

Browser Management and Security: Emerging Strategies, Requirements, and Success Factors

Gabe Knuth | *Principal Analyst*

John Grady | *Principal Analyst*

February 2026

This Omdia eBook was commissioned by Parallels and is distributed under license from Techtarget, Inc.



Research Objectives

The browser was once considered a single application among many in an organization’s environment, but today the browser is increasingly the primary interface to critical applications that access sensitive data and support core business functions. While it’s easy to think the world has moved to browser-based applications (or will soon be 100% browser-based), Windows applications are still in widespread usage. To accommodate this, organizations have deployed many strategies to enable secure access to these applications at various levels (gateway, VPN, VDI/DaaS, remote browser isolation (RBI), browser extensions, enterprise browsers, etc.).

Given these changes, it’s important to take stock of the challenges organizations are facing, strategies they are implementing, and outcomes they are ultimately experiencing. To gain insights into these trends, Omdia surveyed 400 IT and cybersecurity professionals in North America involved with securing device, browser, application, and/or web usage at their organization.

THIS STUDY SOUGHT TO:

Establish the types of applications and methods for delivering them that are in use at organizations today.

Determine the use cases organizations want to support with secure browsing solutions and the attributes and capabilities they require.

Understand the volume, types, and resulting impacts of browser-based attacks security teams are seeing.

Learn about the preferences for secure browsing solution architectures and vendor types.



Key Findings



Application Access Remains Fragmented, but Secure Browsing Solutions See Early Traction

PAGE 4



Browser Extensions, Application Performance, and User Productivity Are Watched Closely

PAGE 8



Browser-based Attacks Are Increasing and Driving Spending Changes

PAGE 11



Existing Approaches Are Fragmented, and Many Cite Challenges

PAGE 14



Enterprise Browsers Lead a Crowded Space, but Use Cases, Features, and Approaches Vary

PAGE 18



Funding Sources Vary, but Spending on Secure Browser Solutions Is Strong

PAGE 22



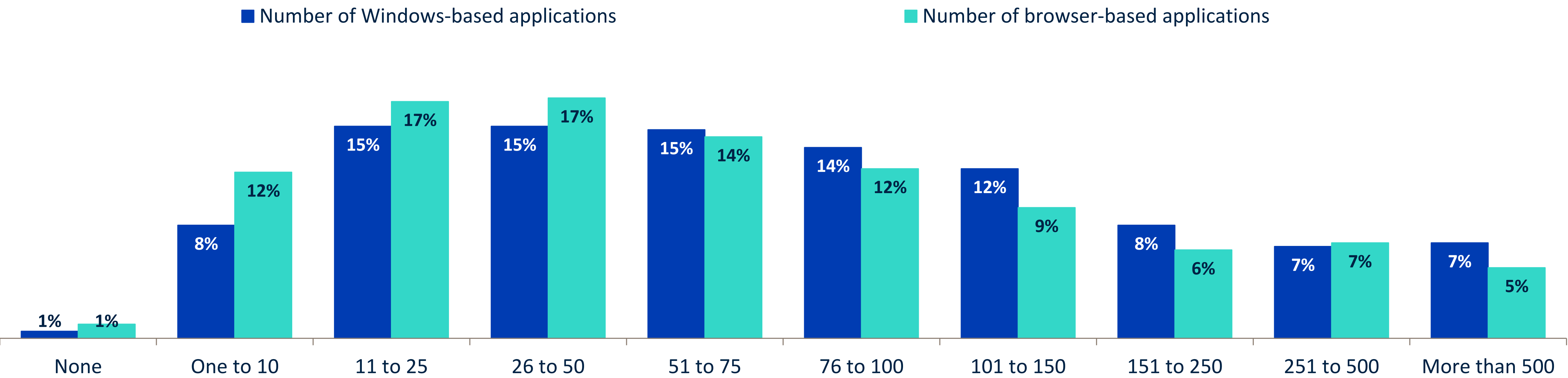
Application Access Remains
Fragmented, but Secure Browsing
Solutions See Early Traction

Reports of the Death of Windows Applications Are Greatly Exaggerated

As organizations plan their application delivery and secure access strategies, taking stock of the entire ecosystem is critical in helping to determine the path forward. The first step in that process is assessing the various types of applications in use. While browser-based applications undoubtedly comprise most of the new application deployments today, it's important to understand that organizations continue to support a fairly even balance of browser- and Windows-based applications.

The longevity of Windows applications in technology ecosystems means they can be delivered in many ways (e.g., locally or via application management, desktop virtualization, scripted installs, imaging, etc.), which amplifies the complexity of application management and access. This makes it important to consider tools that can support all application types in order to avoid tool sprawl and blind spots in the environment.

Approximate number of browser-based and Windows-based applications currently in use.

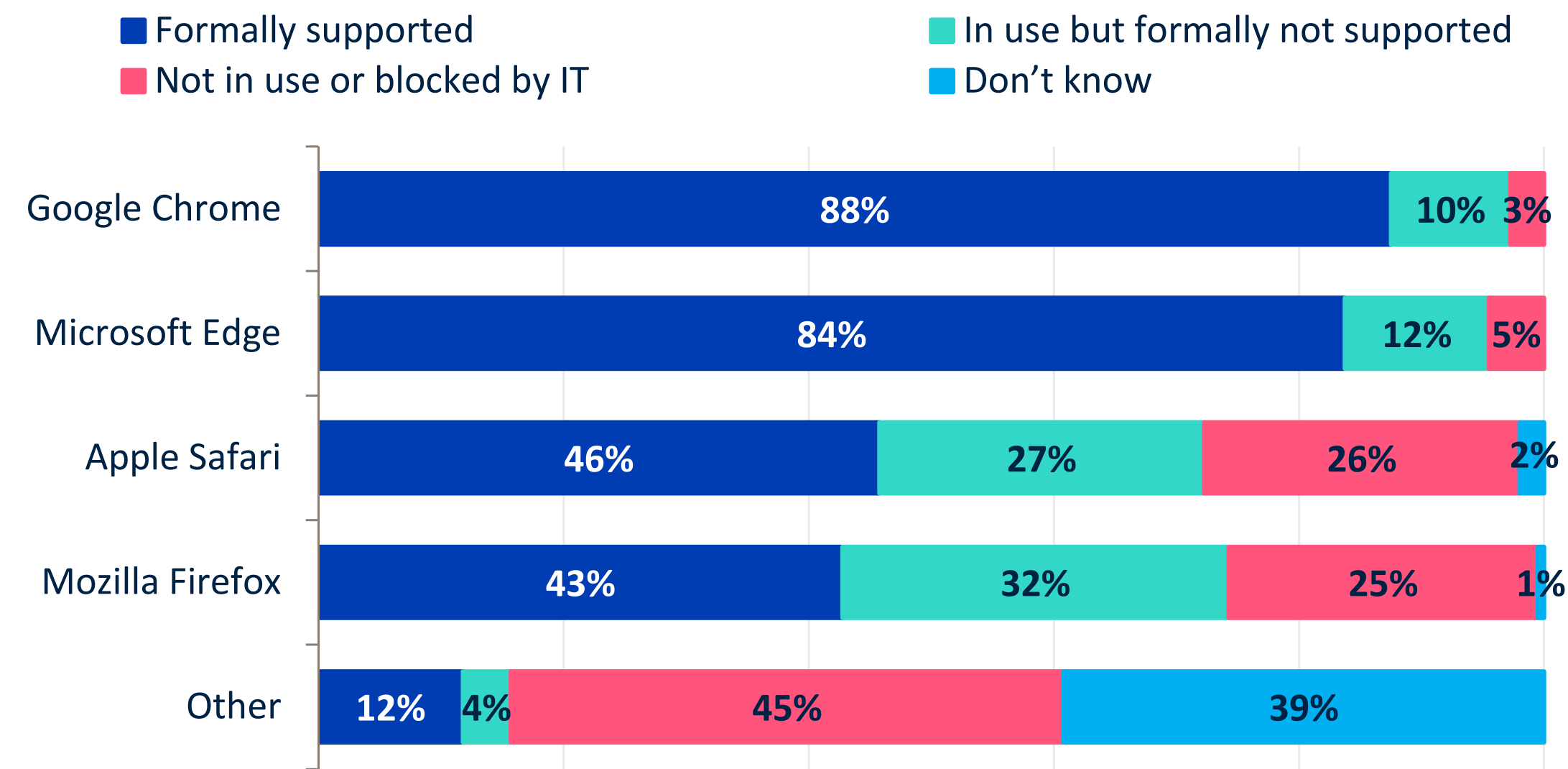


Chrome and Edge Dominate Among Traditional Browsers

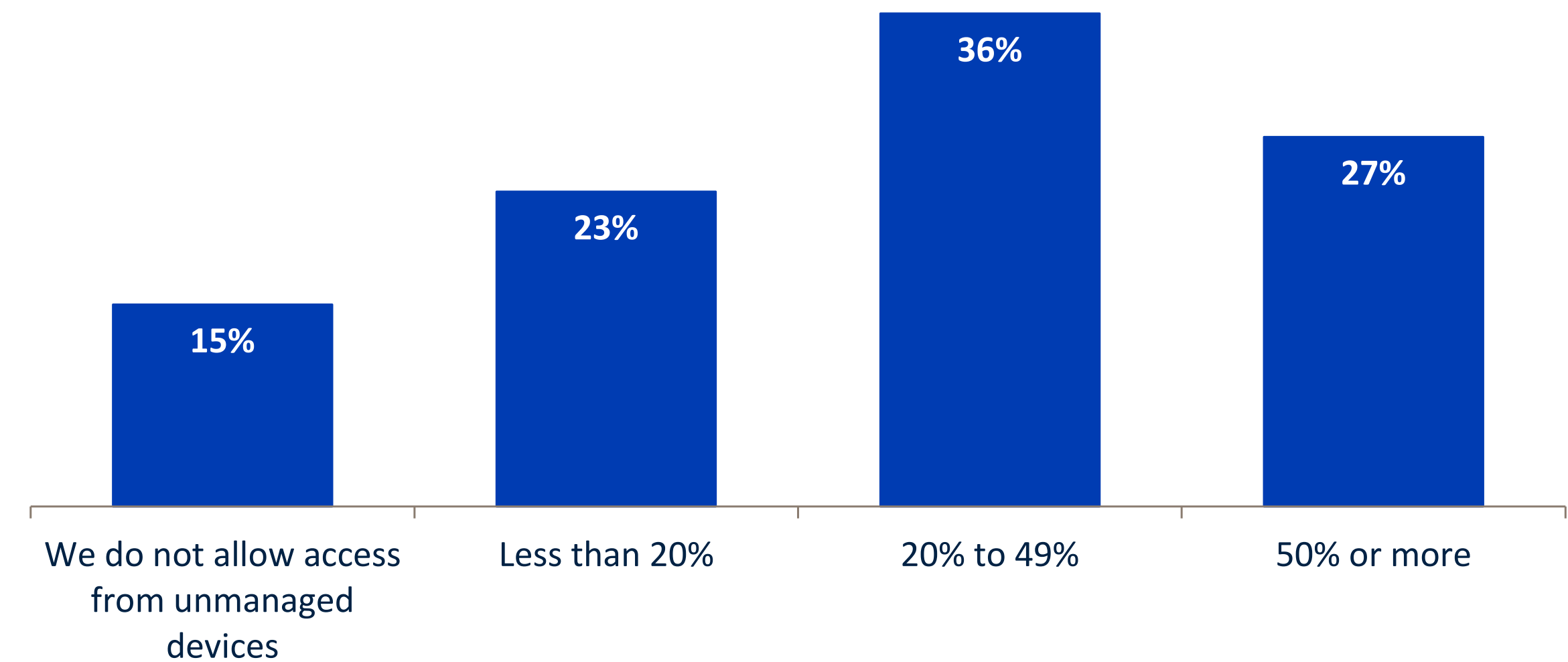
Looking specifically at browsers, Chrome and Edge are by far the most likely to be formally supported by IT. However, that lead is slightly diminished when informal use of Safari and Firefox is also taken into account. This, combined with the 39% of respondents who said “Don’t Know” regarding other browser usage, shows that the user experience and security surface area for browser applications can be significantly larger than just the browsers that are supported.

The unsupported status of browsers that are in use becomes increasingly notable when considering the number of unmanaged devices in use. On average, nearly one-third (32%) of end users access applications via unmanaged devices at least occasionally. Combined, this shows that the perimeter of application access is fairly porous, which helps explain why there’s so much attention devoted to this space.

IT support status of browsers.



Approximate percentage of users who access corporate applications from unmanaged devices.

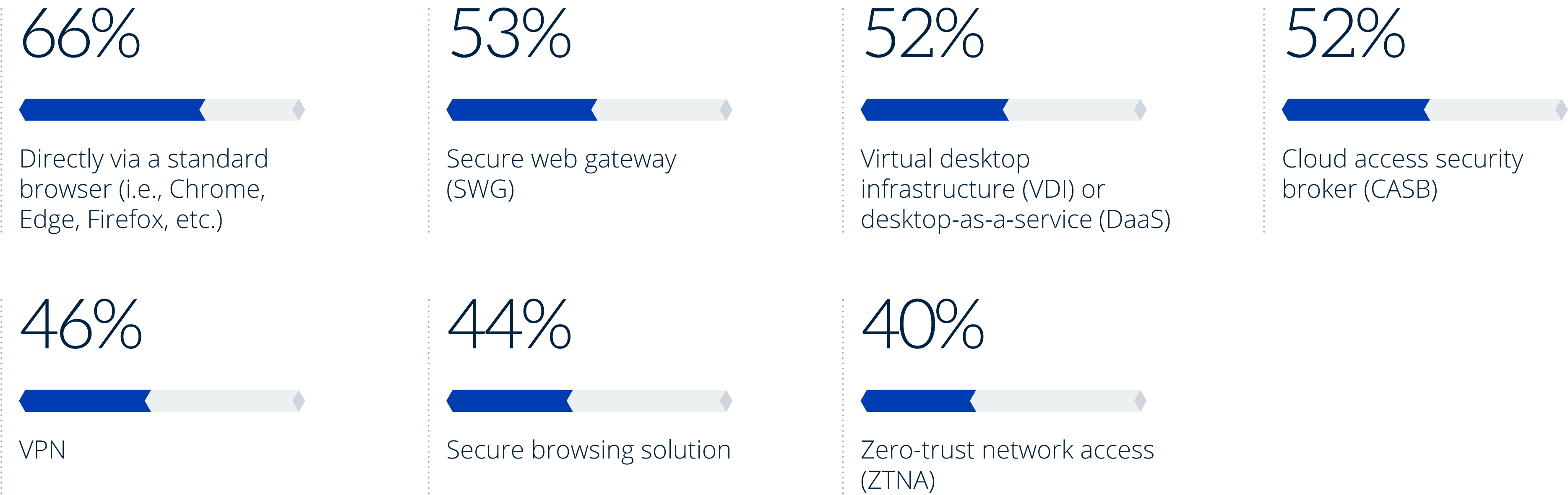


Browser-based Application Delivery Is a Mixed Bag

Unsurprisingly, two-thirds of respondents said browser applications are deployed directly to end users via standard browsers like Chrome, Edge, and Firefox. By itself, this would be concerning, but the data reveals that many tools are used alongside standard browsers to provide secure access.

While secure browsing solutions—the term this study used to describe solutions like enterprise browsers, secure browser extensions, and remote browser isolation (RBI)—are in use across 44% of respondent organizations, more traditional tools were more commonly cited. That said, given that the secure browsing market only recently emerged, this should be viewed as a positive indicator that shows momentum for these types of solutions.

Tools organizations currently use to securely deliver browser-based applications to users.



A man with dark hair and glasses is looking down at a computer screen. The background is a blurred office environment with multiple computer monitors. The entire image has a strong blue color overlay.

Browser Extensions, Application
Performance, and User
Productivity Are Watched Closely

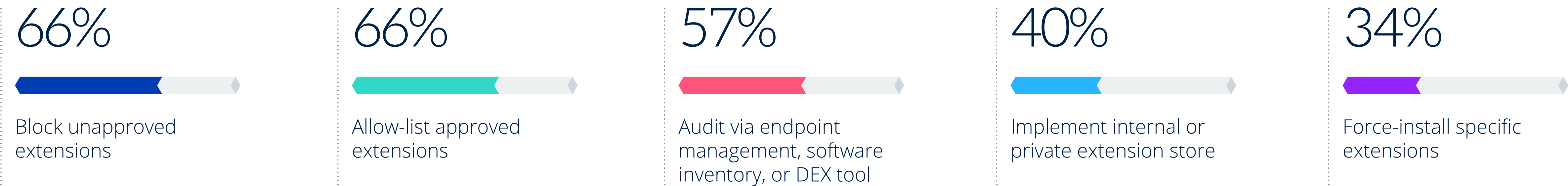
Browser Extensions Are on IT's Radar

Browser extensions present their own security and data loss risks, and as the browser becomes the primary application interface for many users, browser extensions have become front and center for organizations. Management approaches differ, but browser extension management is overwhelmingly in use by IT teams. Although this is generally positive, the number of disparate approaches to extension management could lead to some blind spots or overlap, so organizations may want to dedicate a portion of the browser strategy to extensions.

Do organizations manage, monitor, or restrict browser extensions?



How organizations manage, monitor, or restrict browser extensions.

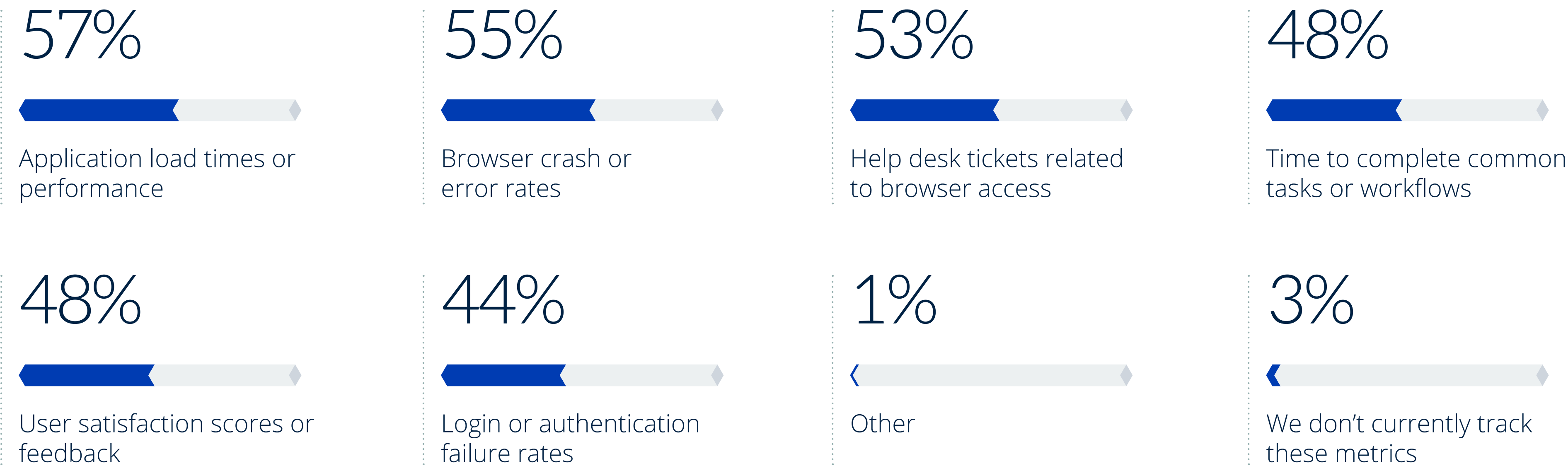


Browser Application User Experience Metrics Matter

As browser usage becomes more mission-critical and browsers evolve into the default workspace for employees, organizations must pay closer attention to the impact issues therein can have on productivity. Respondents indicated that they track a variety of metrics to maintain visibility into productivity impacts, including application load times or performance (57%), browser crash or error rates (55%), help desk tickets related to the browser (53%), and user experience via time to complete tasks (48%) and direct user satisfaction scores or feedback (48%).

While the metrics tracked vary, very few organizations said they did no such monitoring (3%).

User productivity metrics organizations track related to browser-based application access.



A hand holding a smartphone is shown against a dark blue background. A translucent digital overlay is positioned above the phone, depicting a document with horizontal lines. Three red warning icons, each consisting of a triangle with an exclamation mark, are scattered around the document: one to the left, one on the document itself, and one to the right. The overall image conveys a sense of digital security or threat.

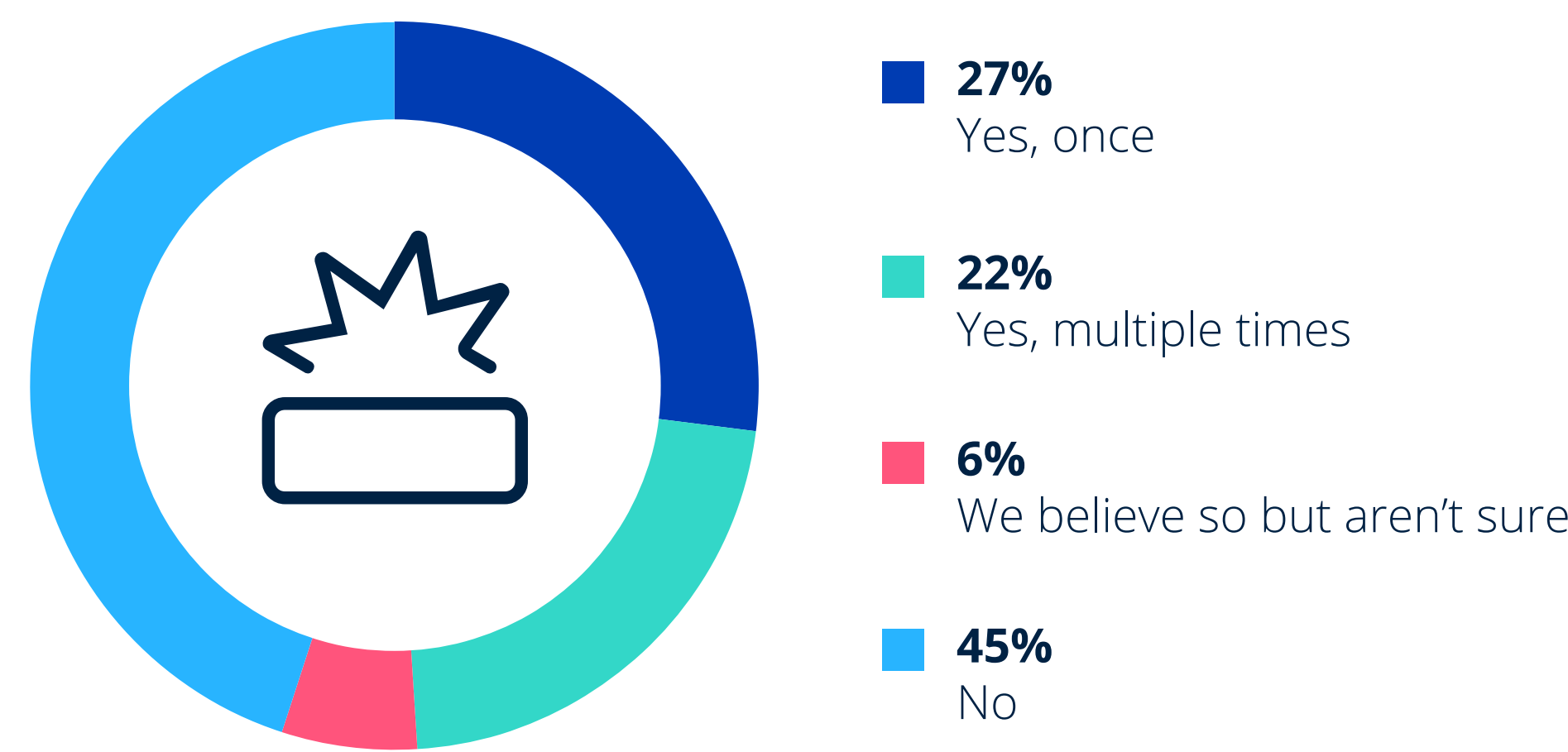
Browser-based Attacks
Are Increasing and Driving
Spending Changes

Browser-Based Attacks Are Common, Varied, and an Increasing Part of the Threat Landscape

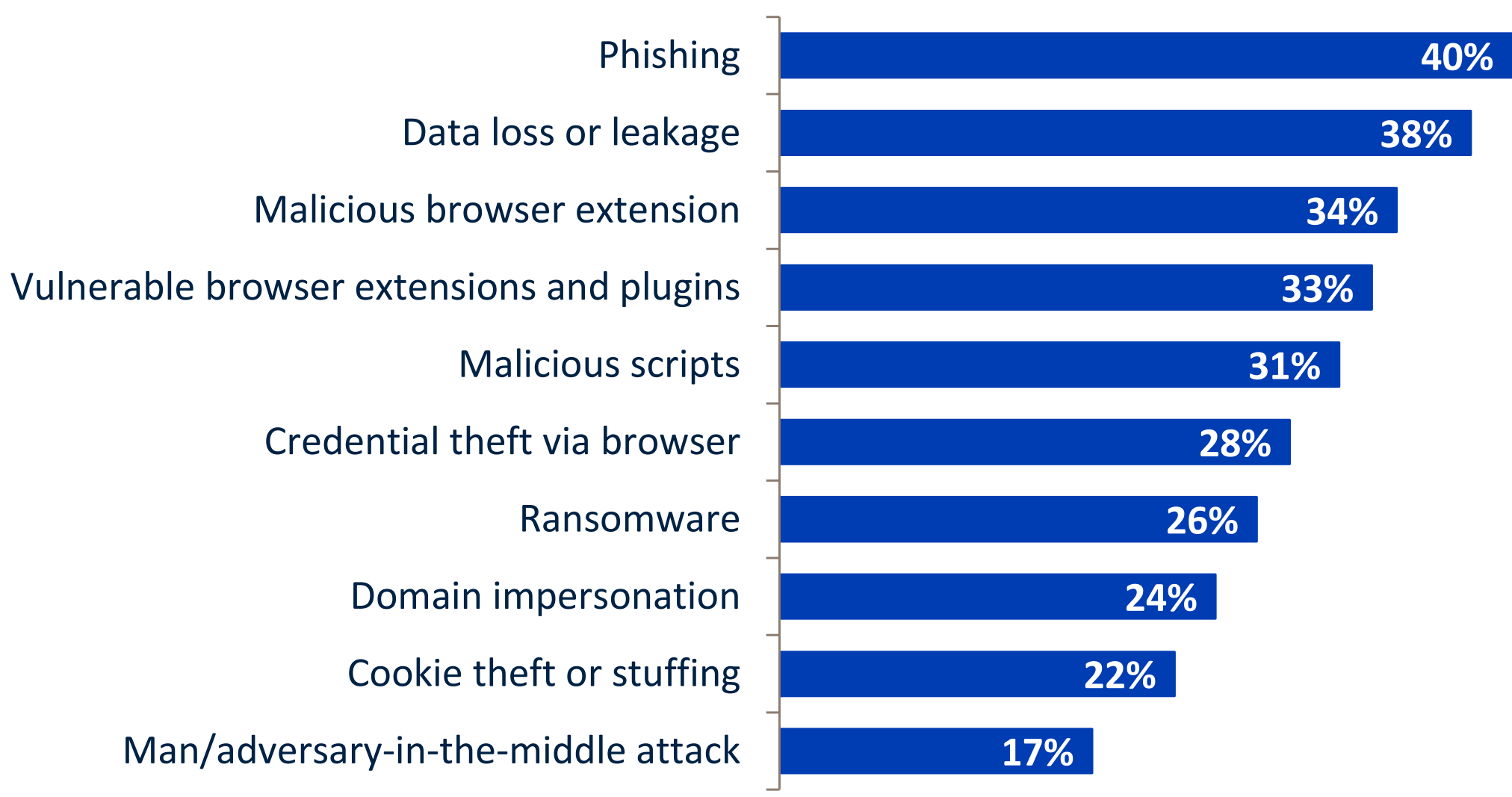
Browsers represent a growing portion of the overall security incidents experienced by respondents, with 68% noting an increase in them over the past two years. When asked about the previous 12 months, more than half (55%) of respondents said they'd been the victim of such an attack or could have been, with 22% saying they'd experienced multiple successful attacks.

The methods or types of attacks vary, with phishing and data loss edging out browser-specific attacks such as malicious browser extensions, vulnerable browser extensions, and malicious scripts. Given the amount of attention organizations reportedly pay to browser extension security, the number of incidents related to browsers would suggest there's still room for improvement.

Have organizations been the victim of a successful attack or security incident via an employee's web browsing or browser-based application use in the last 12 months?



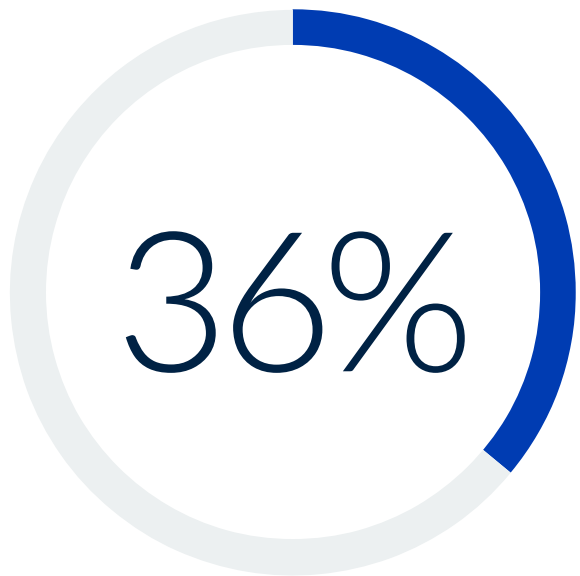
Type of web- or browser-based attack or security incidents experienced.



Browser Security Is a Clear Priority

How have emerging browser threats affected organizations' spending habits? More than one-third (36%) of organizations report that these new threats have caused them to significantly increase their browser security investments, with another 61% indicating they have increased their browser security spending to some extent. Additionally, even with all the other attack vectors security teams must contend with (e.g., AI, cloud, supply chain, insider risk, etc.), browser security is at least a top five priority for nearly nine of 10 respondents. It is clear that organizations understand the role browsers play in the organization and the need to give them additional security attention.

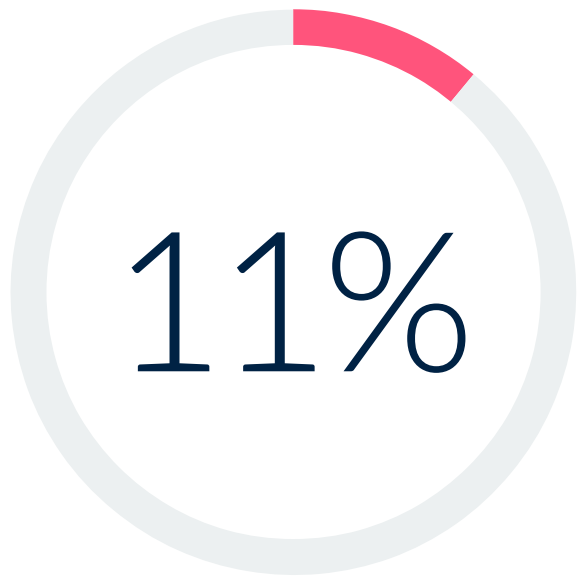
How emerging threats have changed browser security investment priorities.



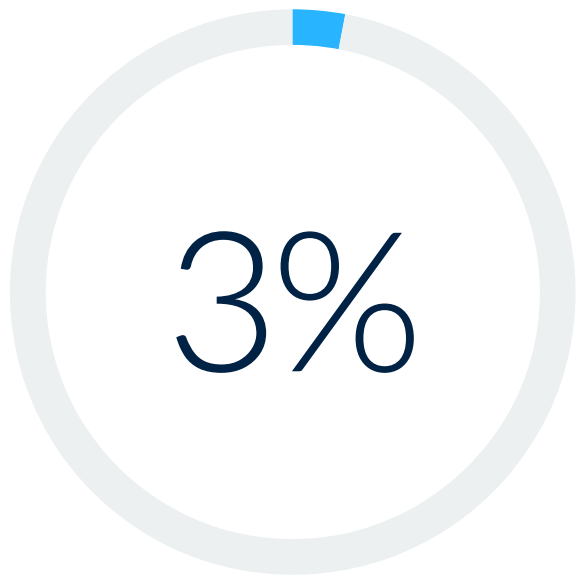
Significantly increased browser security investments



Moderately increased browser security investments

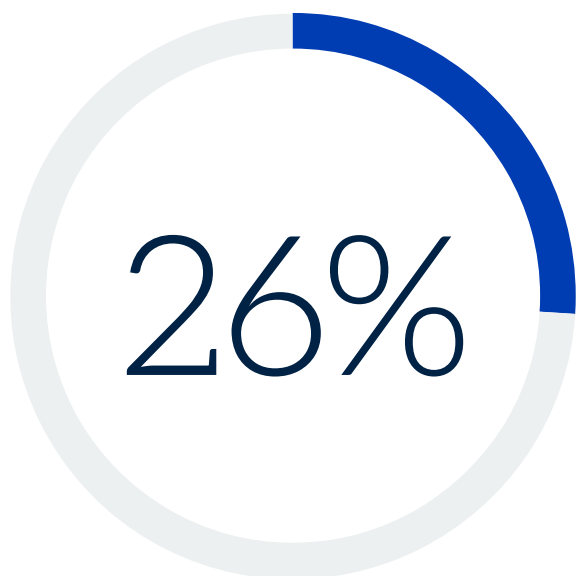


Slightly increased browser security investments

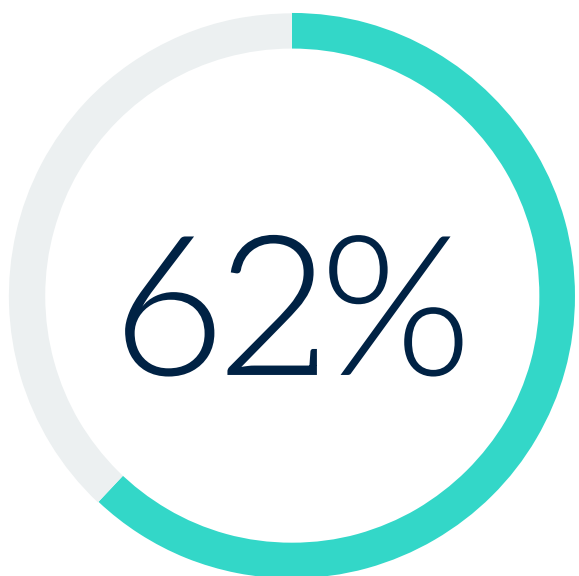


Has had minimal impact on browser security investments

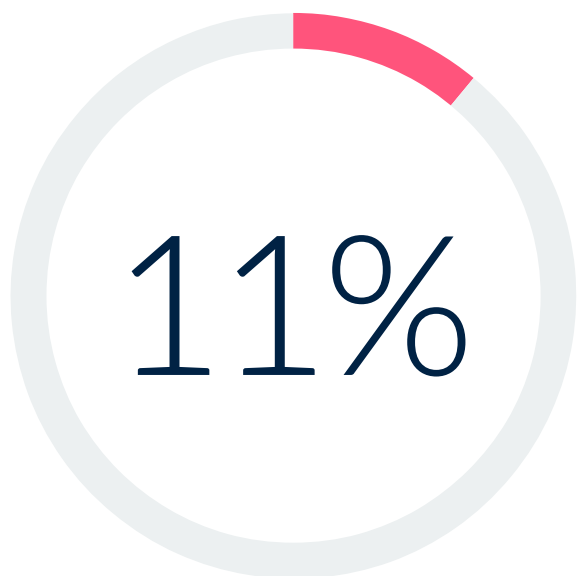
How browser security ranks among overall security priorities.



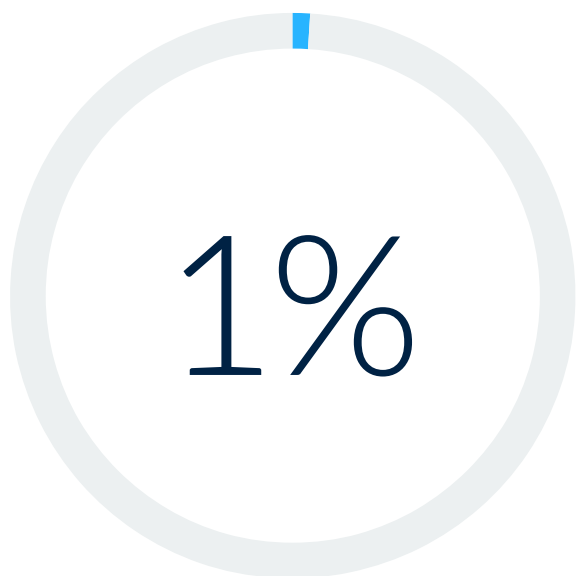
It is our top security priority



It is a top five security priority



It is a top 10 security priority



It is not a top security priority

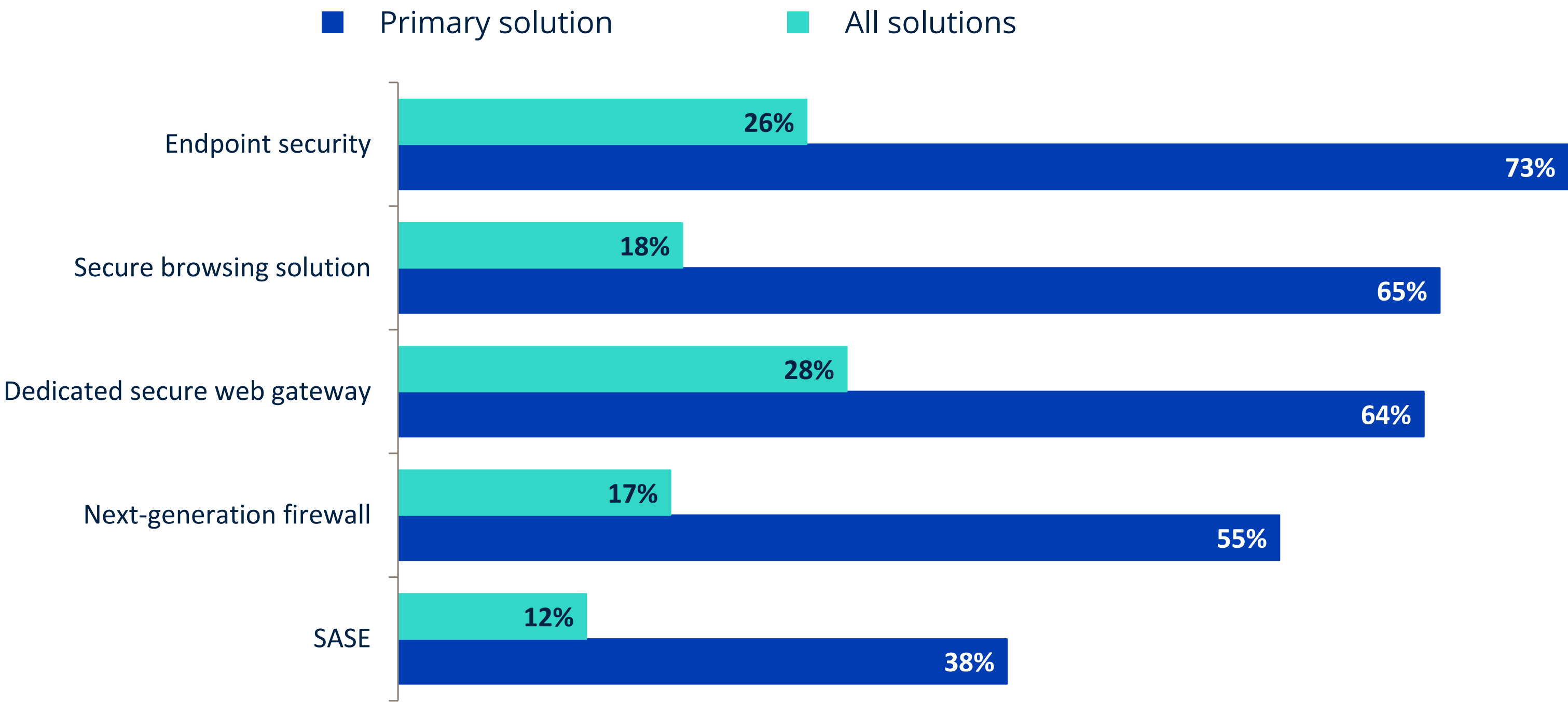


Existing Approaches Are Fragmented,
and Many Cite Challenges

Secure Browsing Is Often Used, but Less Often as the Primary Tool

Similar to the findings regarding the tools used for application access, secure browsing solutions are currently part of a layered approach to protecting against web- and browser-based threats. Nearly two-thirds (65%) indicate that they use secure browsing solutions, though only 18% indicated it was their primary approach. While this was behind endpoint security and secure web gateways, it bears repeating that this is a newer market that has already seen strong adoption.

Solutions organizations use to protect against web- and browser-based threats.

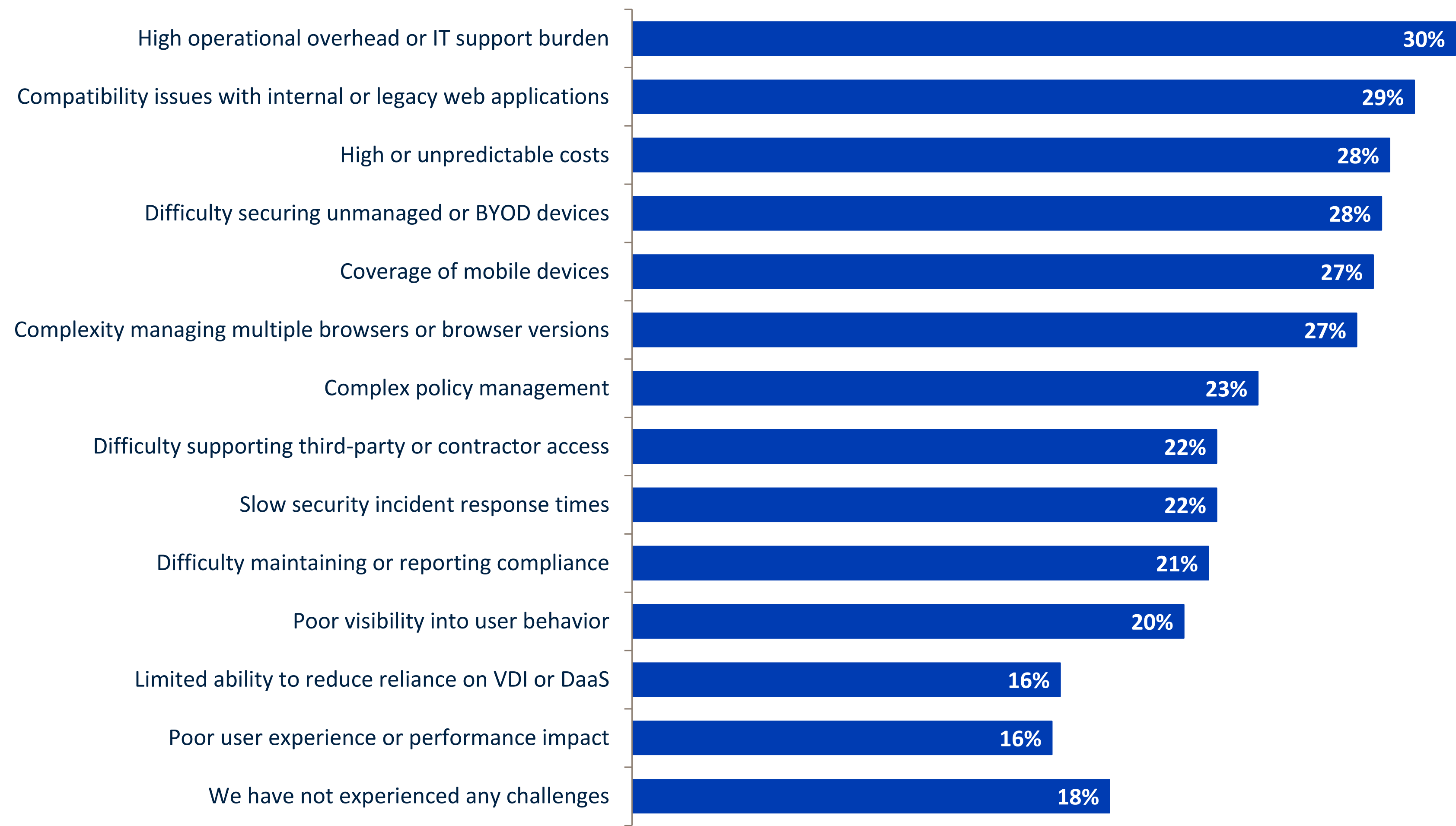


“Nearly two-thirds (65%) indicate that they use secure browsing solutions, though only 18% indicated it was their primary approach.”

Organizations Experience Many Challenges With Traditional Browser Security, but None Are Acute

Part of the reason that so many are turning to secure browsing solutions are the challenges they face from traditional tools. In fact, 82% of respondents using traditional tools as their primary browser security approach cited at least one challenge. These issues can range from operational issues, through cost, to use case coverage. With regard to use cases, compatibility with internal or legacy web applications (29%), difficulty securing unmanaged or BYOD devices (28%), coverage of mobile devices (27%), and difficulty supporting third-party contractor access (22%) were all prominently mentioned. In the long term, organizations need browser security tools that can address all these use cases to limit tool sprawl and reduce complexity.

Challenges organization have experienced with their current primary browser security approach.

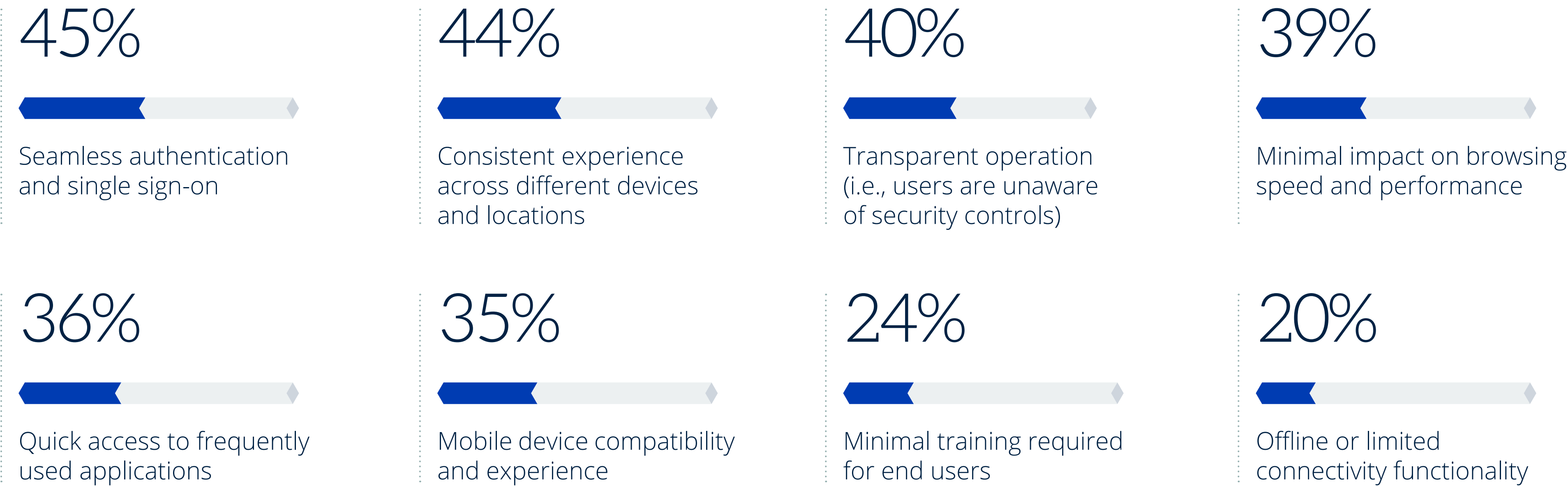


Balancing Security With Productivity and Experience Remains a Challenge

While 40% of respondents said they try to balance browser security with user productivity equally, 56% said they prioritize security.

Ideally, organizations would not have to choose between strong security and use enablement. When it comes to user experience, performance is important as evidenced by 39% of respondents citing it, but ease of use was more commonly mentioned. Specifically, seamless authentication and single sign-on (45%), consistent experience across devices and locations (44%), and transparent operation (40%) were the top responses.

User experience factors that are most important when evaluating browser security solutions.





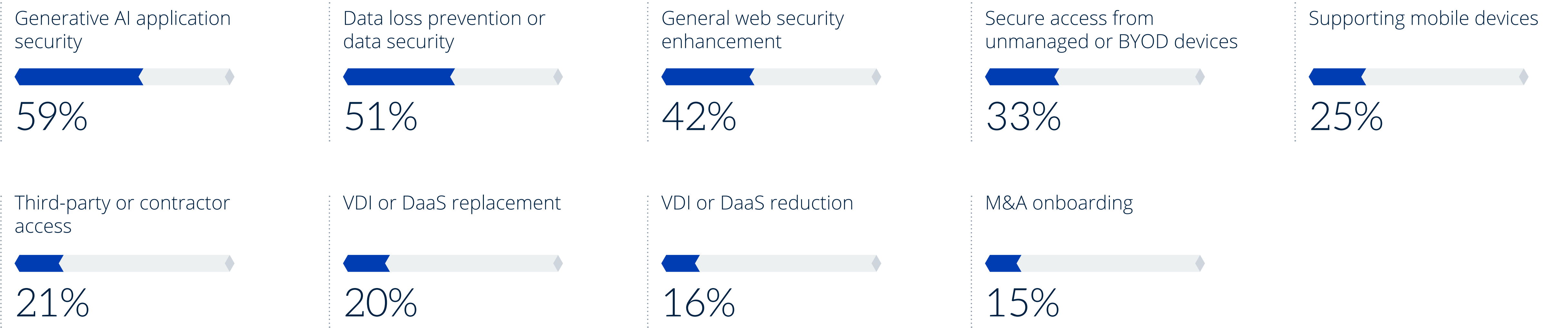
Enterprise Browsers Lead a Crowded
Space, but Use Cases, Features, and
Approaches Vary

Security Versus Access

Secure browsing solutions can be applied to many use cases across both security and secure access. Interestingly, the research revealed that security use cases rated higher. Generative AI security (59%), data loss prevention or data security (51%), and general web security (42%) were ahead of often highlighted use cases such as secure access from unmanaged or BYOD devices (33%) and third-party or contractor access (21%). In fairness, generative AI security can encompass the access component as well, but the broader point is that security is a priority.

This is not intended to imply that access is unimportant. Rather that security teams realize they have a glaring need around emerging technologies like generative AI, as well as defending against emerging threats that other tools cannot address.

Most important use cases for a secure browsing solution.

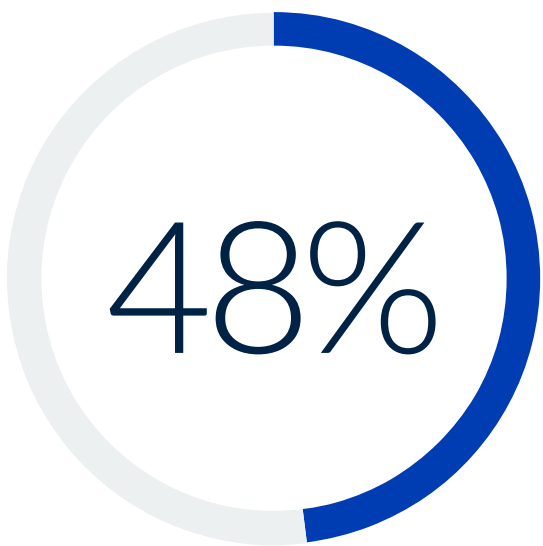


Enterprise Browsers Lead the Interest in Secure Browsing Solutions, but Organizations Are Looking for an Integrated Mix of Solutions

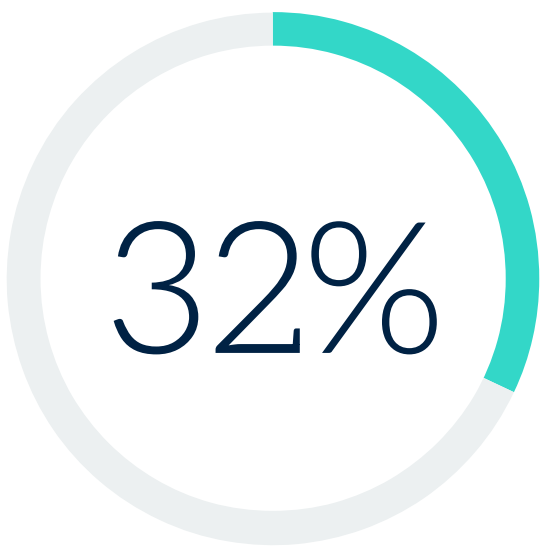
Given the interest in enterprise browsers over the past few years, it's not surprising to see that 30% of respondents ranked them as their most preferred secure browsing solution. However, managed standard browsers and, to a lesser extent, VDI still rank highly as ways of delivering browser-based applications. VDI preference numbers in this case are specifically about browser-based applications and will no doubt be significantly larger for Windows applications.

Though enterprise browsers are the clear preference, most organizations prefer to lean on a system that leverages a mix of solutions (integrated or not), rather than outright replacing tools. This shows that organizations are conscious of using the right tool for the right job, as opposed to consolidating at any cost.

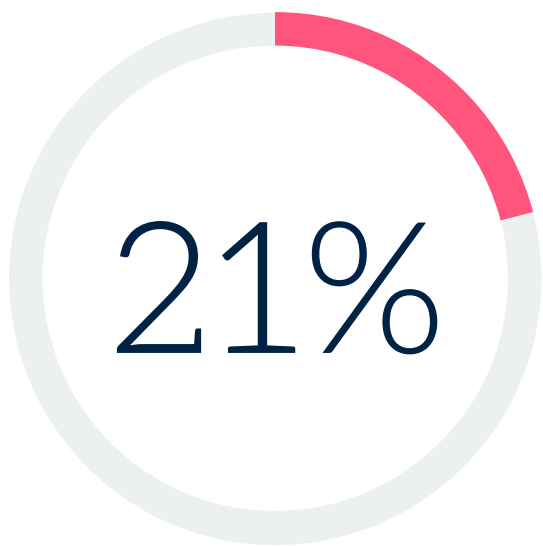
How organizations expect to use a secure browsing solution.



Use a secure browsing solution as an integrated part of existing solutions

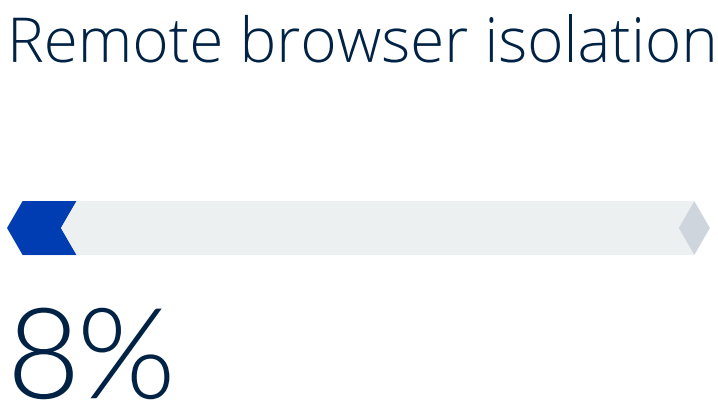
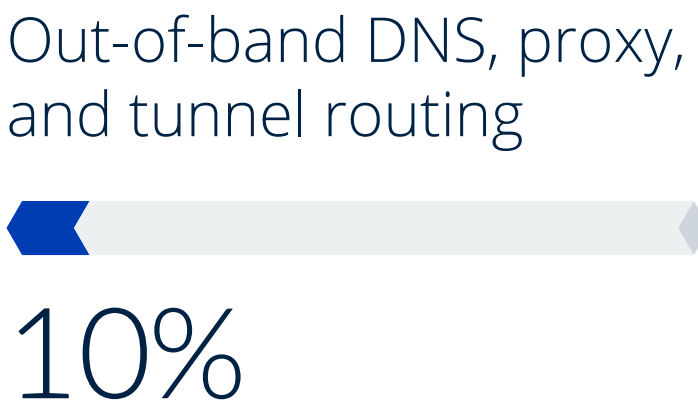
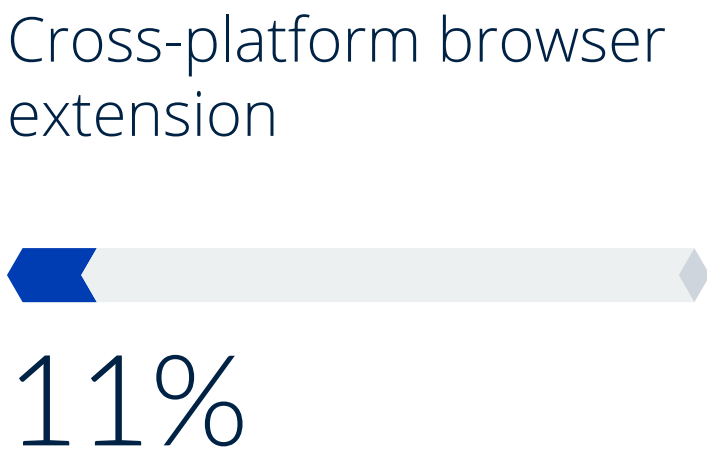
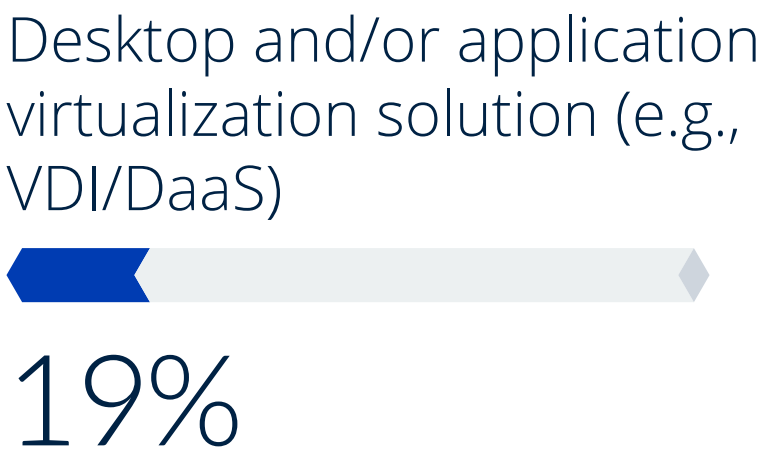
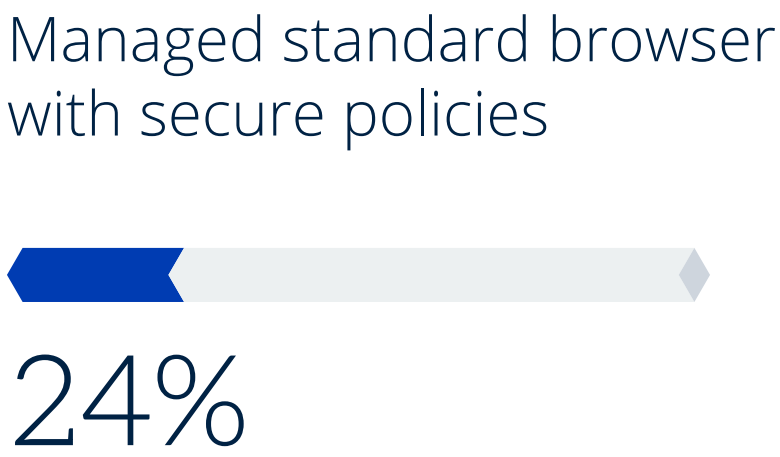
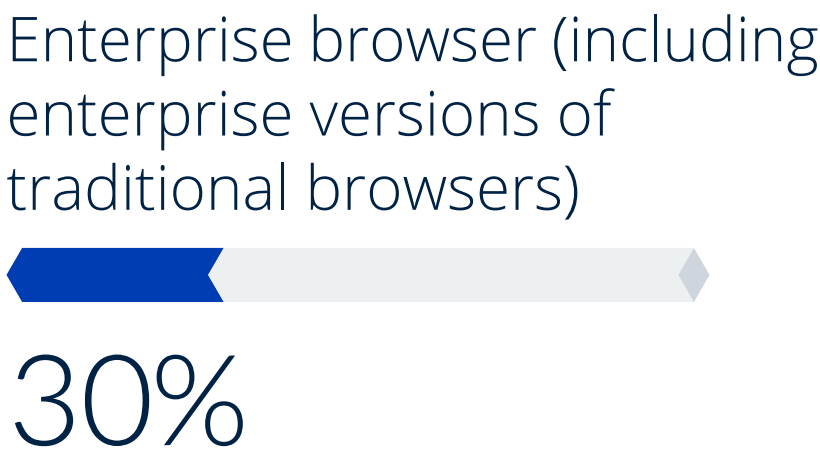


Use a secure browsing solution alongside existing solutions



Replace or retire existing solutions in favor of a secure browsing solution

Most preferred type of secure browsing solution.



Most Are Seeing Clear Benefits, and Expectations Generally Match Reality

Organizations expect—and realize—many benefits from deploying secure browsing solutions. In several cases, experienced benefits outweigh expectations, as is the case among those who reported fewer security incidents, better visibility and auditing, improved user experience, and simplified configuration.

It’s interesting to note that cost savings and VDI reduction or replacement are much further down the list for both expected and realized benefits. In fact, reducing operational costs is the biggest outlier in terms of expected benefits versus realized benefits. This suggests that the perceived value of browser security solutions trumps the desire to reduce costs or eliminate other tools.

Realized and expected benefits from using a secure browsing solution.



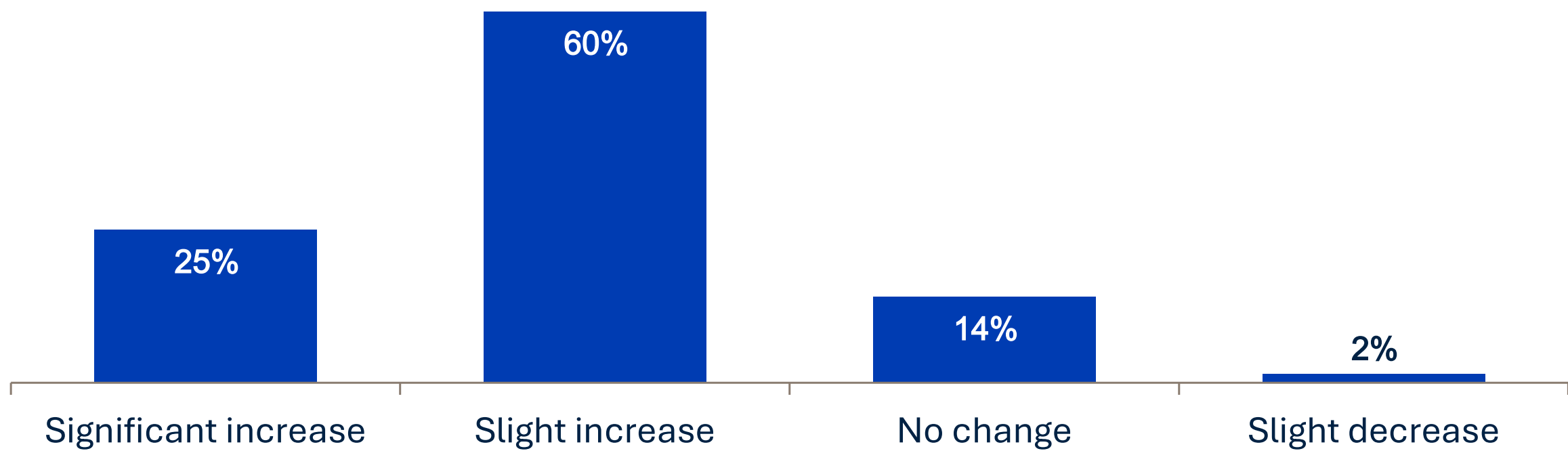


Funding Sources Vary, but Spending on
Secure Browser Solutions Is Strong

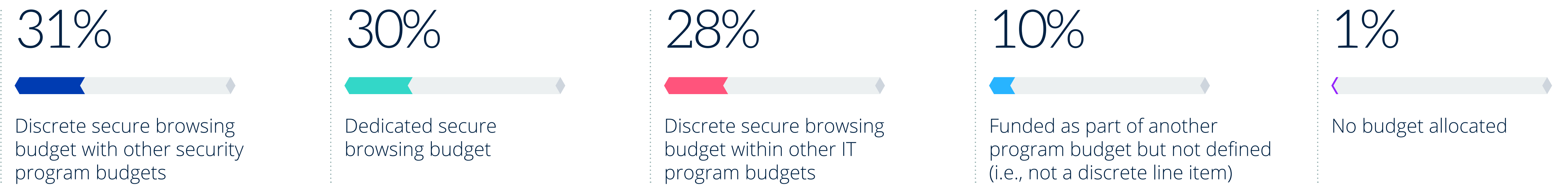
Funding Sources Vary, but Spending Appears Strong

As the market for secure browsing solutions is new, funding models can vary between organizations. Responses presented nearly an even split between allocating a dedicated secure browsing budget (30%), having discrete secure browsing budget within other security program budgets (31%), and having discrete secure browsing budget within other IT program budgets (28%). In the case of the latter two options, secure browsing could be part of web security, endpoint security, endpoint management, network security or SASE, or application delivery. Regardless of the model, 85% of organizations indicated they'd be increasing their secure browsing technology budget over the next 12-24 months, again highlighting the growing importance of this space.

Expected spending change for secure browsing technologies over the next 12-24 months.



Source from which a secure browsing solution is or will likely be funded.





ABOUT

Parallels is a global leader in cross-platform and virtualization solutions that make it simple for businesses and individuals to securely access applications and data on any device, anywhere.

Parallels operates two core businesses. Parallels Desktop enables individuals and organizations to run Windows applications on Mac computers, providing a seamless, native-like experience without changing devices or disrupting workflows. Parallels Workspace Solutions deliver simple, flexible, and secure virtual applications and desktops through Parallels RAS, Parallels DaaS, and Parallels Browser Isolation, offering a modern, cost-effective alternative to traditional VDI across hybrid and cloud environments.

Together, Parallels helps customers reduce complexity, streamline IT operations, improve security, and deliver a seamless user experience across Windows, macOS, Linux, ChromeOS, iOS, Android, the cloud, and emerging application models. To learn more, visit www.parallels.com.

Learn More

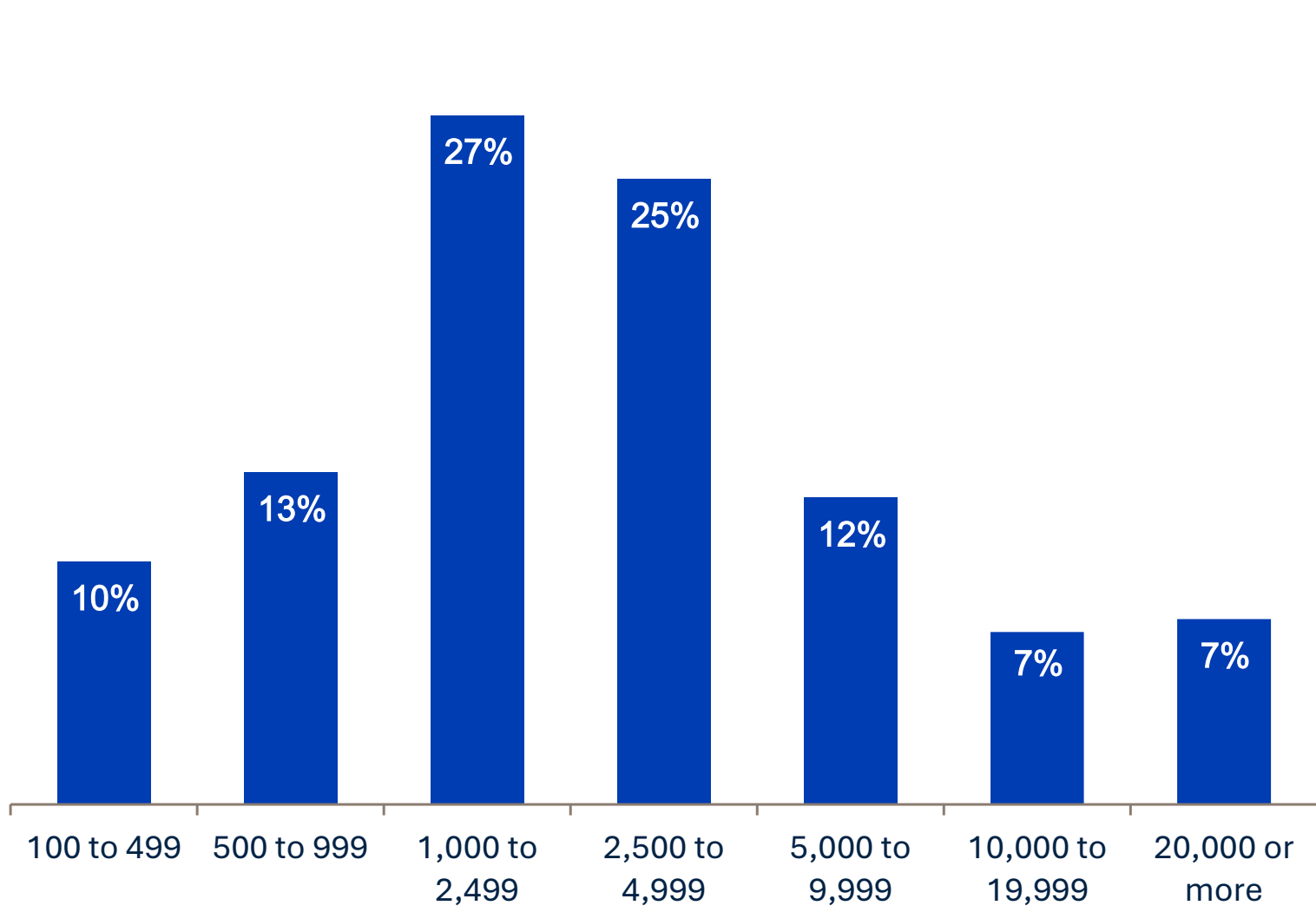


RESEARCH METHODOLOGY AND DEMOGRAPHICS

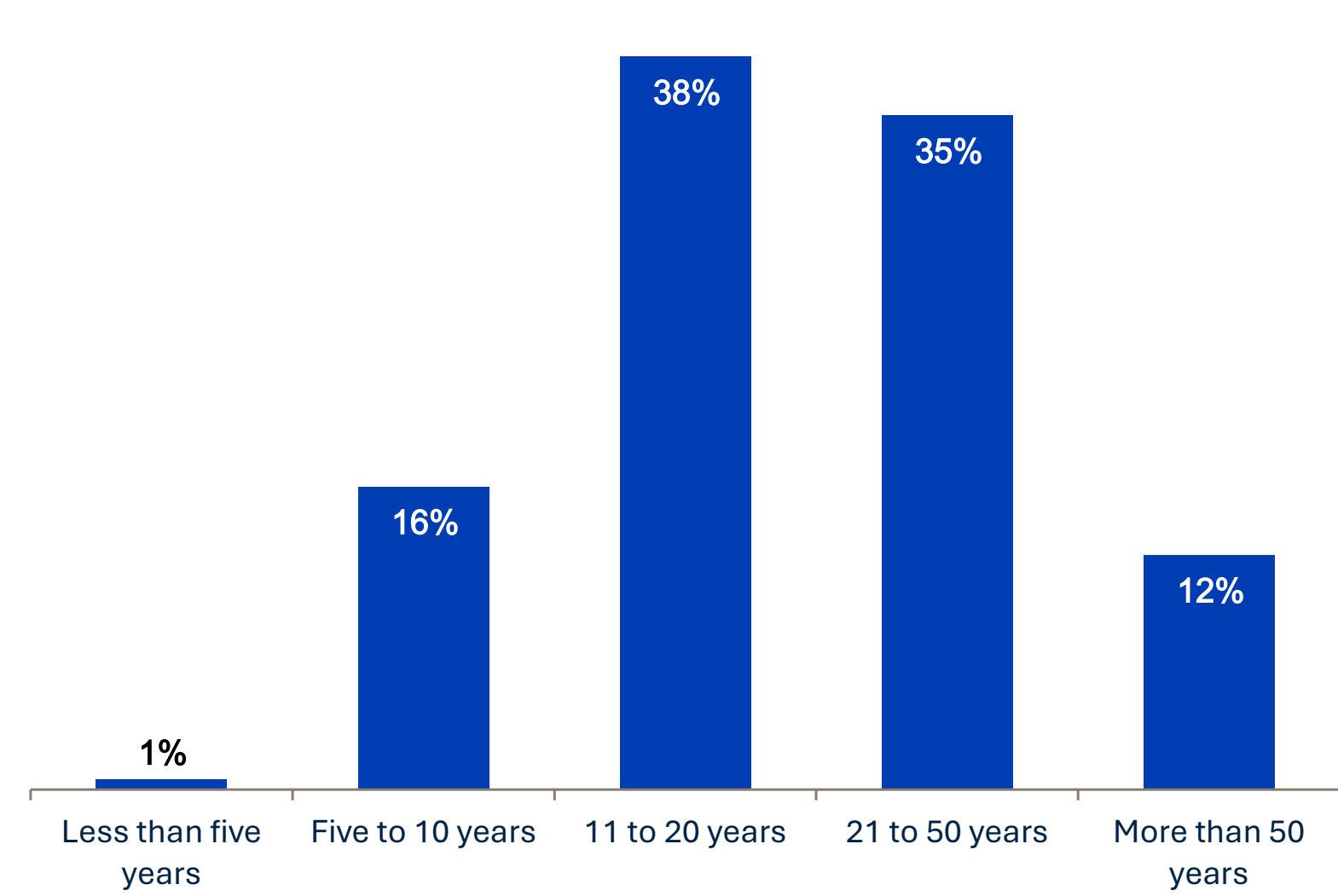
To gather data for this report, Omdia conducted a comprehensive online survey of IT and cybersecurity professionals from private- and public-sector organizations in North America between December 17, 2025, and January 13, 2026. To qualify for this survey, respondents were required to be responsible for securing devices, browsers, applications, and/or web usage at their organization. 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 several criteria) for data integrity, we were left with a final total sample of 400 of IT and cybersecurity professionals.

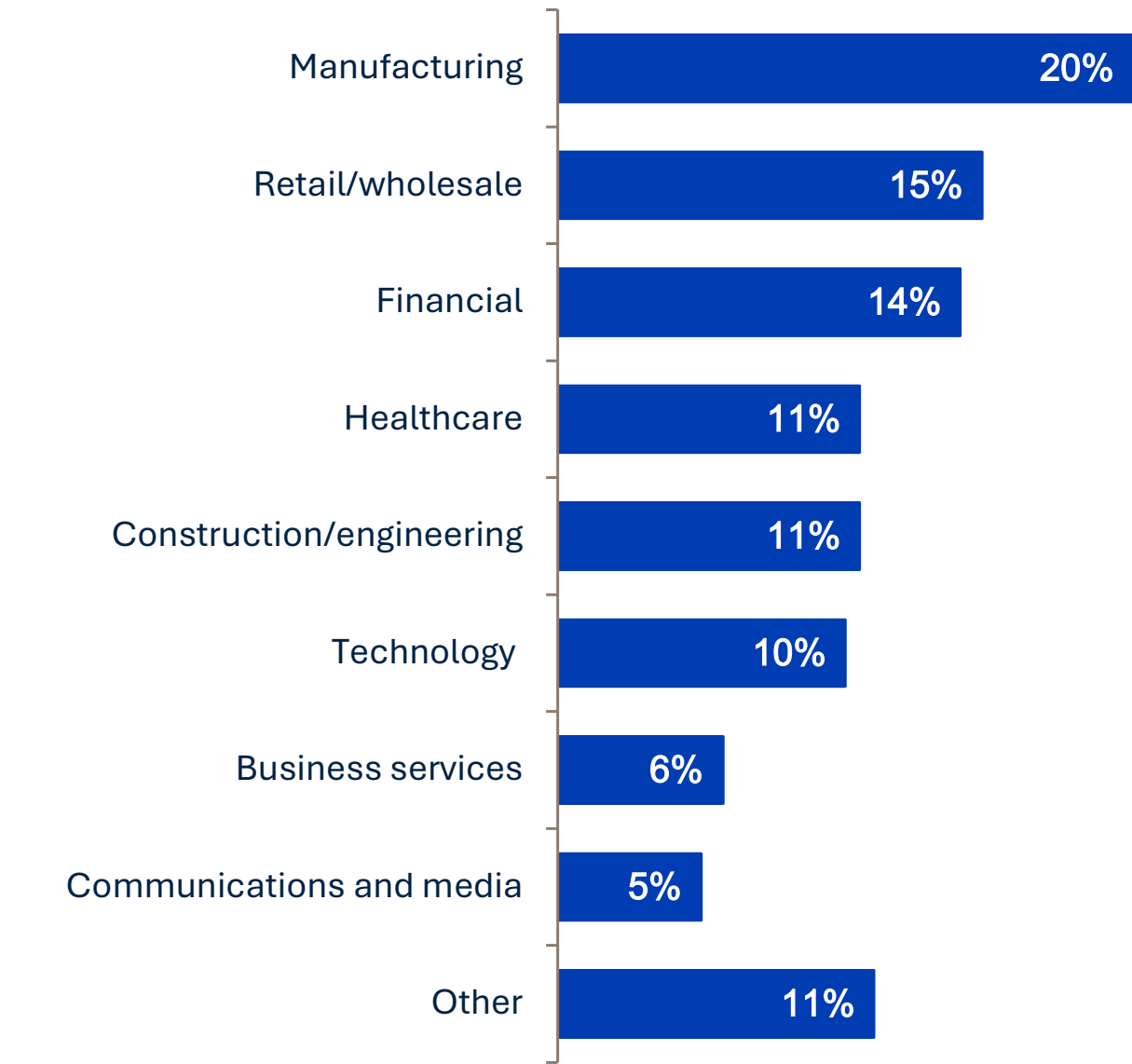
Respondents' organizations by number of employees.



Respondents' organizations by years in operation.



Respondents' organizations by industry.



©2026 TechTarget, Inc. d/b/a Informa TechTarget. All rights reserved. The Informa TechTarget name and logo are subject to license. All other logos are trademarks of their respective owners. Informa TechTarget reserves the right to make changes in specifications and other information contained in this document without prior notice.

Information contained in this publication has been obtained by sources Informa TechTarget considers to be reliable but is not warranted by Informa TechTarget. This publication may contain opinions of Informa TechTarget, which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent Informa TechTarget’s assumptions and expectations in light of currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, Informa 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 Informa 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.



Omdia 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.

© 2026 TechTarget, Inc. All Rights Reserved. Unauthorized reproduction prohibited.