprise Strategy Group surveyed 385 IT and cybersecurity professionals in North America (US and Canada) involved with securing their organization's APIs.

This study sought to:

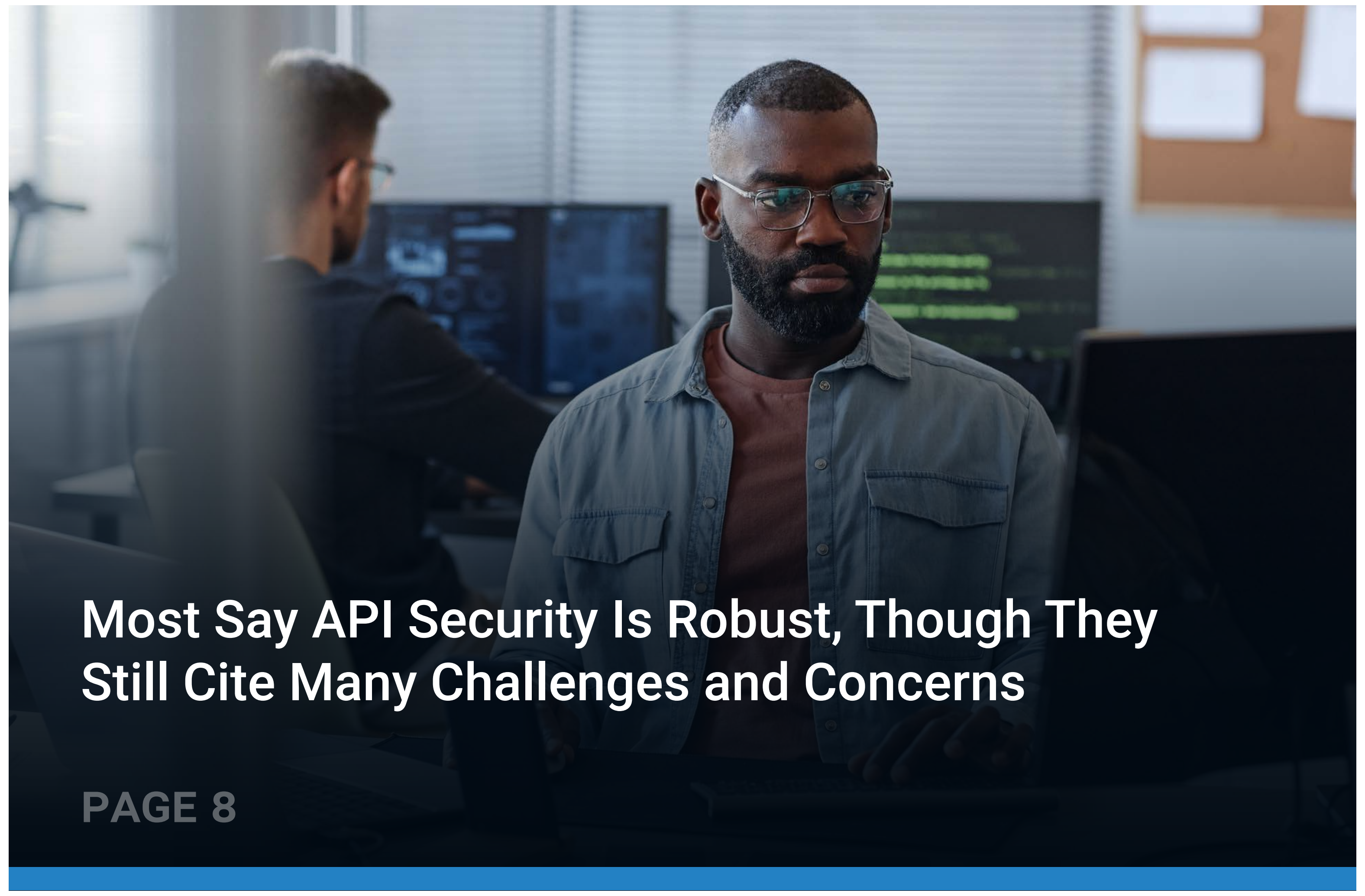
Evaluate usage and proliferation of APIs with modern application development trends.

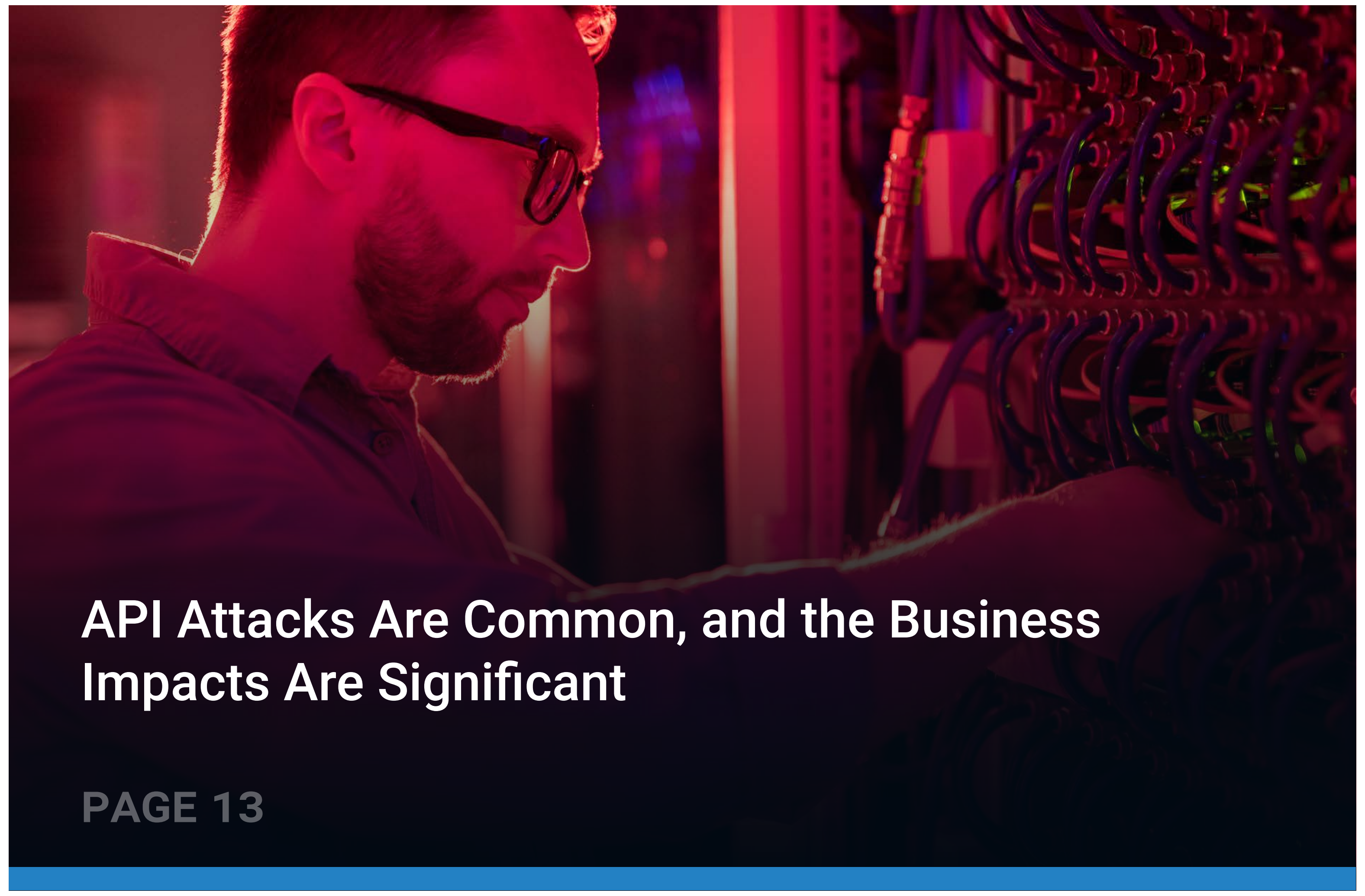
Assess best practices for managing API security risk and protecting applications from attacks.

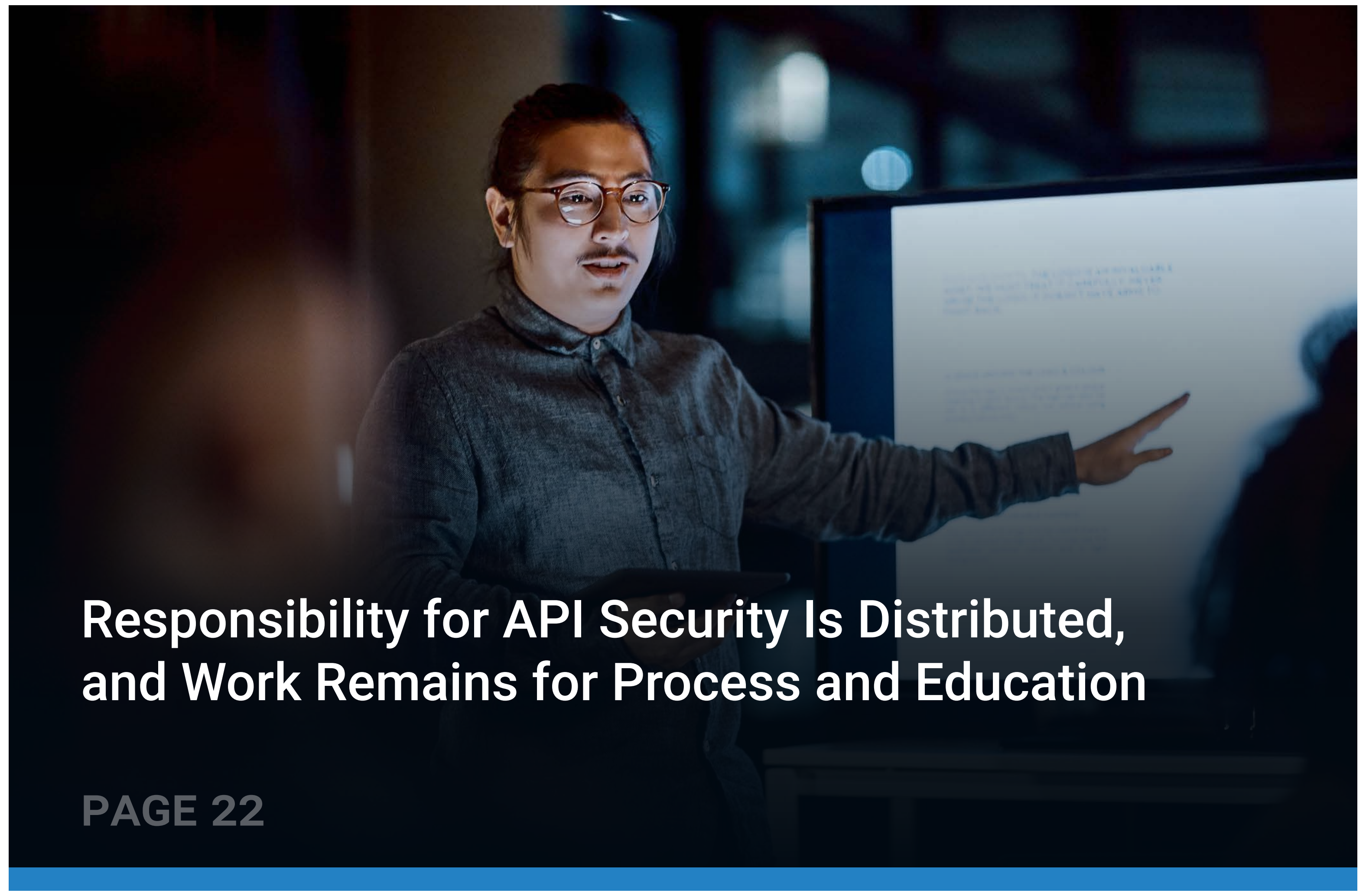
Examine challenges with and concerns over API security.

Understand the roles and personas involved with API security, and awareness of the need for API security across the organization.

Key Findings







BACK TO CONTENTS

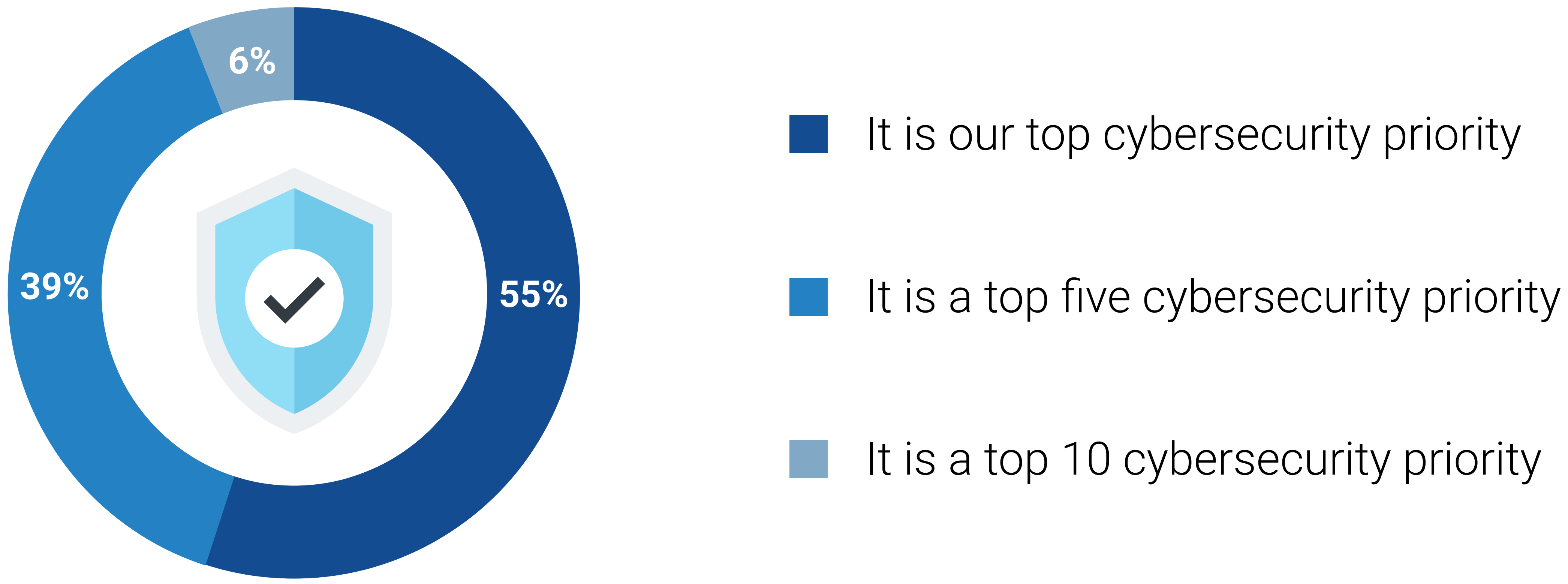
As Cloud-native Development and DevOps Adoption Grow, Application Security Becomes a Priority

A Changing Application Landscape Forces Organizations to Prioritize Security

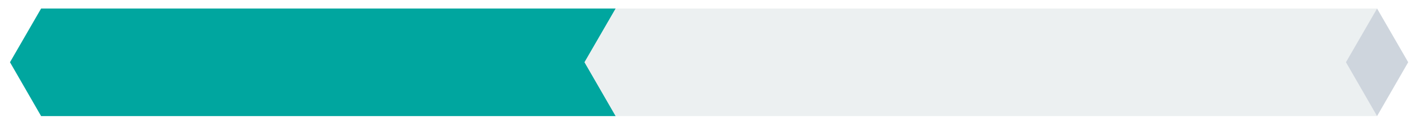
Applications are a critical component in a multitude of internal business processes, and they help connect with customers and drive revenue for many organizations. The use of cloud, cloud-native application architectures, and agile development methodologies have all helped organizations increase the scale and pace at which new applications are developed. More than four in ten organizations (43%) report at least 30% of their production workloads reside in the cloud. Additionally, more than half (52%) of production workloads run on containers or serverless functions, while 54% of organizations have employed DevOps extensively.

Attackers are well aware of these changes as well as the fact that security can at times struggle to keep pace with IT transformation. But the good news is that the vast majority of organizations are emphasizing the security and availability of their applications, with 55% indicating it is their top cybersecurity priority and 39% reporting it is a top five priority.

How do organizations prioritize the security and availability of applications?



43%



of respondents have more than 30% of their **production workloads in the cloud.**

52%

of workloads run on **containers or serverless functions.**

54%

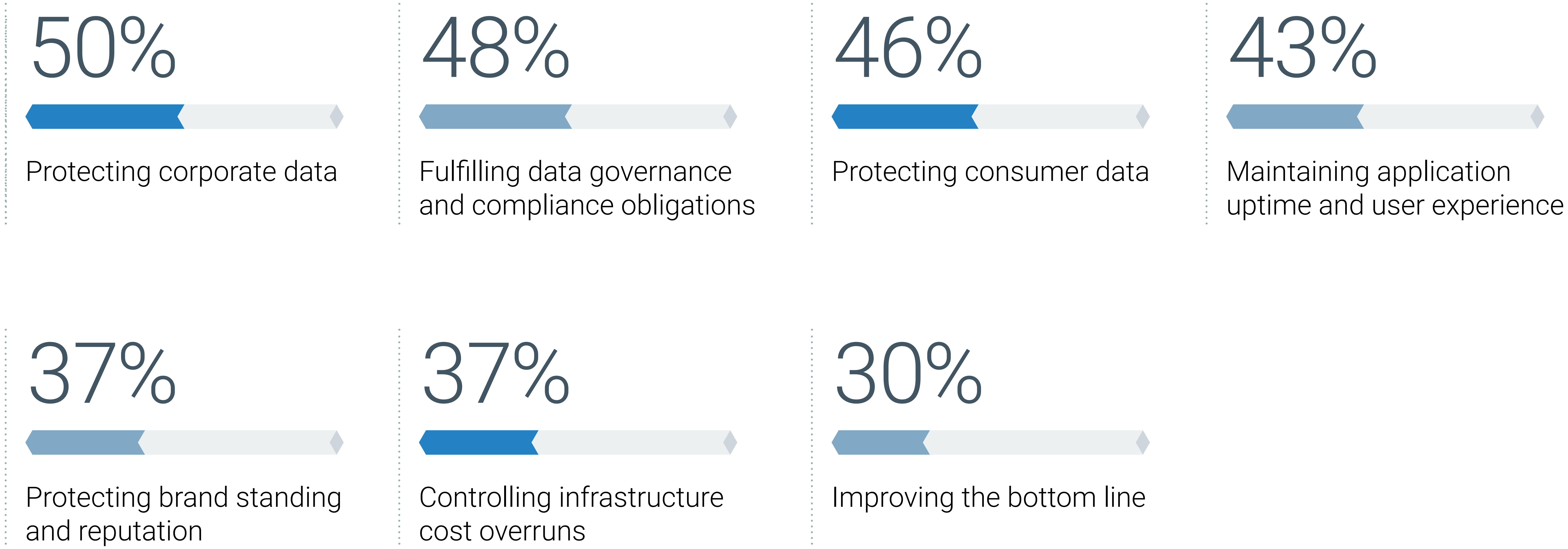
of respondents have employed **DevOps extensively.**

BACK TO CONTENTS

Protecting Data Is Critical

With application security being a clear priority, what specifically do organizations view as the top drivers of their programs? The somewhat surprising answer is protecting data. Half of organizations cited protecting corporate data while 46% cited protecting consumer data. Additionally, 48% pointed to fulfilling data governance and compliance obligations, which can also be tied to data protection. This is not to say that maintaining application uptime and user experience (43%) was ignored, but it appears clear that the constant stream of breaches reported in the news and subsequent impacts to the companies affected are influencing how organizations think about securing their applications.

Critical drivers of application security programs.



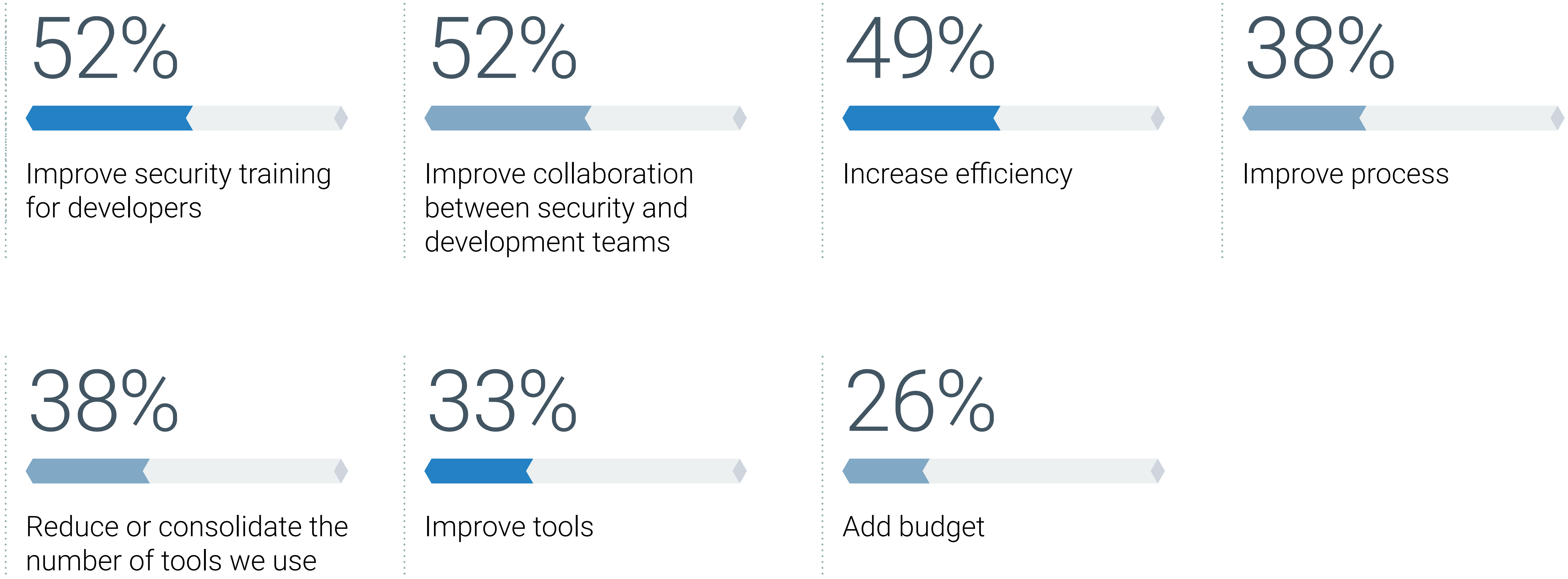
BACK TO CONTENTS

Training and Collaboration Are Key to Application Security Improvement

At the same time, many realize there is room to improve when it comes to application security. The most common actions cited on this front are improving security training for developers (52%) and improving collaboration between security and development teams (52%). In many ways, this reflects the growing focus on secure by design and the reality that responsibility for security is now distributed across the organization. Increasing efficiency (49%) and improving processes (38%) were also cited frequently.

Focusing on either tool consolidation (38%) or improvement (33%) and additional budget (26%) were mentioned, but for most are secondary to better utilizing and optimizing the elements that are already in place.

Most important actions to improve application security.



52%
Improve security training for developers

52%
Improve collaboration between security and development teams

49%
Increase efficiency

38%
Improve process

38%
Reduce or consolidate the number of tools we use

33%
Improve tools

26%
Add budget

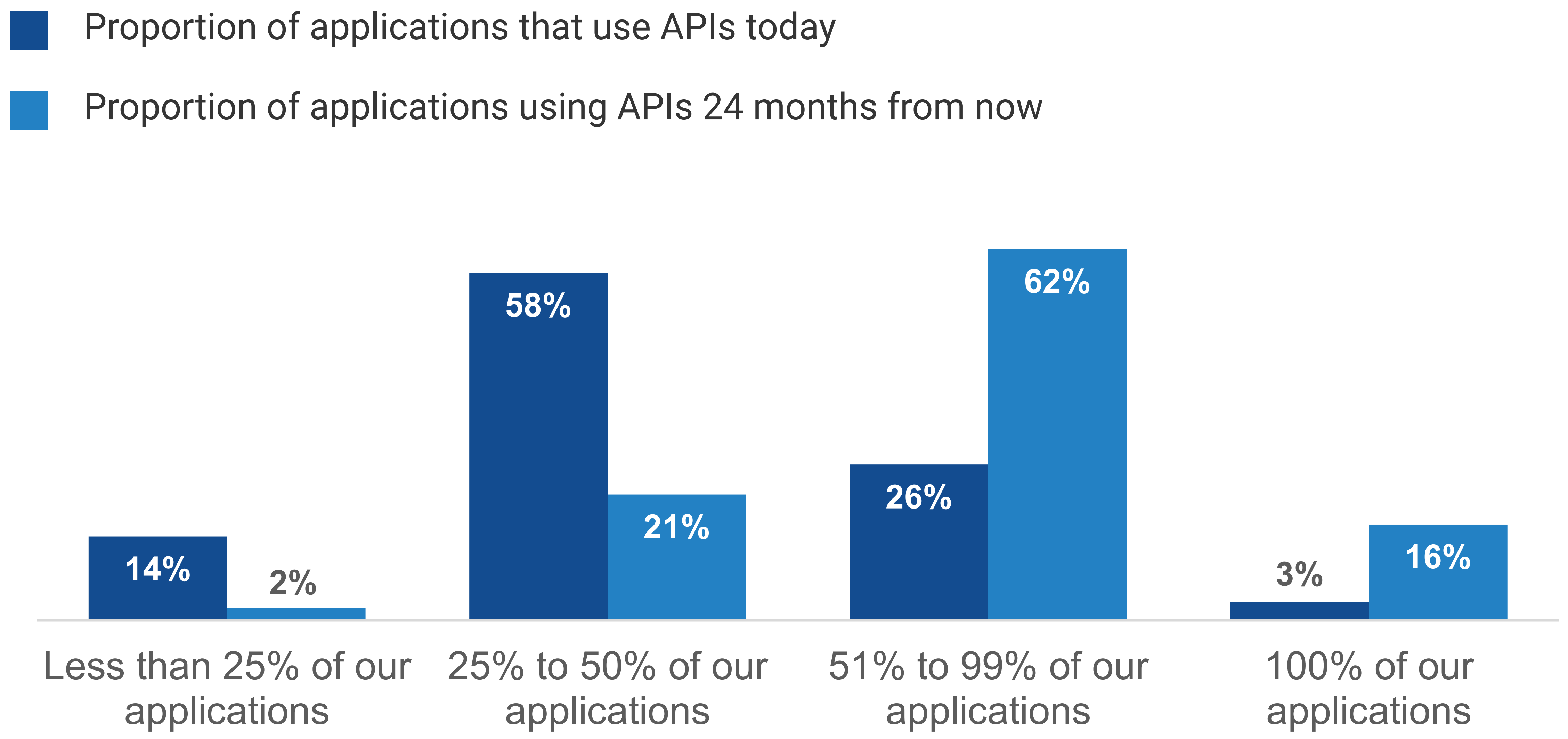
BACK TO CONTENTS

Most Say API Security Is Robust, Though They Still Cite Many Challenges and Concerns

API Proliferation Continues

As part of the evolution of applications, the usage of APIs has grown and is expected to increase significantly. While 29% of organizations report that over half of their applications use APIs today, that is expected to rise to 78% of organizations 24 months from now. With many of these APIs exposed to the internet and connected to other applications, they make up a significant percentage (35%) of cloud and internet traffic today, which will only grow as usage increases. This breadth coupled with the variety of API protocols in use, such as WebSocket for real-time chat and communications functionality, GraphQL for data, and gRPC for microservices, as well as REST and SOAP complicate the situation from a security perspective.

Current API usage.



The API landscape *on average*.

35% of APIs are **exposed** to the internet.

33% of APIs are **connected** to other apps.

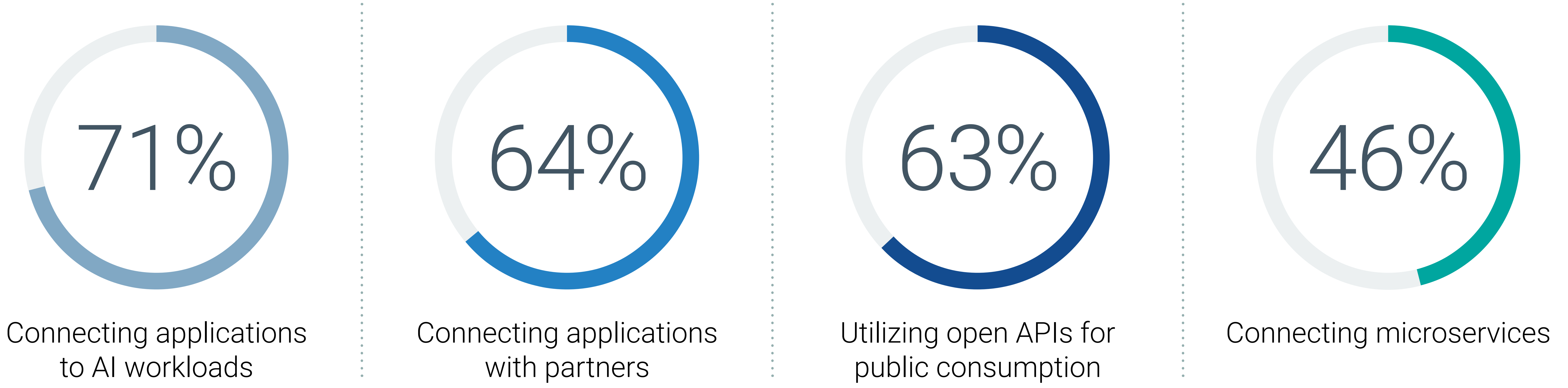
35% of cloud and internet traffic is **API traffic**.

57 APIs per **application**.

Use of APIs for External Connections Highlights Security Criticality

The interconnectedness across trust boundaries, which APIs facilitate, will only continue to grow. Connecting applications with partners (64%) and using open APIs for public consumption (63%) were frequently cited. However, the most common response (cited by 71% of organizations) is using APIs to connect applications to AI workloads. While this may be high, it certainly shows the direction in which application environments are quickly moving. AI is a top priority for nearly every CIO, and security teams must work in lock step to ensure sensitive data is not exposed.

How APIs are used.



> “AI is a **top priority for nearly every CIO,** and security teams must work in lock step to ensure sensitive data is not exposed.”

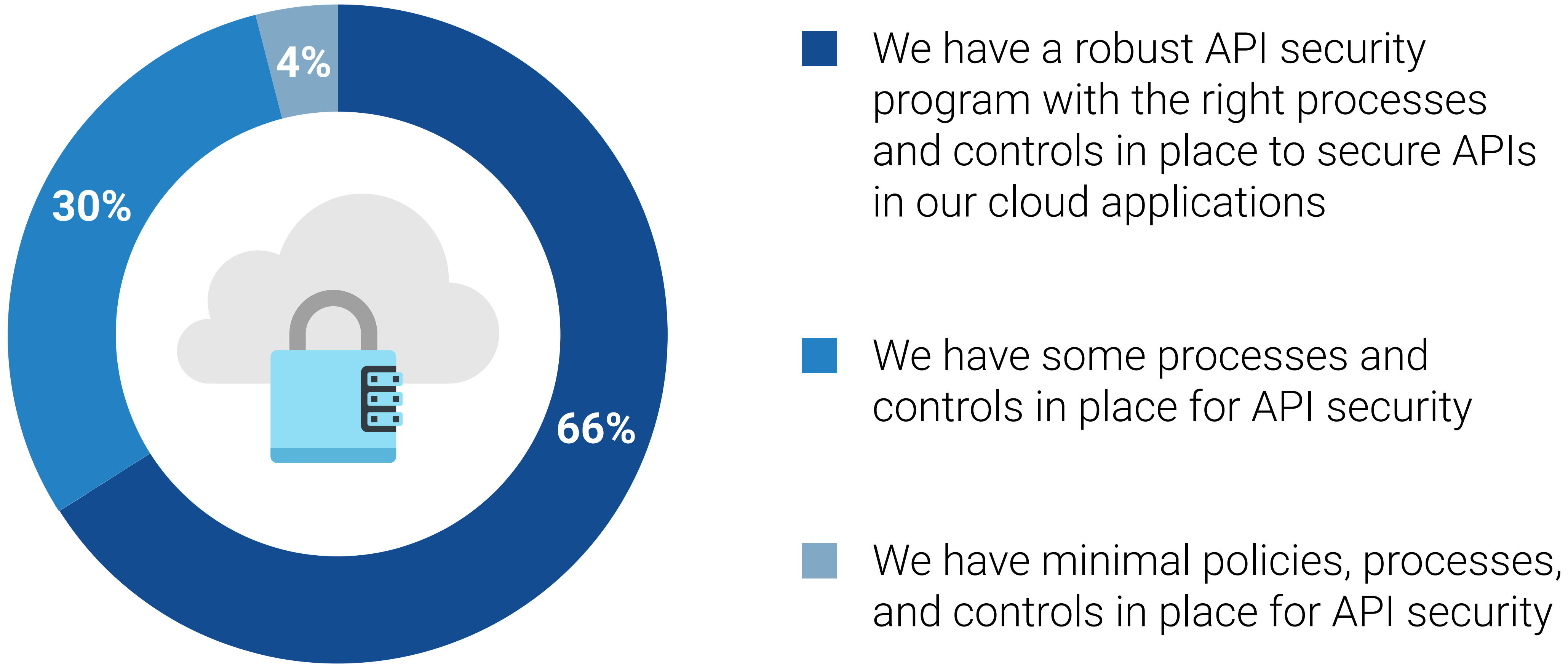
BACK TO CONTENTS

Most Say They Have Robust API Security Processes in Place, yet They Cite a Variety of Challenges

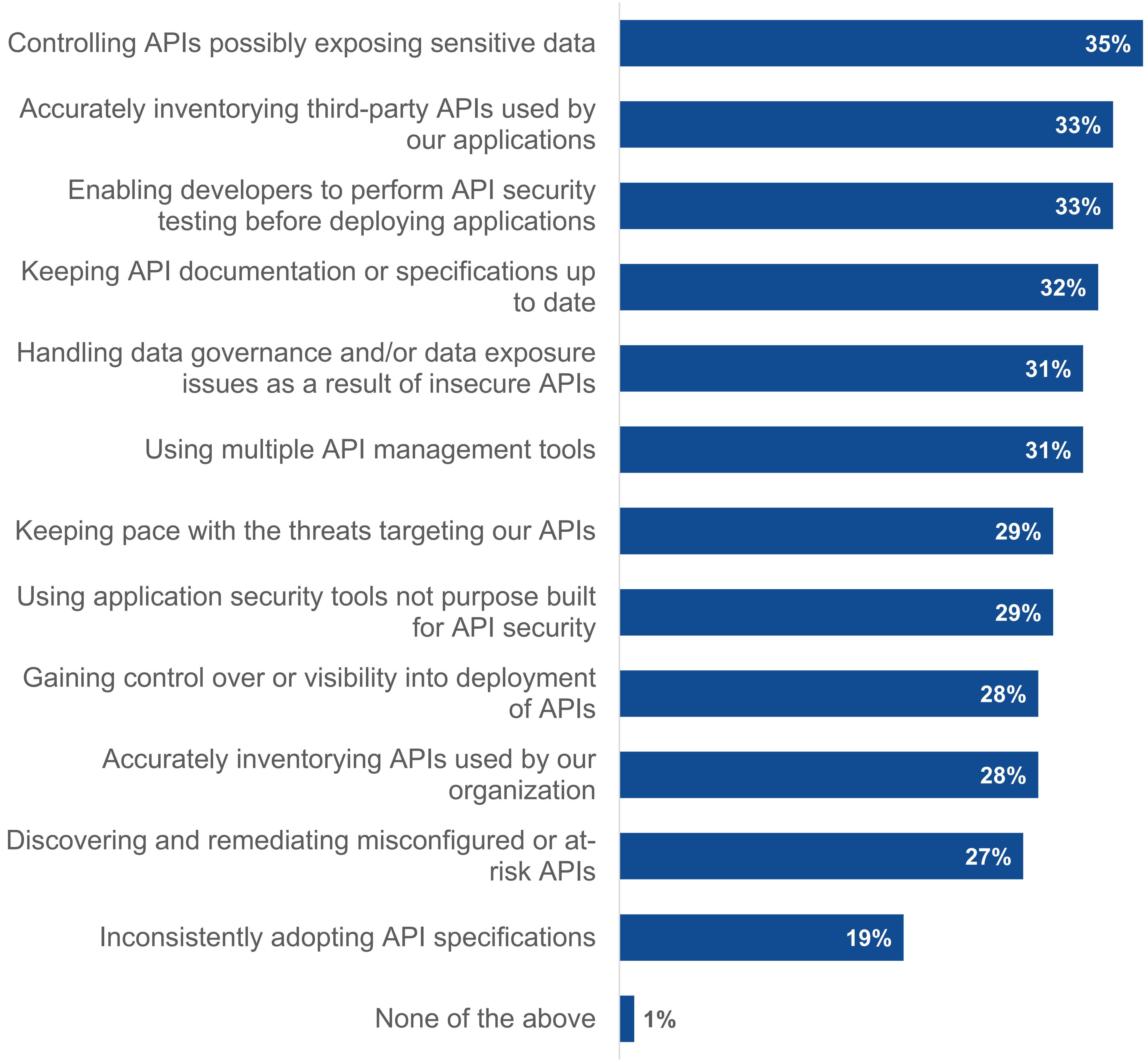
Despite the complexity, a majority (66%) say they have a robust API security program with the right processes and controls in place to secure APIs in their cloud applications. While this may seem like a positive outcome, it belies the security challenges they face. On average, respondents cited more than 3.5 challenges.

Among the most common were controlling APIs exposing sensitive data (35%), accurately inventorying third-party APIs used by applications (33%), enabling developers to perform API security testing before deploying applications (33%), and keeping API documentation or specifications up to date (32%). Keeping pace with the threats targeting APIs (29%) was mentioned slightly less frequently, showing organizations are focused on proactive API security and avoiding missteps rather than reactively responding to threats.

Rating current API security capabilities.



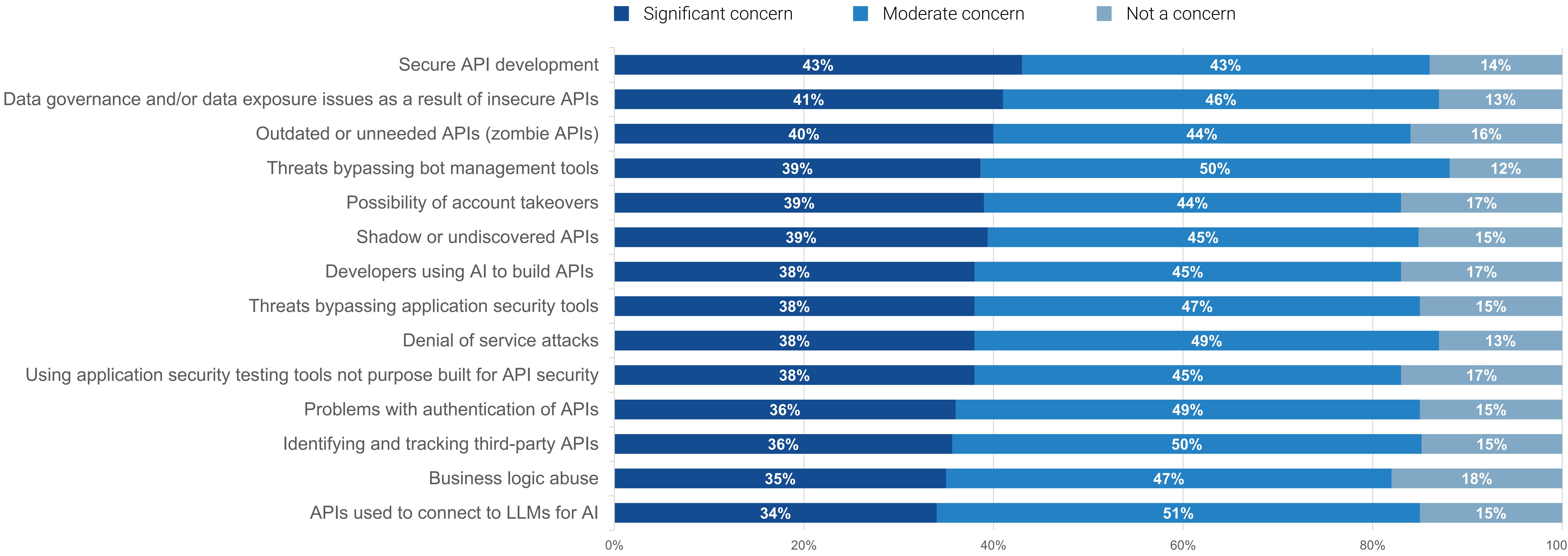
API security challenges.



Most Organizations Have Significant Concerns Across Many Areas

Respondents also expressed high amounts of concern across all API security areas, illustrating the need for comprehensive capabilities to address them. The concerns range from fundamental areas, such as authentication of APIs, to newer territories, like the need to support APIs to connect to LLMs.

API security concerns.



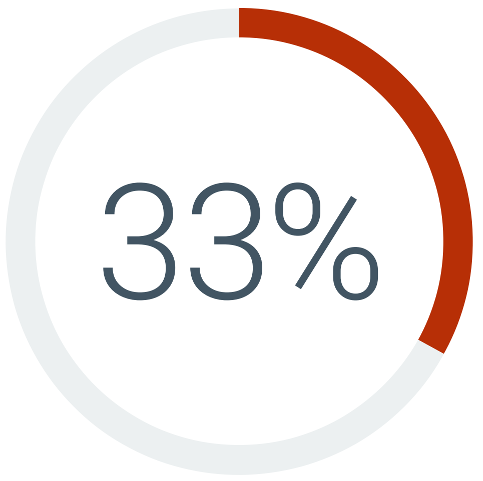
API Attacks Are Common, and the Business Impacts Are Significant

Attacks Are Common and Varied

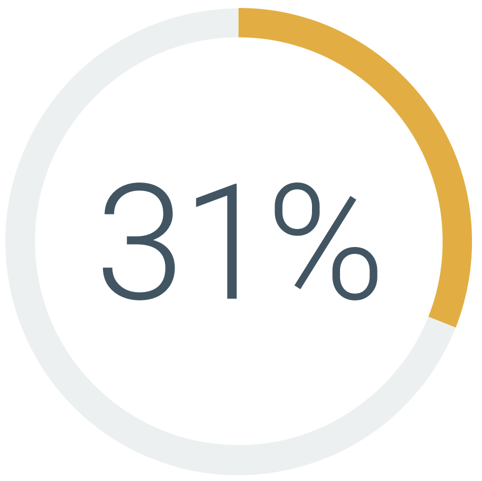
Despite the focus on security, many are facing attacks or incidents related to their APIs. Specifically, 31% said they had suffered one attack or security incident in the last 12 months, while 33% reported multiple.

These attacks and incidents included injection attacks (39%), denial of service attacks (35%), data exposure (34%), content scraping (30%), and ransomware (28%). This variety makes security that much more difficult, as finding exposed data requires different capabilities than protecting against availability or injection attacks.

Prevalence of API attacks.

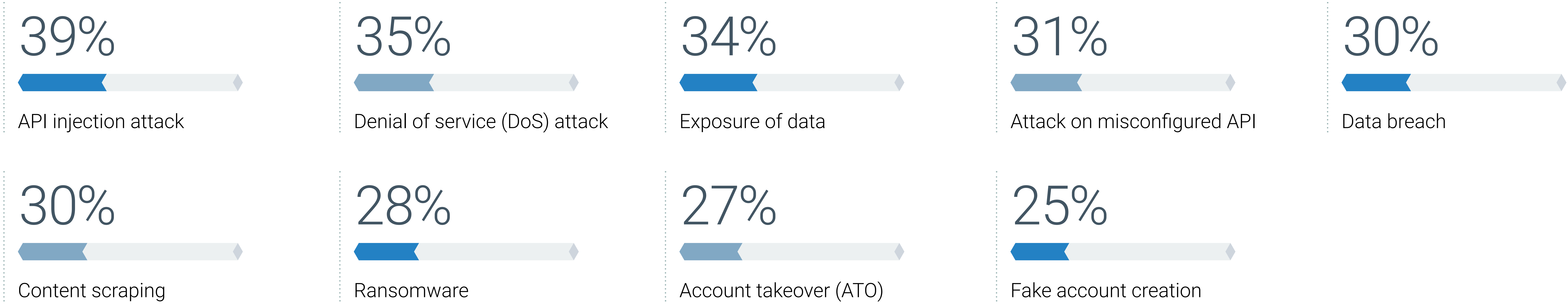


We have experienced **multiple API-related security attacks** in the last 12 months



We have experienced **an API-related security attack** in the last 12 months

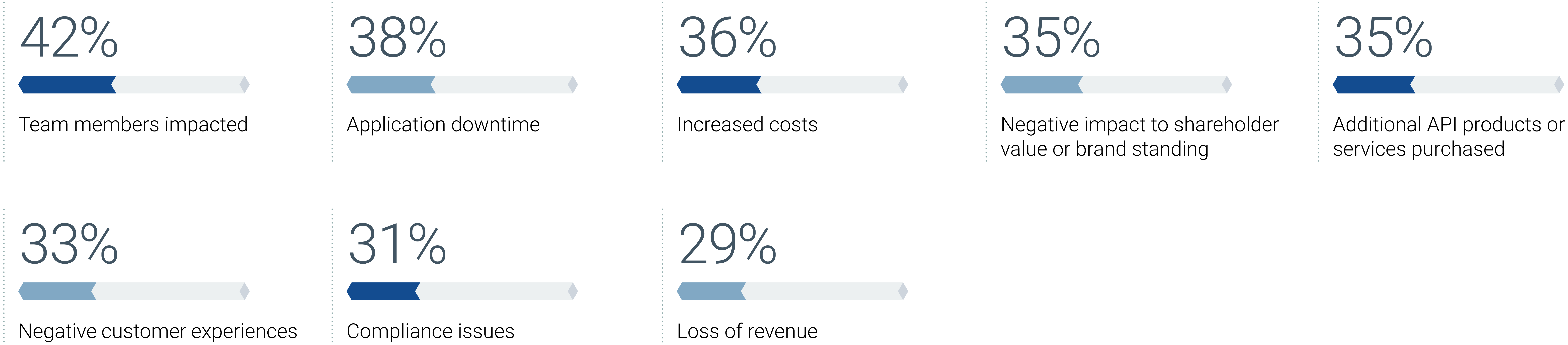
Types of API attacks.



Impacts From Attacks Can Be Significant

Organizations report multiple negative impacts stemming from successful attacks. At the top of the list, 42% say team members were impacted. This can range from requiring additional training to a change in responsibilities or even termination. Application downtime was cited by 38% of organizations. Relatedly, 35% noted negative impact to shareholder value or brand standing, while 33% cited negative customer experiences. Whether applications become unavailable or bad press results from successful attacks, these impacts can be difficult and time consuming to overcome. Finally, 29% reported a loss of revenue following an attack, which highlights why securing API usage is such a priority.

Impacts from API attacks.

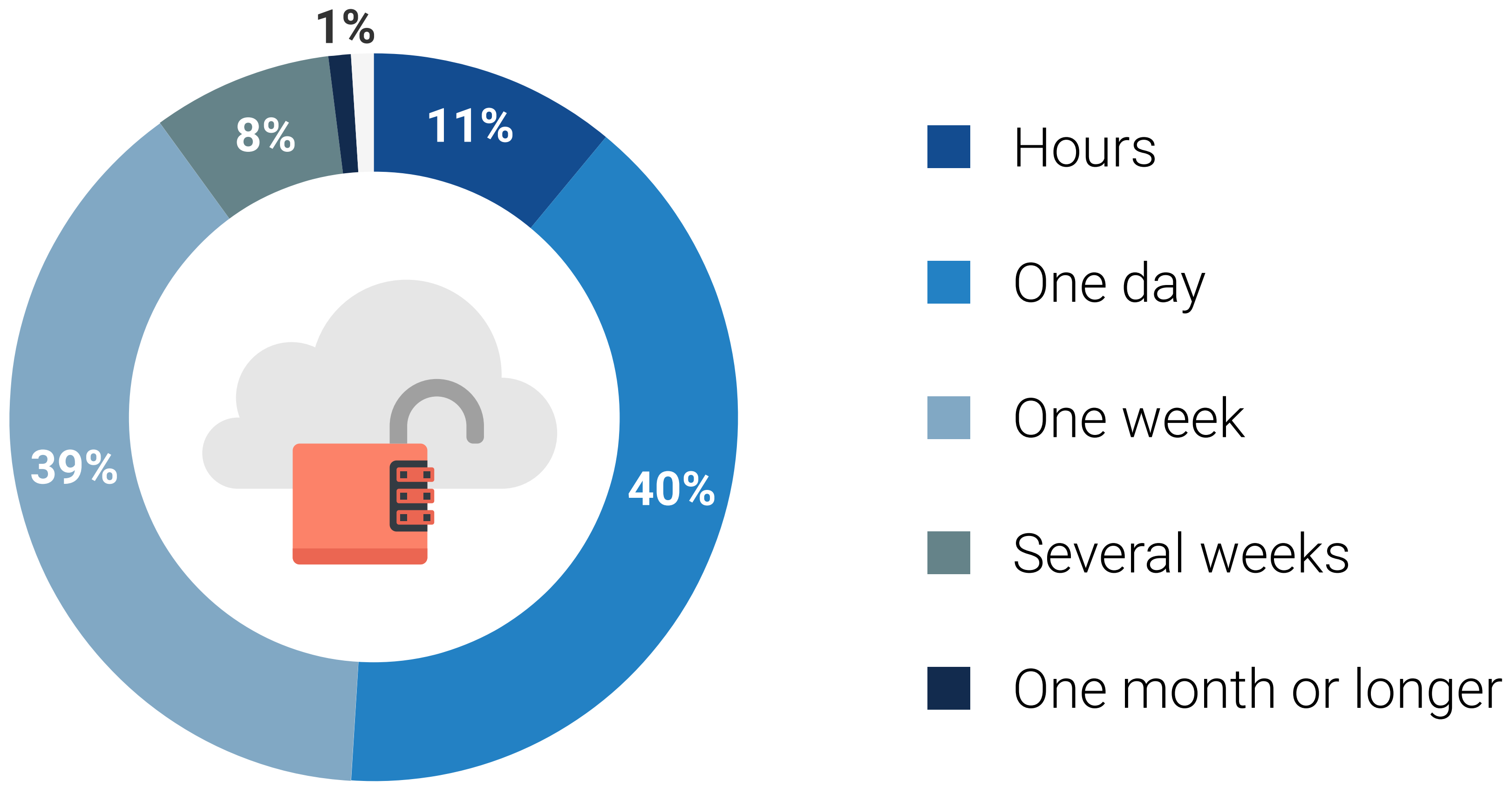


Vulnerability Concerns

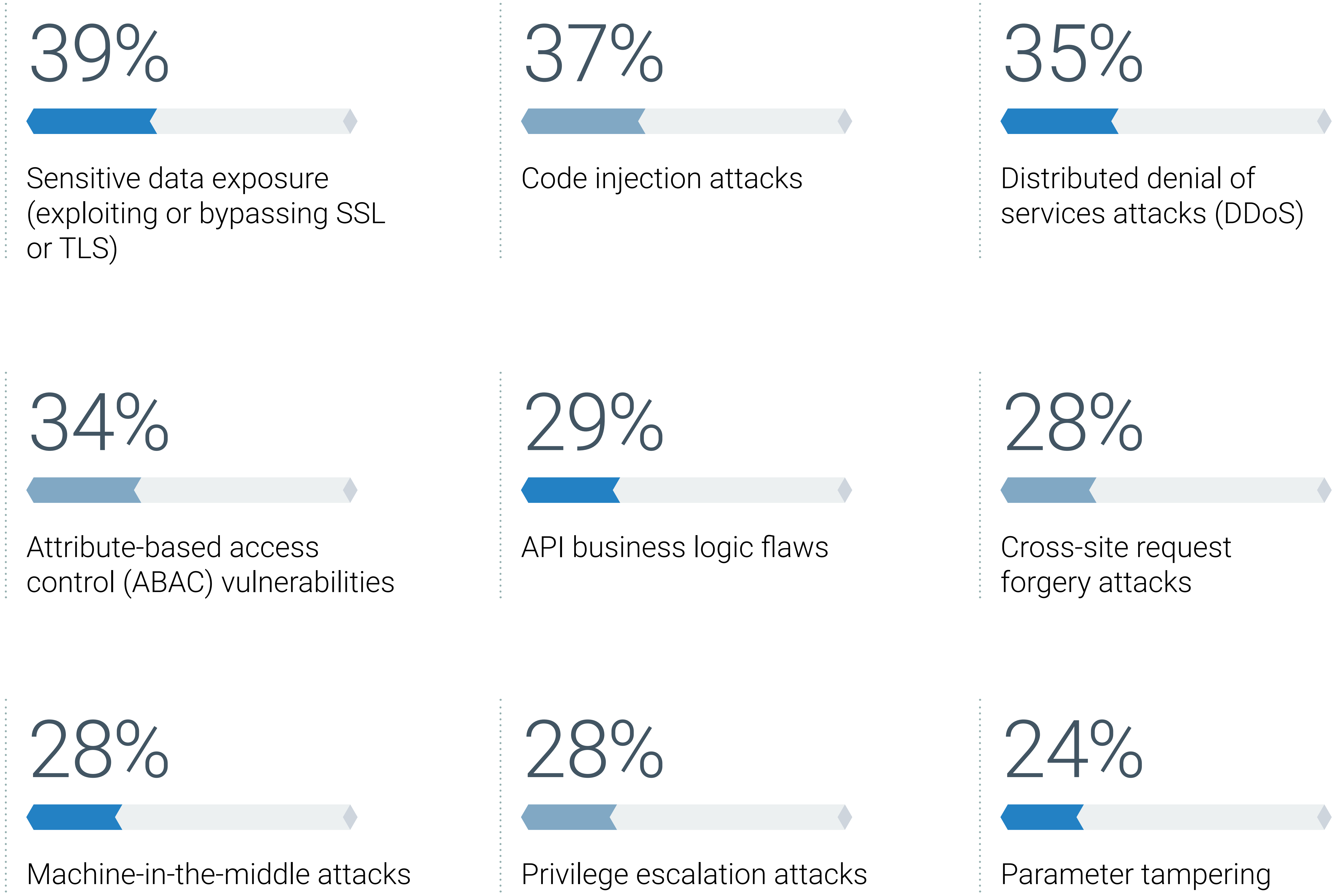
Many of the vulnerabilities respondents most commonly identified as concerning align with the attacks that were reported. Data exposure (39%), injection attacks (37%), and DDoS attacks (35%) were at the top of the list. More API-specific vulnerabilities such as attributed-based access control (34%), business logic flaws (29%), and parameter tampering (24%) were also common.

Unfortunately, the vast majority say that remediating these vulnerabilities takes one day or more. Moreover, nearly half say remediation takes one week or longer. With attackers moving as fast as they do, addressing issues quickly becomes critical.

Time required to remediate an API vulnerability.



API vulnerabilities of greatest concern.



39%

Sensitive data exposure (exploiting or bypassing SSL or TLS)

37%

Code injection attacks

35%

Distributed denial of services attacks (DDoS)

34%

Attribute-based access control (ABAC) vulnerabilities

29%

API business logic flaws

28%

Cross-site request forgery attacks

28%

Machine-in-the-middle attacks

28%

Privilege escalation attacks

24%

Parameter tampering

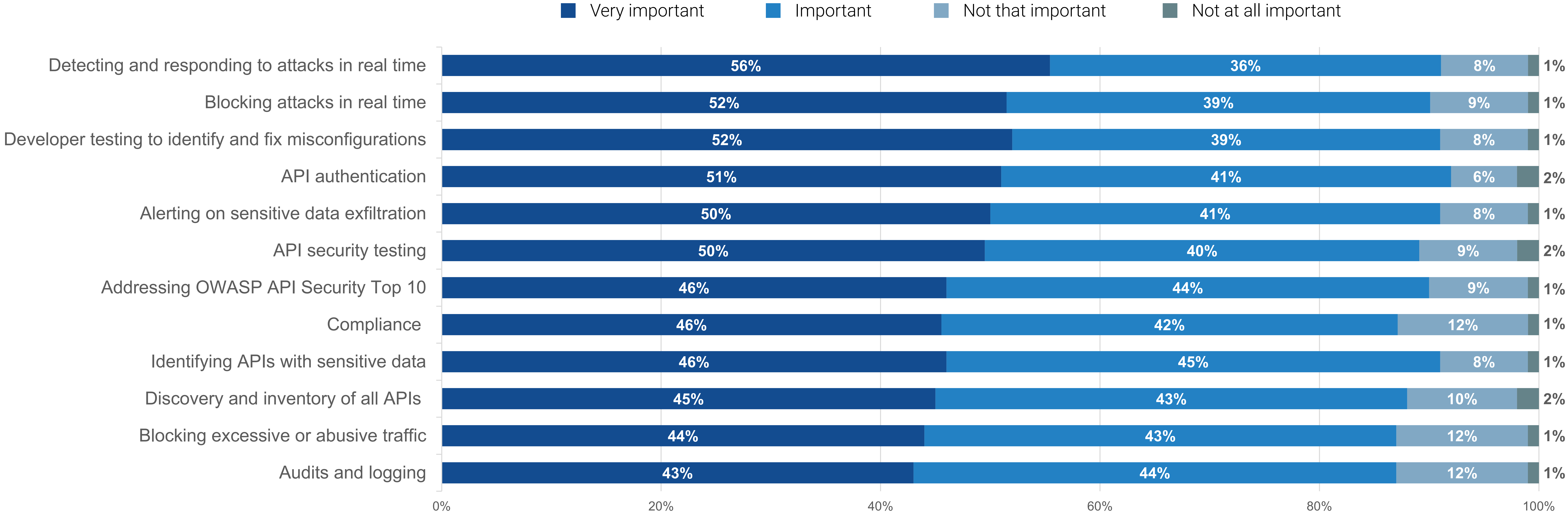
BACK TO CONTENTS

API Security Requires a Wide Range of Capabilities

API Security Requires a Range of Capabilities

There is near uniform agreement that all API security capabilities are important, with roughly nine out of ten respondents indicating each is very important or important. This also spans pre-deployment, threat prevention, and management use cases. In terms of criticality, attack detection and response rated at the top of the list, with more than half (56%) rating it as very important. Developer testing to identify and fix misconfigurations was also rated highly, with 52% saying it is very important. Discovery and inventorying of all APIs was rated very important by 45%. Conversely, while auditing and logging was at the bottom of the list, 43% of respondents still rated it as very important.

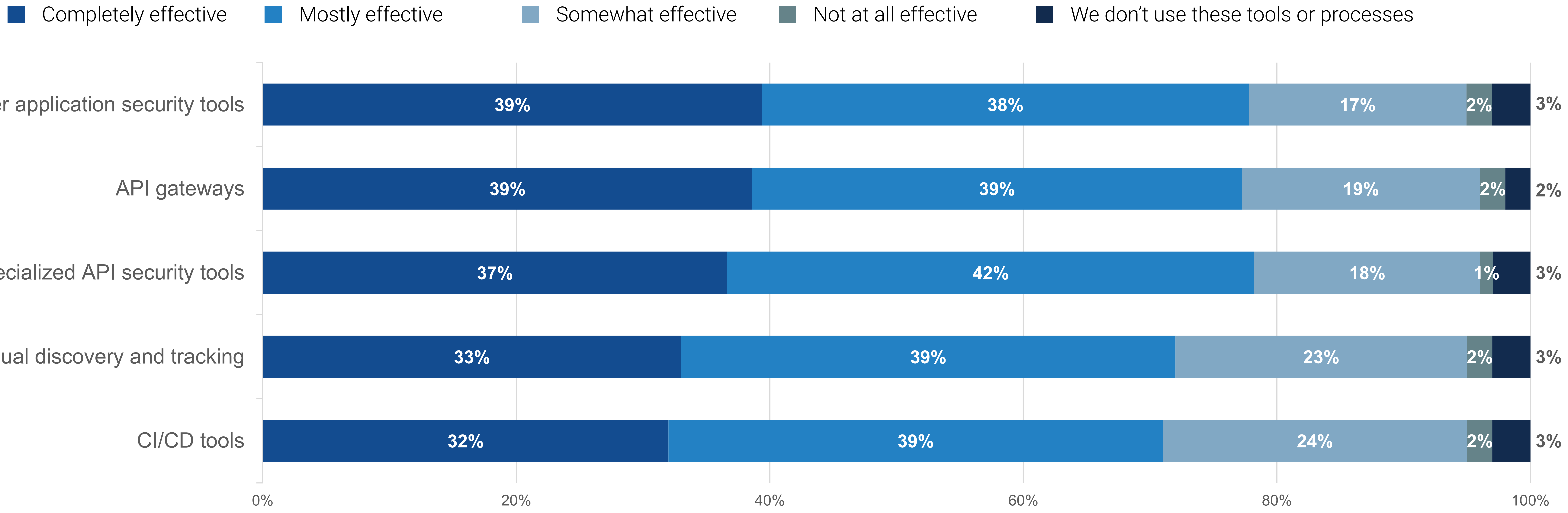
Importance of API security capabilities.



Effectiveness of API Discovery and Tracking Tools

Inventory and discovery of APIs are foundational to building and running secure applications. Despite rating some tools as completely effective, organizations typically utilize multiple tools, including security and API gateway tools, as well as manual tracking to try to ensure they have comprehensive visibility of APIs.

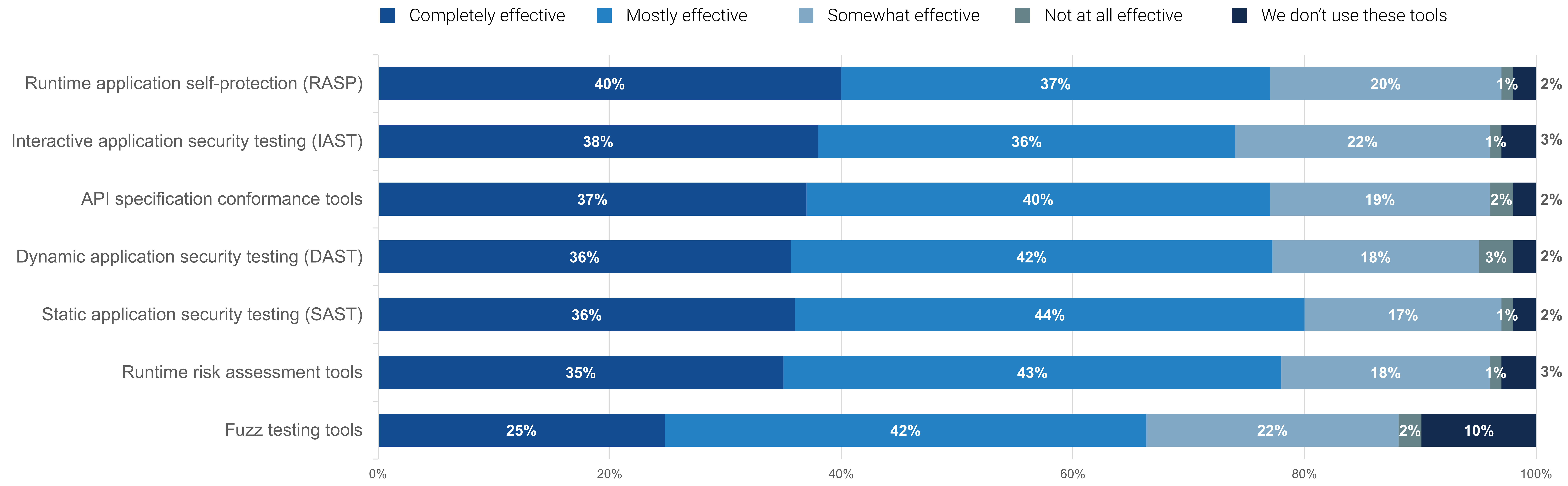
Effectiveness of API discovery and tracking tools.



Effectiveness of Tools to Discover and Remediate API Coding Errors

Organizations are also using multiple application security tools to remediate coding issues. These include testing tools, runtime application self-protection (RASP), and API specification conformance tools.

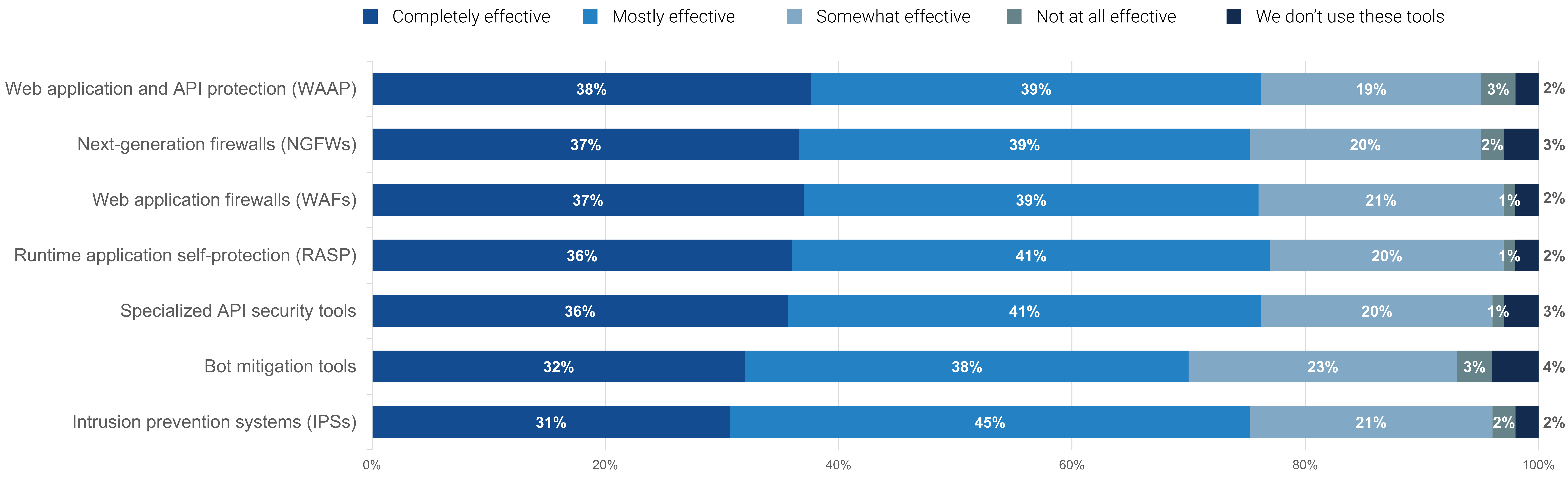
Effectiveness of tools to discover and remediate API coding errors.



Effectiveness of Tools to Stop or Block Attacks on APIs

Organizations also typically use multiple tools to stop or block attacks on APIs. In terms of efficacy, the majority rated tools such as web application and API protection (WAAP) and next-generation firewalls (NGFWs) the highest for being completely effective. RASP and specialized API security tools also rated highly for being mostly or completely effective.

Effectiveness of tools to stop or block attacks on APIs.



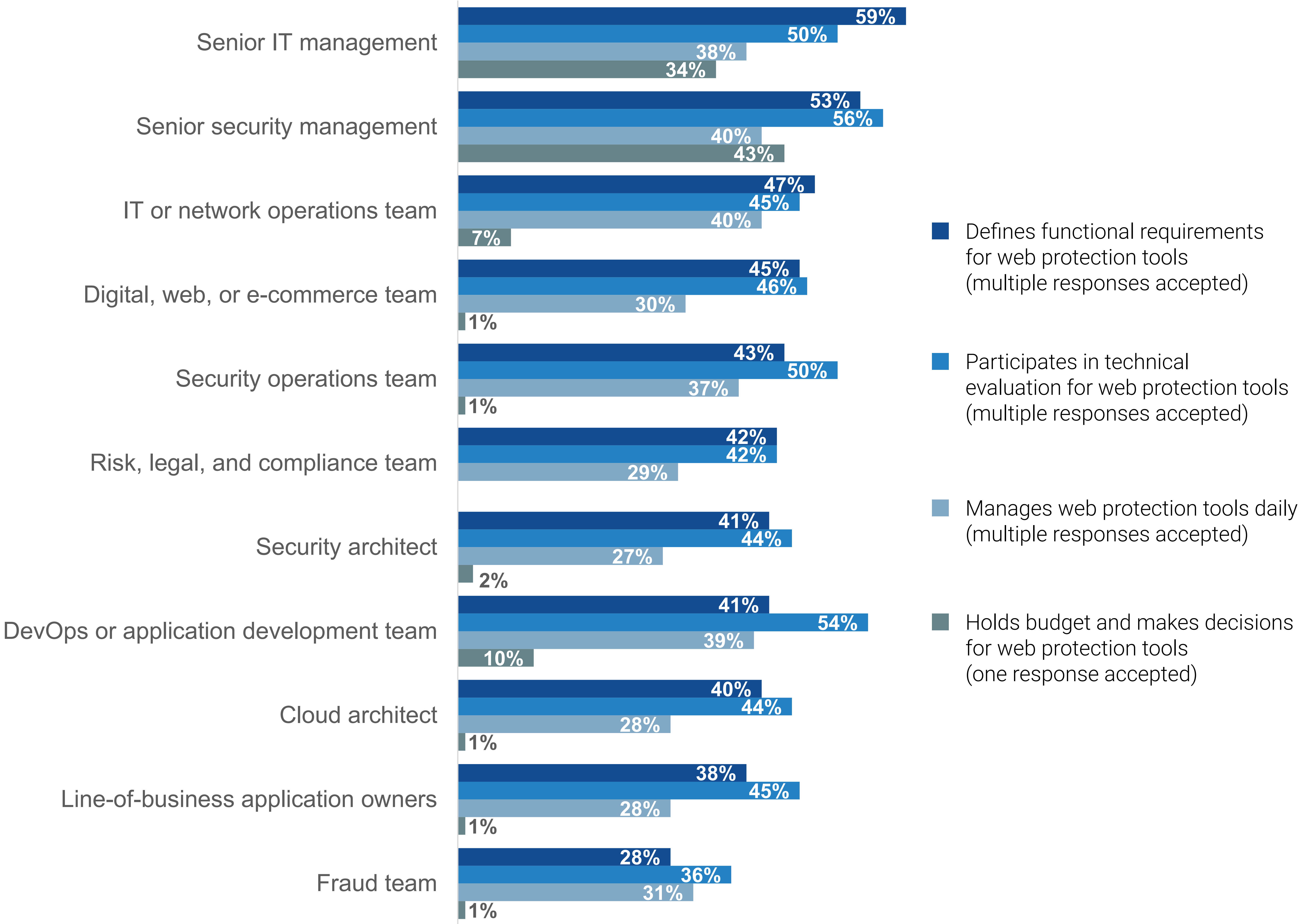
Responsibility for API Security Is Distributed, and Work Remains for Process and Education

API Security Is a Team Sport

A variety of roles and personas have control or influence over API security decisions. Senior management across both IT and security is very involved throughout the process, from defining functional requirements and evaluating technical aspects of tools to making the final decision.

However, roles including IT and network operations teams; security operations; digital, web, or ecommerce teams; and DevOps or application development teams are highly involved as well. This means organizations must focus on cross-functional collaboration and breaking down traditional silos to ensure API security programs are successful and effective.

Individuals involved with API security.



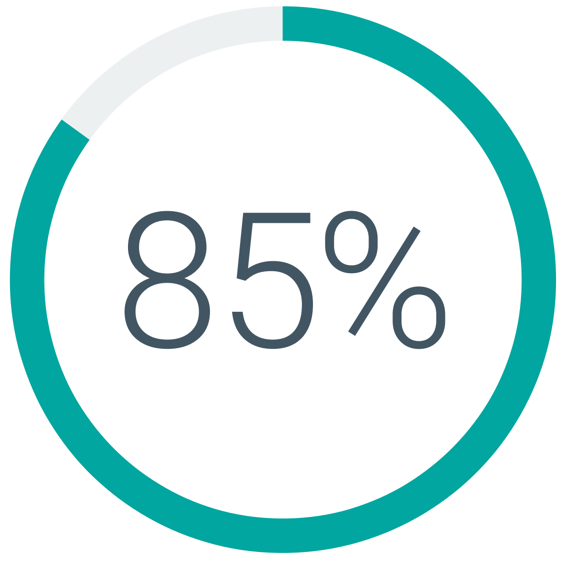
BACK TO CONTENTS

Timing, Awareness, and Training Are Moving in the Right Direction

Further highlighting the collaborative efforts around API security, half of respondents say security teams become involved *before* APIs are published. Unfortunately, that leaves 41% involving security teams as APIs are published, and 10% doing so only once they are live and in production. So, while this data represents a positive finding, there is room for improvement.

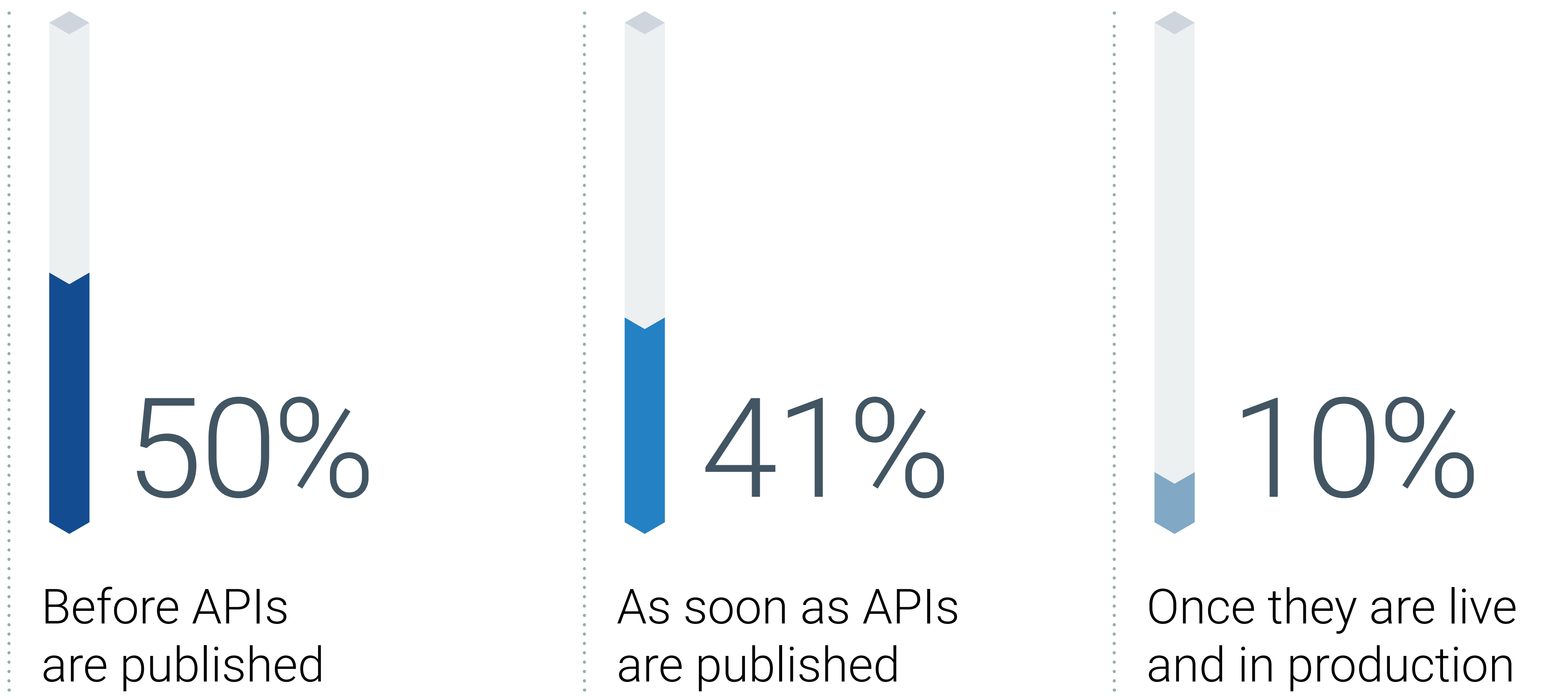
Nearly nine out of ten (85%) say their development teams receive formal API security training, which also shows the emphasis organizations are placing on this education. However, currently only 59% say their developers have a high level of knowledge of API risks, with 33% reporting a good level of knowledge. Over time, training should continue to raise these numbers and help a greater percentage of developers fully understand the security risks around APIs.

Formal API security training for development teams.

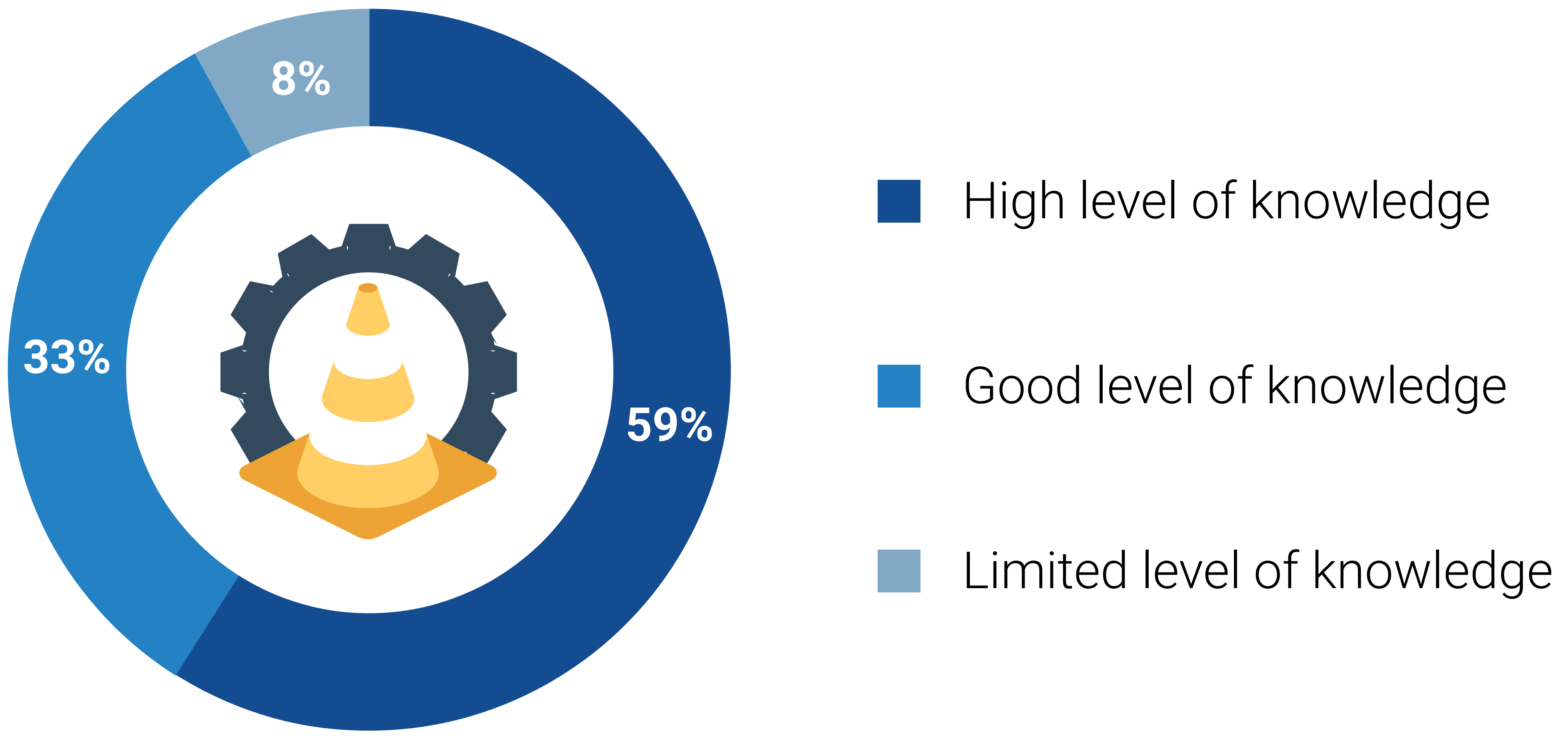


We provide **formal API security training** to our development teams

Timing of security involvement in publishing of APIs.



Developer awareness of API security risks.



BACK TO CONTENTS

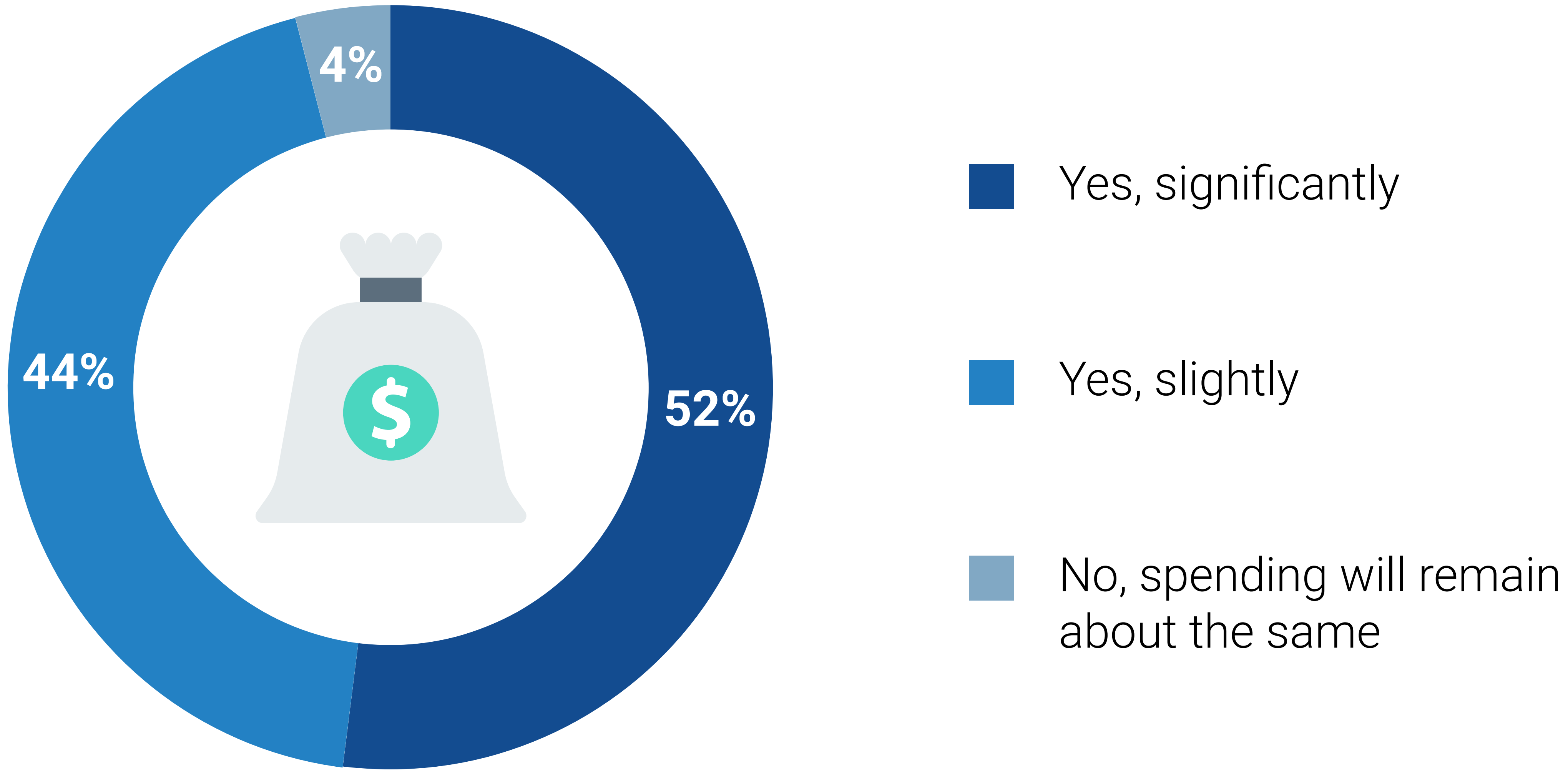
Budgets Appear Strong, but Many Will Focus on Process and Strategy

API Security Spending Plans

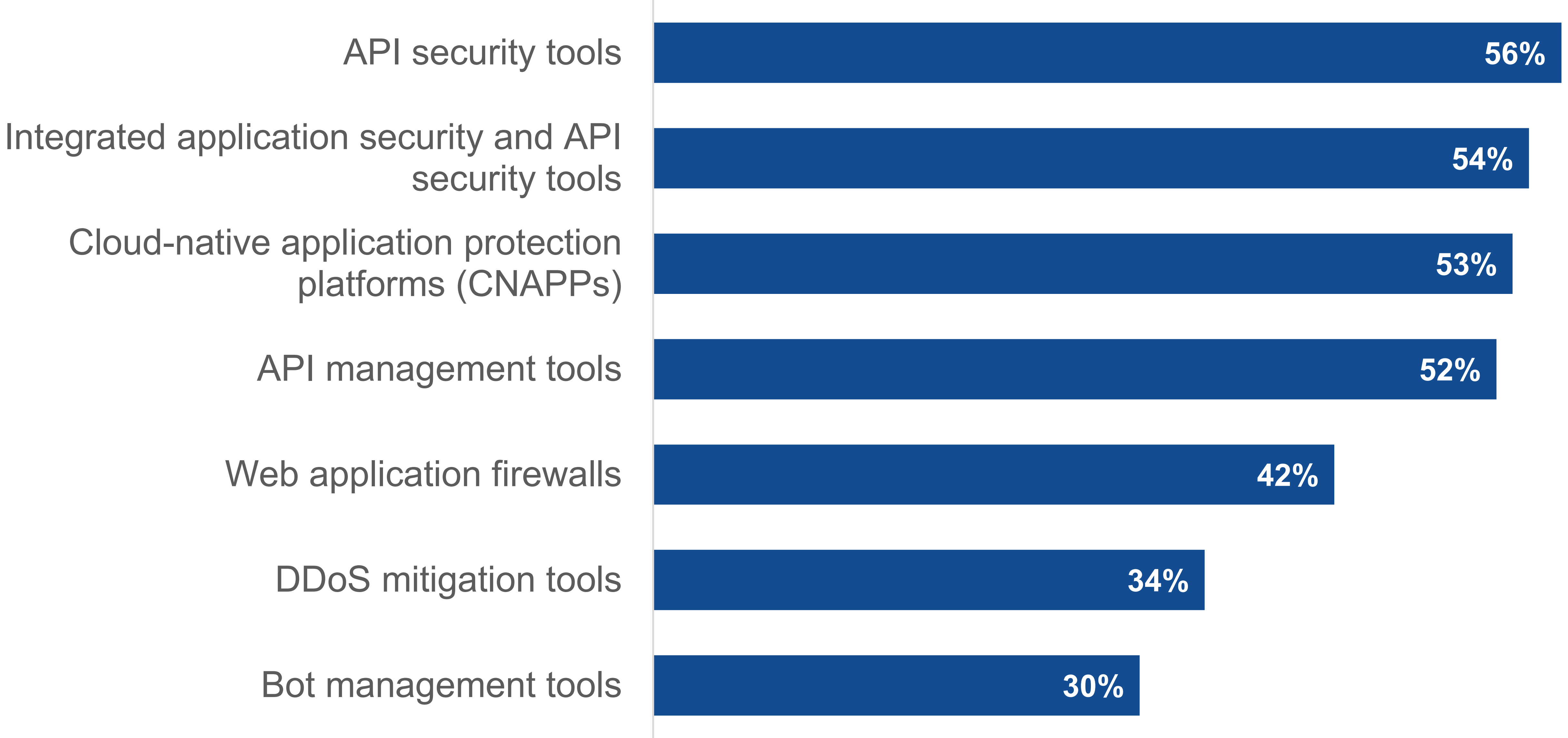
Planned spending on API security appears strong, with 52% indicating it will increase significantly, and 44% anticipating a slight increase. No organizations reported plans to decrease spending.

Dedicated API security tools were most likely to see an increase in spending, cited by 56% of respondents. Many also reported plans to increase spending on integrated application security and API security tools (54%), CNAPPs (53%), and API management tools (52%). This reflects the fact that API security is still fairly new, with many organizations still working toward maturity. Over time, it is likely that spending on dedicated tools will continue to increase given the criticality organizations are placing on API security.

Will API security spending over the next 12-18 months increase?



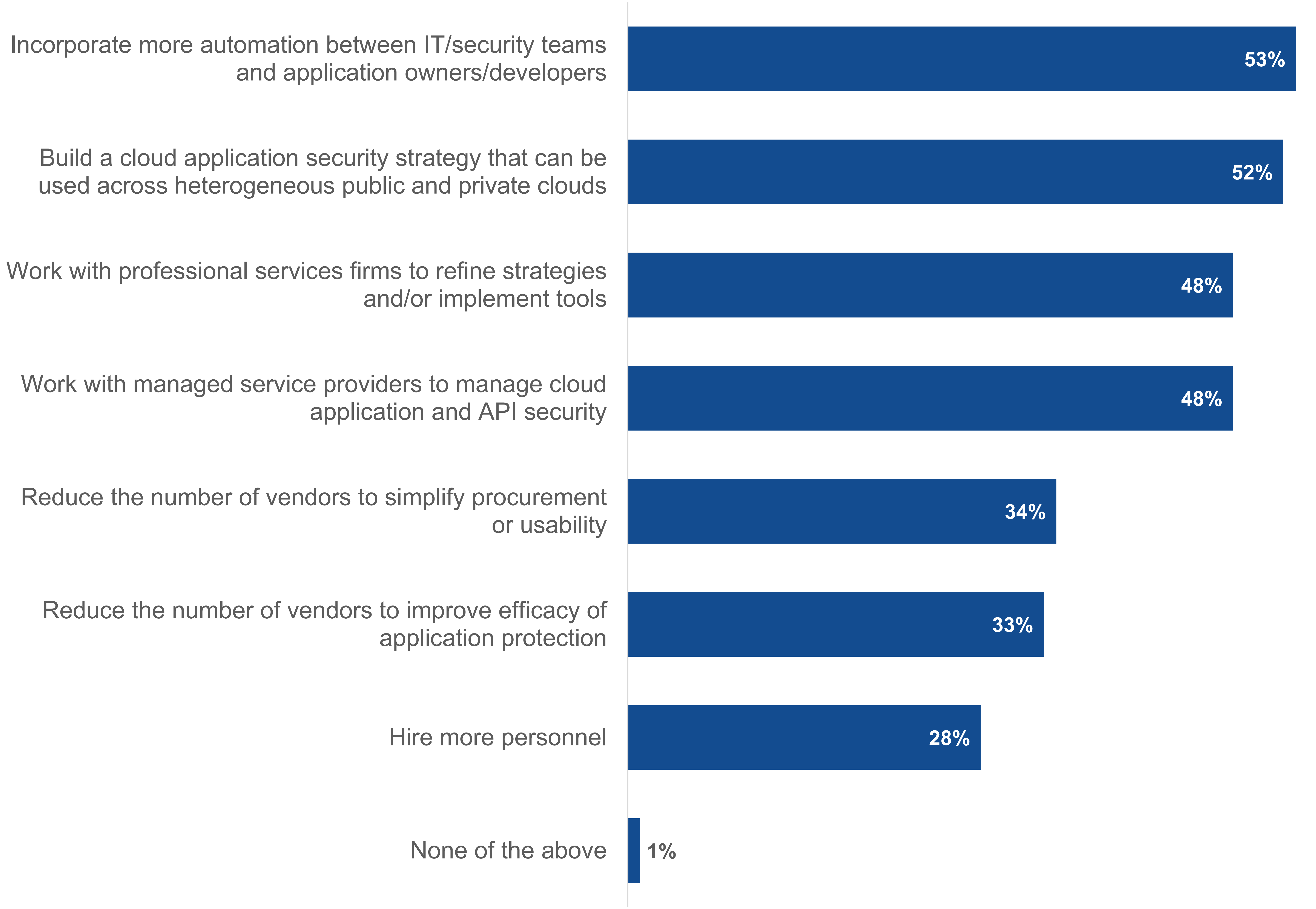
Areas in which API security spending will increase the most.



Optimizing API Security to Support Growth and Scale

From an improvement and optimization perspective, a majority of organizations (53%) are planning to incorporate more automation between security teams and application owners. Based on the scale of API usage and speed of application development, automation is the best bet security teams have to keep pace. Providing consistency across heterogeneous public and private clouds is also a key area of focus, as cited by 52% of respondents. Finally, working with service providers—either professional services firms to refine strategies or implement tools (48%) or managed services providers to manage cloud application and API security (48%)—can help overcome skill shortages and better utilize the time of the staff organizations do have.

Actions expected to be taken to improve or optimize API security.



CEQUENCE

ABOUT

Cequence, a pioneer in API security and bot management, is the only solution that delivers Unified API Protection (UAP), uniting discovery, compliance, and protection across all internal, external, and third-party APIs to defend organizations against attacks, business logic abuse, and fraud. The flexible deployment model supports SaaS, on-premises, and hybrid installations, and APIs can be onboarded in less than 15 minutes without requiring any app instrumentation, SDK, or JavaScript integration. Cequence solutions scale to handle the most demanding government, Fortune and Global 500 organizations, securing more than 8 billion daily API interactions and protecting more than 3 billion user accounts.

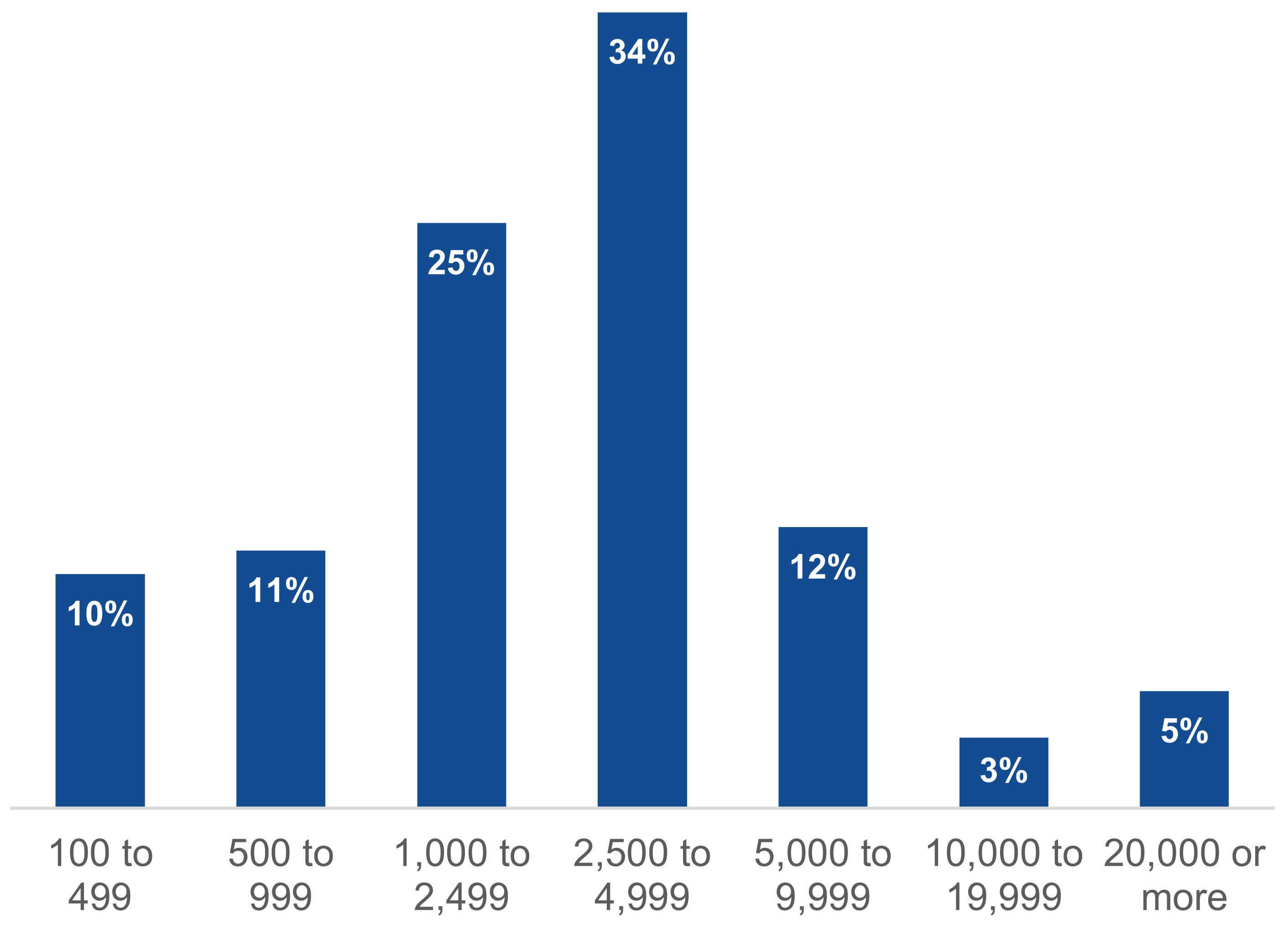
LEARN MORE

RESEARCH METHODOLOGY AND DEMOGRAPHICS

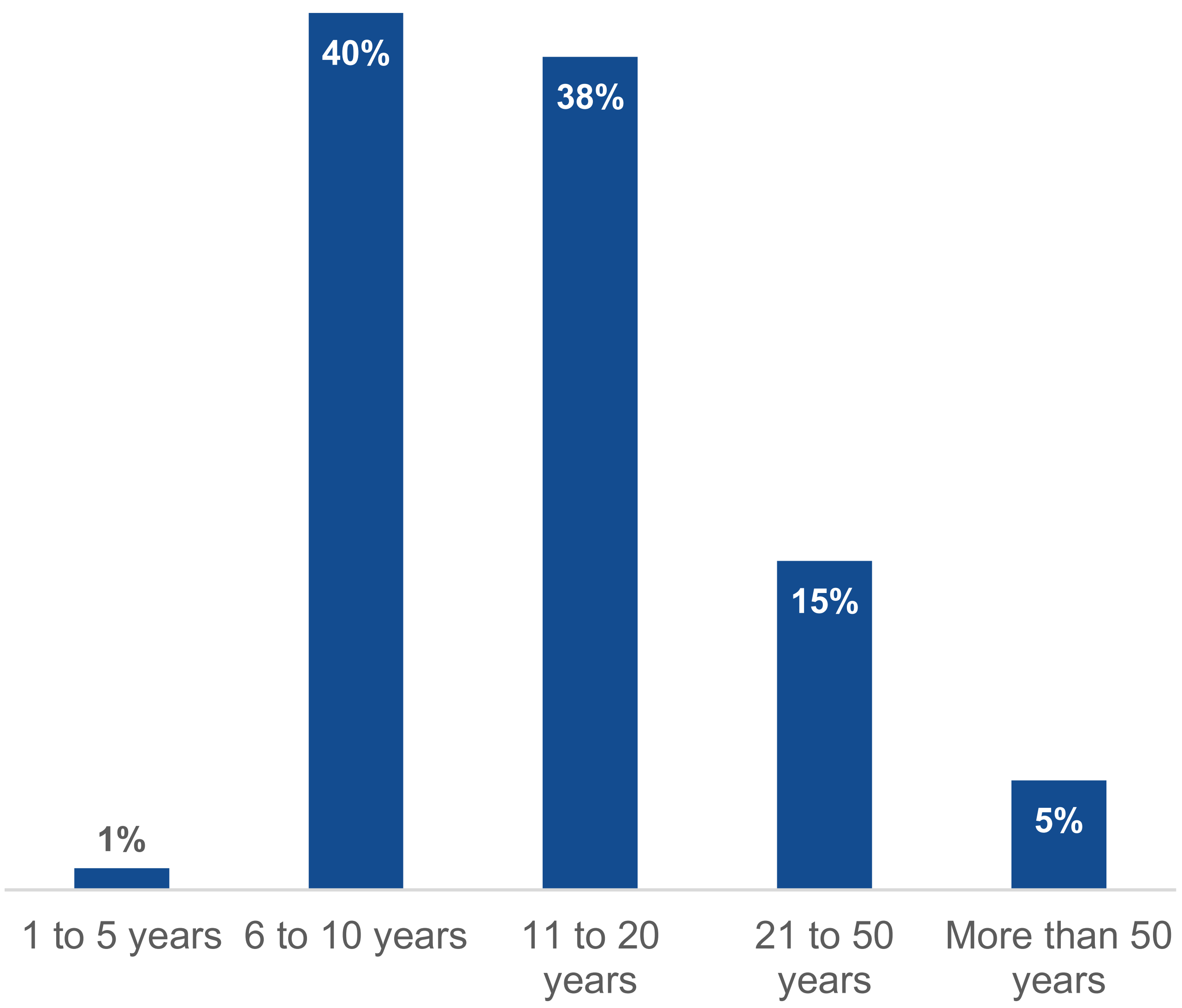
To gather data for this report, TechTarget's Enterprise Strategy Group conducted a comprehensive online survey of IT and cybersecurity professionals from private- and public-sector organizations in North America between August 8, 2024, and August 28, 2024. To qualify for this survey, respondents were required to be involved with securing their organization's APIs. 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 385 IT and cybersecurity professionals.

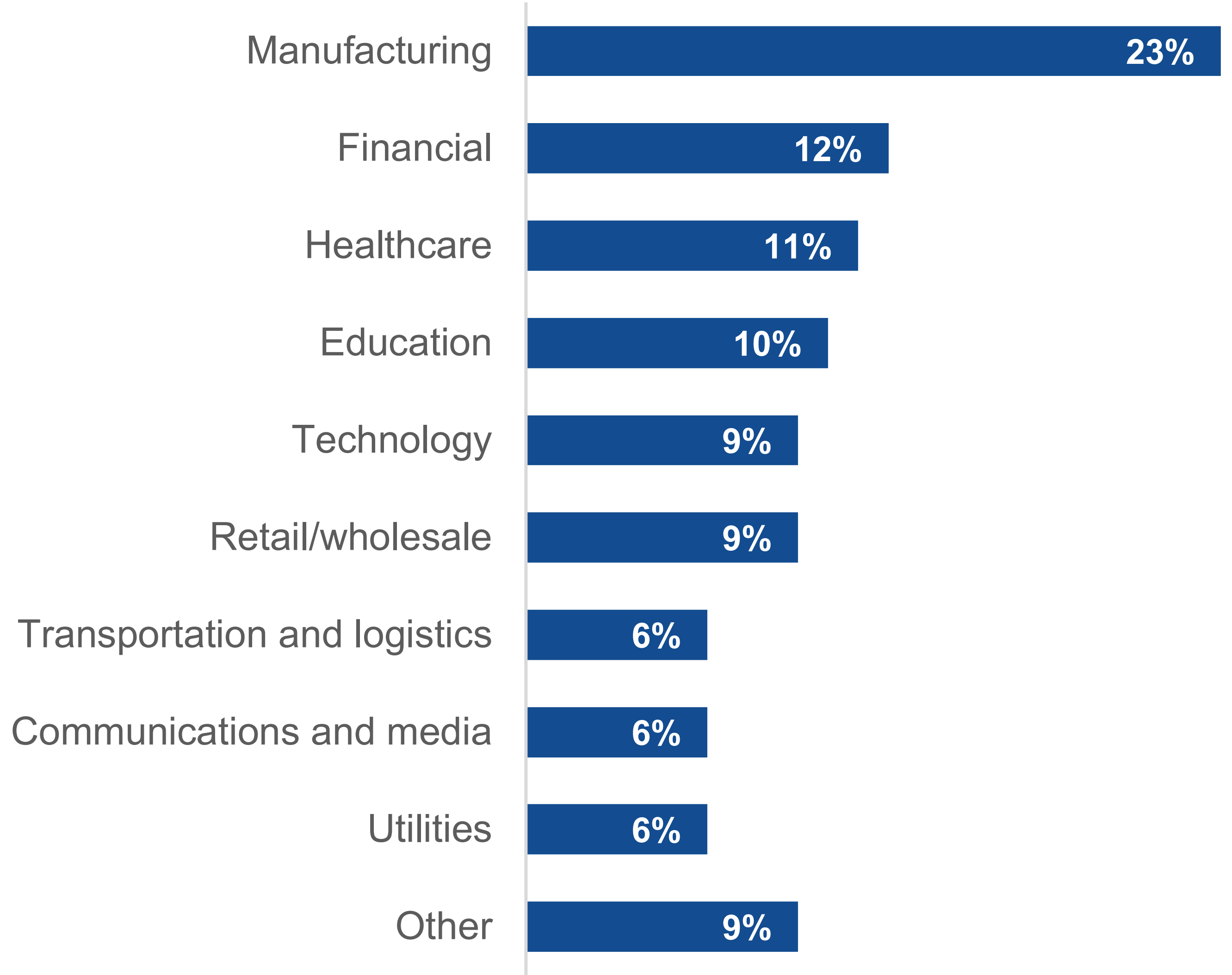
Respondents by number of employees.



Respondents by age of organization.



Respondents by industry.



Enterprise Strategy Group™
by TechTarget

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.