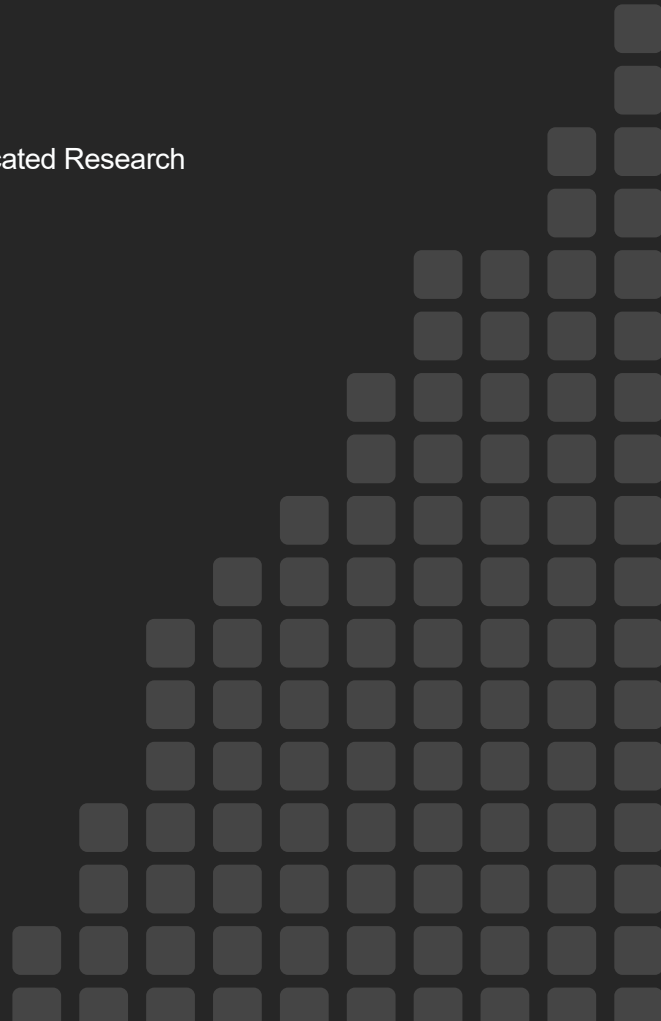


RESEARCH REPORT

# Securing the API Attack Surface

By Melinda Marks, Senior Analyst and Bill Lundell, Director of Syndicated Research  
Enterprise Strategy Group

August 2023



# Contents

<b>Executive Summary</b> .....	<b>3</b>
<b>Report Conclusions</b> .....	<b>3</b>
<b>Introduction</b> .....	<b>4</b>
<b>Research Objectives</b> .....	<b>4</b>
<b>Research Findings</b> .....	<b>5</b>
<b>Application Development Modernization Necessitates Cybersecurity Modernization</b> .....	<b>5</b>
<b>API Growth Is Exacerbating Security Risk</b> .....	<b>8</b>
<b>API Security Incidents Are Pervasive, Resulting in Many Challenges and Shortcomings</b> .....	<b>13</b>
<b>Building an Effective API Security Strategy Involves a Variety of Tools and Developer Participation</b> .....	<b>18</b>
<b>Organizations Are Committed to and Investing in Solidifying API Security Posture</b> .....	<b>25</b>
<b>Conclusion</b> .....	<b>27</b>
<b>Research Methodology</b> .....	<b>29</b>
<b>Respondent Demographics</b> .....	<b>30</b>

# Executive Summary

## Report Conclusions

TechTarget's Enterprise Strategy Group (ESG) recently surveyed 397 IT, cybersecurity, and application development professionals responsible for evaluating, purchasing, and managing API security solutions at midmarket (100 to 999 employees) and enterprise (1,000 or more employees) organizations in North America (the United States and Canada).

Based upon the gathered data, the report illustrates that:

- **Application development modernization necessitates cybersecurity modernization.** While only one in five organizations currently support more than half of their public-facing web applications with a microservices, cloud-native architecture, this is expected to more than quadruple within the next 24 months. Additionally, the vast majority of organizations currently employ a DevOps methodology to some degree. 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 such as misconfigurations and vulnerabilities, many organizations report their security teams lack visibility into development processes and/or that developers are skipping security processes.
- **API growth is exacerbating security risk.** More than three-quarters of organizations report that they have an average of 26 APIs per application deployed, and a majority are using open APIs for public consumption, connecting applications with partners, and/or connecting microservices. While slightly 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. 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, with more than one-third of organizations releasing updates daily, and another 40% doing so on a weekly basis.
- **API security incidents are pervasive, resulting in many challenges and shortcomings.** Nearly three-quarters of organizations believe they have a robust API security program with processes and controls in place, including API security tools, web application firewalls, and API gateways. However, despite having multiple products in place addressing API security, more than half of organizations faced multiple incidents, and 35% faced at least one incident within the last year. Organizations have suffered a range of security incidents from insecure APIs, including data exposure, account takeover, and/or denial of service attacks. The most common API security concerns include authentication, which is alarming because every connection needs effective authentication to be secure, as well as many visibility concerns.
- **Building an effective API security strategy involves a variety of tools and developer participation.** Organizations are looking for API security solutions with a comprehensive set of features to deal with security issues like identifying and tracking APIs, authenticating APIs, and blocking attacks or excessive traffic. To further mitigate risk, security should be involved in securing APIs before they are deployed, and while more than half of teams responsible for securing APIs are involved with development as soon as or before they are published, there is still a lot of room for improvement. However, it is promising that the majority of organizations rate a high percentage of their developers as having a solid level of API security knowledge, which is a byproduct of the fact that 89% of organizations provide formal API security training to their development teams.
- **Organizations are committed to and investing in solidifying API security posture.** Most organizations have a dedicated budget for API security, and 95% expect to increase their investments in API security solutions to some extent 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.

# Introduction

## 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 surveyed 397 IT, cybersecurity, and application development professionals at organizations in North America (US and Canada) responsible for evaluating, purchasing, and managing API security solutions.

This study sought to answer the following questions:

- Approximately what percentage of public-facing web applications are based on a microservices, cloud-native architecture today? How is this expected to change, if at all, over the next 24 months?
- How frequently do organizations' developers (and/or DevOps teams) deliver new software builds to production? How is this expected to change, if at all, over the next 6 to 12 months?
- What security challenges do organizations face with the faster development cycles of CI/CD?
- What is the average number of APIs per application? What proportion of cloud-native applications use APIs today? How is that expected to change, if at all, over the next 24 months?
- Have organizations experienced a security incident related to insecure APIs in the last 12 months? What type of security incident(s) did organizations suffer as a result of insecure APIs?
- What are the biggest challenges organizations have faced with API security? What types of API vulnerabilities are of greatest concern?
- How long does it typically take for organizations to remediate an API vulnerability? How do organizations ensure APIs do not expose sensitive data?
- How would organizations describe the collective level of understanding their development teams have of security risks for APIs?
- Do organizations provide formal API security training to their development teams?
- When new APIs are published, when does the team responsible for securing them become involved?
- What is the source from which API security is funded, or will likely be funded? Do organizations expect to increase their spending on API security technologies, services, and personnel over the next 12-18 months?
- What do organizations expect to increase their API security spending on the most over the next 12-18 months?
- What actions do organizations expect to take over the next 12-18 months to implement or optimize their web application and API protection strategies?

Survey participants represented a wide range of industries including manufacturing, technology, financial services, and retail/wholesale. For more details, please see the Research Methodology and Respondent Demographics sections of this report.

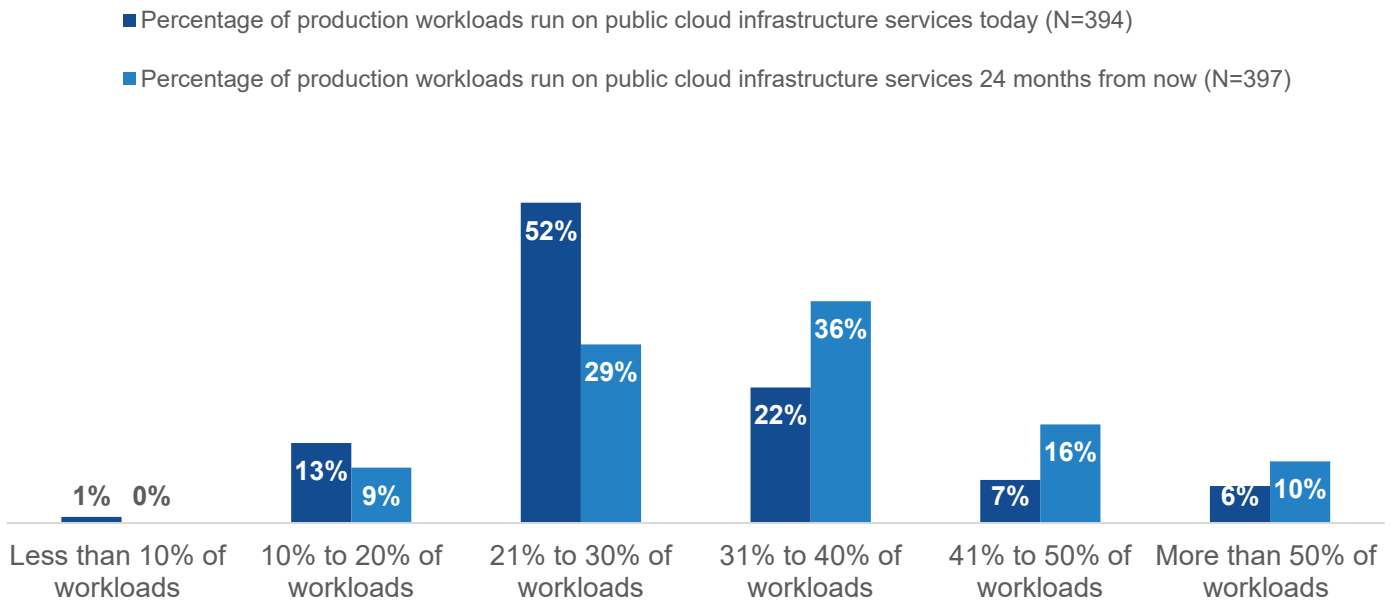
# Research Findings

## Application Development Modernization Necessitates Cybersecurity Modernization

Organizations are increasingly moving their production applications and workloads to public cloud platforms. While just more than one-third (35%) of organizations report that more than 30% of all their production workloads run on public cloud infrastructure today, this is expected to increase to 62% of organizations over the next two years (see Figure 1).

**Figure 1. Production Workloads Continue to Be Moved to Public Cloud Infrastructure**

**Of all the production server workloads, including application containers, used by your organization, approximately what percentage is run on public cloud infrastructure services (i.e., IaaS) today? How do you expect this to change, if at all, over the next 24 months? (Percent of respondents)**



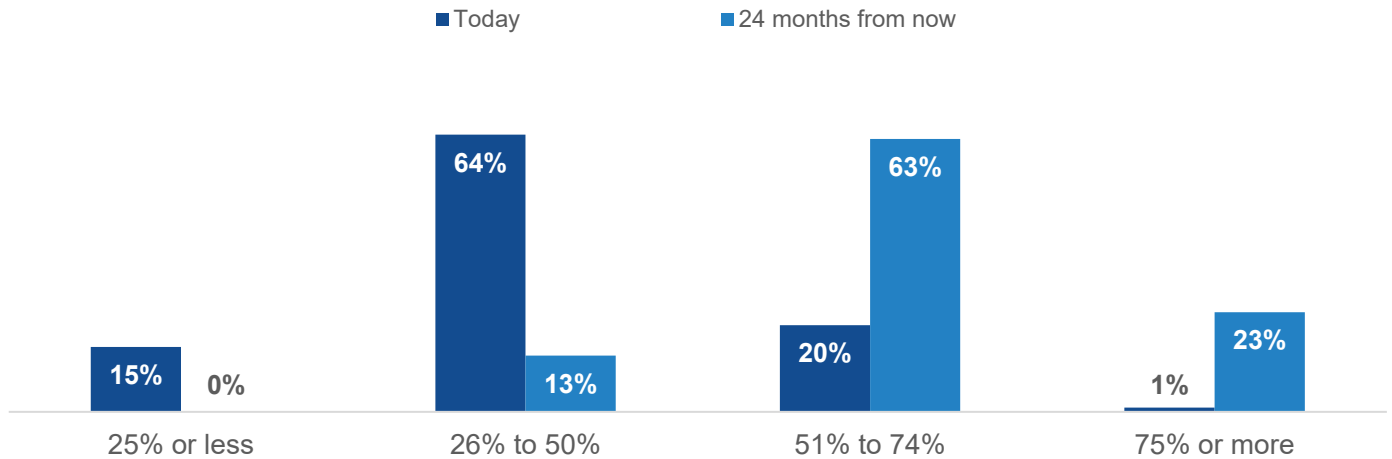
Source: Enterprise Strategy Group, a division of TechTarget, Inc.

By leveraging the state-of-the-art technologies and services from cloud service providers (CSPs) and microservices application architectures, organizations can efficiently build and deploy their applications faster to serve their employees, partners, and customers. According to Figure 2, only 21% of organizations support more than half of their public-facing web applications with a microservices, cloud-native architecture; however, this is expected to more than quadruple within the next 24 months.

Organizations are also leveraging DevOps methodologies for continuous integration and continuous deployment (CI/CD) of applications. As seen in Figure 3, the vast majority of organizations currently employ a DevOps methodology, either extensively (57%) or in a limited fashion (31%). 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.

**Figure 2.** Cloud-native Architectures Are Becoming Increasingly Common for Web Applications

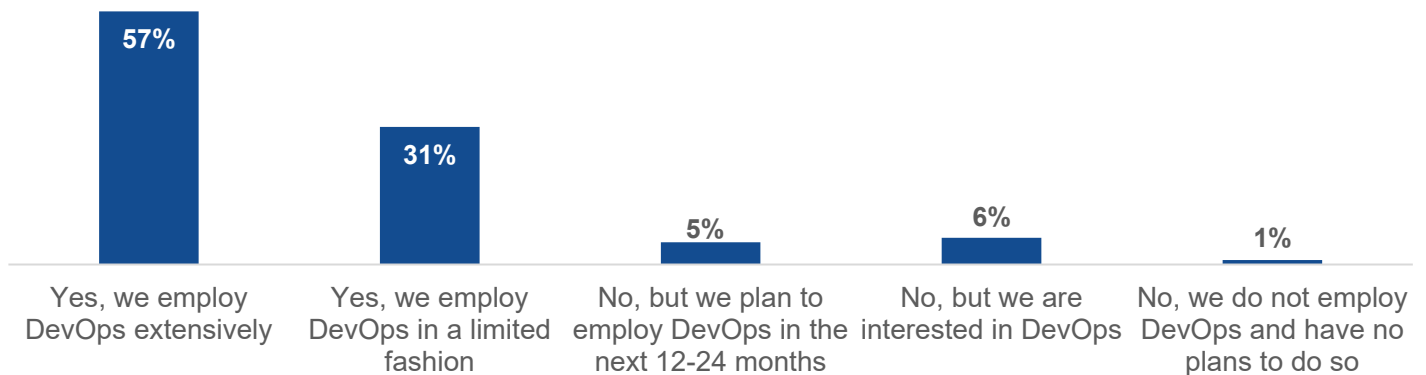
**Approximately what percentage of your organization’s public-facing web applications are based on a microservices, cloud-native architecture today? How do you expect this to change, if at all, over the next 24 months? (Percent of respondents, N=397)**



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

**Figure 3.** Most Organizations Are Leveraging a DevOps Methodology

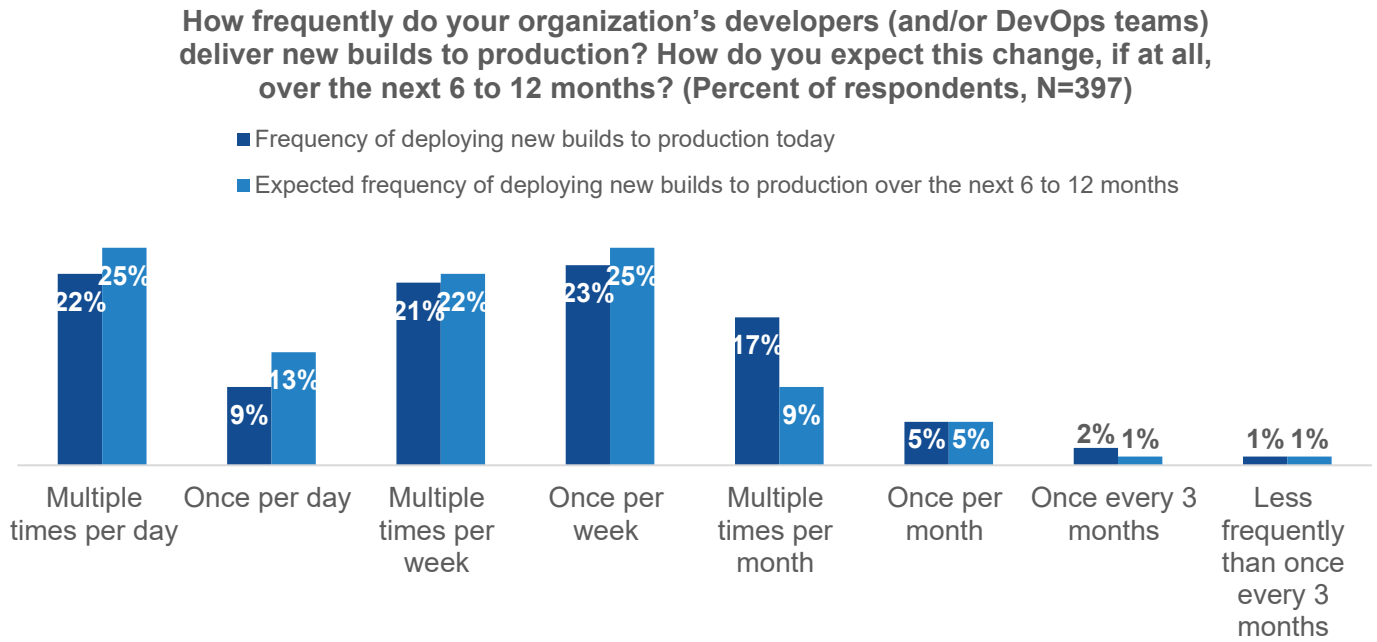
**Does your organization employ a DevOps methodology to automate the continuous integration and continuous delivery (CI/CD) of code and application infrastructure? (Percent of respondents, N=397)**



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

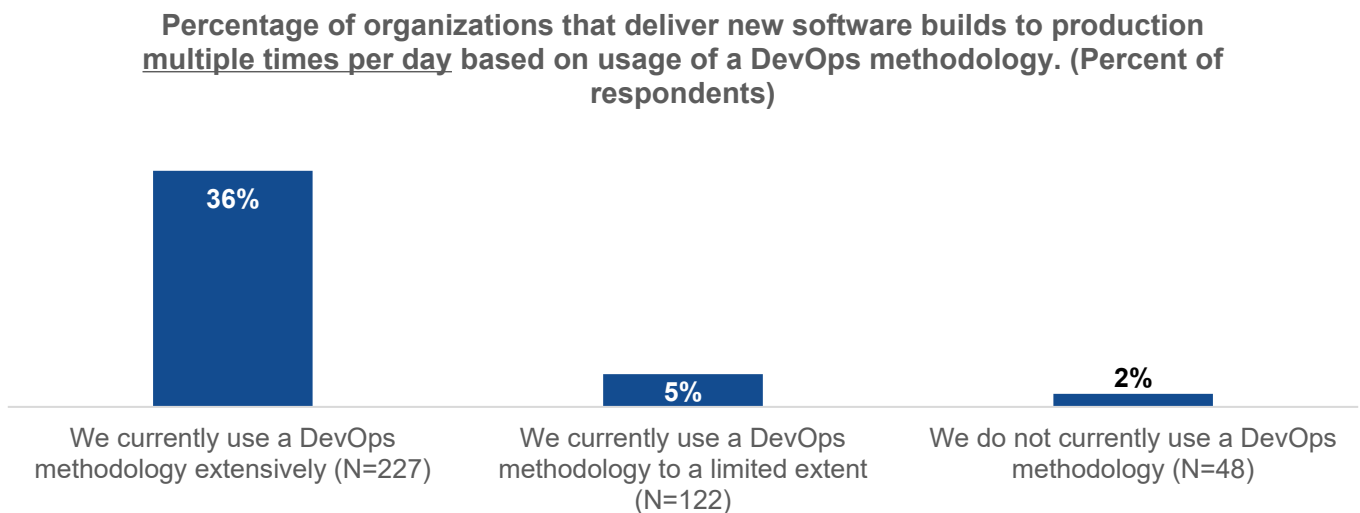
Many organizations currently release new builds daily, and developers expect to increase the frequency of releases, raising challenges for security to keep up with the rapid pace. Specifically, nearly one-third of organizations indicated their developers are releasing new software builds to production daily (9%) or even multiple times per day (22%), which is expected to increase to 38% in the next 12 months (see Figure 4). Not surprisingly, extensive users of DevOps are significantly more likely to already be deploying multiple new software builds to production on a daily basis (see Figure 5).

**Figure 4.** New Software Builds Continue to Get Pushed to Production Faster...



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

**Figure 5.** ...Especially for Extensive DevOps Methodology Users

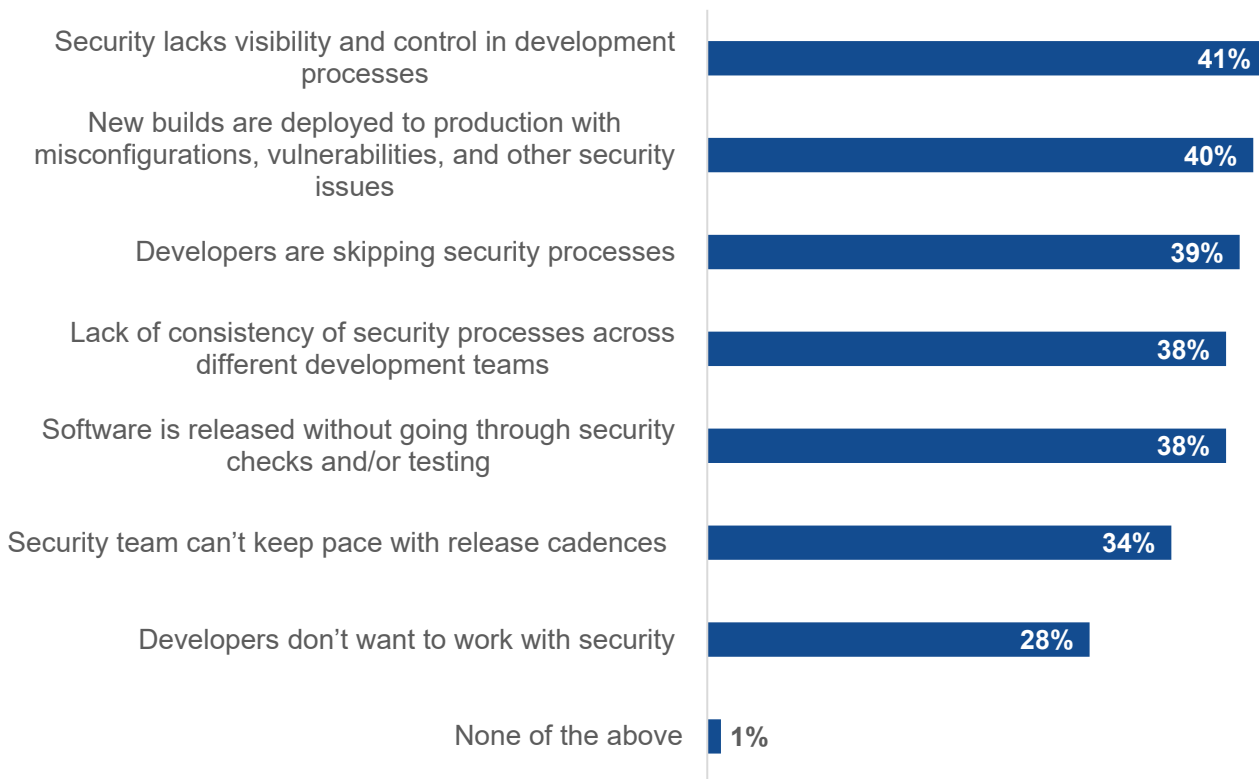


Source: Enterprise Strategy Group, a division of TechTarget, Inc.

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 such as misconfigurations and vulnerabilities, many organizations report their security teams lack visibility into development processes and/or that developers are skipping security processes (see Figure 6). IT and security teams must strike the right balance in order to incorporate security into the development processes without slowing operations down.

**Figure 6.** Lack of Visibility and Misconfigurations Are Most Common Security Challenges Associated with Faster Development Cycles

**What security challenges does your organization face with the faster development cycles of CI/CD? (Percent of respondents, N=397, multiple responses accepted)**



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

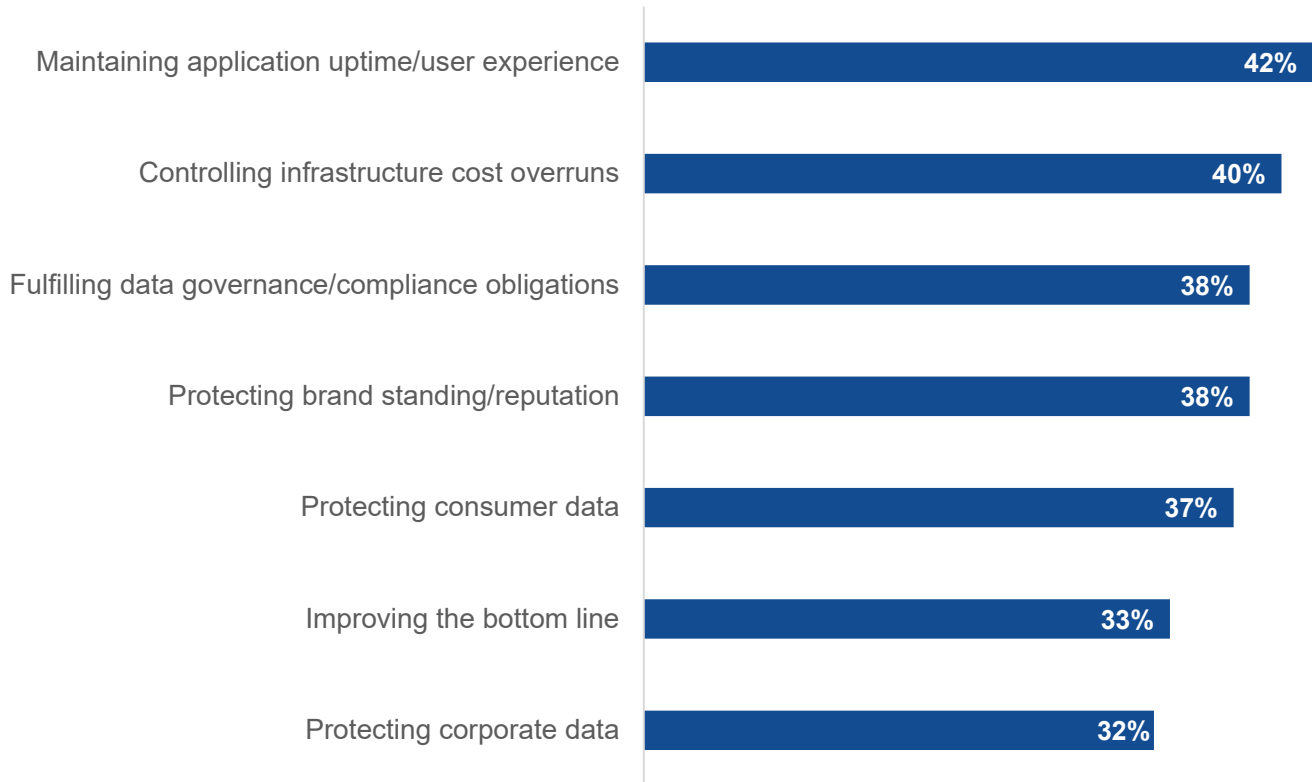
### API Growth Is Exacerbating Security Risk

Application security teams are aligning their goals with development teams to deliver cloud-based software applications that meet business objectives for growth and customer service. According to Figure 7, the most common consideration driving cloud application programs are application uptime/user experience (42%), controlling cost overruns (40%), fulfilling data governance and compliance obligations (38%), protecting brand/reputation (38%), and protecting consumer data (37%).



**Figure 7.** Critical Drivers of Cloud Application Programs

**What are the most critical drivers of your organization’s cloud application program? (Percent of respondents, N=397, three responses accepted)**

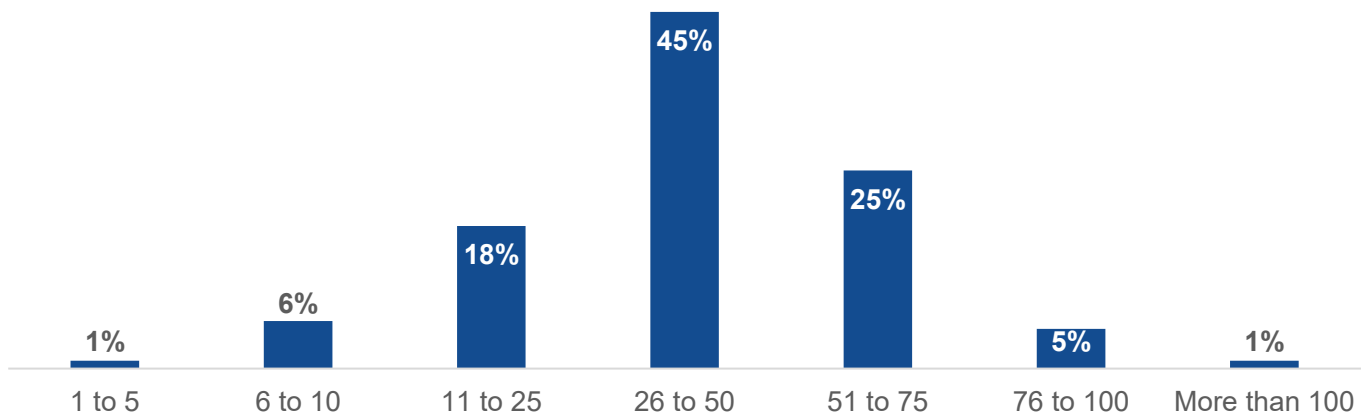


Source: Enterprise Strategy Group, a division of TechTarget, Inc.

The data further shows that as developers utilize APIs in their applications, security teams need to address their usage to manage security risk. More than three-quarters (76%) of organizations report that they have an average of 26 APIs per application deployed (see Figure 8). Furthermore, Figure 9 reveals that a majority of organizations are using open APIs for public consumption (67%), connecting applications with partners (64%), and/or connecting microservices (51%) as API use cases. Security teams need to ensure every connection is secure to meet their key business drivers of keeping applications running and secure.

**Figure 8.** Security Risk with High Numbers of APIs per Application

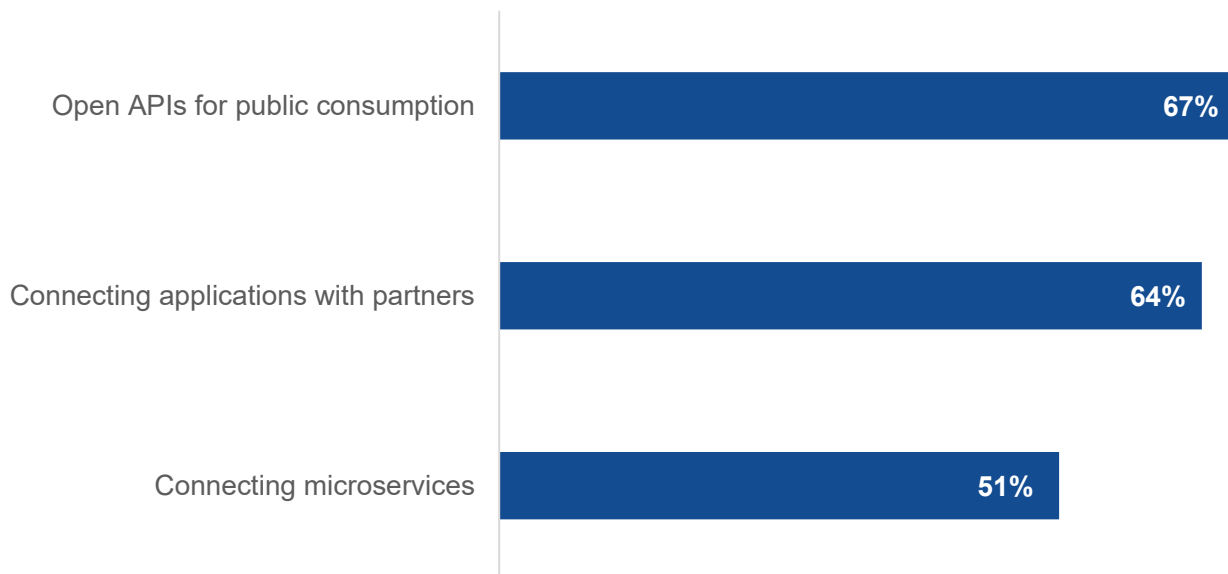
What would you estimate is the average number of APIs per application?  
(Percent of respondents, N=397)



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

**Figure 9.** API Use Cases

How is your organization using APIs? (Percent of respondents, N=397, multiple responses accepted)

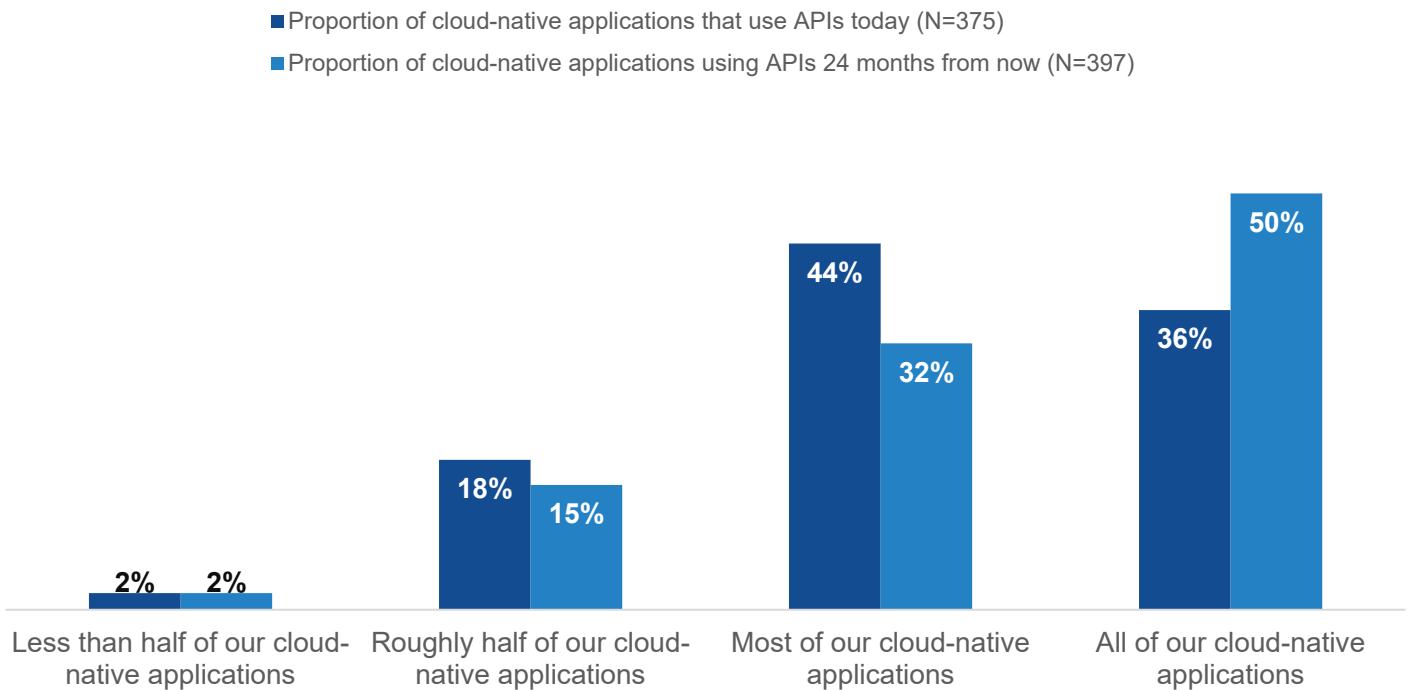


Source: Enterprise Strategy Group, a division of TechTarget, Inc.

As cloud-native development with microservices-based applications continues to grow, they require APIs to access services, data, or other applications. And as developers create more complex applications, the number of APIs can grow. Indeed, while slightly more than one-third (36%) of organizations say all of their applications use APIs today, this is expected to grow to 50% over the next two years (see Figure 10).

**Figure 10.** Growing Proportion of Cloud-native Applications Using APIs

**What proportion of your organization’s cloud-native applications use APIs today? How do you expect that to change, if at all, over the next 24 months?  
(Percent of respondents)**

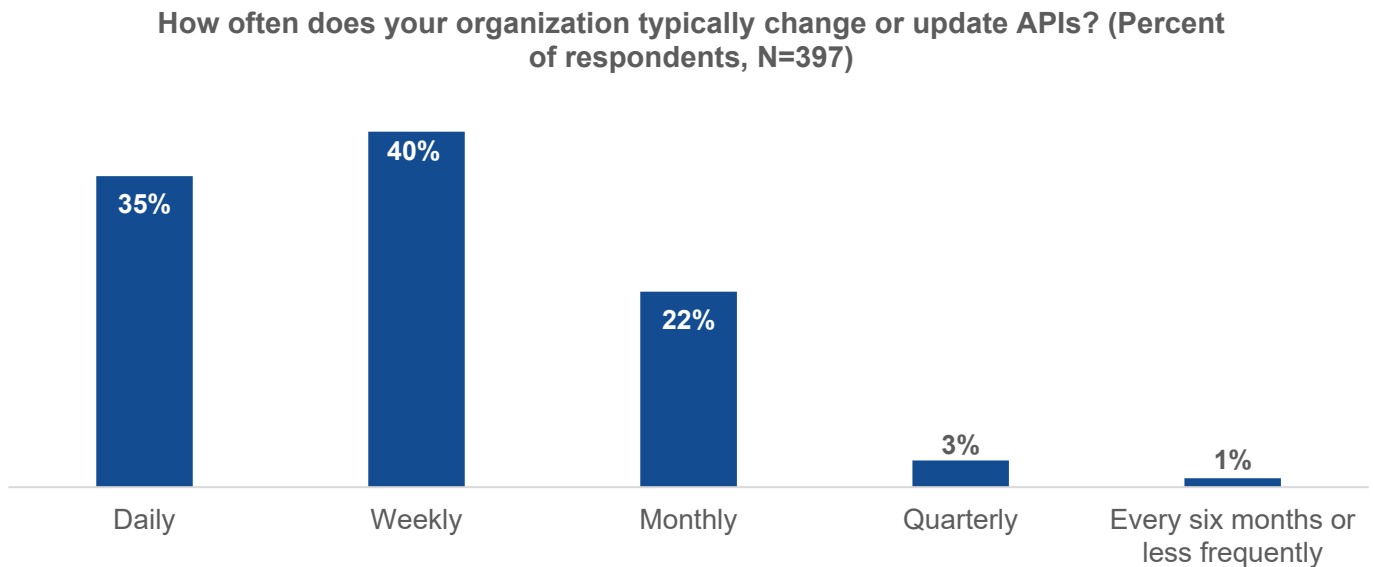


Source: Enterprise Strategy Group, a division of TechTarget, Inc.

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 (see Figure 11).

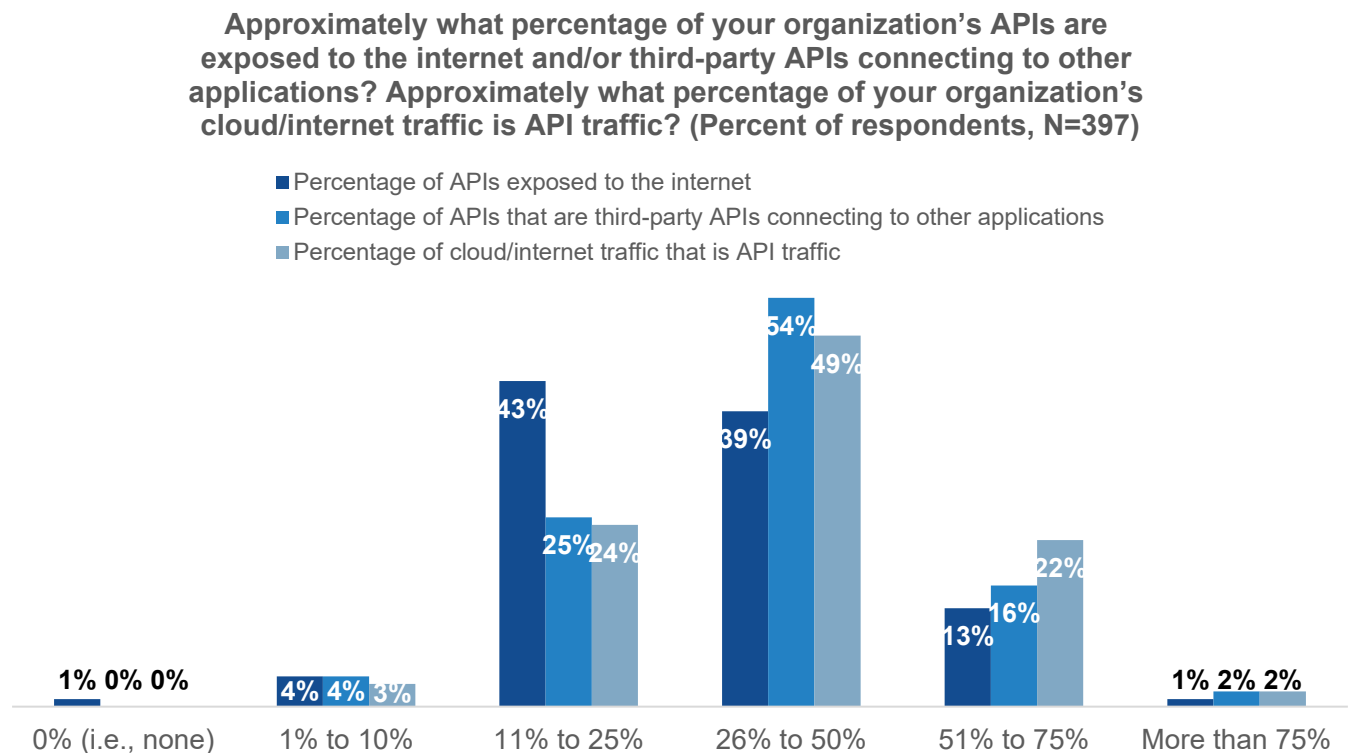
APIs are important for building modern applications that can call other services, applications, or data. Every API or update can add attack surface if it is not secured because of the way that they are connected and the related exposure. While most applications use APIs, the majority of organizations report that no more than half are internet-facing (see Figure 12). This indicates that many are internal-facing, likely for connecting multiple microservices. Additionally, 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 their companies or with 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.

**Figure 11.** Most Organizations Are Updating APIs on at Least a Weekly Basis



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

**Figure 12.** API Connections and Exposures



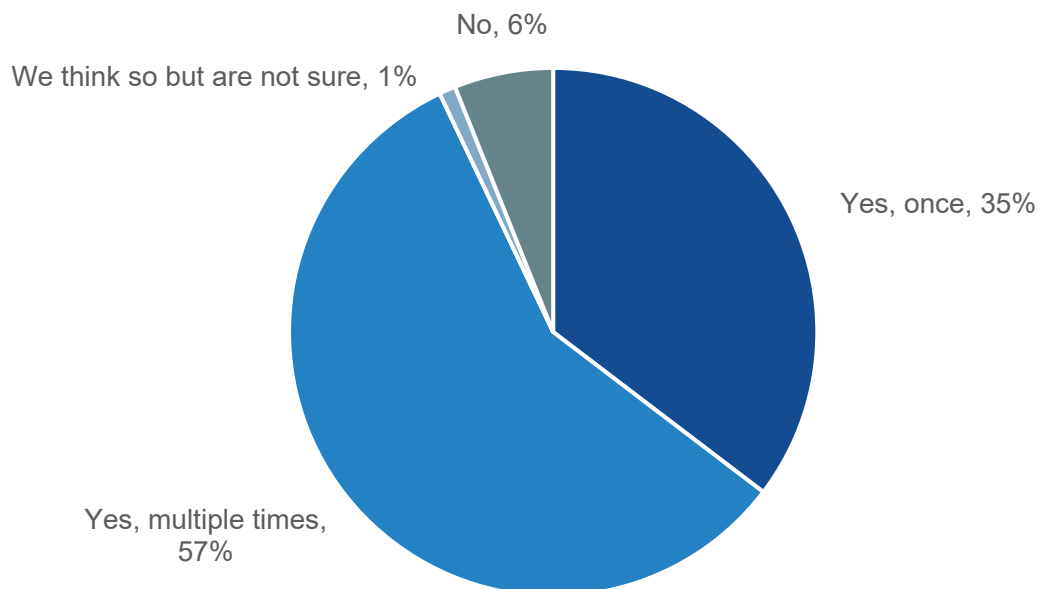
Source: Enterprise Strategy Group, a division of TechTarget, Inc.

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

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 (see Figure 13).

**Figure 13.** Security Incidents from Insecure APIs Are Pervasive

**Has your organization experienced a security incident related to insecure APIs in the last 12 months? (Percent of respondents, N=397)**

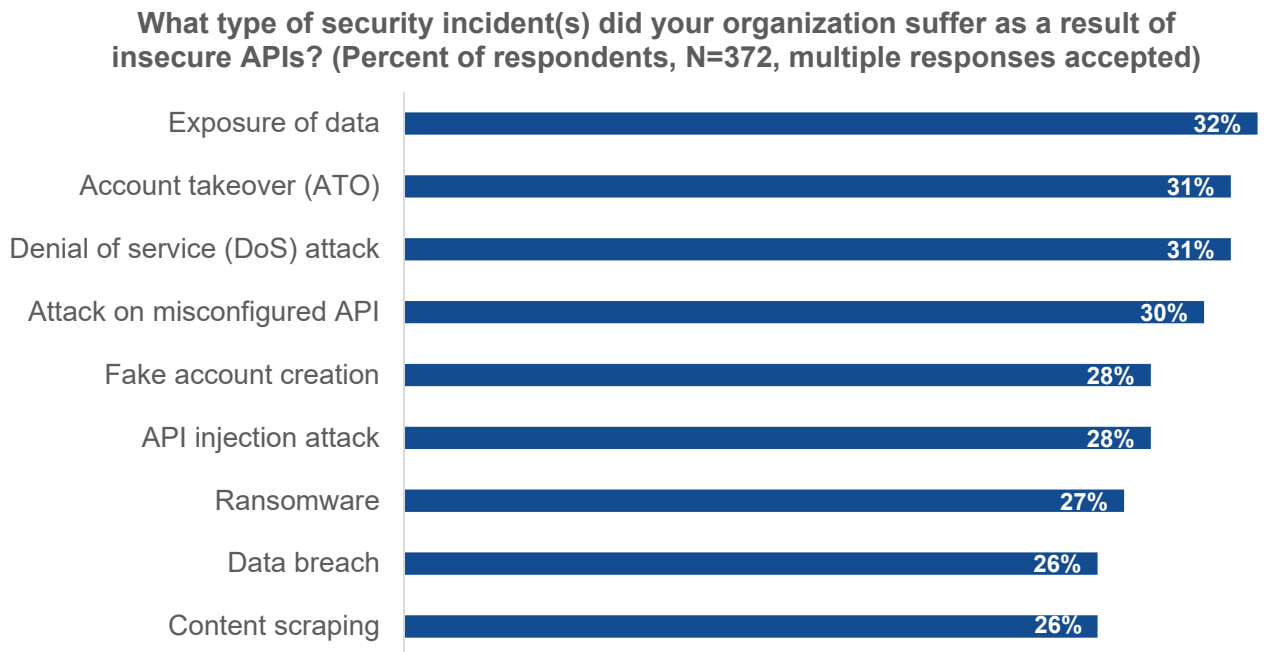


*Source: Enterprise Strategy Group, a division of TechTarget, Inc.*

Security teams need effective ways to manage security risk to support the growing usage of APIs because they increase the attack surface exposing them to a wide variety of attacks. Organizations have suffered a range of security incidents from insecure APIs, including data exposure, account takeover, and/or denial of service attacks (see Figure 14).

Not surprisingly, Figure 15 confirms these attacks can have serious consequences for organizations, including impacting team members (43%), the need for additional web application protection products or services (37%), negative impacts to shareholder value and brand standing (35%), negative customer experiences (33%), and cost overruns (31%). These impacts impede them from meeting their top application security drivers mentioned earlier, including maintaining application uptime, controlling costs, maintaining data governance, supporting customer service, and protecting consumer data.

**Figure 14.** Data Exposure, Account Takeover, and DoS Most Common API Security Incidents



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

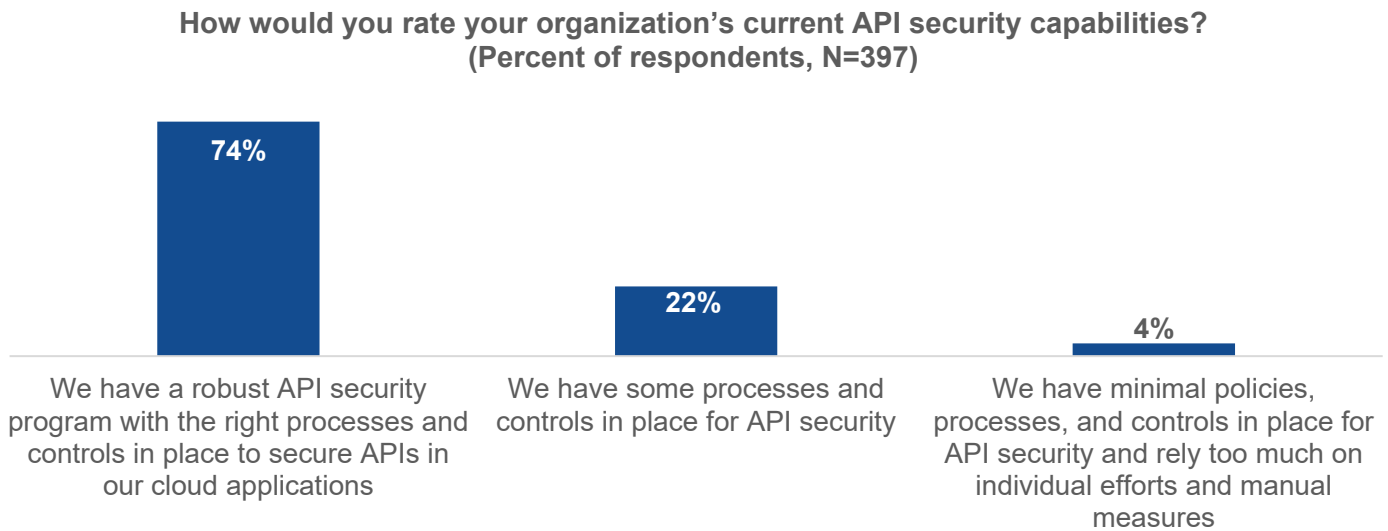
**Figure 15.** Impacts of Attacks on Web Applications and APIs



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Nearly three-quarters (74%) of organizations believe they have a robust API security program with processes and controls in place for API security (see Figure 16). This may be due to the fact that the majority have a variety of tools in place, including API security tools (59%), web application firewalls (57%), and API gateways (50%), to protect their web applications (see Figure 17).

**Figure 16.** Most Organizations Are Confident in Their API Security Capabilities



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

**Figure 17.** Organizations Are Using a Plethora of Discrete Tools to Protect Web Applications

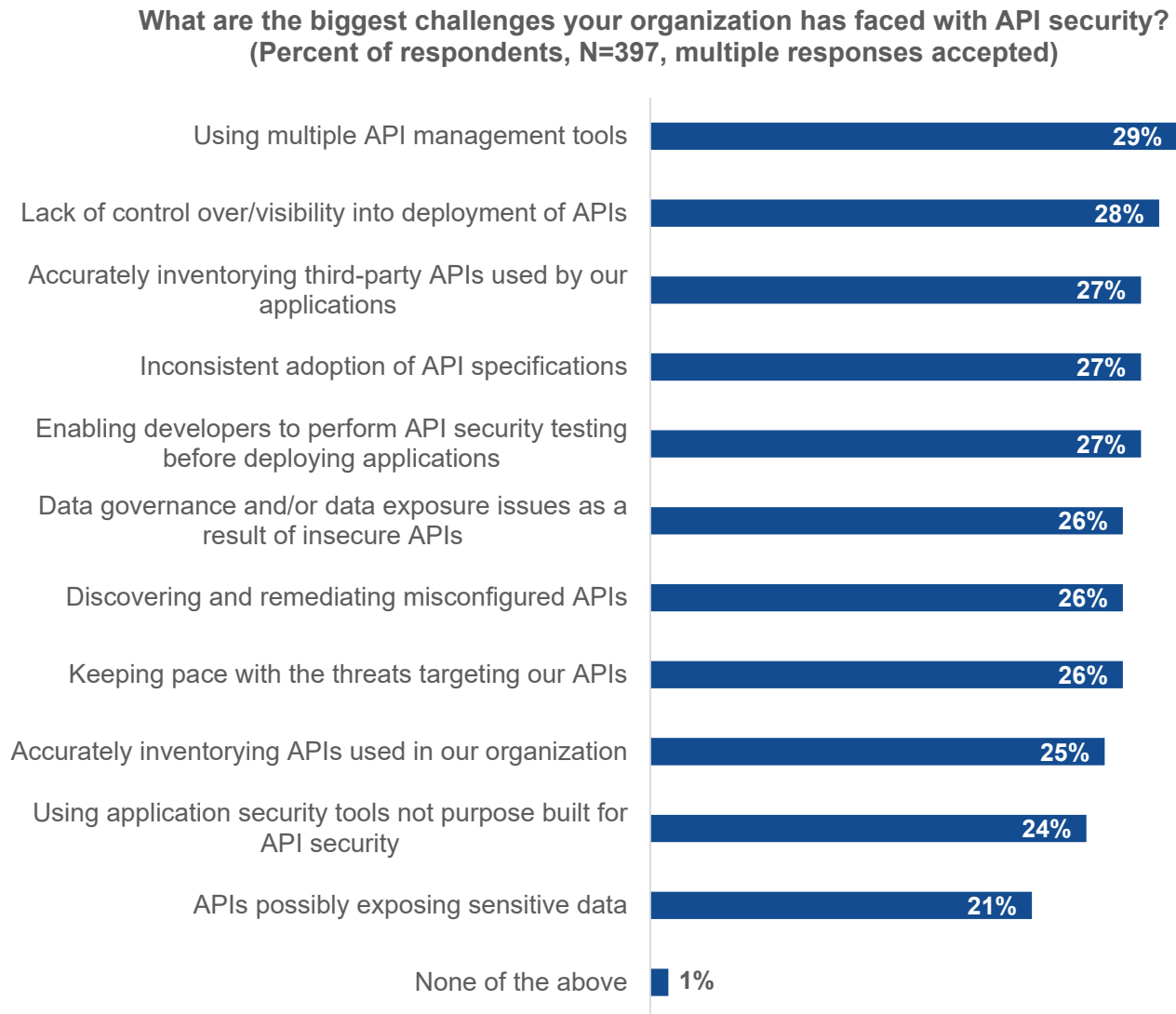


Source: Enterprise Strategy Group, a division of TechTarget, Inc.

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 (see Figure 18). For APIs, organizations are particularly challenged with inventories that would enable them to consistently apply security processes and policies.

**Figure 18.** Most Common API Security Challenges Include Tool Excess and Limited Visibility

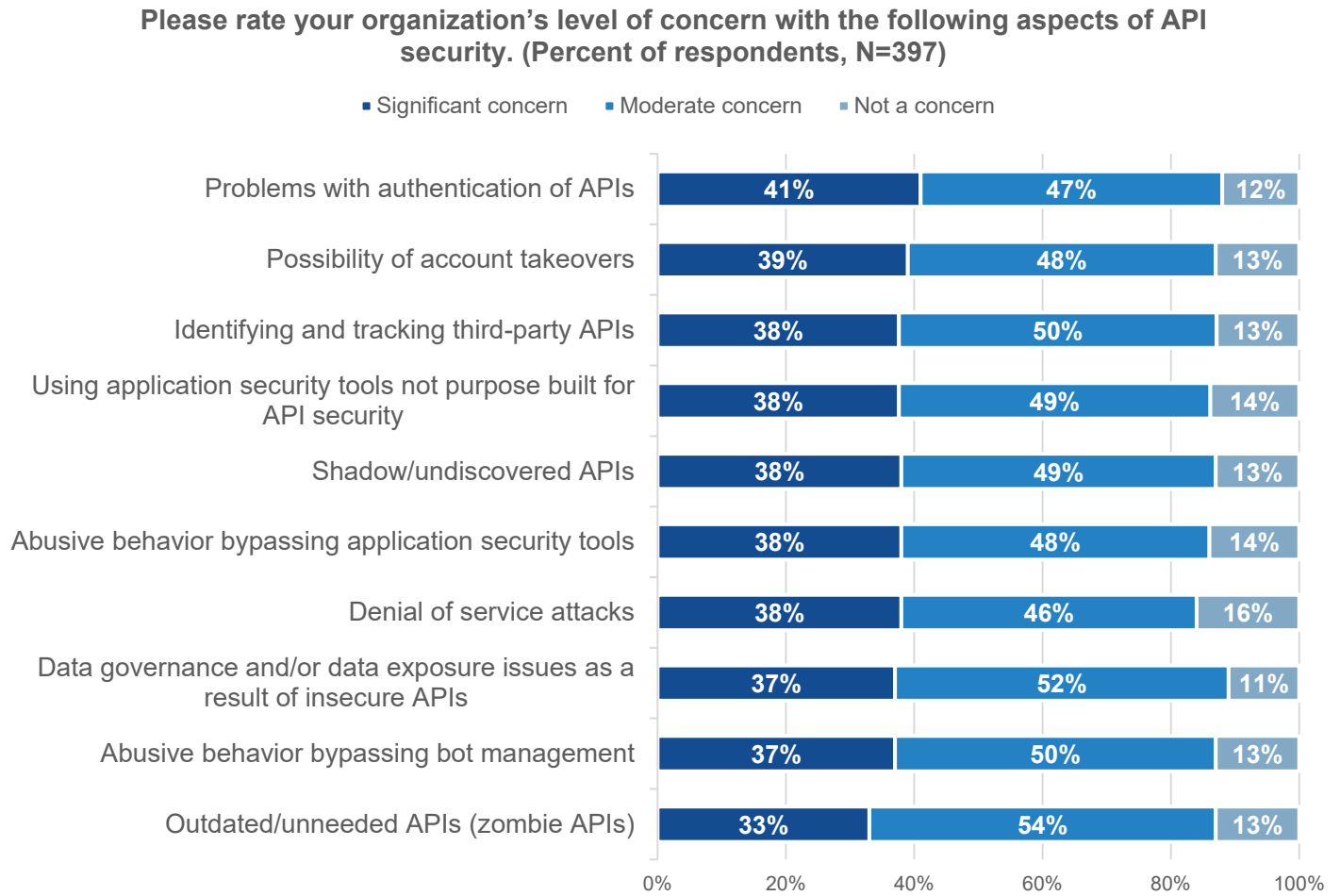


Source: Enterprise Strategy Group, a division of TechTarget, Inc.

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 (see Figure 19). 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.



**Figure 19. Organizations Are Experiencing Concerns Over Many Aspects of API Security**

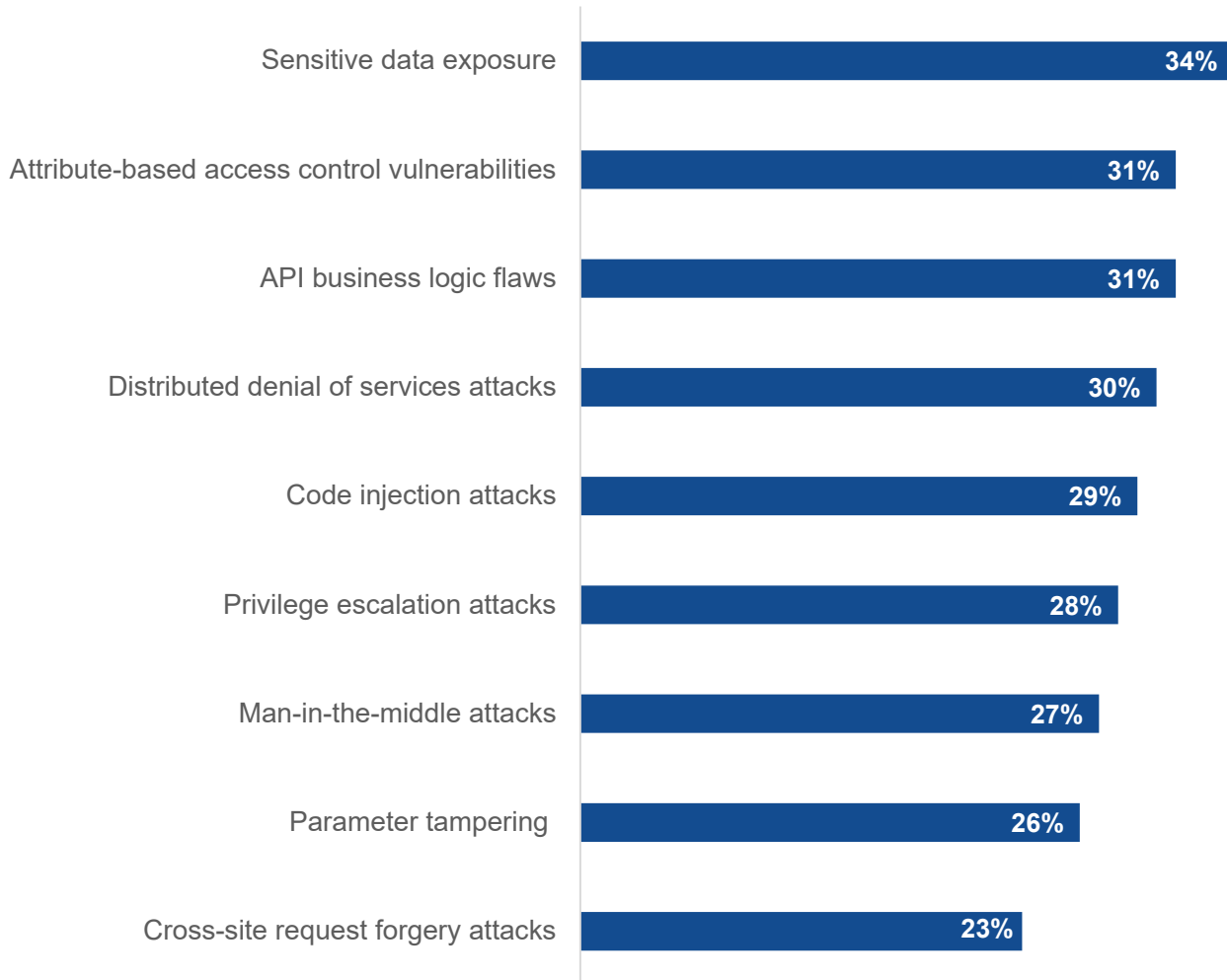


Source: Enterprise Strategy Group, a division of TechTarget, Inc.

APIs play such an important role in modern applications by connecting them to other services, applications, and data. While this enriches applications with greater features and capabilities so that organizations can offer more services to their users, security is important to ensure the applications and their users are not vulnerable to a range of attacks. Figure 20 reveals that organizations are concerned about possible exposure and the wide range of API security susceptibilities that could expose them to serious attacks, including sensitive data exposure (34%), access control vulnerabilities (31%), and/or API business logic flaws (31%).

**Figure 20.** API Vulnerabilities of Greatest Concern

**Moving forward, which types of API vulnerabilities are of greatest concern to your organization? (Percent of respondents, N=397, three responses accepted)**



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

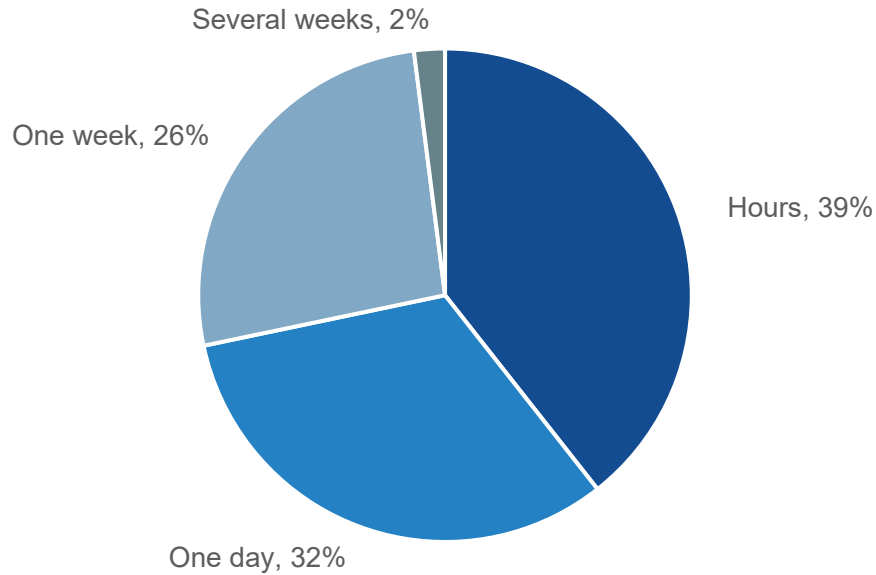
### Building an Effective API Security Strategy Involves a Variety of Tools and Developer Participation

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. Figure 21 shows that nearly three-quarters (71%) of organizations 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 (see Figure 22). 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.

**Figure 21.** Time It Typically Takes to Remediate an API Vulnerability

**How long does it typically take for your organization to remediate an API vulnerability? (Percent of respondents, N=397)**



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

**Figure 22.** Methods of Ensuring APIs Do Not Expose Sensitive Data Are Still Frequently Manual

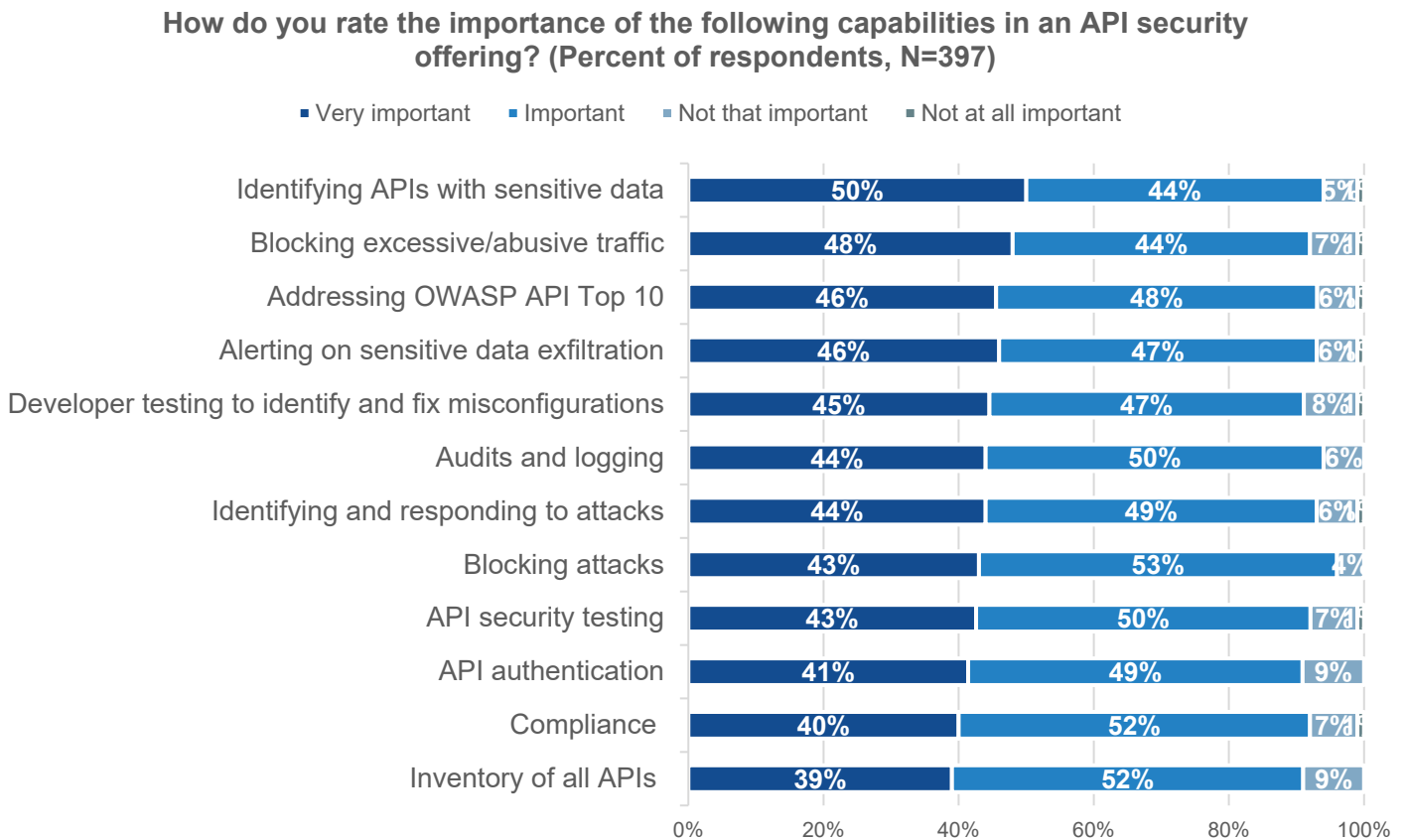
**How does your organization ensure APIs do not expose sensitive data? (Percent of respondents, N=397, multiple responses accepted)**



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

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. According to Figure 23, half of respondent organizations cited identifying APIs with sensitive data, which would help provide context to prioritize actions for better protection, as a *very important* capability of an API security offering.

**Figure 23.** Key API Security Capabilities Include Identifying Sensitive Data and Blocking Abusive Traffic

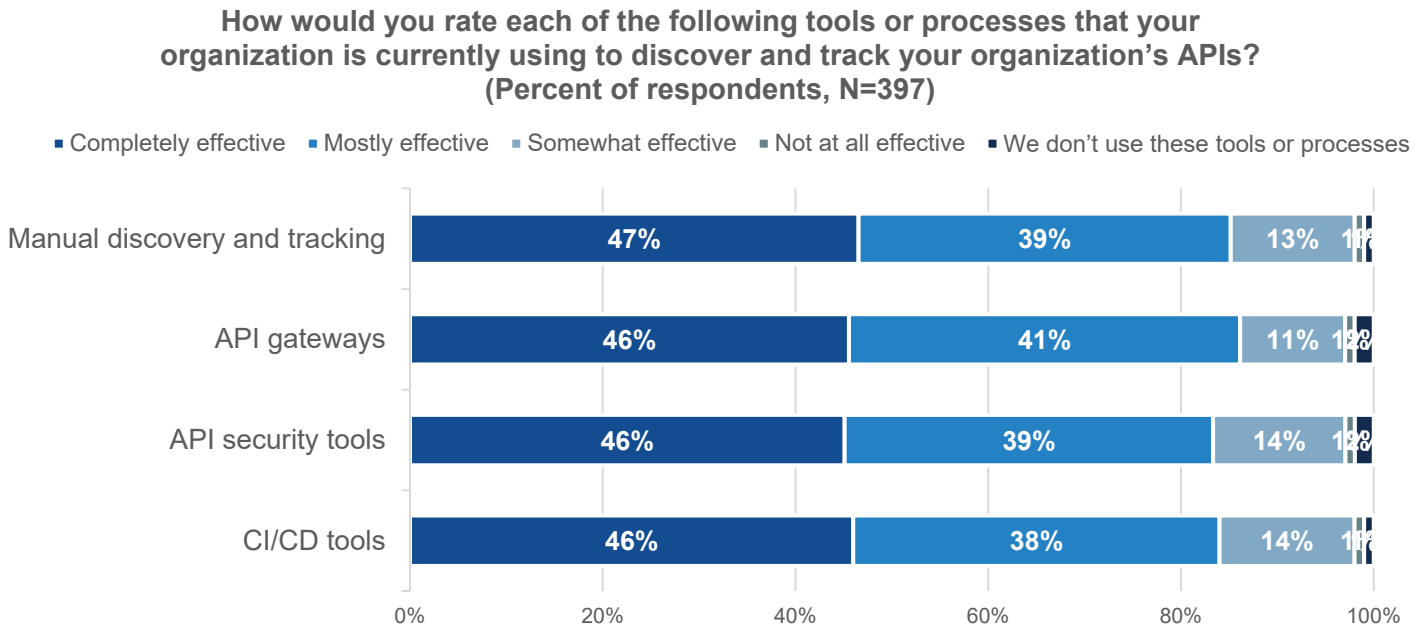


Source: Enterprise Strategy Group, a division of TechTarget, Inc.

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 (see Figure 24). 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.

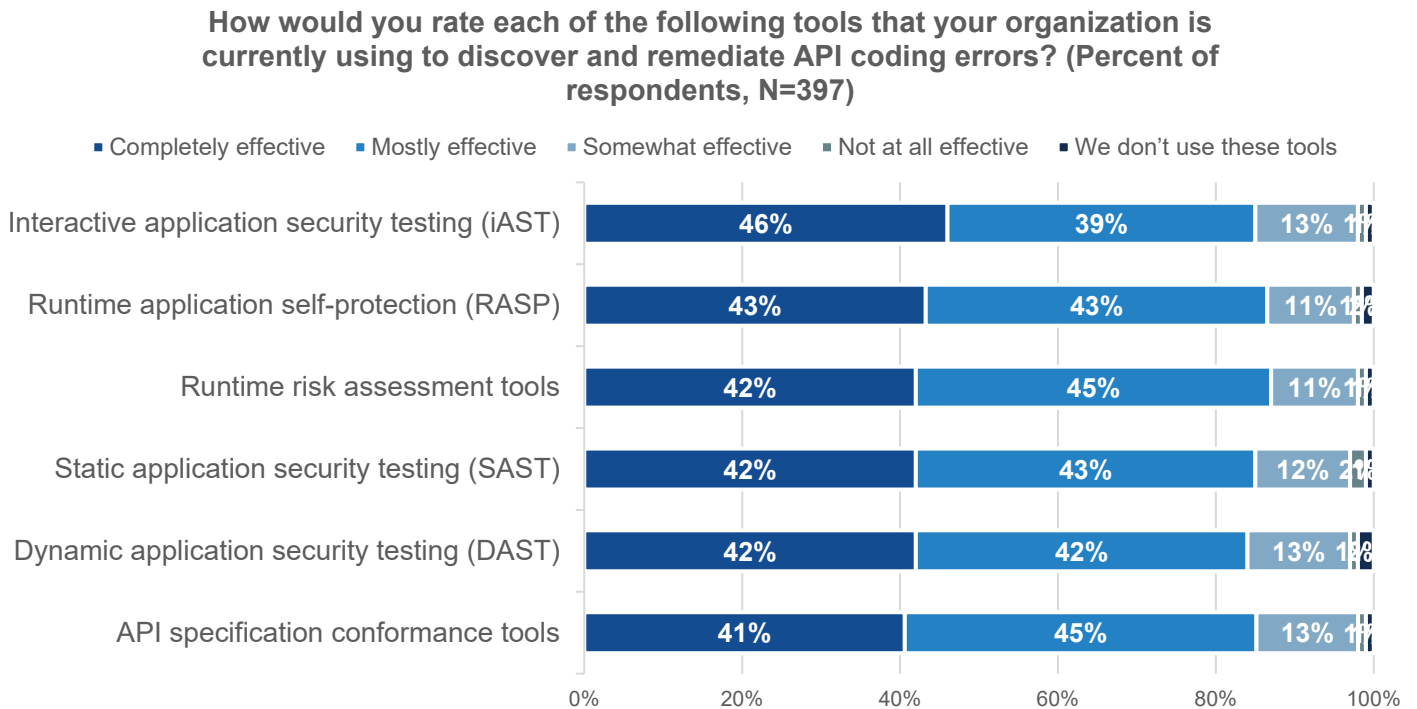
For remediating API coding issues, organizations are typically utilizing their multiple application security tools, including testing tools, runtime application self-protection, runtime assessment tools, and API specification conformance tools. As was the case with discovery and tracking API tools and processes, these tools were mostly rated as completely or mostly effective, with nearly half classifying iAST tools as completely effective (see Figure 25).

Figure 24. Effectiveness of Discovery and Tracking Processes and Tools



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

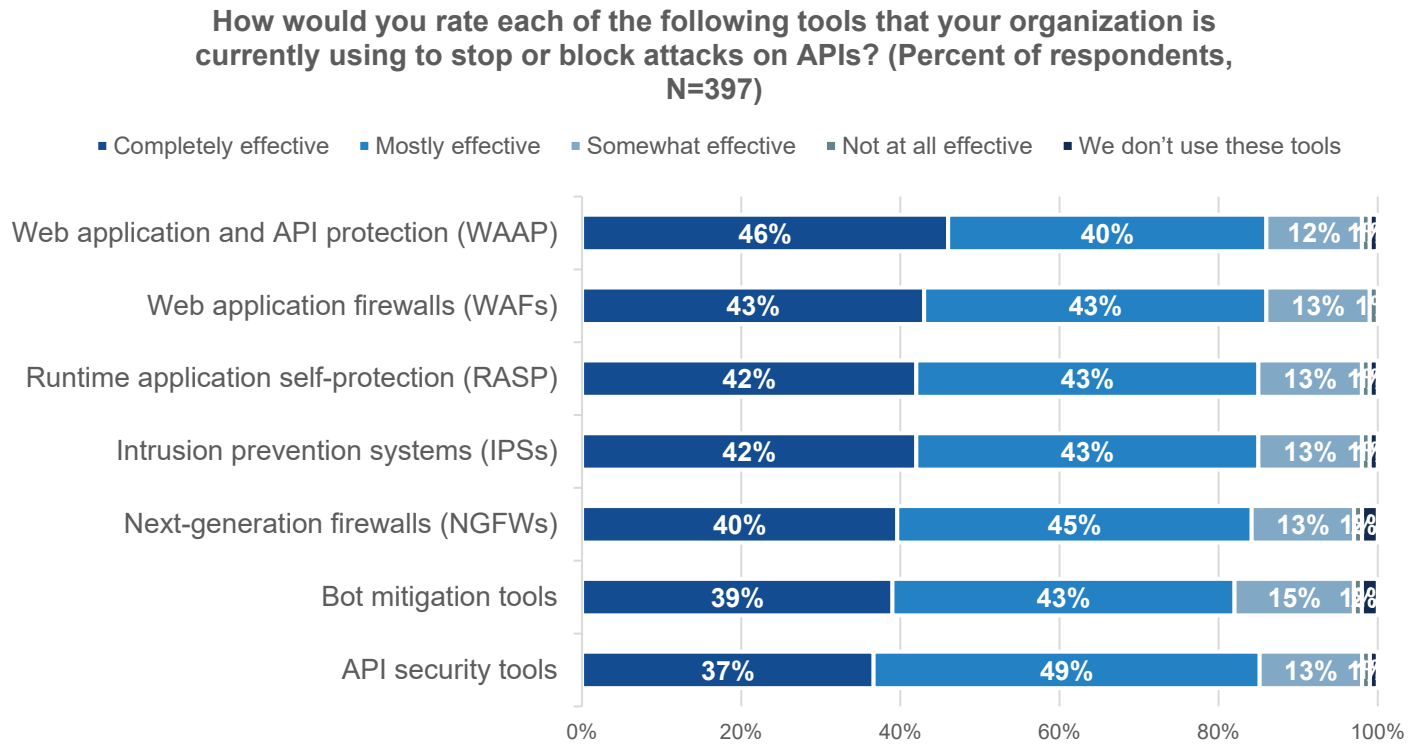
Figure 25. API Code Remediation with Application Security Tools



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

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 these tools as mostly or completely effective. Although the numbers are close, the highest rated was web application and API protection (WAAP), followed by web application firewalls (WAF), and runtime application self-protection (RASP) tools. WAAP combines four critical types of protection, WAF, DDoS mitigation, bot management, and API security, so it is interesting to see its growing usage and acceptance (see Figure 26).

**Figure 26.** Effectiveness of Tools in Stopping or Blocking Attacks on APIs

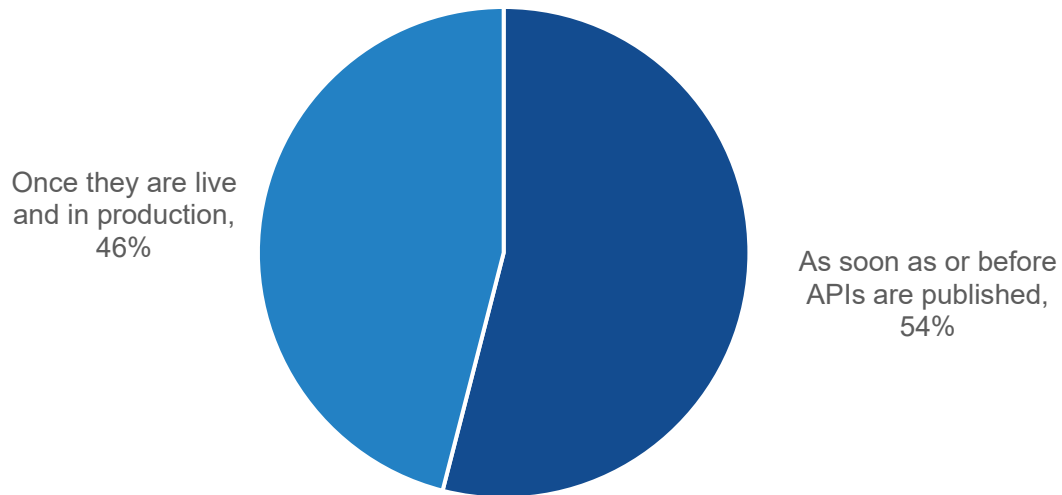


*Source: Enterprise Strategy Group, a division of TechTarget, Inc.*

To mitigate risk, security should be involved in securing APIs before they are deployed. So, while more than half (54%) of teams responsible for securing APIs are involved with development as soon as or before they are published, there is still a lot of room for improvement (see Figure 27). However, it is promising that the majority of organizations rate a high percentage of their developers as having either a good (22%) or high (71%) level of API security knowledge (see Figure 28).

Figure 27. Most Organizations Take a Proactive Approach to Securing APIs...

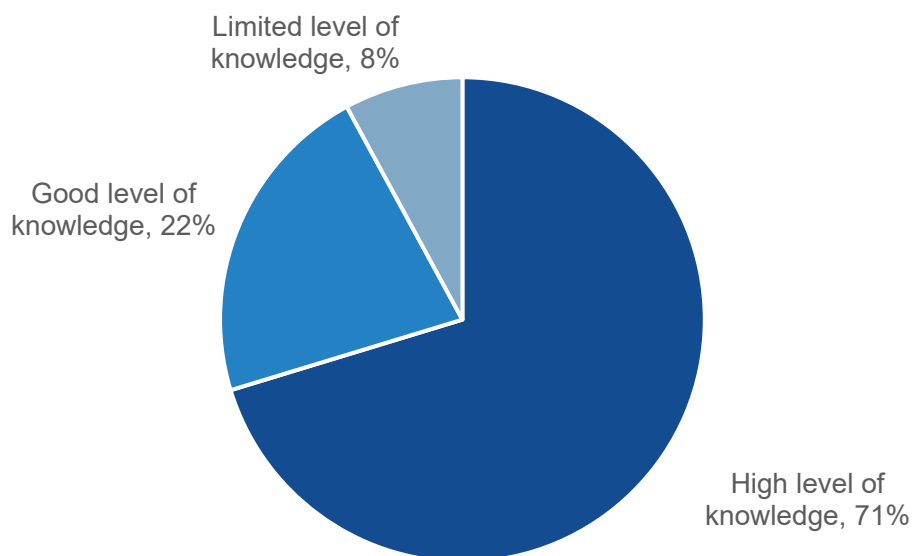
When new APIs are published, when does the team responsible for securing them become involved? (Percent of respondents, N=397)



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Figure 28. ...And Believe Their Developers Have a Solid Understanding of API Risk

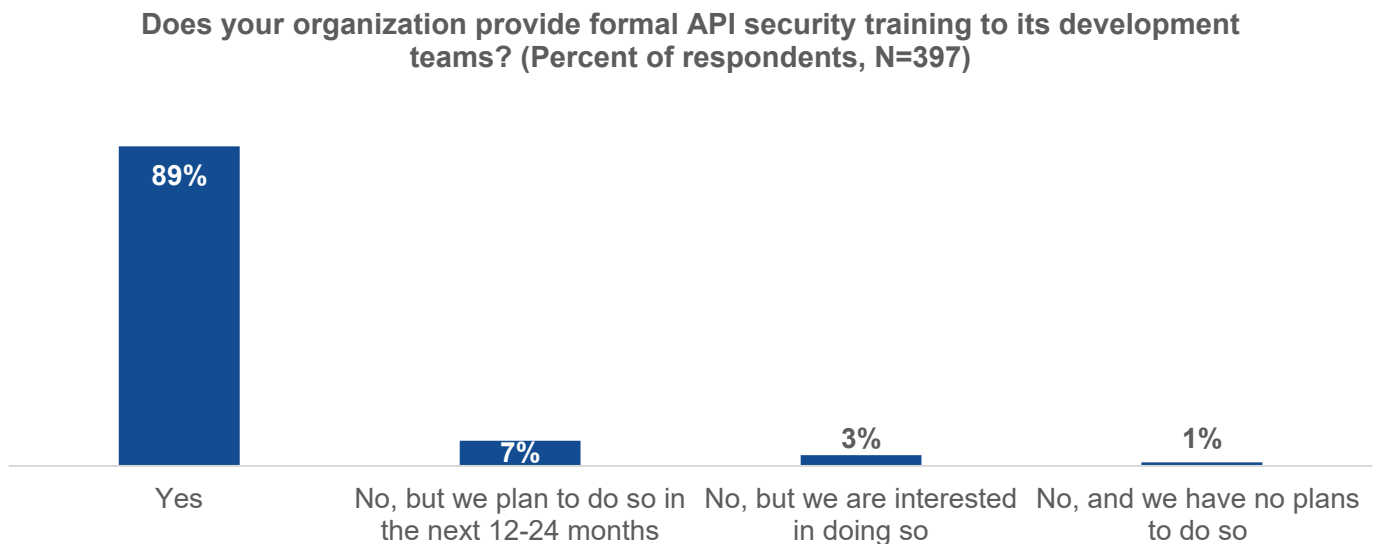
Generally speaking, how would you describe the collective level of understanding your organization's development teams have of security risks for APIs? (Percent of respondents, N=397)



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

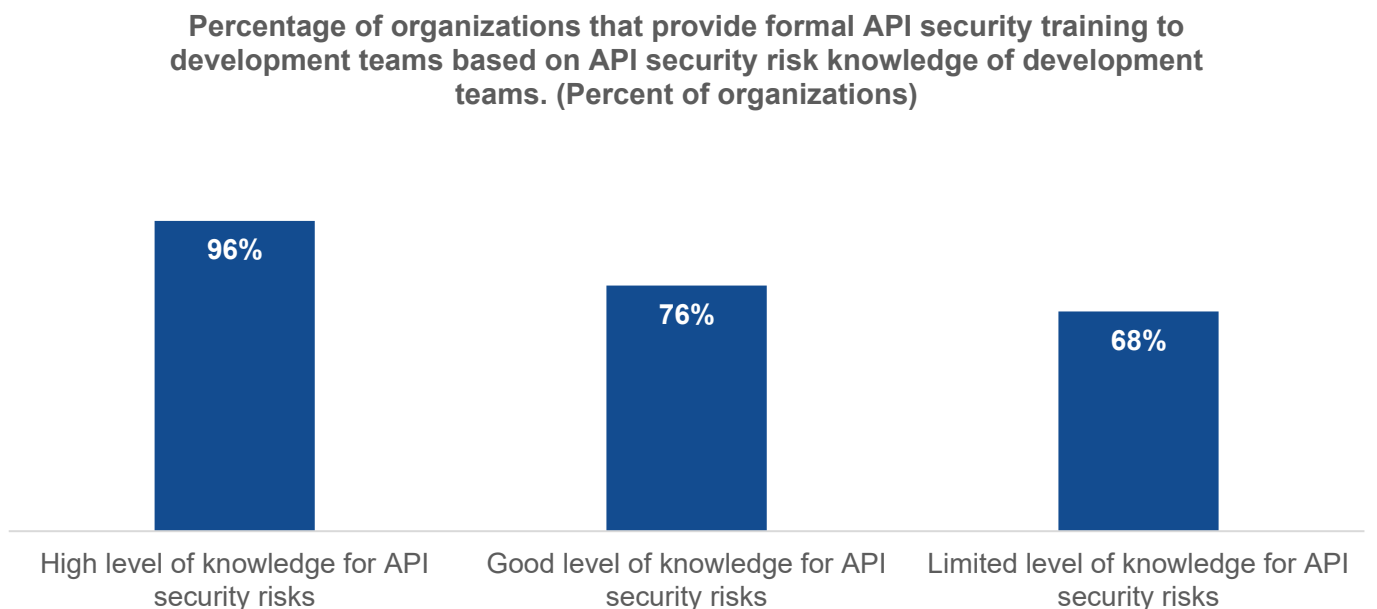
Overall, 89% of organizations provide formal API security training to their development teams (see Figure 29). However, there is a strong correlation between training and the level of awareness organizations believe their developers have with regard to API risk. Specifically, Figure 30 reveals that 96% of organizations that report their developers have a high level of knowledge about API risk provide formal API security training compared with only 68% of those citing limited levels of API security awareness.

**Figure 29.** Nearly All Organizations Provide Developers with Formal API Security Training...



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

**Figure 30.** ...Which Correlates to More API Risk-aware Developers



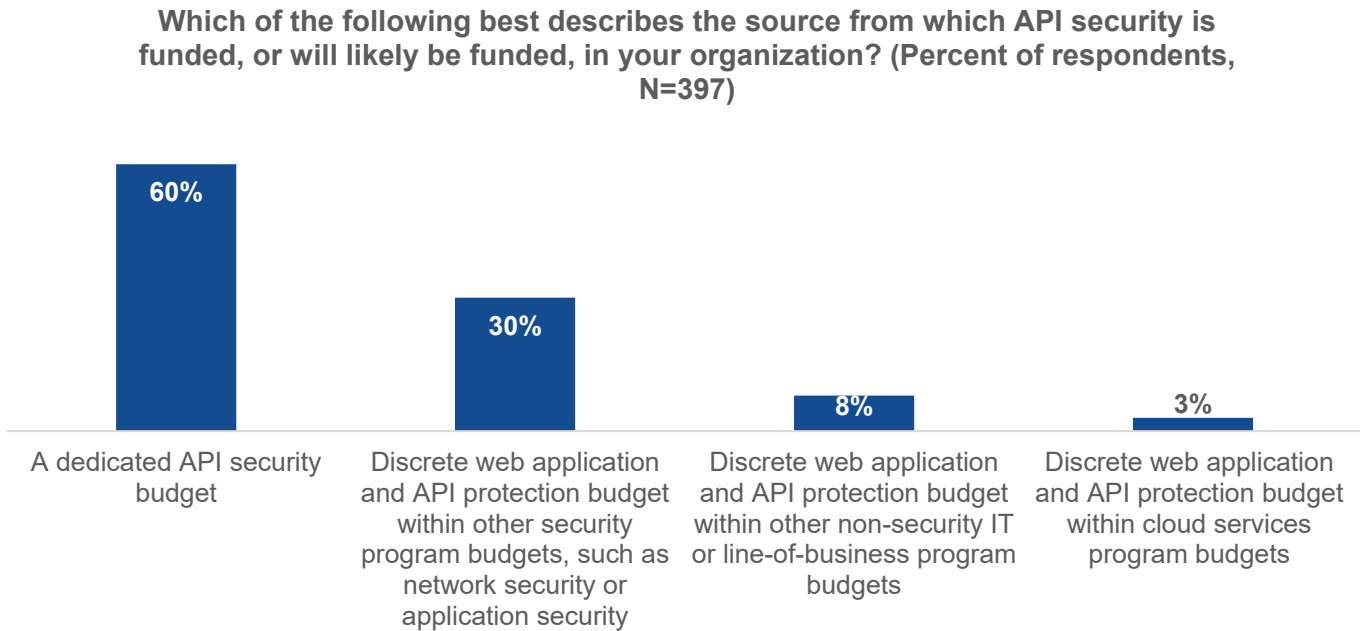
Source: Enterprise Strategy Group, a division of TechTarget, Inc.



## Organizations Are Committed to and Investing in Solidifying API Security Posture

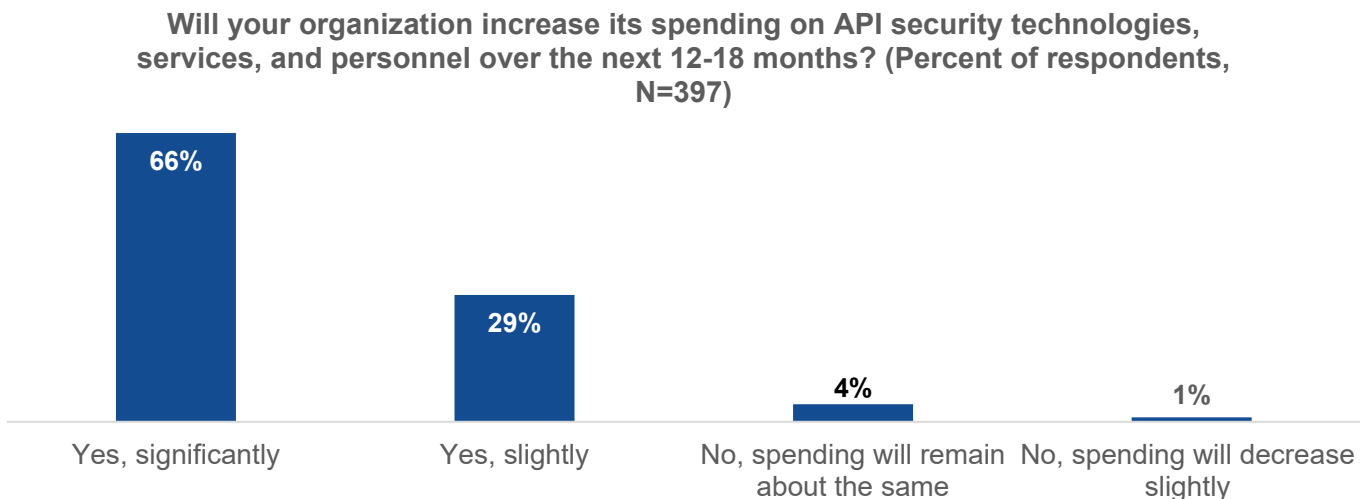
Organizations are prioritizing investing in API security because of its importance in enabling digital transformation. Indeed, Figure 31 shows that most (60%) organizations have a dedicated budget for API security, and 95% expect to increase their investments in API security solutions to some extent over the next 12-18 months (see Figure 32).

**Figure 31.** Most Organizations Report Having a Dedicated API Security Budget...



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

**Figure 32.** ...And Expect API Security Spending to Increase over the Next 12-18 Months

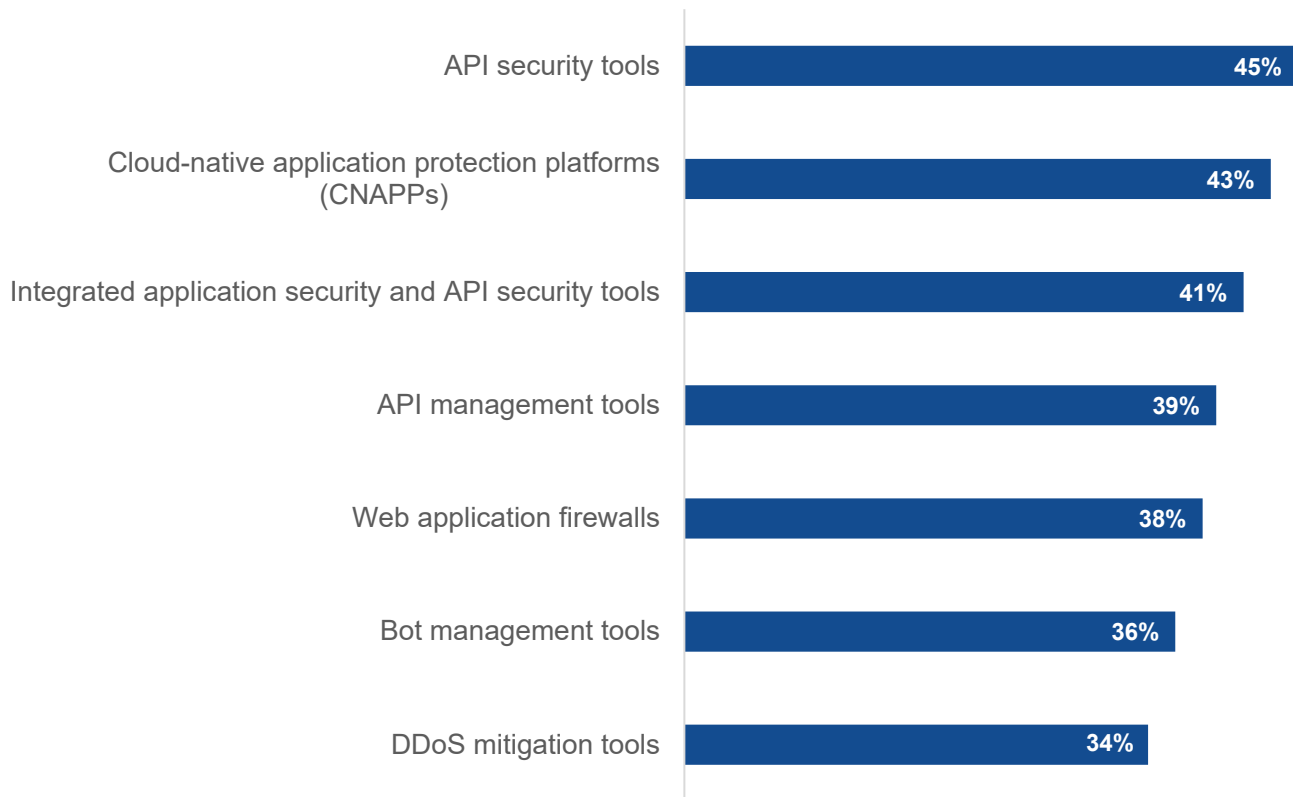


Source: Enterprise Strategy Group, a division of TechTarget, Inc.

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 (see Figure 33).

**Figure 33.** Areas of Expected Increased API Security Spending

**On which of the following do you expect your organization to increase its spending the most over the next 12-18 months? (Percent of respondents, N=378, multiple responses accepted)**



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

What steps do organizations anticipate taking to optimize their web application and API protection strategies over the next 12-18 months? The plurality of organizations anticipates building a holistic cloud application security strategy that covers both on- and off-premises cloud deployments (see Figure 34). Other common actions include working with MSPs to manage cloud application and API security (37%) and incorporating more automation between security and application development teams (36%). 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.

**Figure 34.** The Importance of API Security for Cloud Security Optimization



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

## Conclusion

This research shows the growing usage of APIs in software applications and the need to secure and protect them. While APIs are powerful in enabling developers to build more dynamic applications with rich features by connecting to resources and other applications, every connection is a potential attack surface that needs to be secured. As most organizations have experienced incidents due to insecure usage of APIs, security teams are investing in API security solutions to ensure they can protect their software applications as development teams utilize APIs to expand their offerings for increased business growth. What's needed? ESG recommends the following key considerations for an effective approach to API security:

- Collaborate with development teams.** The research shows that application security objectives are aligned with development and operations goals, including ensuring application uptime and customer service, meeting compliance regulations, controlling costs, protecting brand reputation, and securing user data. As developers increasingly use APIs in different ways to augment their applications, it's important that they are aware of security risk, and it's important to incorporate security as early as possible in development processes. The research showed 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 opportunity for earlier involvement. Awareness and training are also important, as the research showed the correlation between formal API security training programs and higher levels of API security risk knowledge.

- **Gain full visibility of APIs with inventory and tracking.** With the proliferation of APIs as development scales with faster, more frequent releases, it can be easy to lose track of the APIs, increasing exposure to attacks. The research showed 25% of organizations are challenged by keeping accurate inventories of APIs. A majority of organizations are concerned about the security risk of shadow/undiscovered APIs (87%) and outdated/unneeded (zombie) APIs (87%). Organizations should look for solutions that can give them full visibility to discover and track APIs to effectively manage their security.
- **Drive efficient remediation of API security issues.** For security to support increasing product releases that add functionality and services to their applications via frequent updates, they need to speed remediation to respond quickly to vulnerabilities or incidents. The data shows that more than two-thirds can respond within a day, with 39% reporting the ability to respond within hours. When applications are running in the cloud with vulnerabilities exposing 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. This is not sustainable. Security teams need fewer tedious manual tasks and solutions that can automate alerting to drive efficient actions for rapid remediation.
- **Look for a comprehensive solution.** An effective API security program requires a comprehensive set of features and capabilities that span the software development lifecycle to proactively mitigate risk and to ensure rapid response to an incident. The research shows that organizations are looking for a wide range of capabilities to address their current challenges, including API identification and tracking, API authentication, and ways to block attacks or excessive traffic. Identifying APIs with sensitive data was cited as a very important capability of an API security offering, as it would minimize the time and manual efforts necessary to gain the context needed to prioritize actions to protect sensitive company, partner, or customer data.

## About Graylog

Graylog elevates cybersecurity and IT operations through its comprehensive SIEM, Centralized Log Management and API Security solutions. Graylog provides the edge in Threat Detection & Incident Response across diverse attack surfaces. The company's unique blend of AI/ML, advanced analytics and intuitive design makes cybersecurity smarter, not harder. Graylog is also ideal for troubleshooting daily IT performance and availability issues. Unlike competitors' complex, costly setups, Graylog offers both power and affordability, simplifying the IT and security challenge. Founded in Hamburg, Germany and now headquartered in Houston, Texas, Graylog solutions are deployed in more than 50,000 installations across 180 countries. Learn more at [Graylog.com](https://graylog.com), or connect with us on [X \(Twitter\)](#) and [LinkedIn](#).



LEARN MORE

## Research Methodology

To gather data for this report, Enterprise Strategy Group conducted a comprehensive online survey of IT, cybersecurity, and application development professionals from private- and public-sector organizations in North America (United States and Canada) between March 9, 2023 and March 14, 2023. To qualify for this survey, respondents were required to be personally responsible for evaluating, purchasing, and utilizing API security solutions. 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.

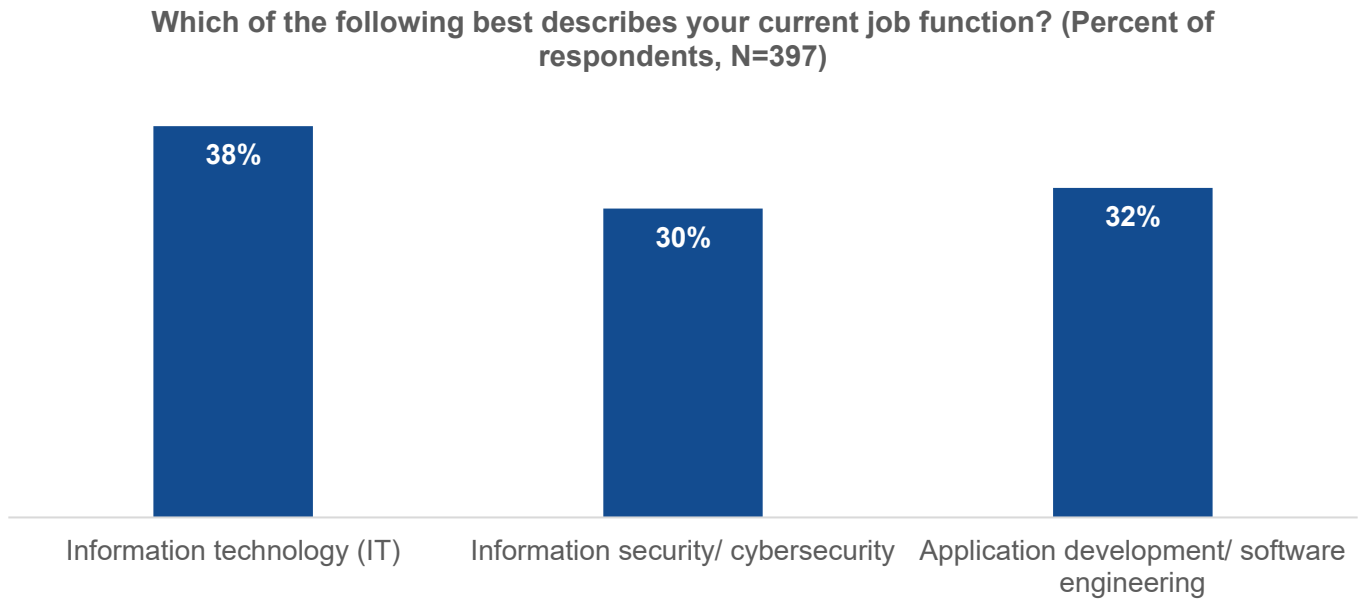
Please see the *Respondent Demographics* section of this report for more information on these respondents.

Note: Totals in figures and tables throughout this report may not add up to 100% due to rounding.

## Respondent Demographics

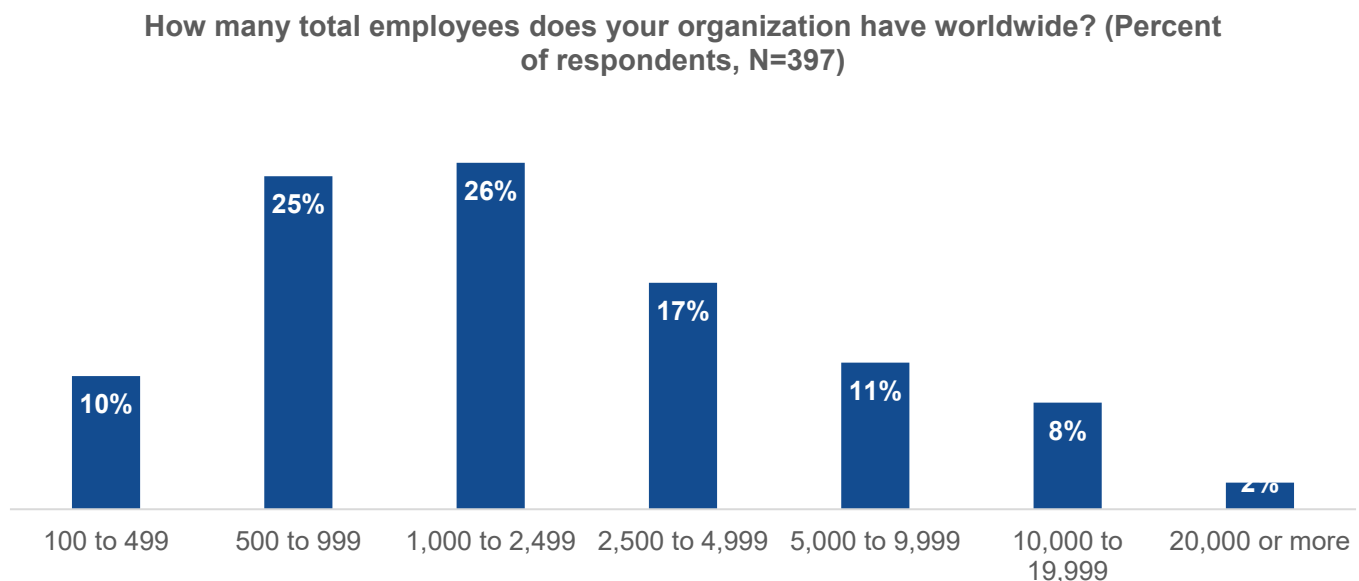
The data presented in this report is based on a survey of 397 qualified respondents. Figure 35 through Figure 38 detail the demographics of the respondent base at an individual and organizational level.

**Figure 35.** Respondents by Job Function



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

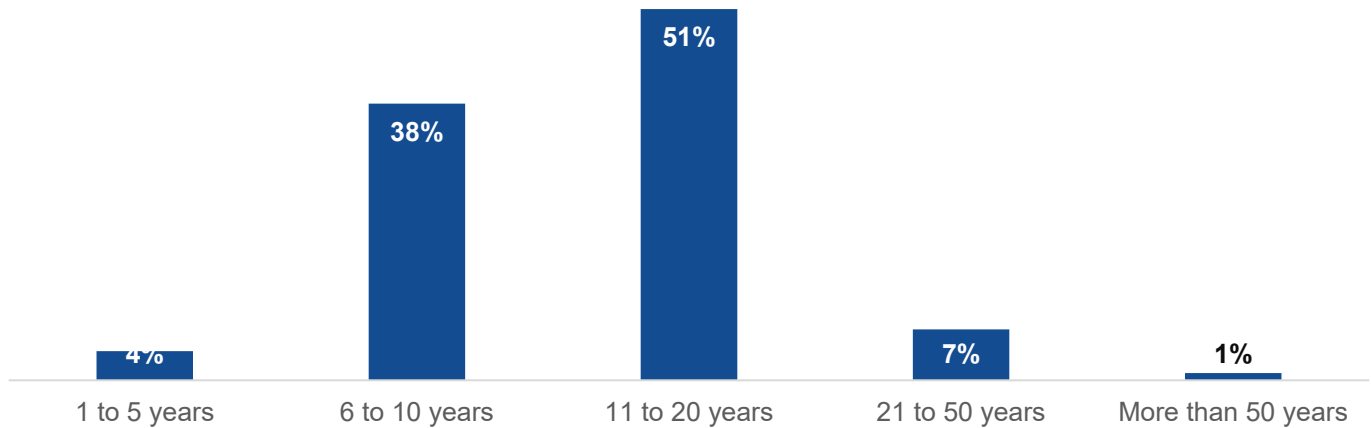
**Figure 36.** Respondents by Number of Employees



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

**Figure 37.** Respondents by Age of Organization

**For approximately how long has your current employer been in existence?  
(Percent of respondents, N=397)**

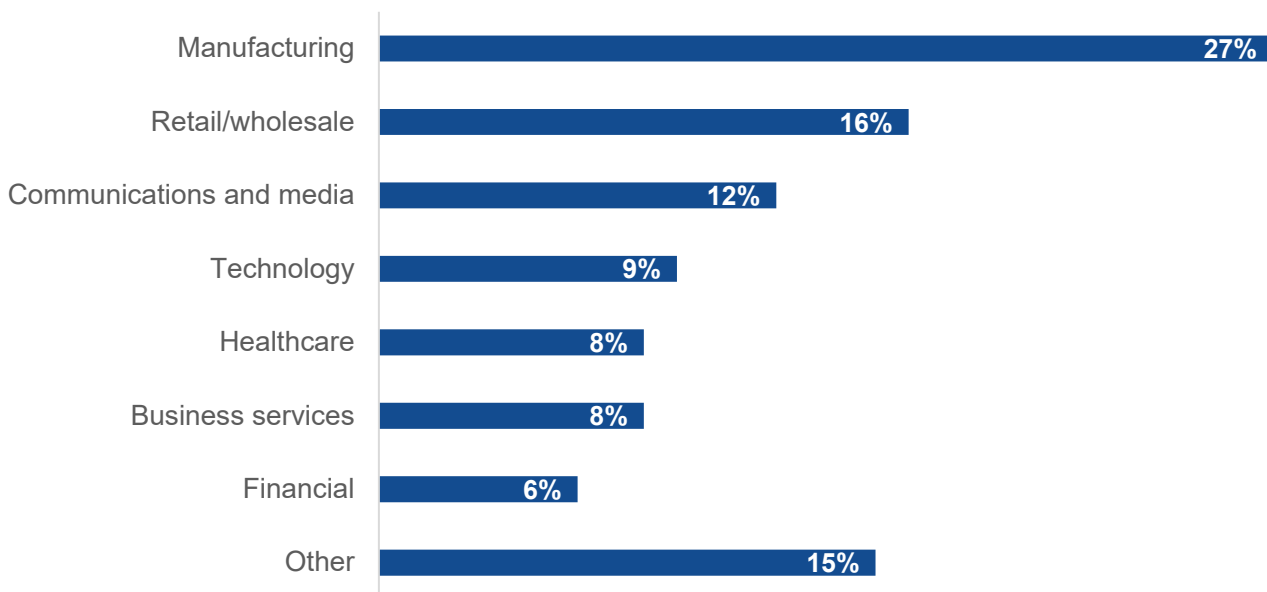


Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Respondents were asked to identify their organization’s primary industry. In total, ESG received completed, qualified responses from individuals in 21 distinct vertical industries. Respondents were then grouped into the broader categories shown in Figure 38.

**Figure 38.** Respondents by Industry

**What is your organization’s primary industry? (Percent of respondents, N=397)**



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

©TechTarget, Inc. or its subsidiaries. All rights reserved. TechTarget, and the TechTarget logo, are trademarks or registered trademarks of TechTarget, Inc. and are registered in jurisdictions worldwide. Other product and service names and logos, including for BrightTALK, Xtelligent, and the Enterprise Strategy Group might be trademarks of TechTarget or its subsidiaries. All other trademarks, logos and brand names are the property of their respective owners.

Information contained in this publication has been obtained by sources TechTarget considers to be reliable but is not warranted by TechTarget. This publication may contain opinions of TechTarget, which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent TechTarget's assumptions and expectations in light of currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, TechTarget makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.


Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of TechTarget, is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact Client Relations at [cr@esg-global.com](mailto:cr@esg-global.com).

---

#### **About Enterprise Strategy Group**

TechTarget's Enterprise Strategy Group provides focused and actionable market intelligence, demand-side research, analyst advisory services, GTM strategy guidance, solution validations, and custom content supporting enterprise technology buying and selling.

 [contact@esg-global.com](mailto:contact@esg-global.com)

 [www.esg-global.com](http://www.esg-global.com)