

Balancing Requirements for Application Protection:

Teams Desire Consolidation
but Need Specialized Protection

John Grady | Principal Analyst

ENTERPRISE STRATEGY GROUP

JANUARY 2025

Research Objectives

Application environments are more complex than ever, with web applications increasingly cloud-resident, containerized, connected via APIs, and delivered via CDNs. On top of this increasingly heterogeneous environment, security responsibility is distributed across a variety of roles and personas. This has resulted in complexity and tool sprawl as security teams struggle to keep pace. Attackers use this to their advantage through exploits against known vulnerabilities and advanced campaigns that use a variety of tactics, such as bots, that amplify denial-of-service and credential attacks on web applications and the APIs that tie them together. While platforms are attractive, security cannot be compromised. Security leaders need to understand the actions that forward-thinking organizations have undertaken to properly assess which tools are best positioned to solve the key business challenges they face.

To gain insights into these trends, TechTarget’s Enterprise Strategy Group surveyed 383 IT and cybersecurity professionals in North America (US and Canada) involved with securing their organization’s web applications and APIs.

This study sought to:

Determine how changing application environments have impacted security strategies and the challenges security teams face in navigating this transition.

Assess the collaboration across the teams responsible for application security, including fraud and loss-prevention teams when it comes to bot-based attacks.

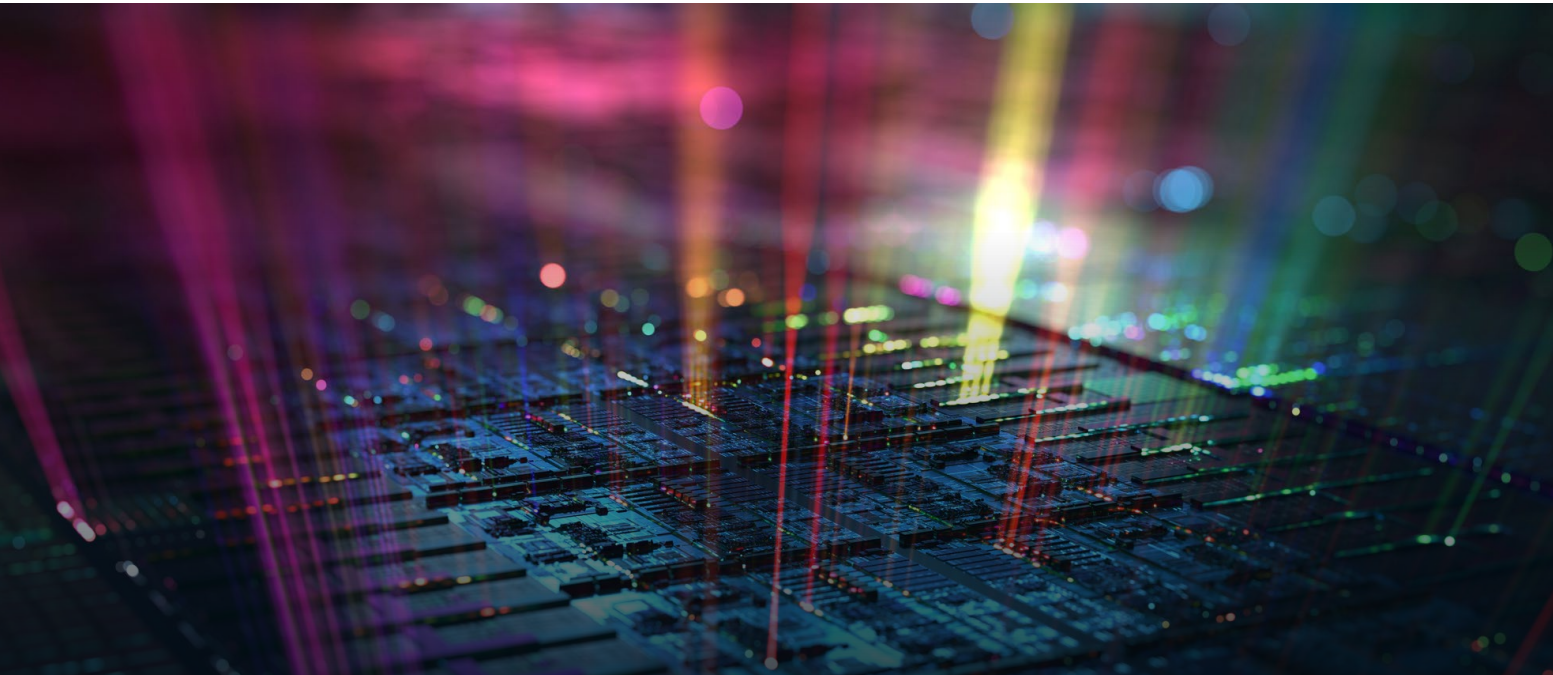
Understand the types and prevalence of web application, bot, and DDoS attacks as well as their impact on respondent organizations.

Highlight the key requirements buyers have for web application and API protection solutions.

Note: Totals in figures and tables throughout this eBook may not add up to 100% due to rounding or organizations choosing more than one answer to select questions.



Key Findings



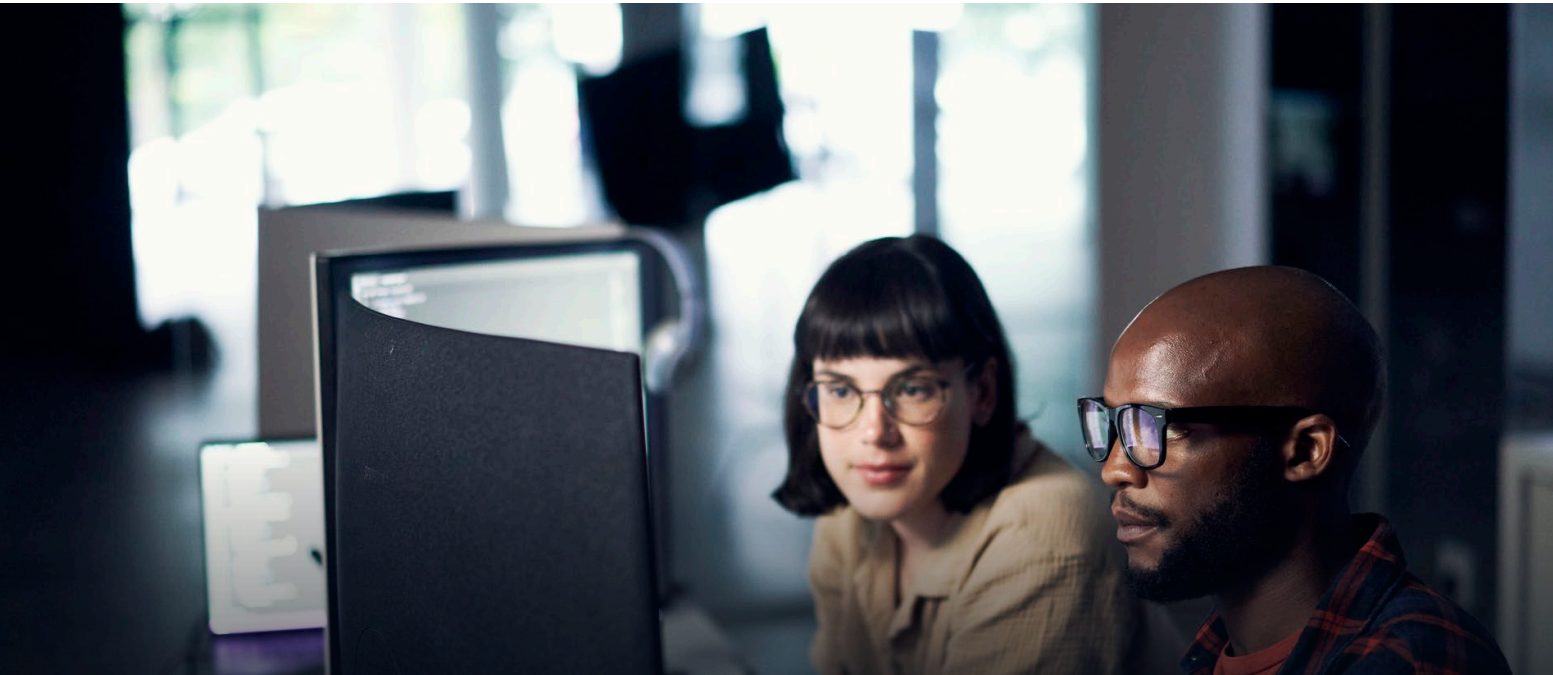
Application Environments Continue to Evolve, Opening the Door for Attacks

PAGE 4



Most Organizations Use Multiple WAFs but Are Interested in Consolidation

PAGE 9



Bot Incidents Are Varied, and Most Organizations Rely on Specialized Tools

PAGE 12



DDoS Attacks Vary, and Most Organizations Subsequently Use Multiple Forms of Protection

PAGE 17



Despite Bot and DDoS Tool Preferences, Application Protection Consolidation Is Desired

PAGE 21



Spending Intentions Appear Strong, but Focus Is Fragmented

PAGE 25

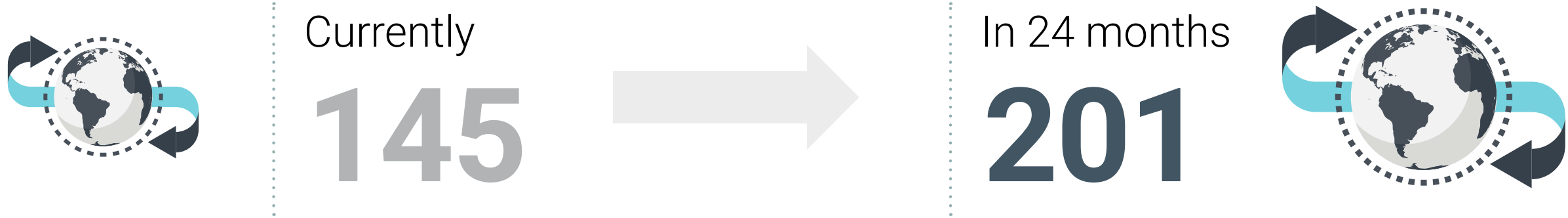


**Application Environments Continue to Evolve,
Opening the Door for Attacks**

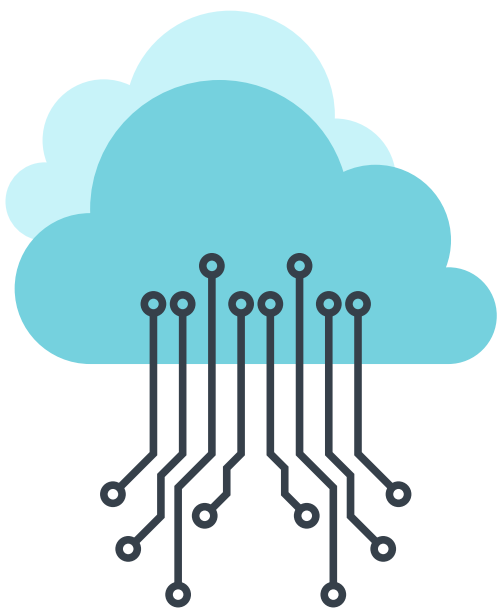
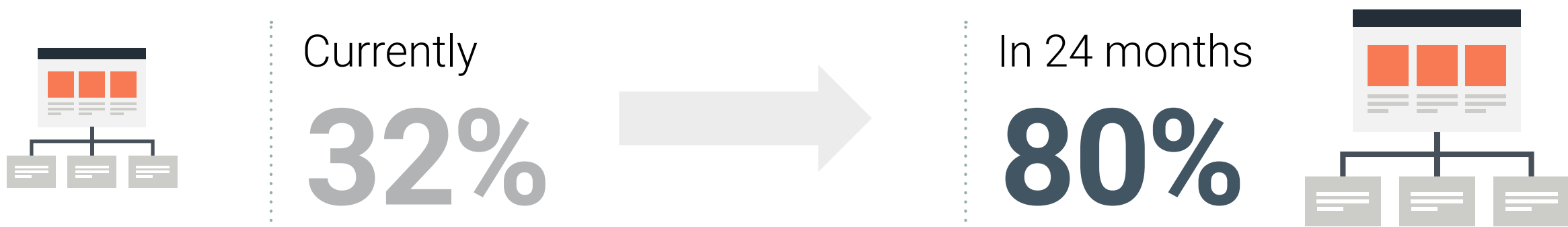
Web Application Environments Continue to Evolve

Web application environments continue to grow in scale and complexity. In fact, Enterprise Strategy Group research respondents support an average of 145 applications, with 88% saying they use two or more cloud service providers (CSPs). Additionally, the number of organizations noting that at least half their applications use APIs is expected to more than double (32% versus 80%) over the next two years.

Average web applications and websites per organization:



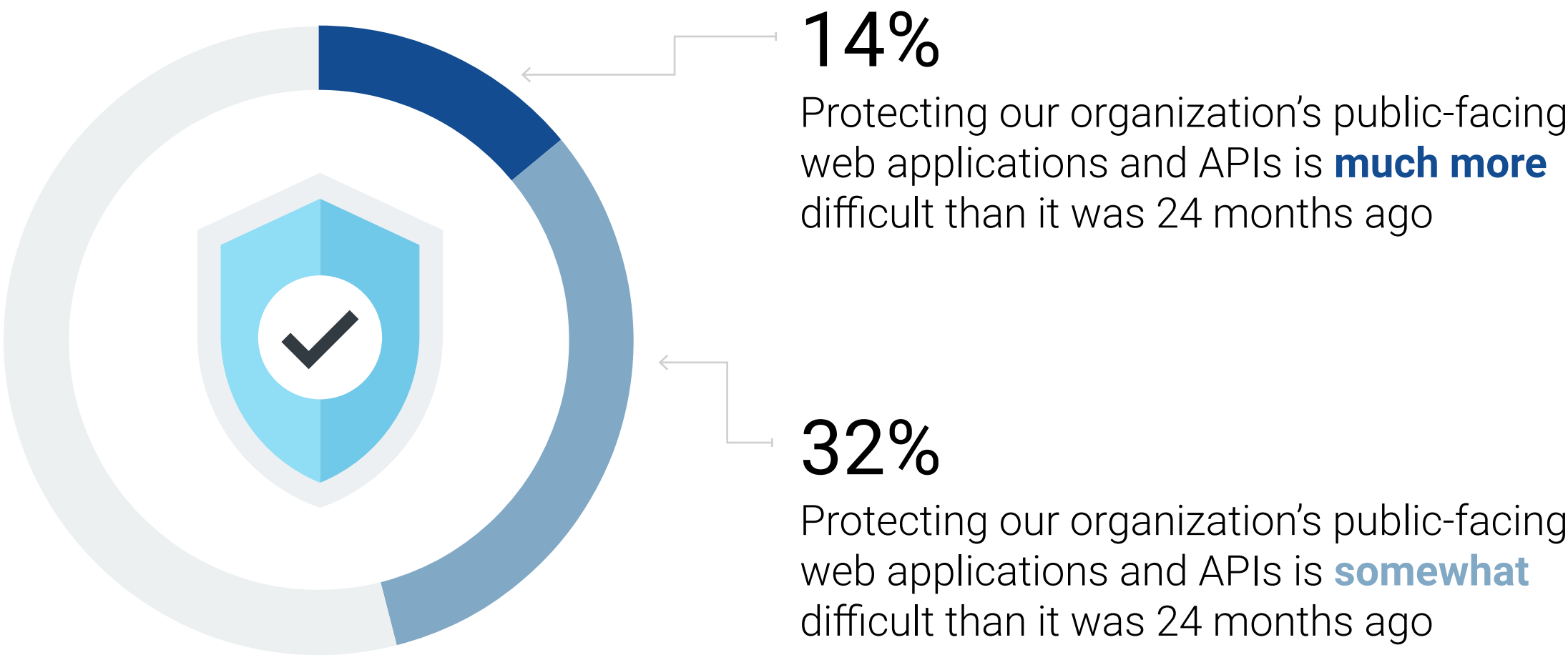
Organizations with at least half of applications using APIs:



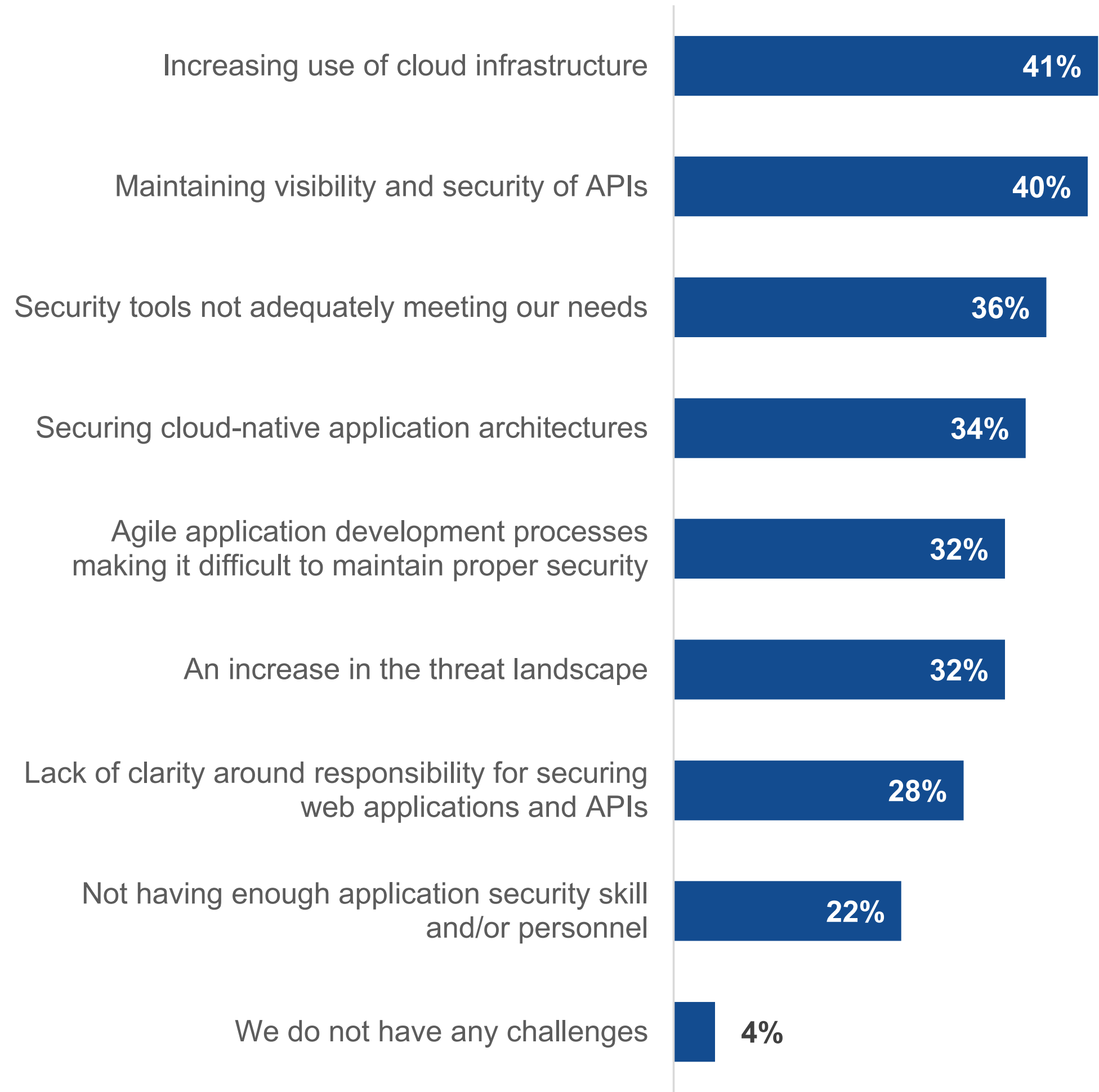
Changing Web Application Environments Commonly Contribute to Protection Challenges

Unfortunately, many of the changes in web application environments are creating issues for security teams. Nearly half (46%) say protecting web applications and APIs is more difficult than it was two years ago. Further, a variety of security challenges were cited by respondents, with many relating back to these environmental changes. The use of cloud infrastructure (41%), maintaining visibility and security of APIs (40%), and securing cloud-native architectures (34%) were all prominently cited.

Additionally, 36% indicated that security tools do not meet their needs, while 22% pointed to a lack of application security skill and/or personnel. Finally, the threat landscape itself remains a core concern, with 32% citing it as a challenge. All told, application security teams have a lot on their plate.



Public-facing web application security challenges.

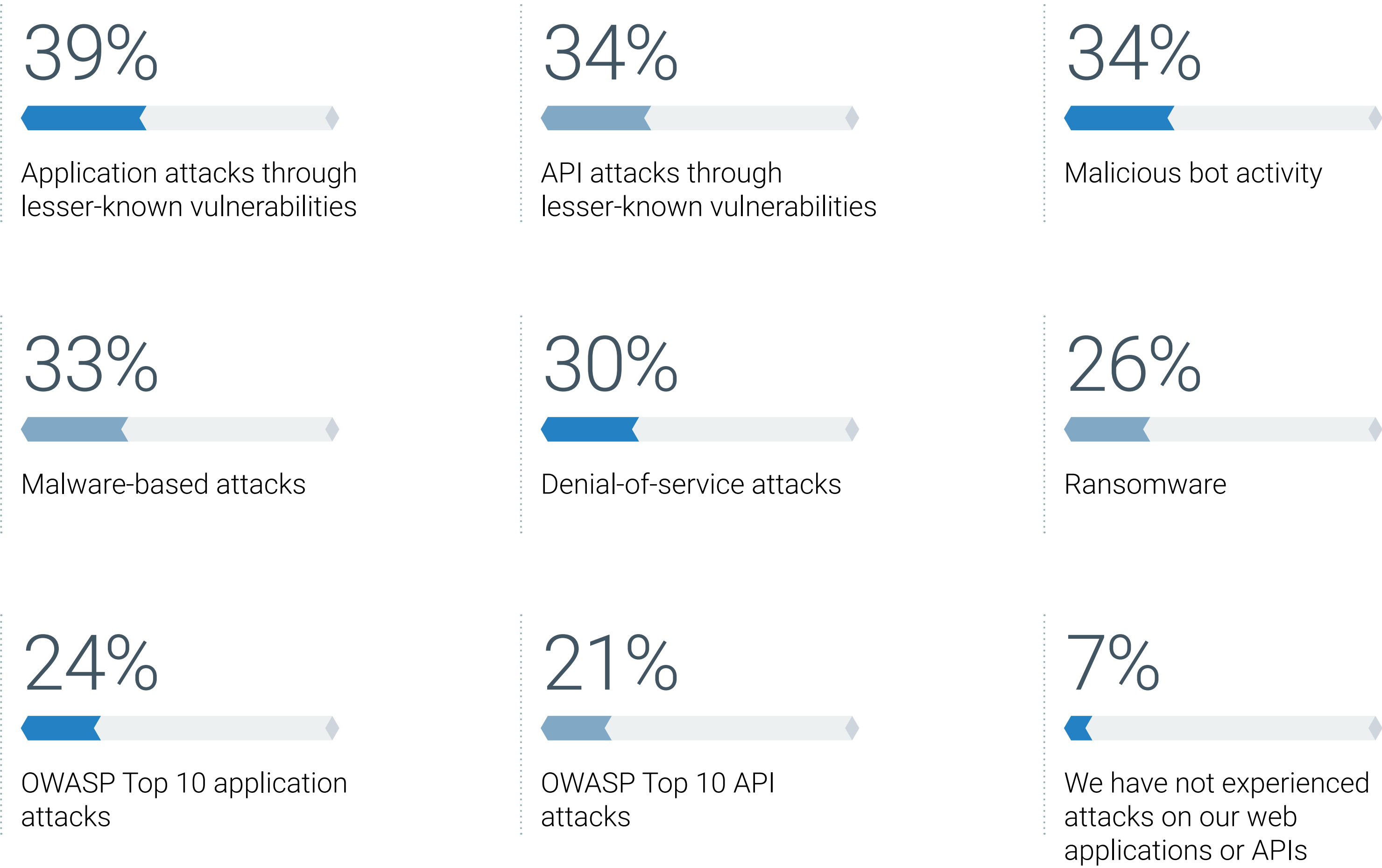


All Threat Vectors Are Being Exploited

Even more importantly, most organizations are experiencing attacks, and different types of attacks at that. Attacks on both applications and APIs via lesser-known vulnerabilities (rather than OWASP Top 10 attacks) were at the top of the list of experienced attacks, cited by 39% and 34% of respondents, respectively. Malicious bot activity was also reported by 34% of organizations, while 30% saw DoS attacks. Ransomware was also noted by 26% of organizations.

Ensuring proper protection against this wide-range of attack types can be difficult, especially for organizations that are resource constrained. Many attacks are multi-pronged. They may leverage bots to attack both APIs and the application itself or use DDoS as a diversionary tactic, making it impossible to focus solely on one threat vector at the expense of another.

Web application and API attacks experienced within the past two years.



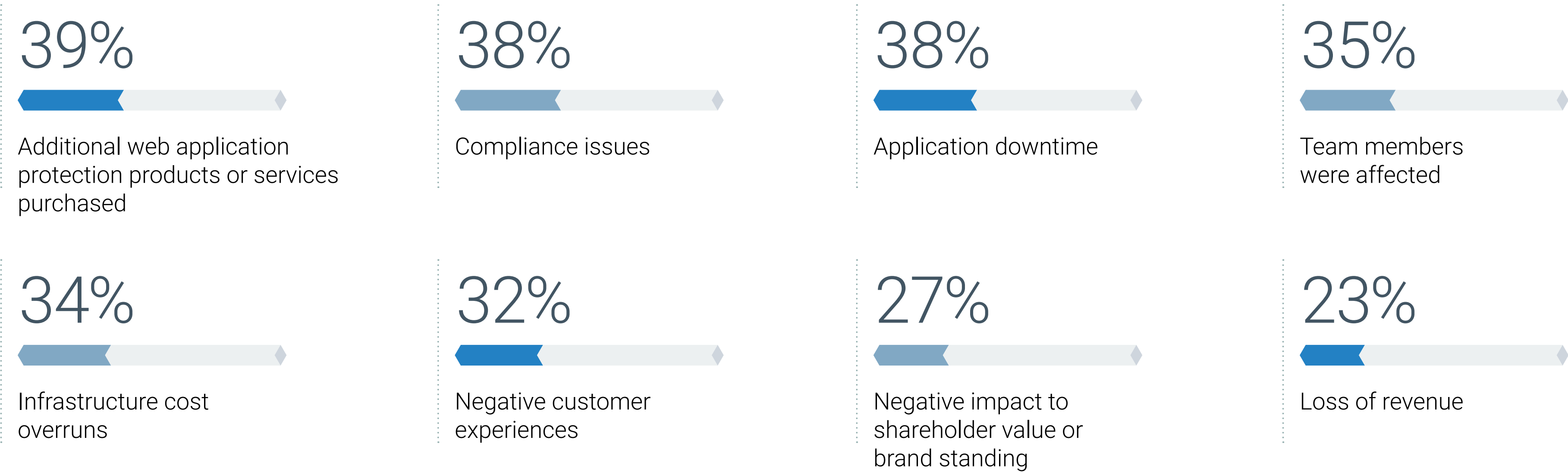
Attack Impacts Are Varied and Often Hit the Bottom Line

Worse yet, the impact from these attacks can be significant. While only 23% of respondents indicated a loss of revenue following an attack, impacts indirectly impacting the bottom line were common.

Specifically, 38% reported application downtime, 34% cited infrastructure cost overruns, 32% reported negative customer experiences, and 27% pointed to a negative impact to shareholder value or brand standing. Compliance issues (38%), personnel impacts (35%), and new tool purchases (39%) were also reported.

Security teams struggling to get buy-in from their IT and business counterparts on application security priorities should highlight these factors. Illustrating exactly how these scenarios can affect operations can help create urgency and bridge the gap between security and business priorities.

Impacts from attacks on web applications and APIs .



“Security teams struggling to get buy-in from their IT and business counterparts on application security priorities **should highlight these factors.**”



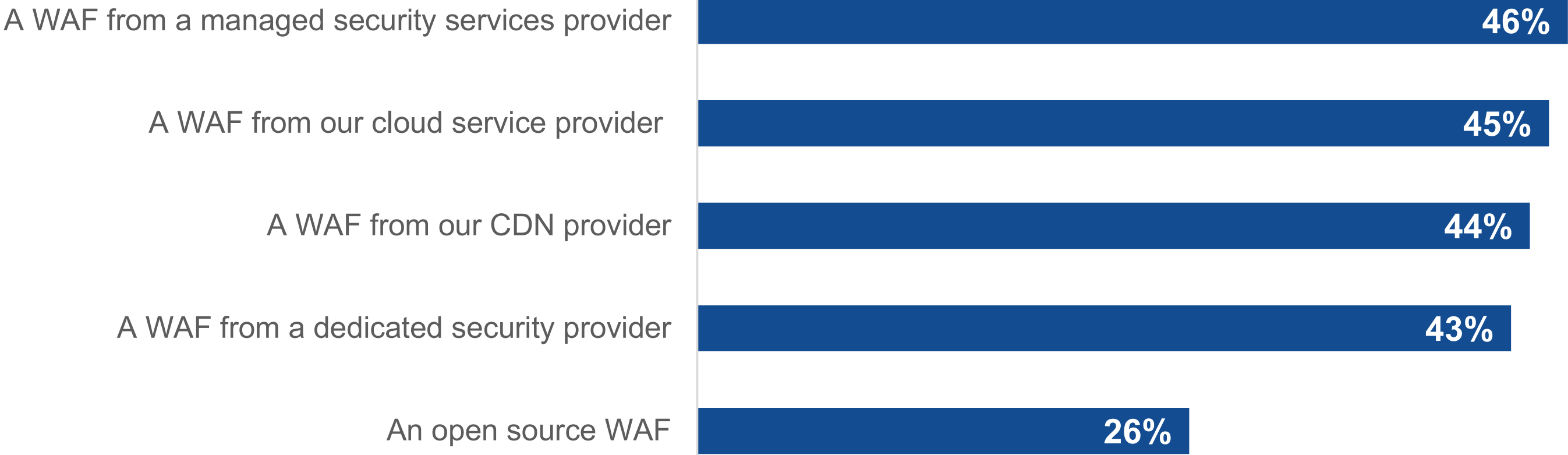
**Most Organizations Use Multiple WAFs
but Are Interested in Consolidation**

Most Use Multiple WAFs, Often Due to Environmental and Team Changes

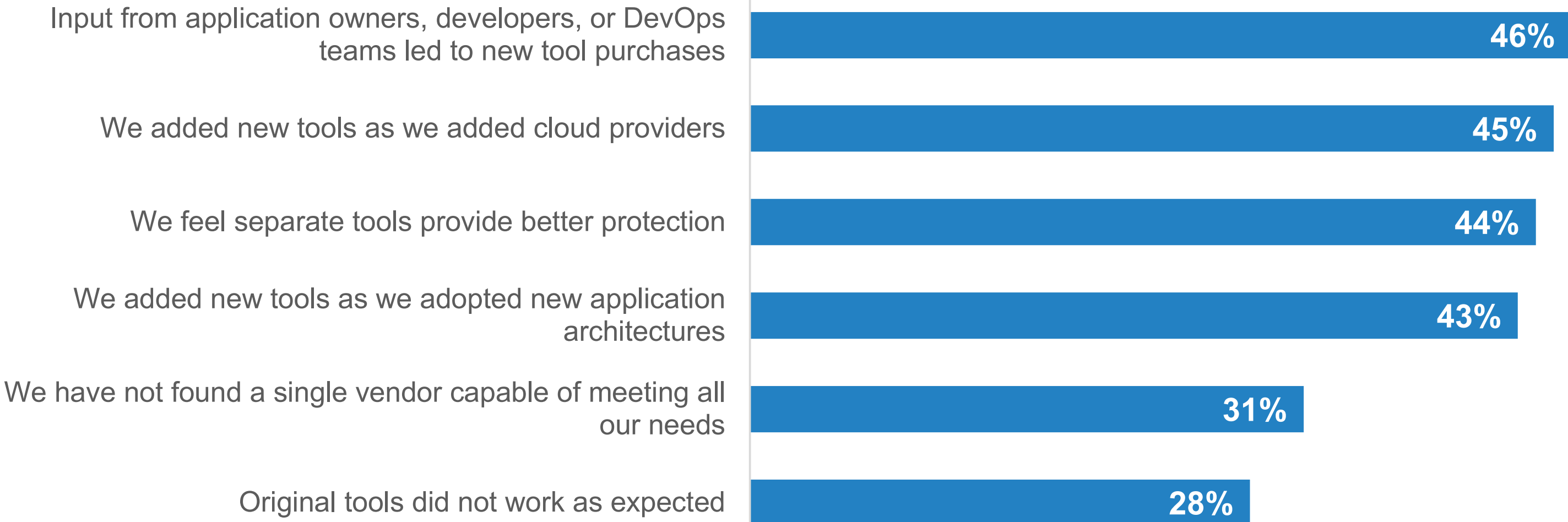
Web application firewalls remain the foundation for most organizations’ application security strategy to prevent attacks and address the challenges discussed earlier. Yet WAF sprawl appears to be a real issue. In fact, two-thirds of organizations (67%) said they use multiple WAFs. There was little difference in usage across managed security service providers (46%), CSPs (45%), CDNs (44%), and dedicated security provides (43%). Only open source WAFs showed comparatively less usage (26%).

While 44% of respondents indicated they use multiple tools because it provides better protection, many pointed to natural sprawl over time. This can come due to input from app owners and developers (46%), adding cloud providers (45%), or modernizing application architectures (43%). Many also pointed to tool deficiencies as a reason to use multiple WAFs. Nearly one-third (31%) said they had not found a single vendor able to meet their needs, while 28% said their original WAF did not work as expected.

Types of WAFs in use.



Reasons for using multiple WAFs.

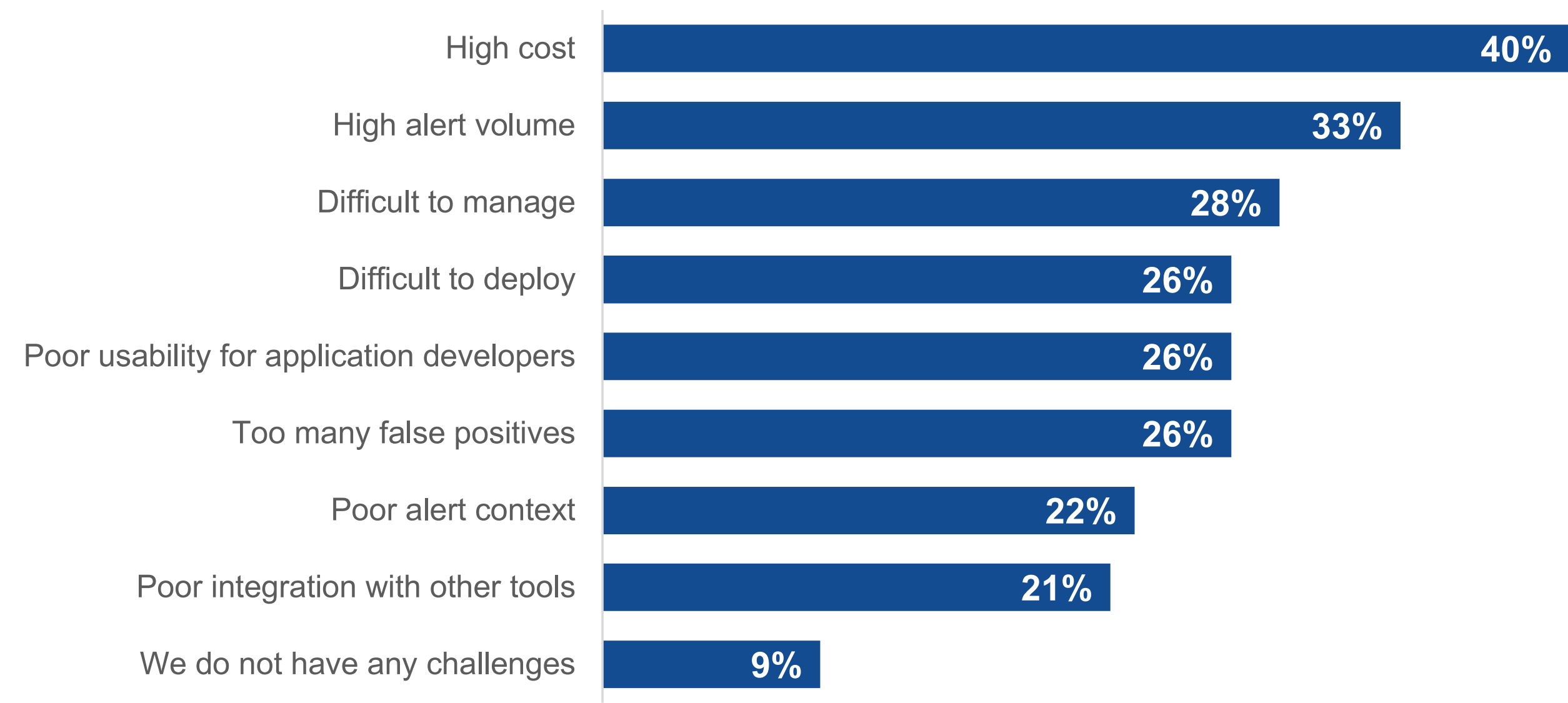


Security Teams Face a Variety of WAF Challenges

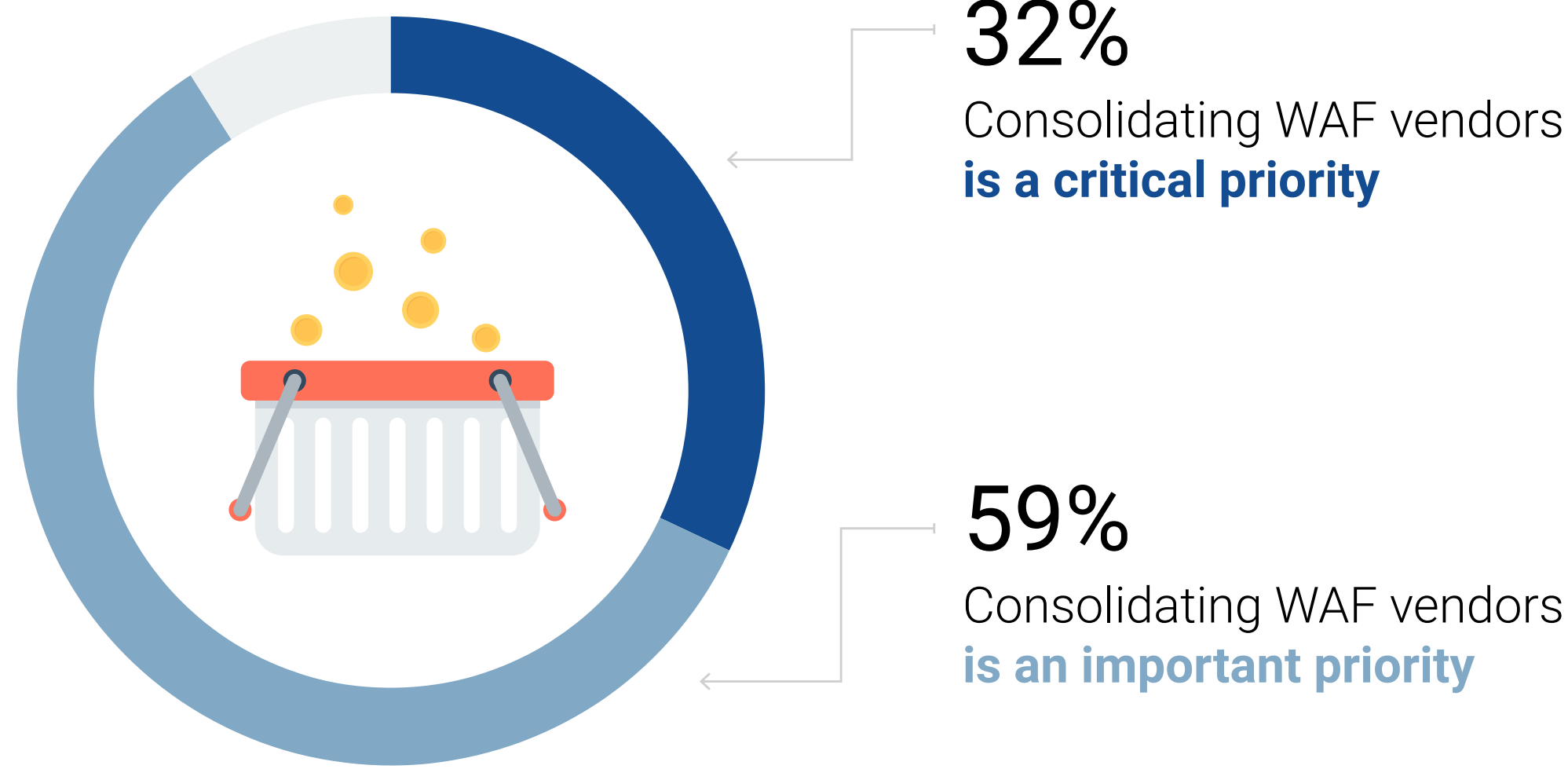
Even with multiple tools in place (or perhaps due to that fact), many respondents continue to identify WAF challenges. The most common issue cited was cost, which 40% of respondents selected. While the upfront cost of WAF tools is a major part of this, it also includes the ongoing operational costs. Many of the other challenges cited play into this, including high alert volumes (33%), management difficulty (28%), deployment issues (26%), and false positives (26%). Two other related issues noted were poor alert context (22%) and poor integration with other tools (21%). As noted earlier, with attackers increasingly using multi-pronged attacks, consistent visibility and the ability to correlate telemetry threat vectors becomes critical. Without that context and tool integration, security teams are at a disadvantage.

Due to all these factors, it should be no surprise that 91% of organizations say consolidating WAF vendors is a critical or important priority.

Web application firewall challenges.



Importance of consolidating WAF vendors.



A man and a woman are working together in an office. The man, in the foreground, is wearing glasses and a plaid shirt, looking at a computer monitor. The woman, behind him, is also wearing glasses and a light-colored top, looking at the same monitor. The office is dimly lit, with light coming from the monitors and windows in the background.

Bot Incidents Are Varied, and Most Organizations Rely on Specialized Tools

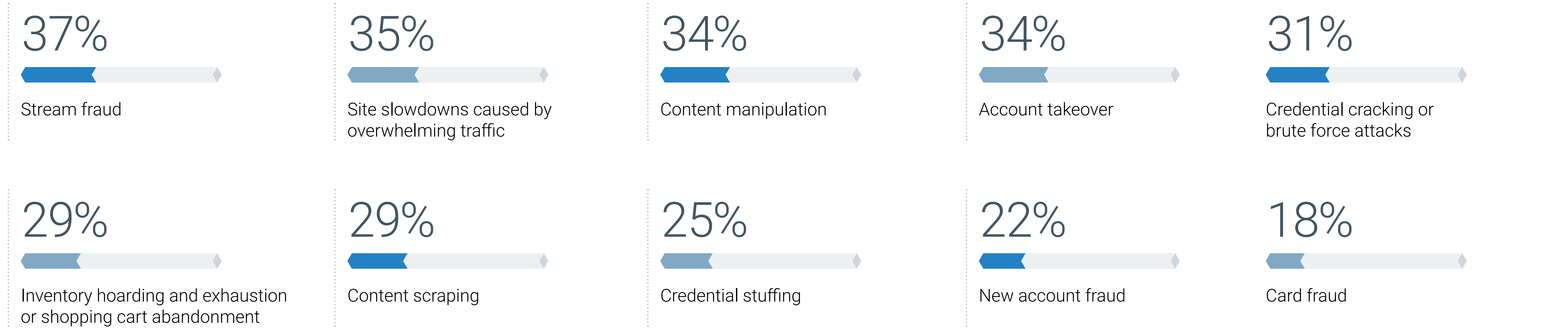
Bot Incidents Are Varied

Managing traffic and mitigating attacks generated by bots have been growing issues over the last few years. With attackers using sophisticated bots that more closely mimic human actions, it has become harder to differentiate legitimate from automated traffic.

Further, attackers can leverage bots in a variety of ways, leading to everything from availability issues to outright fraud. As shown earlier, more than a third of organizations have experienced malicious bot activity. Among those respondents, stream fraud was the most common issue seen from bots (37%), followed by site slowdowns (35%) and content manipulation (34%).

Identity attacks were also common with account takeover (34%), credential cracking or brute force attacks (31%), credential stuffing (25%), and new account fraud (22%) all reported.

Types of bot activity experienced in the past two years.

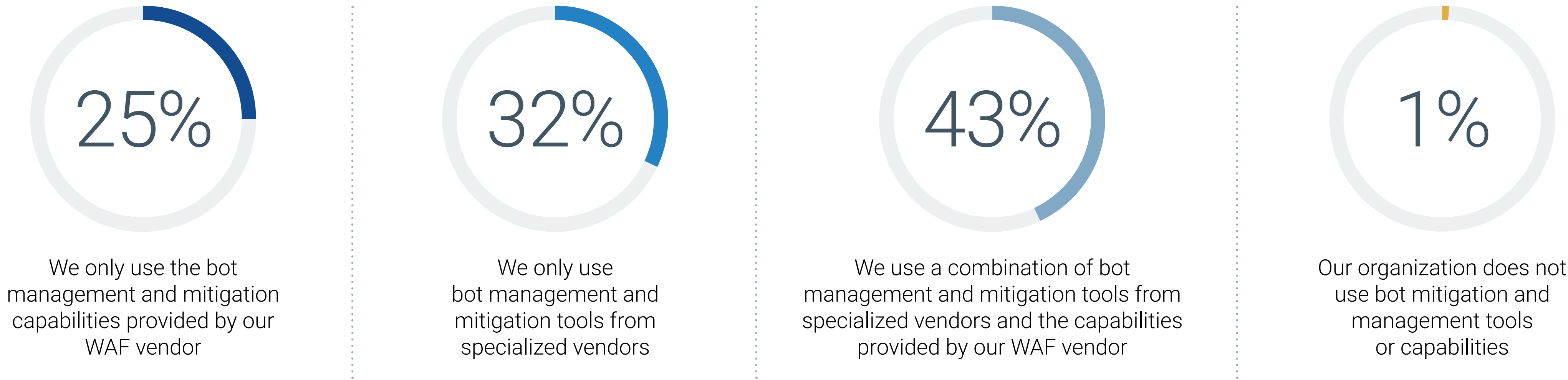


Most Are Turning to Specialized Bot Management Tools

Security teams have multiple options to combat these bot-related issues. Many WAF vendors offer bot control of some kind as part of their solution, though the nature of the capabilities can vary widely. On the other end of the spectrum, specialized bot management and mitigation tools are available that serve not only cybersecurity teams but also fraud and loss-prevention teams.

Among respondents, a quarter indicated they use only the bot management capabilities from their WAF vendor and 32% use only specialized bot management tools, while 43% use a combination of the two approaches. As the diversity and sophistication of bot activity increases, strong efficacy and the ability to granularly control mitigation becomes even more important.

Approaches to bot management.

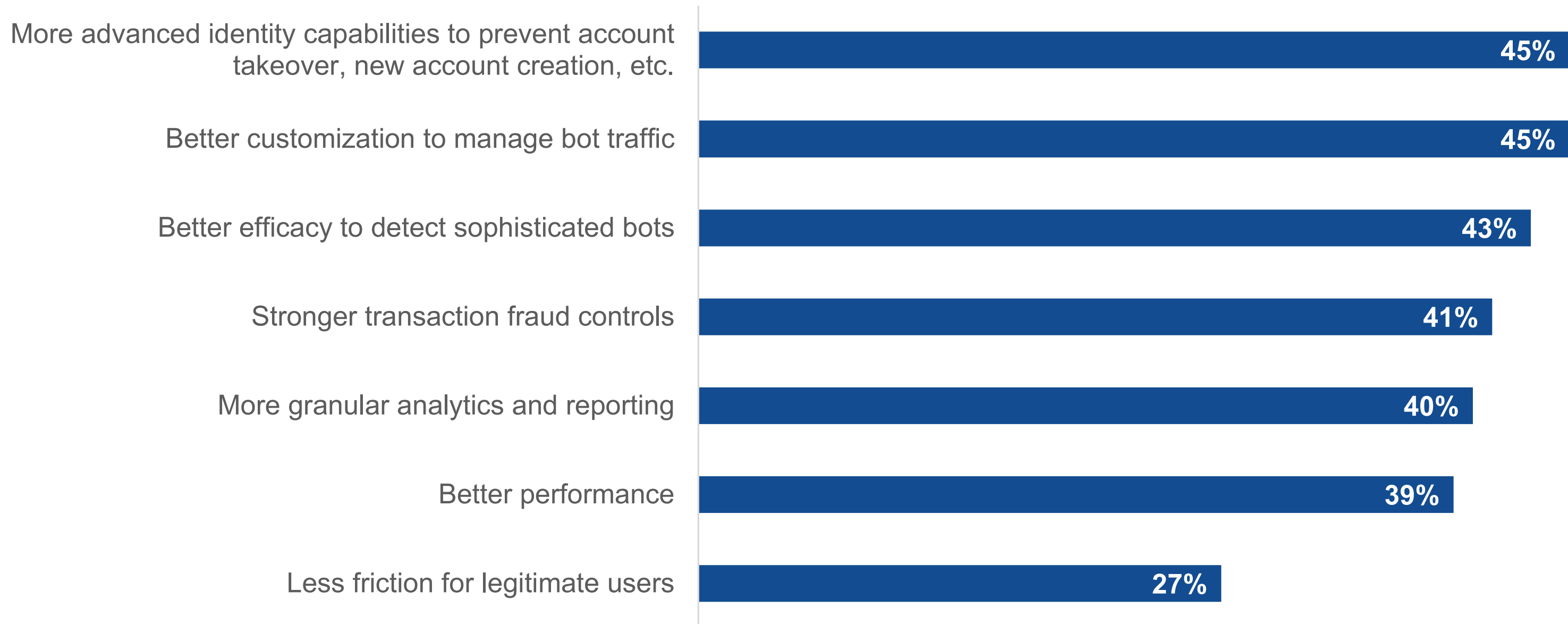


Reasons to Use Specialized Bot Solutions

The organizations relying on specialized bot management solutions cite a variety of reasons for doing so. Nearly half (45%) feel they provide more advanced capabilities to address the variety of identity attacks previously discussed. Similarly, 45% believe they provide better customization to manage bot traffic, which is an important factor as it is not always desirable to immediately block automated traffic. Some bots such as web crawlers are legitimate, and even in cases of malicious bots, giving away the fact that they have been detected too early in the cycle can give attackers an advantage.

Better efficacy (43%), more granular analytics and reporting (40%), and better performance (39%) were also mentioned. Interestingly, less friction for legitimate users was only noted by 27% of respondents, perhaps indicating that users feel that bot capabilities in WAFs can provide comparable results on this front.

Reasons for using specialized bot management tools.



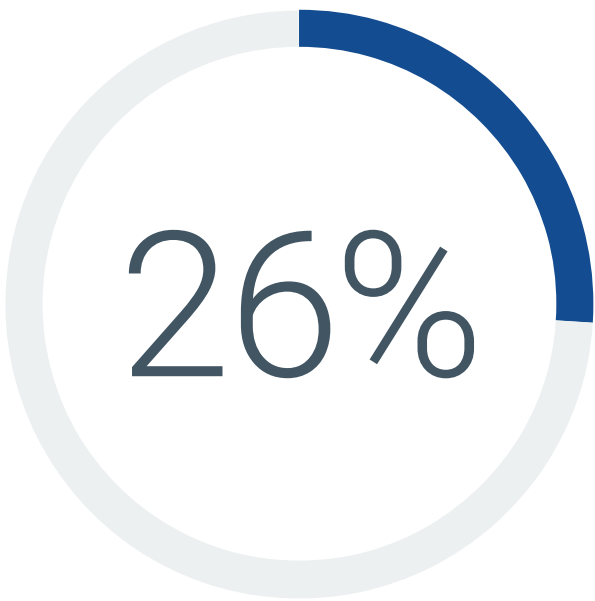
“Some bots such as web crawlers are legitimate, and even in cases of malicious bots, giving away the fact that they have been detected too early in the cycle **can give attackers an advantage.**”

Nearly Half Use Bot Features in Their WAF Simply Because They're There

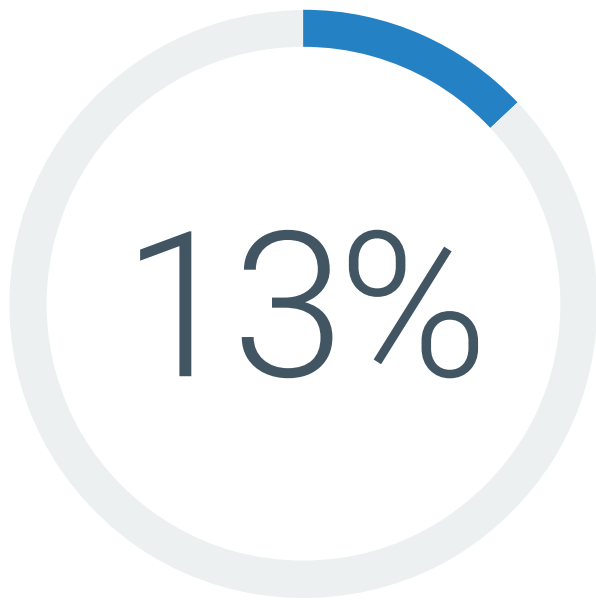
Those organizations using both specialized solutions and the bot capabilities in their WAF were asked why they use multiple tools. Just more than one-quarter (26%) said they do so for a layered approach to provide strong protection, while only 13% said different teams prefer different solutions for certain bot issues. Some respondents are in a transition period, with 17% saying they are in the process of consolidating, but it takes time.

But the most common response was that integrated bot capabilities in the WAF are used because they are available. This indicates that while many are using those capabilities, they may not be relying on them as heavily as specialized tools.

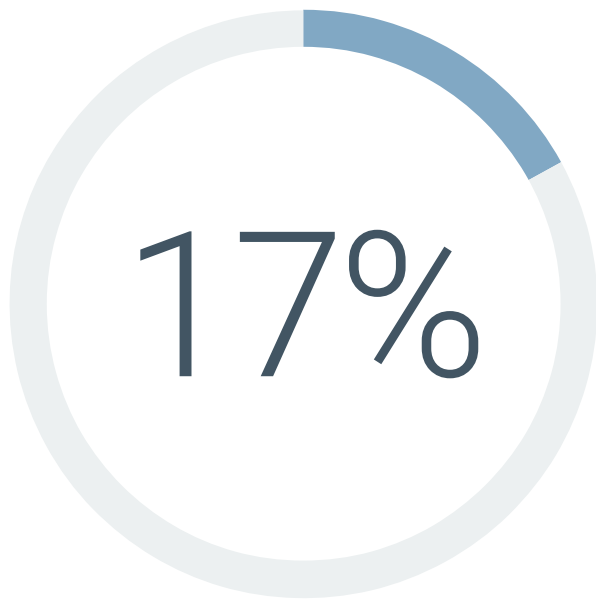
Biggest reason for using both specialized and WAF vendor-provided bot management tools.



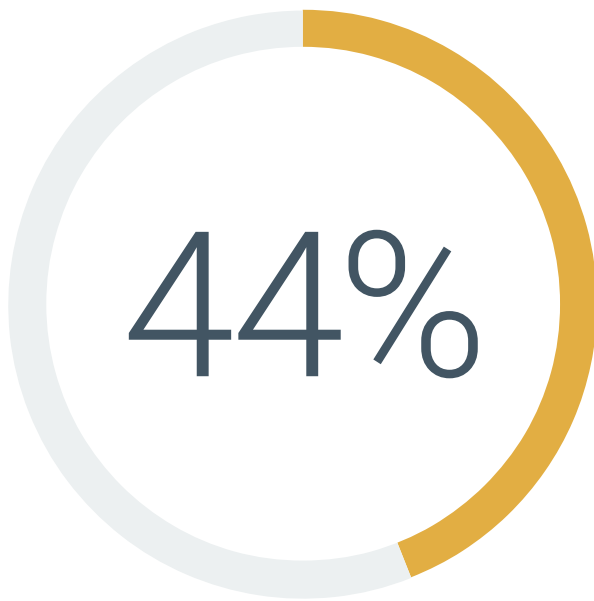
We believe a layered approach provides the strongest protection



Different teams at our organization prefer different solutions for certain bot issues



We are consolidating or switching solutions, but the process takes time



We primarily use a specialized solution but take advantage of the integrated capabilities in our WAF since they are available



**DoS Attacks Vary, and Most Organizations
Subsequently Use Multiple Forms of Protection**

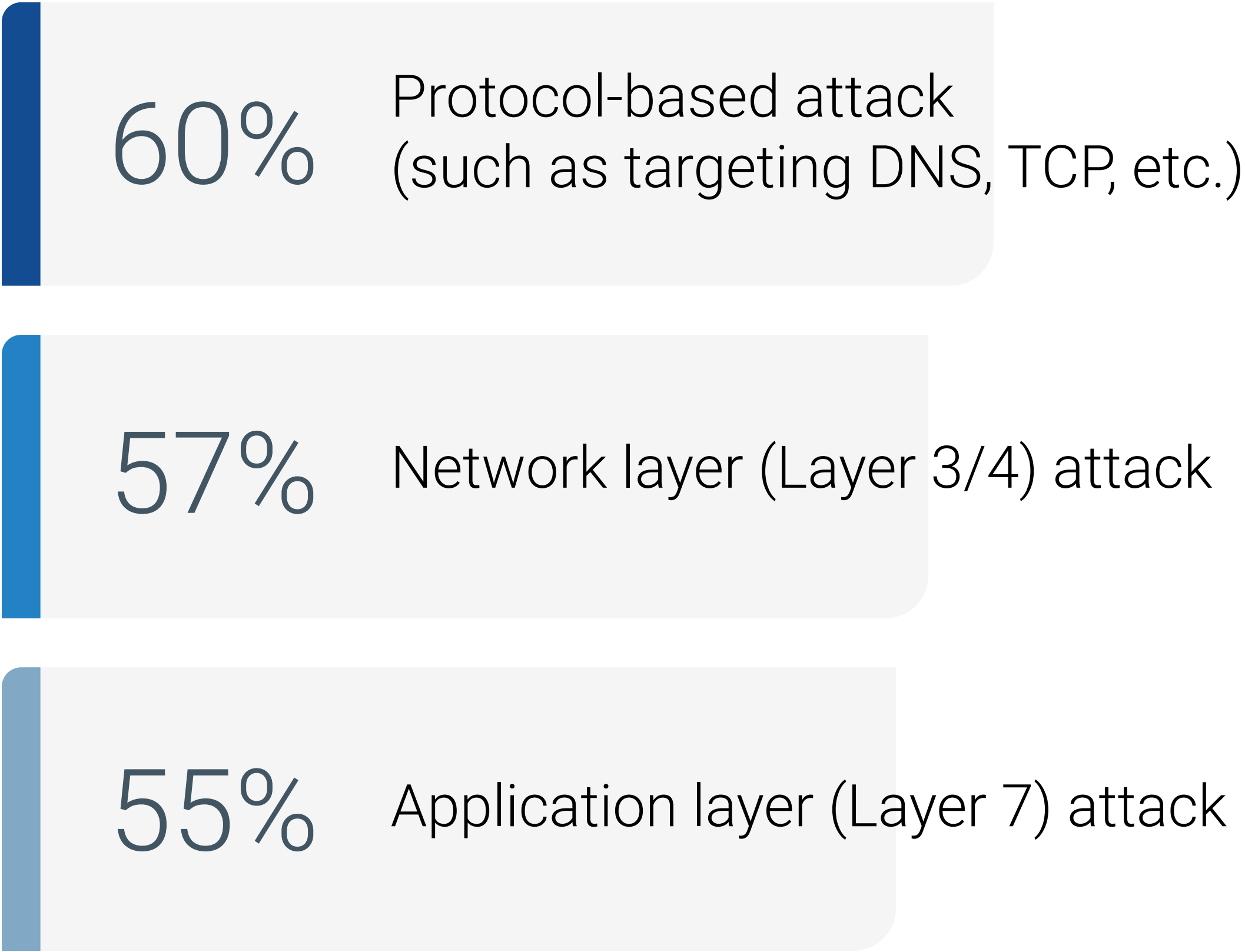


Most Organizations Report a Mix of DoS Attack Types

Denial-of-service attacks are an interesting facet of cybersecurity. While they have been used by attackers for decades, their position in the public consciousness seems to ebb and flow based on the size and severity of headline-generating attacks. Regardless, they are a consistent and significant issue for cybersecurity teams.

As shown earlier, 30% of respondents said they had experienced DoS attacks. The types of attacks seen varied across protocol-based attacks including DNS (60%), network layer attacks (57%), and application layer attacks (55%). With different types of tools and teams often responsible for each vector, this can pose a problem for organizations trying to efficiently maintain protection against DoS attacks.

Types of DoS attacks experienced.

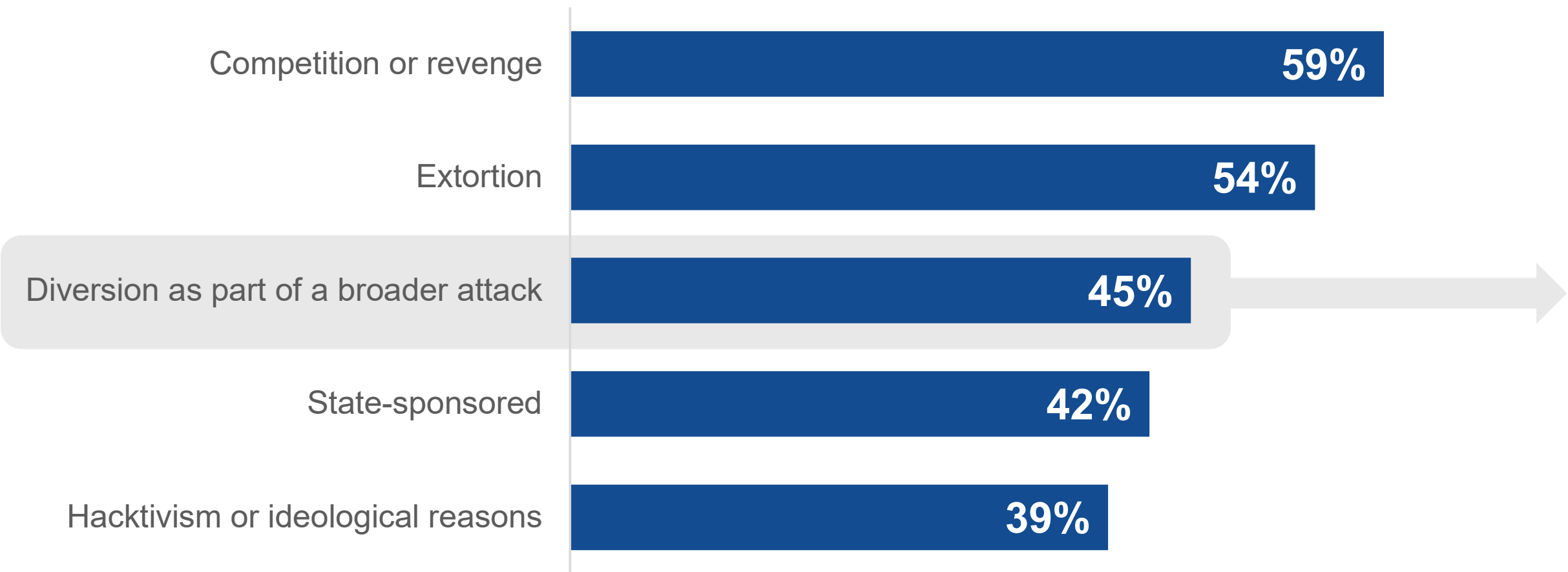


DoS Attack Motivations Vary, and Diversions Are Often Successful

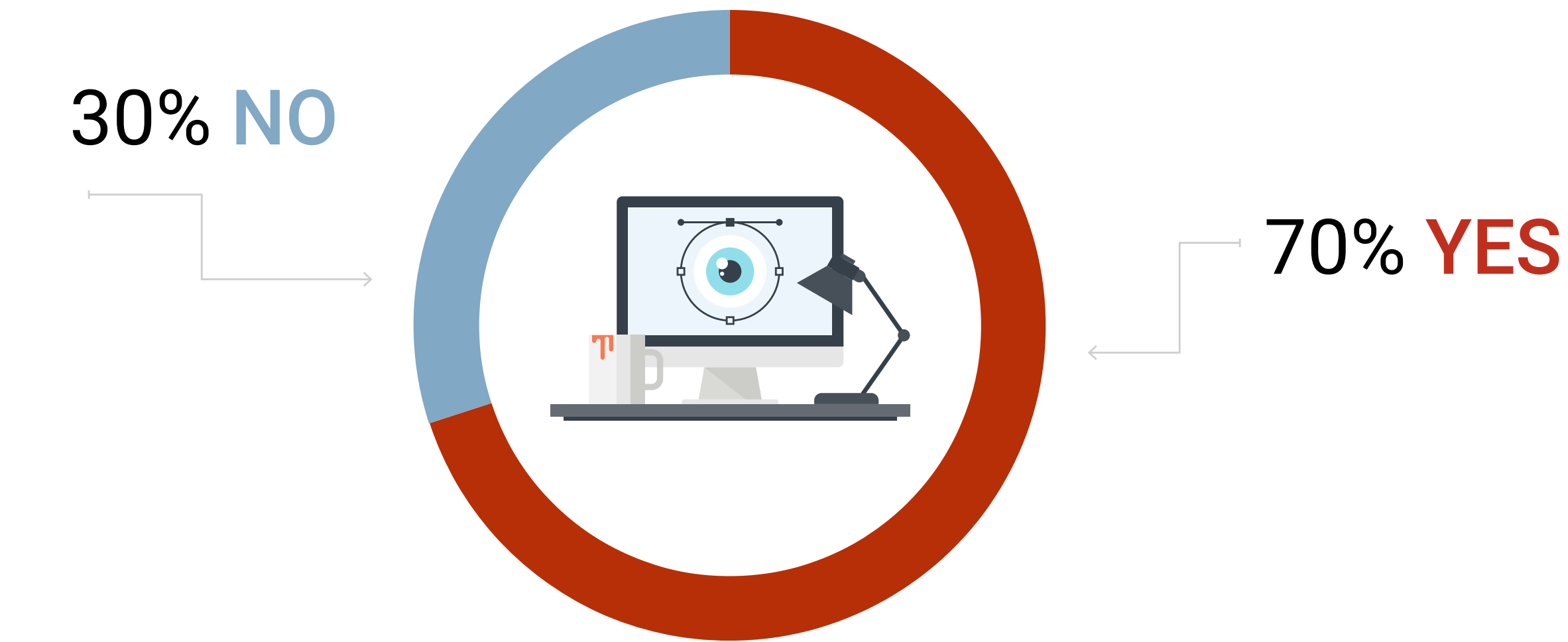
Another issue security teams face is the range of motivations that can lead to a DoS attack. Competition or revenge attacks were most common (59%), followed closely by extortion (54%) as a driver. Ransomware often generates headlines these days, but using a DoS attack for a ransom is clearly still common. State-sponsored (42%) and hacktivist attacks (39%) were also reported.

Yet one of the most interesting findings was the prevalence of diversionary DoS attacks. Nearly half (45%) of those suffering a DoS attack within the past 24 months said it was used as a diversion as part of a broader attack (i.e., to compromise other systems or steal data). Even more concerning, 70% of those experiencing this type of DDoS attack said it was successful. This makes ensuring accurate and timely mitigation that much more important to ensure security teams can focus on detecting other potential facets of the attack.

DoS attack motivations.



Was an experienced diversionary attack ultimately successful?

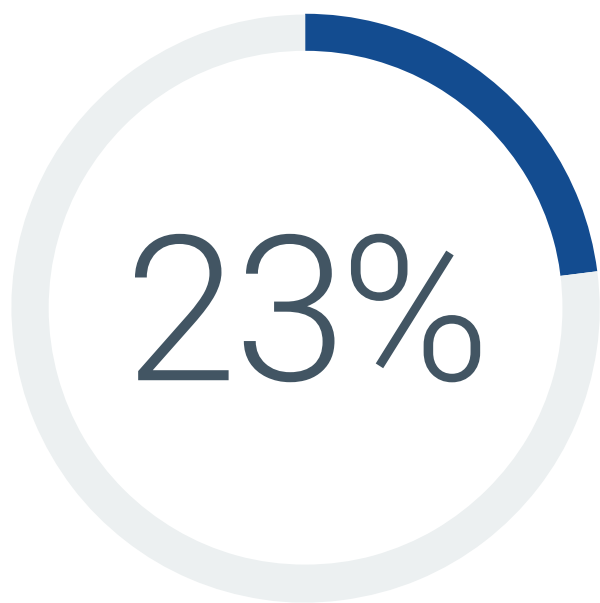




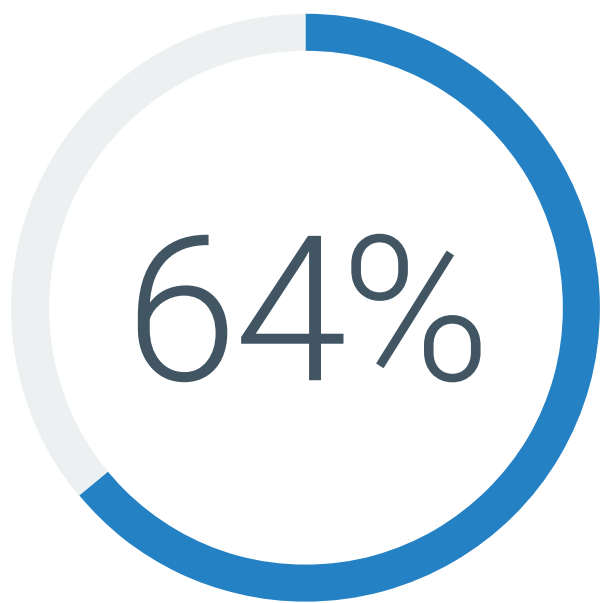
Most Organizations Use Multiple DoS Protection Providers

The good news is that most respondents do have tools in place to protect against both Layer 3/4 and Layer 7 attacks. Only 12% said they have tools in place for one or the other but not both. Nearly one-quarter (23%) say they use a single provider to protect against both network layer and application attacks, but the majority (64%) use separate providers for Layer 3/4 and Layer 7 attacks. Similar to bot management, security teams may feel that dedicated solutions provide better protection, but the increased complexity of managing so many different tools does come at a cost.

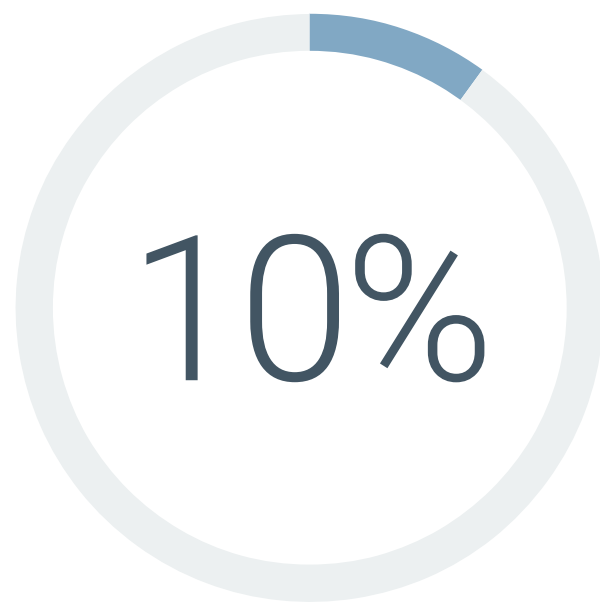
Approach to protecting against DoS attacks.



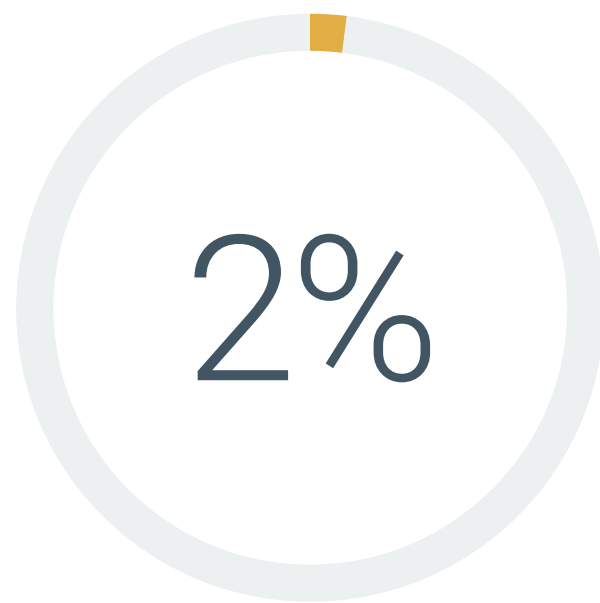
We use a single provider that protects against Layer 3/4 volumetric attacks and Layer 7 application attacks



We use separate providers to protect against Layer 3/4 volumetric attacks and Layer 7 application attacks



We only have tools in place to protect against Layer 3/4 volumetric attacks



We only have tools in place to protect against Layer 7 application attacks



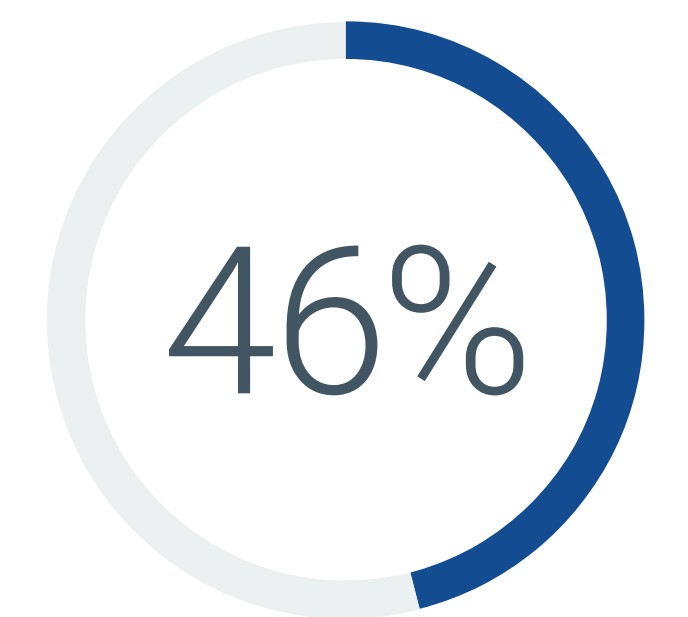
**Despite Bot and DDoS Tool Preferences,
Application Protection Consolidation Is Desired**

More Say They Are Moving to Consolidated Web Application Security Solutions

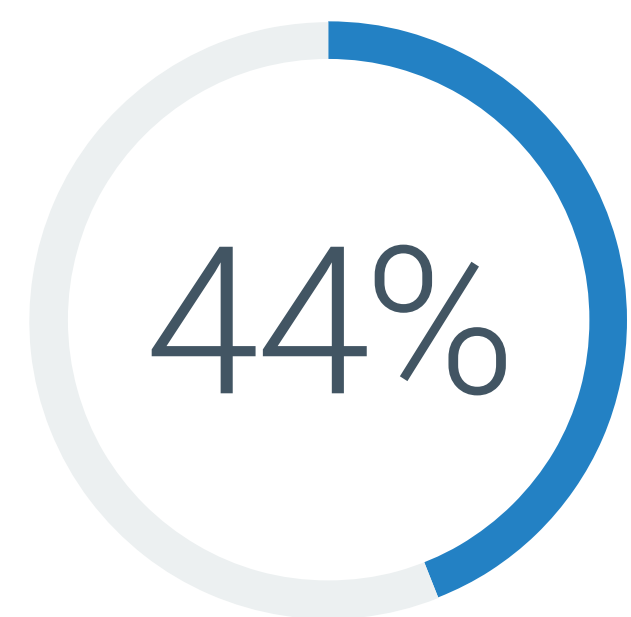
Over the last few years, converged web application and API protection platforms covering WAF, bot management, DDoS protection, and API security have seen increased interest. Indeed, nearly half (46%) say they either already use or are in the process of deploying such a consolidated solution. An additional 44% are planning to deploy a consolidated solution in the next 12-24 months.

The potential for diminishing returns from relying on too many siloed point tools can be high, especially for security teams that are understaffed or under skilled. This does not mean every organization will follow this path or fully replace specialized solutions with a converged approach. But the value in an integrated approach that more efficiently provides better context across multiple threat vectors is clear to many organizations.

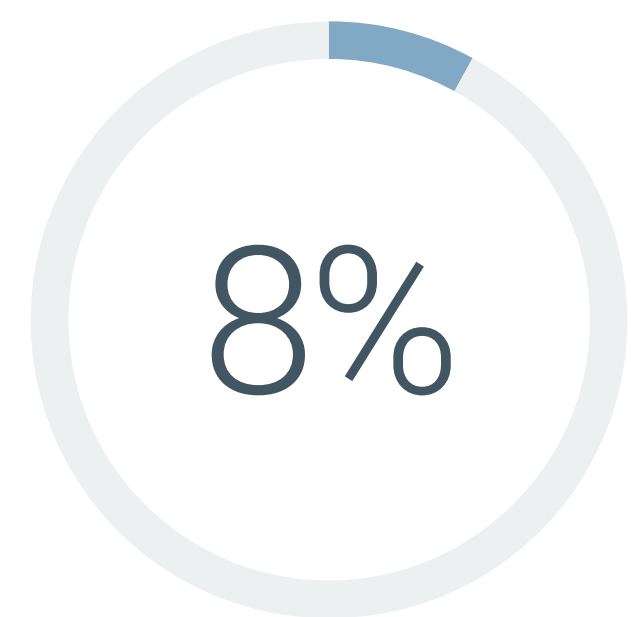
Position on application protection consolidation.



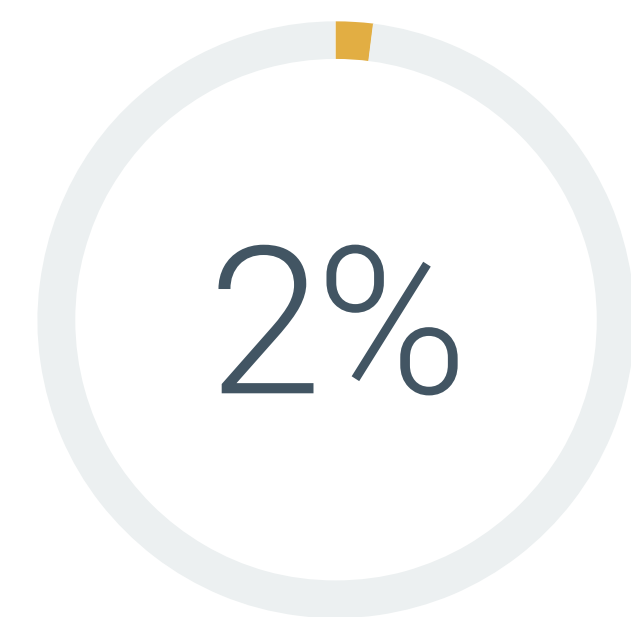
We already use or are in the process of deploying a consolidated solution



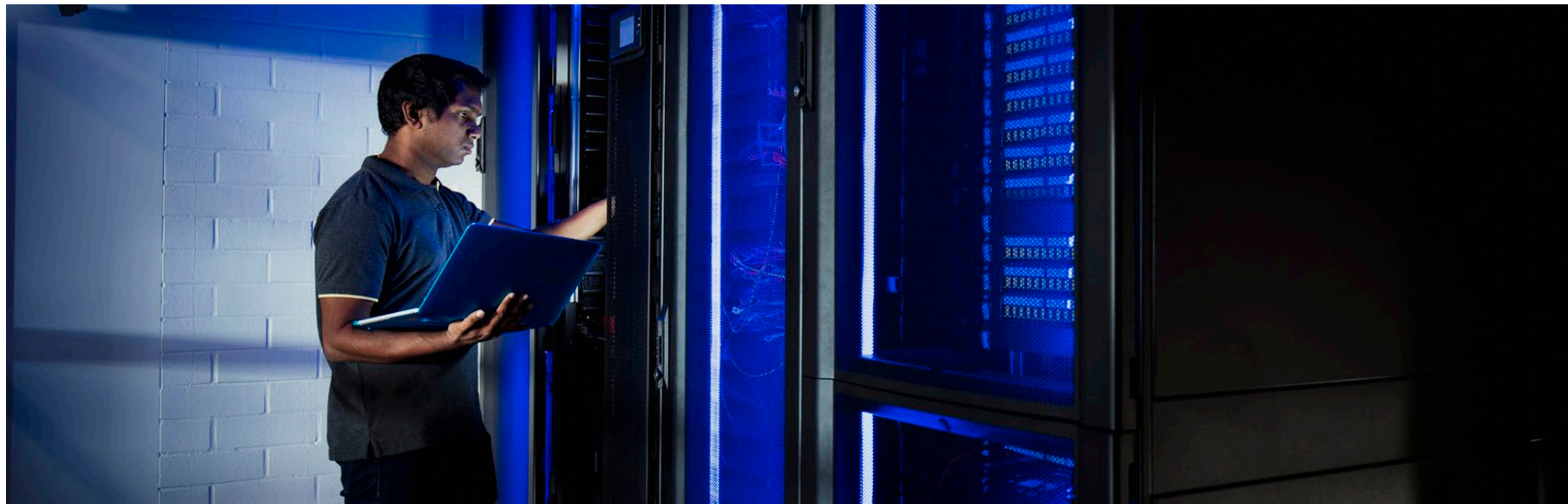
We are planning to deploy a consolidated solution in the next 12-24 months



We are planning to deploy a consolidated solution but do not have a timeline



We may be interested in deploying a consolidated solution but would have to learn more

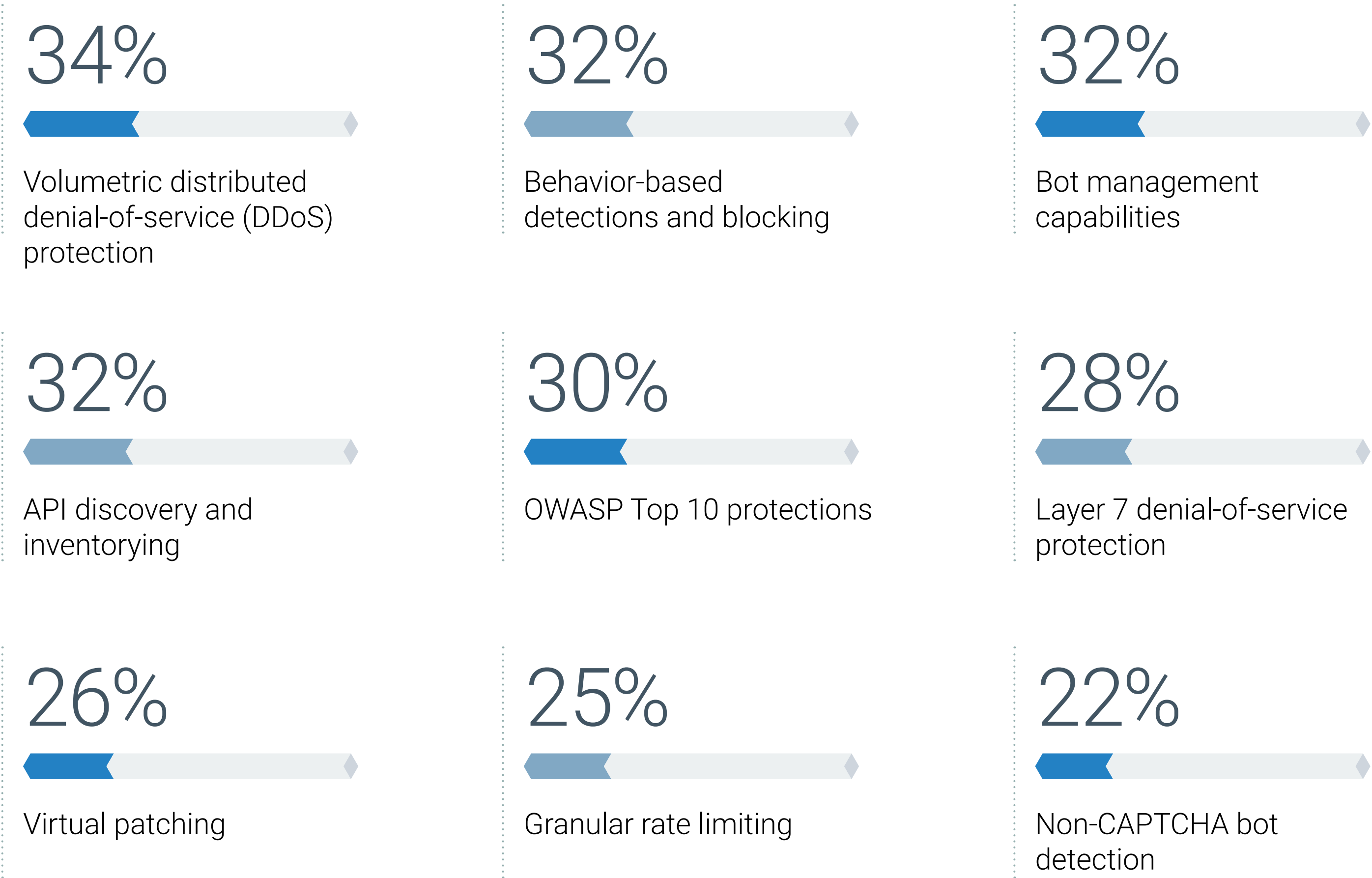


Consolidated Solutions Need a Broad Range of Capabilities

That said, to be effective, a consolidated web application protection solution requires a broad range of capabilities. As one may expect, there was little separation in cited importance across the core areas of volumetric DDoS protection (34%), bot management (32%), and API discovery and inventorying (32%).

For core WAF functionality, behavior-based detections and blocking (32%) rather than rule-based blocking was high on the list. Additionally, despite OWASP Top-10 attacks being less common, 30% expressed interest in these capabilities for foundational protection. Organizations considering converged solutions should compare capabilities against not only other platforms but also purpose-built tools for API security or bot management to understand any trade-offs they may be making.

Key capabilities in consolidated application protection solutions.

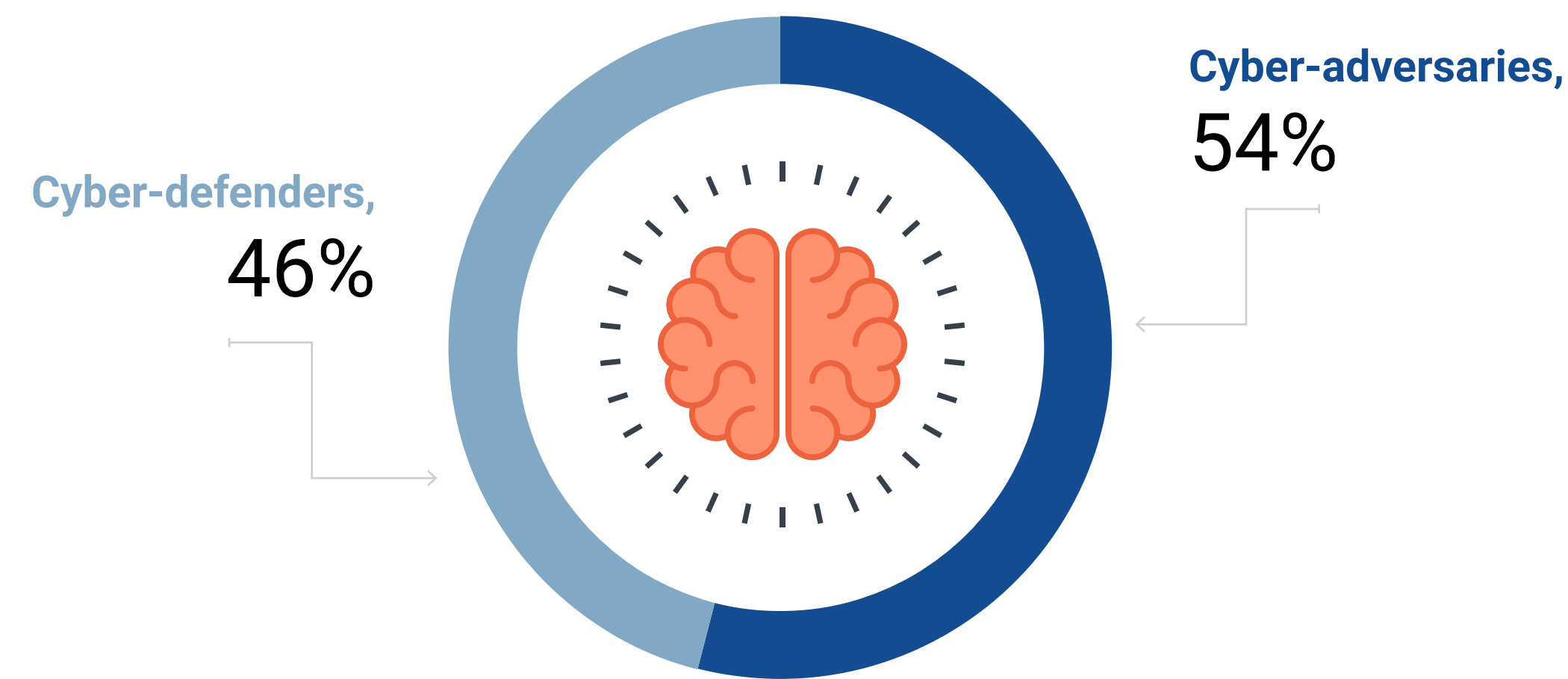


A Slight Majority Say Cyber-adversaries Have an Edge, but AI Can Help Defenders

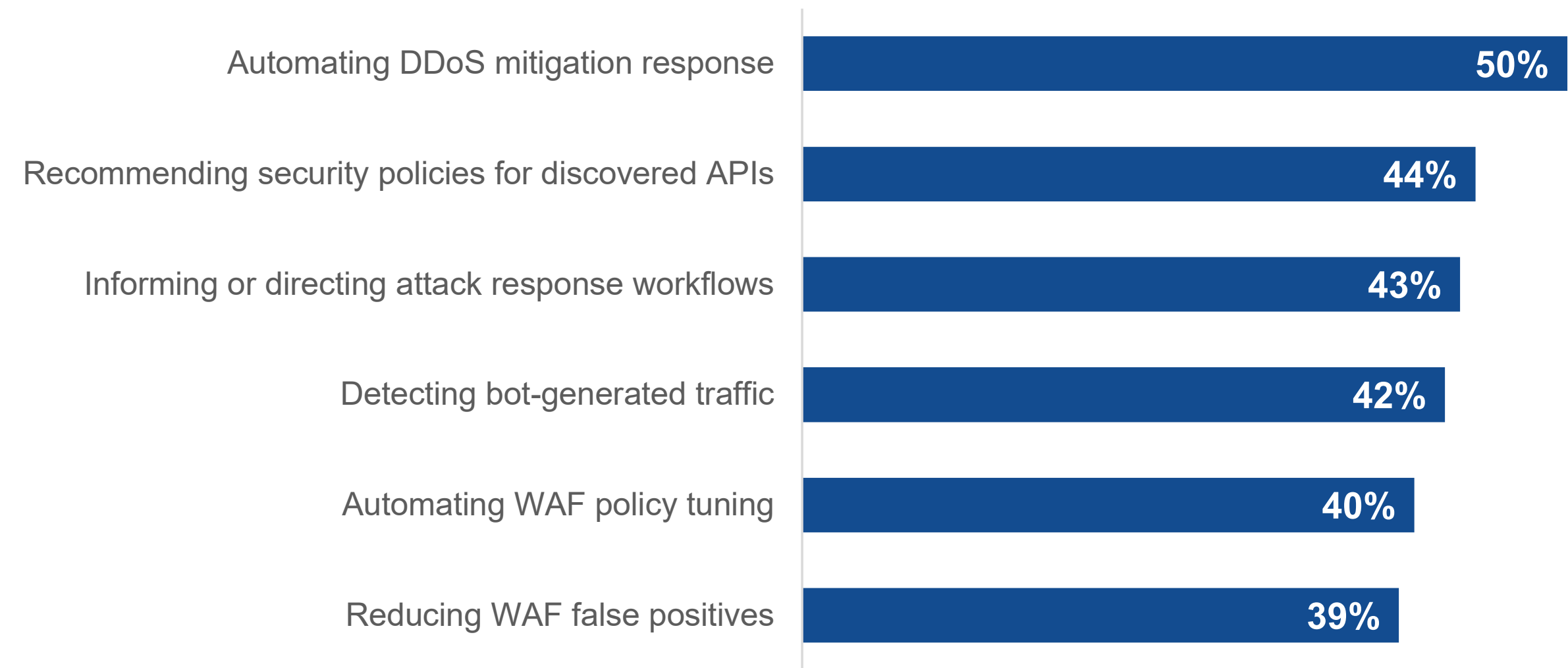
No cybersecurity conversation today is complete without discussing AI and its impact on the market. In this study, respondents were asked whether cyber-defenders or cyber-adversaries will gain the biggest advantage from AI and generative AI, specifically regarding web applications and APIs. While a slight majority of respondents (54%) believe adversaries have the advantage over defenders (46%), organizations overall are bullish on the impact of AI for defenders across all the core web application and API security areas.

Specifically, half of organizations believe AI will have the biggest impact automating DDoS mitigation response, addressing one of the key issues discussed earlier. Recommending policies for discovered APIs (44%) and informing or directing attack response workflows (43%) were also commonly cited. Detecting bot traffic was noted by 42% of respondents, while 40% believe AI will help with WAF policy tuning and 39% say it could reduce WAF false positives. If AI can deliver meaningful improvement across even some of these areas, security teams will greatly benefit.

Group that gains the biggest advantage from AI on web applications and APIs.



Areas of application protection in which AI is expected to have the biggest impact.





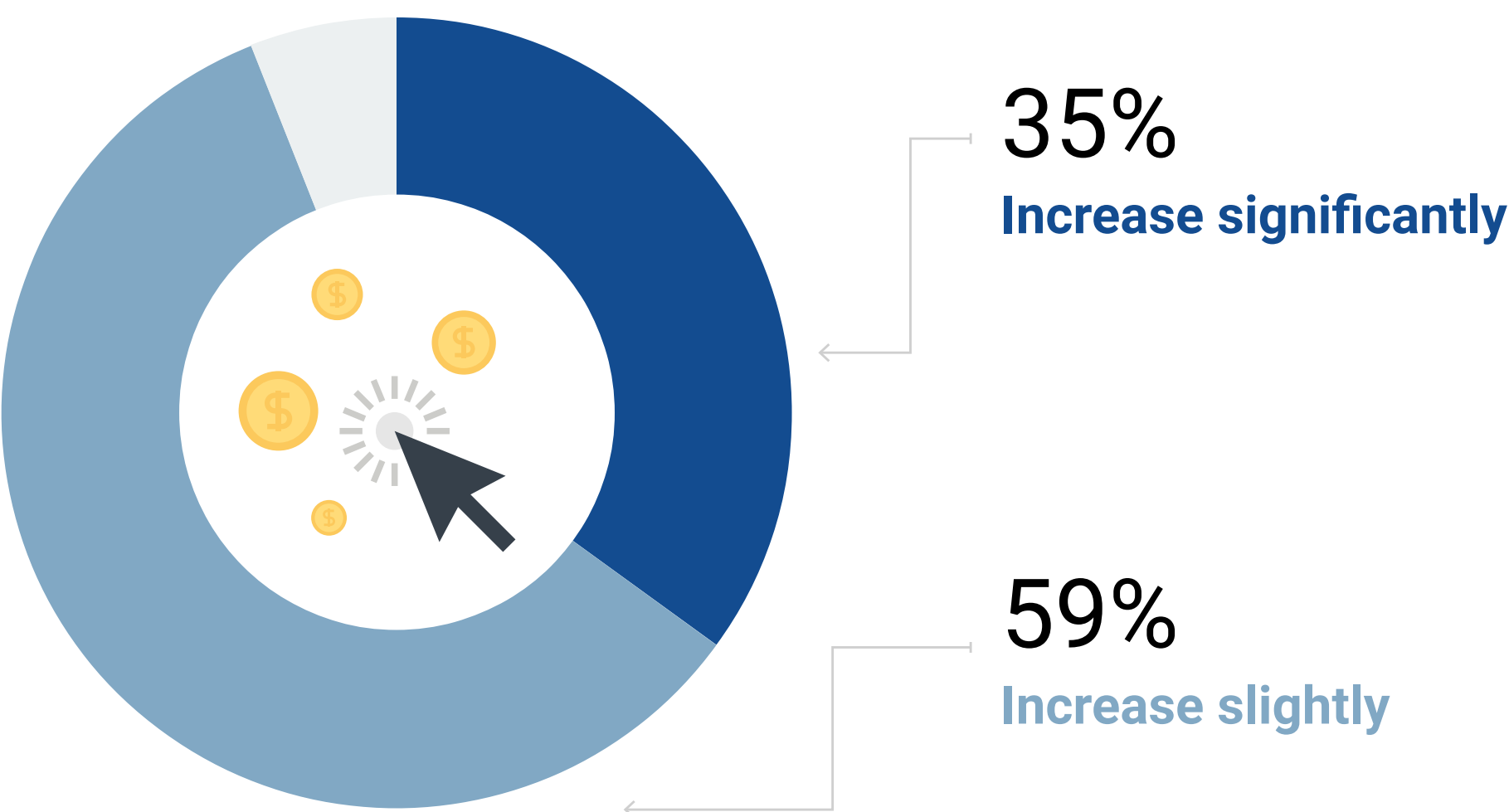
**Spending Intentions Appear Strong,
but Focus Is Fragmented**

Nearly All Expect Application Protection Spending to Increase, but No Consensus as to Where

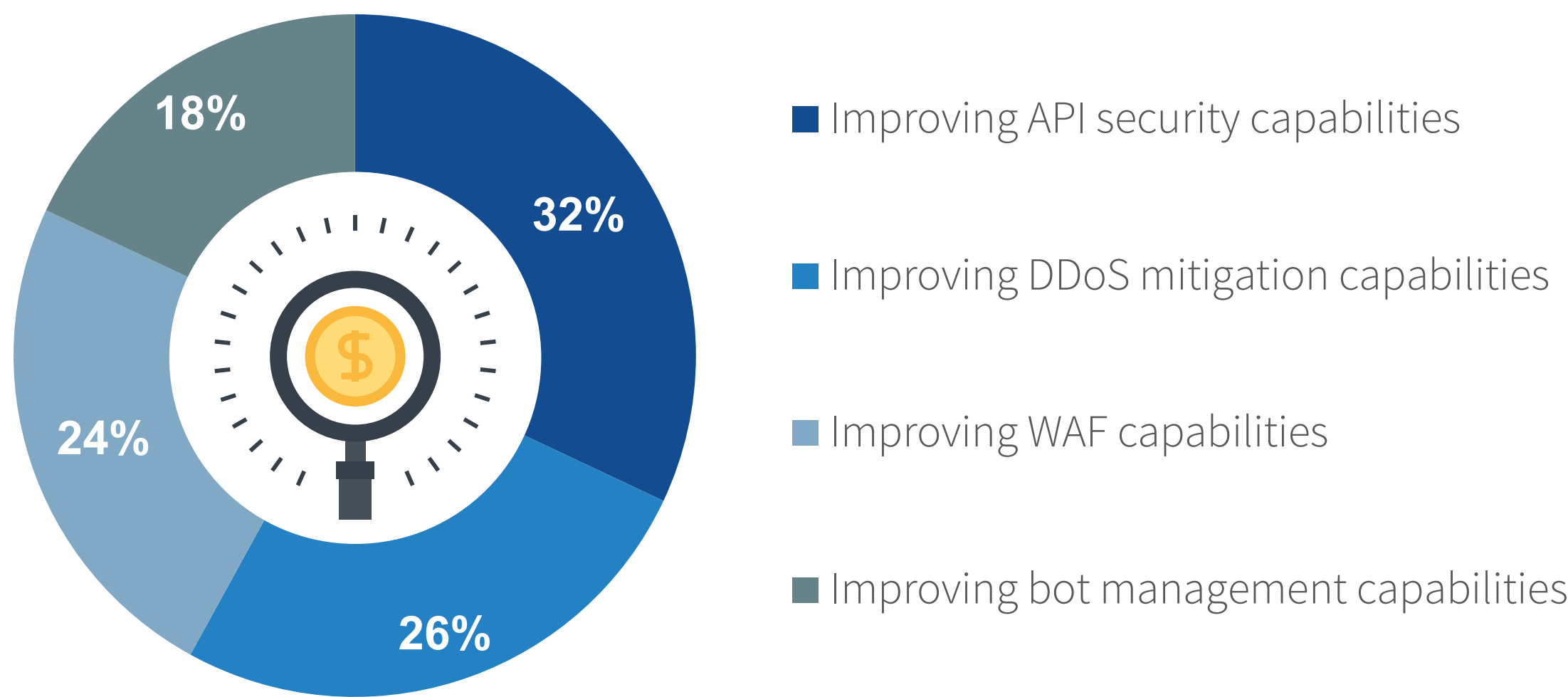
As one may expect based on the challenges organizations cite and the criticality of protecting public-facing web applications, many are prioritizing spending in this area. Specifically, 35% expect to significantly increase spending on web application and API protection, while 59% expect to increase spending slightly. No respondents anticipate spending declining over the next 12-18 months.

How that increased spending will be directed will vary from organization to organization. API security will be a priority moving forward, with 32% saying increased spending will be focused most on improving those capabilities. Just over a quarter (26%) will direct increased spending toward DDoS the most, while 24% will focus on improving WAF capabilities. Finally, 18% will focus on bot management capabilities the most.

Anticipated change in application protection spending over the next 12-18 months.



Areas increased application protection spending will be focused the most.

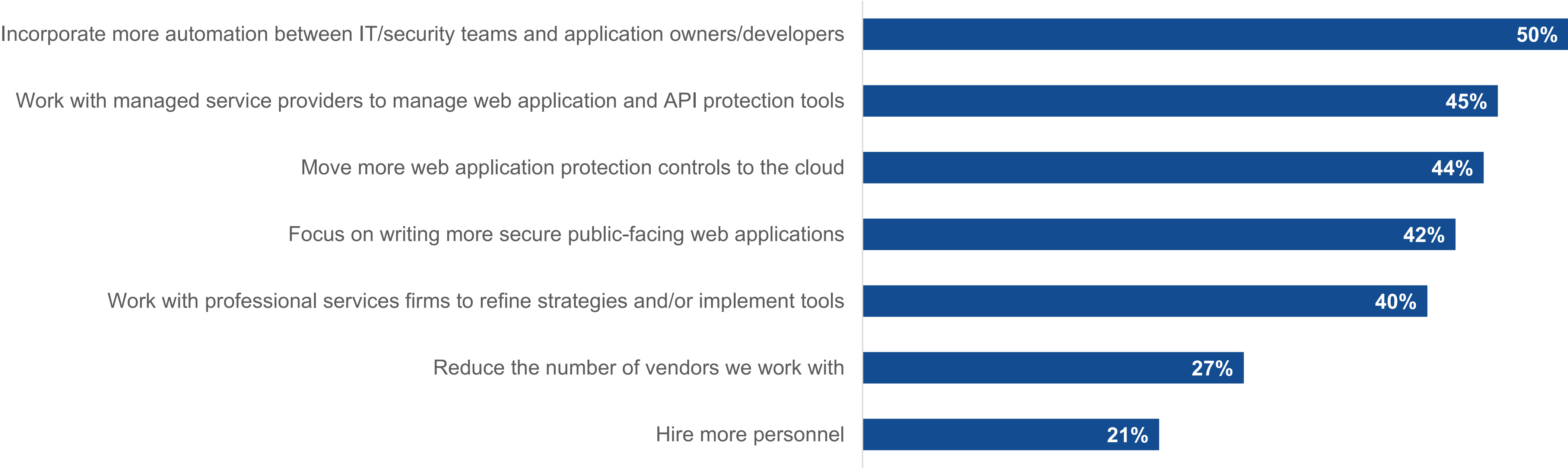


A Variety of Actions Are Planned, but Services Will Be Critical

Respondents also plan to take a variety of actions to implement and optimize their web application and API strategies. The friction between security and development teams continues to pose problems, so half hope to address that through more automation to improve workflows. Services will also play an important role, with 45% planning to work with managed service providers, and 40% planning to work with professional services firms for planning and/or implementation.

Foundational priorities such as moving more controls to the cloud (44%) and writing more secure applications (42%) were also commonly cited. But surprisingly, despite the preferences for consolidation, only 27% plan to reduce the number of vendors they work with. This again points to the fact that consolidation will be nuanced, take time, and vary from one organization to the next.

Key priorities for application protection moving forward.





ABOUT

Fastly’s powerful and programmable edge cloud platform helps the world’s top brands deliver online experiences that are fast, safe, and engaging through edge compute, delivery, security, and observability offerings that improve site performance, enhance security, and empower innovation at global scale. Compared to other providers, Fastly’s powerful, high-performance, and modern platform architecture empowers developers to deliver secure websites and apps with rapid time-to-market and demonstrated, industry-leading cost savings. Organizations around the world trust Fastly to help them upgrade the internet experience.

LEARN MORE

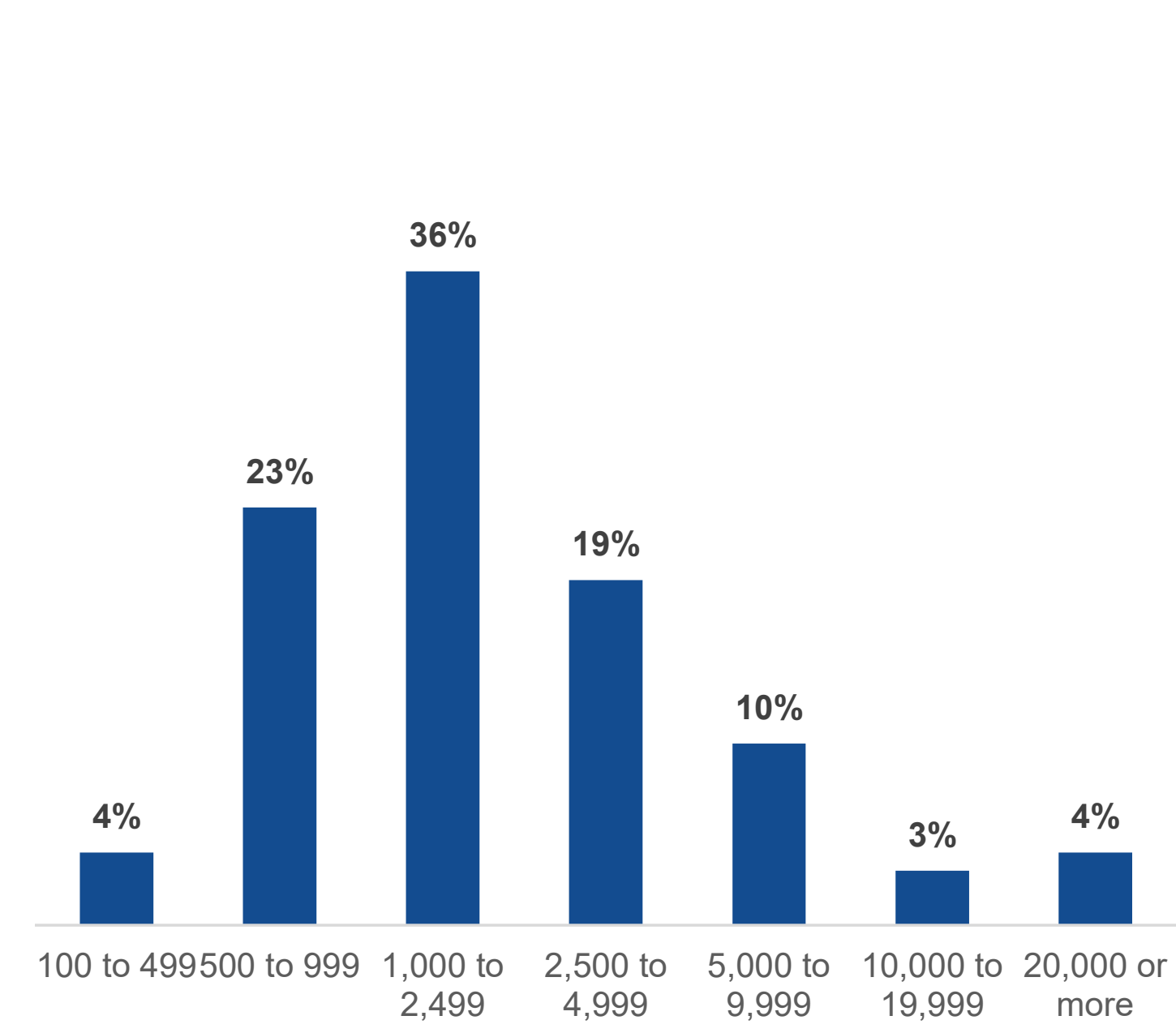


RESEARCH METHODOLOGY AND DEMOGRAPHICS

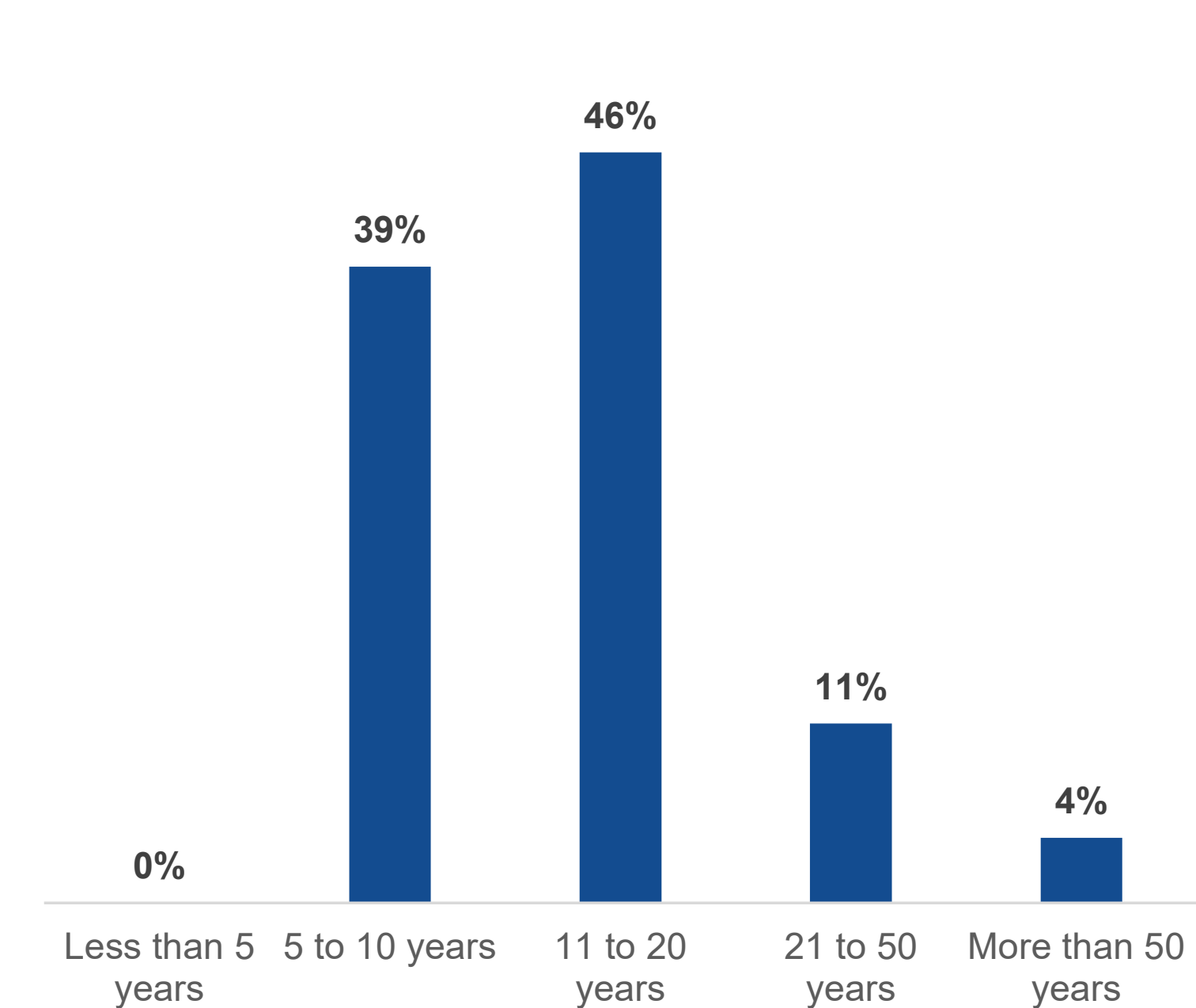
To gather data for this report, TechTarget’s Enterprise Strategy Group conducted a comprehensive online survey of IT and cybersecurity professionals from private- and public-sector organizations in North America between November 1, 2024, and November 14, 2024. To qualify for this survey, respondents were required to be involved with securing their organization’s web applications and 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 383 IT and cybersecurity professionals.

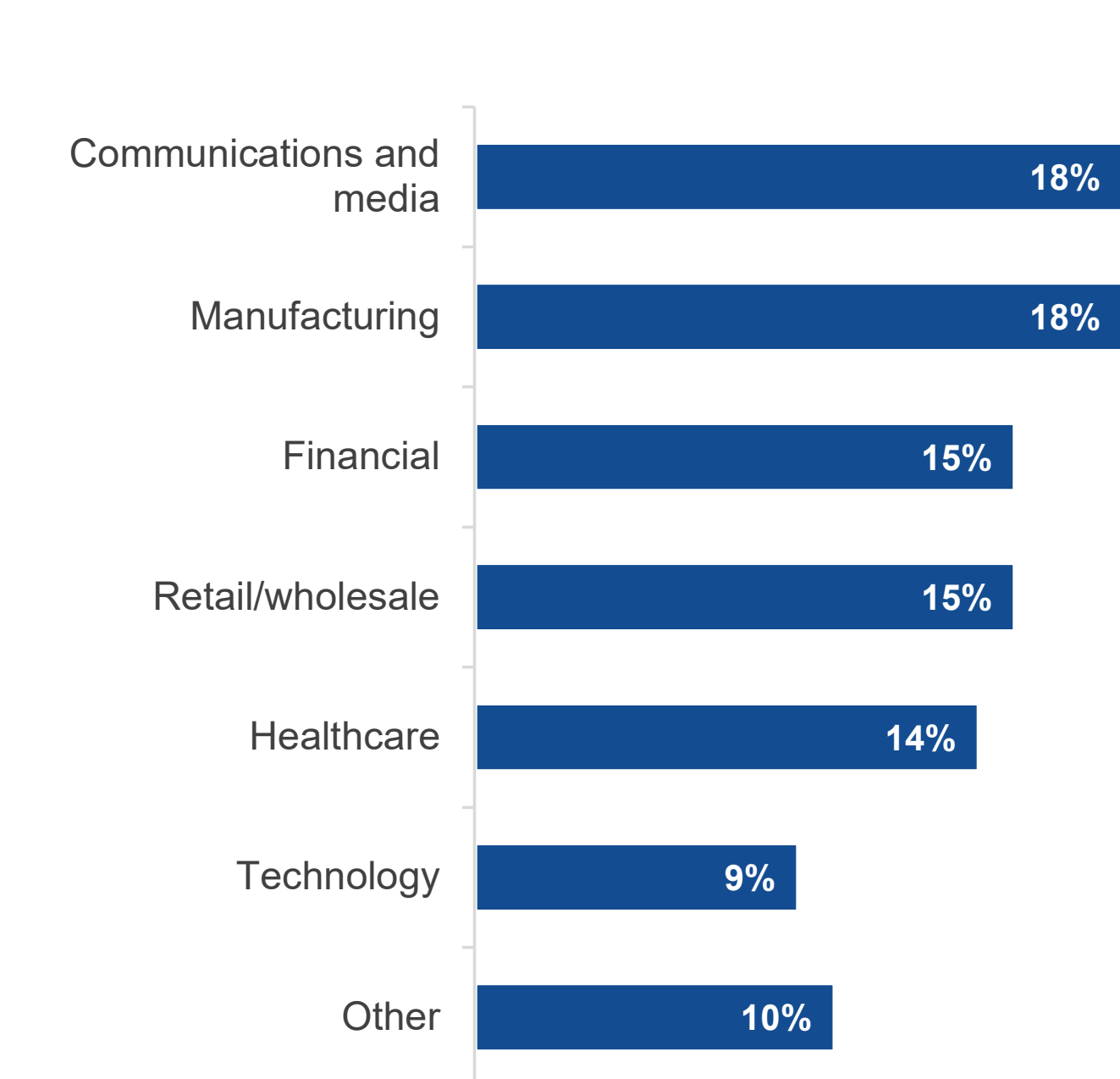
Respondents’ organizations by number of employees.



Respondents’ organizations by years in operation.



Respondents’ organizations by industry.



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

This publication is copyrighted by TechTarget, Inc. 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, Inc., 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.



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.

© 2025 TechTarget, Inc. All Rights Reserved.