Enterprise Strategy Group™

Modernization at Risk: Addressing Enterprise IT Tech Debt

Noman Pathan | Market Research Analyst
Gabe Knuth | Senior Analyst, End-user Computing & User Protection
ENTERPRISE STRATEGY GROUP

JULY 2025

Research Objectives

This eBook examines how organizations are adapting their application access strategies in response to evolving business needs and emerging approaches to address those needs. It is based on data collected via a custom research project conducted by Enterprise Strategy Group. This research sought to determine:

- **The role of browsers in organizational productivity and security goals.**
- **The challenges and investments organizations face with secure access technologies and their impact on organizational technical debt.**
- **How technical limitations impact these goals.**
- **The impact that enterprise browsers are having in these areas.**

While this research was conducted for Island, it was executed by Enterprise Strategy Group in a blinded fashion, such that respondents were not aware of the sponsor of the research.

The data discussed in this eBook is from a web-based survey of 500 IT and cybersecurity decision-makers in the United States at organizations with more than 1,000 employees across multiple verticals. For more information, please see the "Research Methodology and Respondent Demographics" section of this eBook.

HIGHLIGHTED FINDINGS:

Most enterprise applications are browser-based: Today, organizations reported that 52.5% of their business-critical apps are browser-based, and 75% of organizations indicated there will be an increase in browser-based application usage in the next 24 months.

Most sensitive data is accessed via a consumer web browser: 53% of organizations indicated that their sensitive data is accessed via consumer browsers (e.g. Chrome, Edge, Safari, Firefox, etc.).

26% of IT operational costs are attributable to technical debt: Technical debt impacts all areas of IT and results in higher maintenance costs, increased system vulnerabilities, and integration challenges, especially in areas like secure access to applications and data.

Enterprise browser usage is expected to grow: 85% said they believed an enterprise browser can help reduce technical debt in their organization.

Contents

BACK TO CONTENTS

The Hidden Enemy of Innovation: Technical Debt

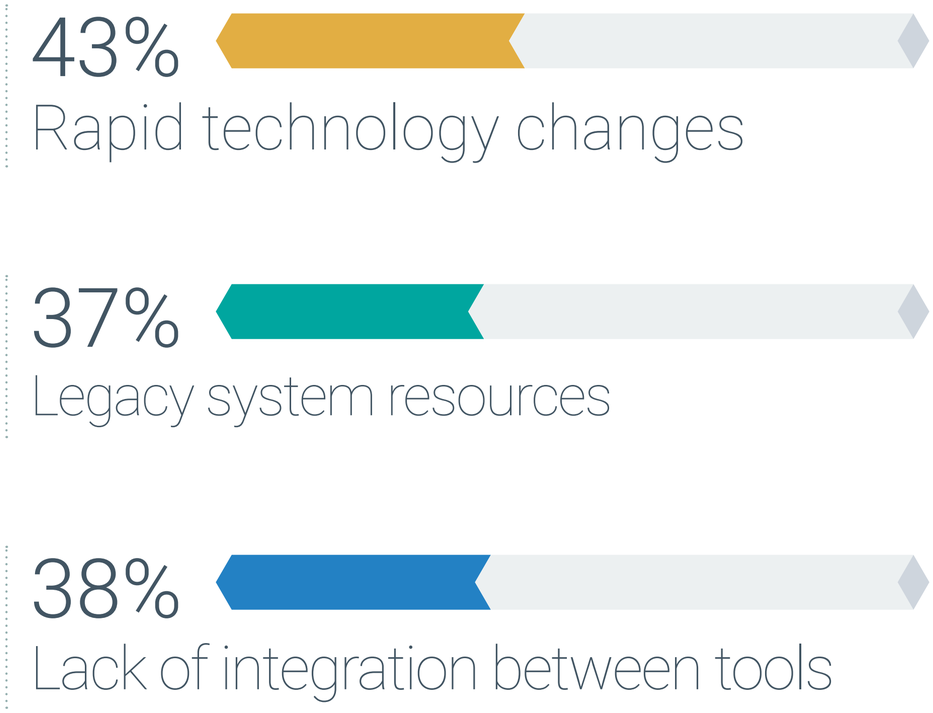
The Evolution of Enterprise Application Access

In response to emerging technology and growth opportunities over time, organizations have been in a constant state of adapting their application and data access strategies, leveraging the best available technologies at each step along the way. As technology evolves, though, often what was once a best-of-breed solution is replaced by something more capable or useful in modern contexts.

This continuous evolution can lead to technical debt, as organizations maintain existing systems while implementing new ones. Our research shows that the primary factors contributing to technical debt include rapid technology changes (43%), a lack of integration between tools (38%), and legacy system resources (37%). Additional factors like tight deadlines, changing requirements, mergers, and insufficient staffing also play a role, highlighting how technical debt often stems from having to balance immediate business needs with available options.

Managing technical debt requires understanding that past technology choices were often the best available options of their time, while remaining open to new purpose-built solutions as they emerge. This is even more important when considering the costs of tech debt.

Top Factors That Create Technical Debt.



Note: Respondents could choose up to three answers.

BACK TO CONTENTS

"Across enterprises, research shows that 26% of IT operating costs are attributed to **maintaining existing technology infrastructure** characterized as technical debt—nearly 6% of the overall IT budget."

From Limited Options to Growing Complexity: The Cost of Technology Evolution

Across enterprises, research shows that 26% of IT operating costs are attributed to maintaining existing technology infrastructure characterized as technical debt—nearly 6% of the overall IT budget. While that represents a significant financial investment, the impacts extend beyond IT to end users, security, and the business itself. Organizations identified the following as some of the biggest burdens from the accrual of new technologies:

47%
Higher maintenance costs: Managing and maintaining various systems requires significant resources.

37%
IT team dissatisfaction: Technology teams face increasing complexity in managing multiple solutions.

36%
Increased system vulnerabilities: The combination of various tools and systems can expand the attack surface.

30%
Integration challenges: Connecting existing systems with new technologies creates additional complexity.

These impacts shine a light on a key challenge in enterprise technology: Even when organizations make the best choices available to them, the accumulation of necessary but separate tools and systems can create both operational and security challenges (i.e., tech debt).

This is particularly evident in organizational efforts to provide secure access to sensitive data and applications, where many approaches have been implemented over the years and remain in use today, like VDI, remote browser isolation, and VPNs.

BACK TO CONTENTS

Diverse Application and Sensitive Data Access Approaches Expand Risk

Organizations have adapted their application and data access approaches to meet changing business needs, implementing solutions that made the most sense for their requirements at each stage. Today, this has resulted in diverse data environments that reflect years of strategic choices.

The research illustrates this diversity: 77% of organizations maintain sensitive data in cloud storage and file sharing tools, while 68% operate in hybrid cloud environments. Organizations also keep sensitive data in SaaS applications, on-premises locations, public cloud infrastructure, or even on the endpoints themselves.

The result is a complex landscape that has involved multiple different access solutions that were the best options at the time of deployment. This environment presents natural challenges, especially regarding security. Organizations in this study reported an average of six sensitive data leakage incidents in the last 12 months, with 25% experiencing more than 10 incidents.

With browser-based applications becoming increasingly central to how organizations operate, the way enterprises approach application access and security is evolving once again. As we'll explore in the next section, this shift presents both new considerations and opportunities for modernization (and the elimination of tech debt).

Where Sensitive Data Resides: Organizations Often Use Multiple Approaches.

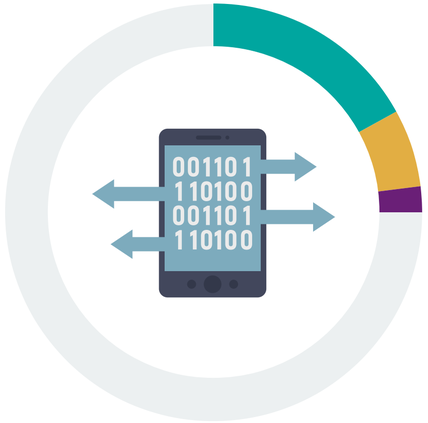
77%

Cloud storage and file sharing tools

68%

Hybrid cloud

Sensitive Data Leakage or Suspected Leakage Events in the Last 12 Months.



17%
11 to 15

6%
16 to 20

2%
More than 20

BACK TO CONTENTS

Browser-based Applications: Evolution and Opportunity

"According to the research, **more than half of business-critical applications (51%) are browser-based,** and reliance on browser-based applications is expected to increase in the next 24 months, as reported by 75% of respondents."

Browser-based Applications: The New Standard

According to the research, more than half of business-critical applications (51%) are browser-based, and reliance on browser-based applications is expected to increase in the next 24 months, as reported by 75% of respondents.

This momentum toward the browser-based apps has been building for some time and is the direct result of a couple of different trends:

1. **Device flexibility:** Browser-based applications work across different devices and operating systems, eliminating the need to develop and maintain separate versions for each platform.
2. **Simplified management:** Browser-based applications reduce the overhead of installing, patching, and maintaining traditional desktop applications.

As browser-based applications grew in popularity, organizations adapted by implementing various secure access technologies like VPNs, desktop virtualization (VDI and DaaS), and remote browser isolation. These solutions represented the best available options at the time, helping organizations balance security and accessibility needs.

While these tools continue to serve their purpose (which can often be in support of other, non-browser app use cases), organizations are now exploring ways to simplify their application delivery approach as browser-based applications become even more central to business operations.

The Usage of Browser-based Applications Over the Next 24 Months.

BACK TO CONTENTS

The Growing Role of Browser-based Access

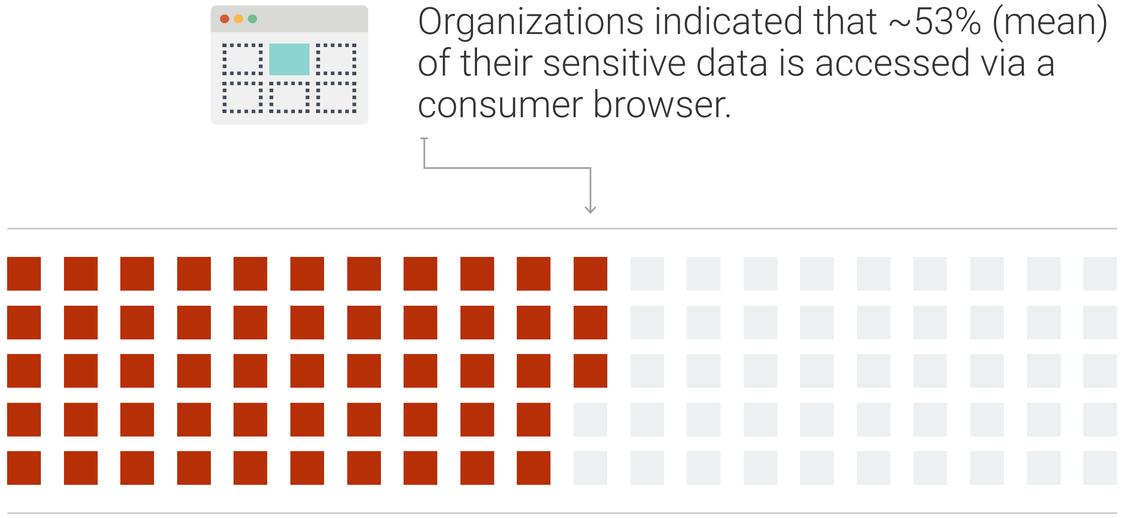
The increasing role of browsers in modern business applications is clear: Research shows that 53% of sensitive data is accessed through browsers. This highlights how effectively browsers have enabled secure app and data access across cloud, hybrid, remote, and on-premises environments.

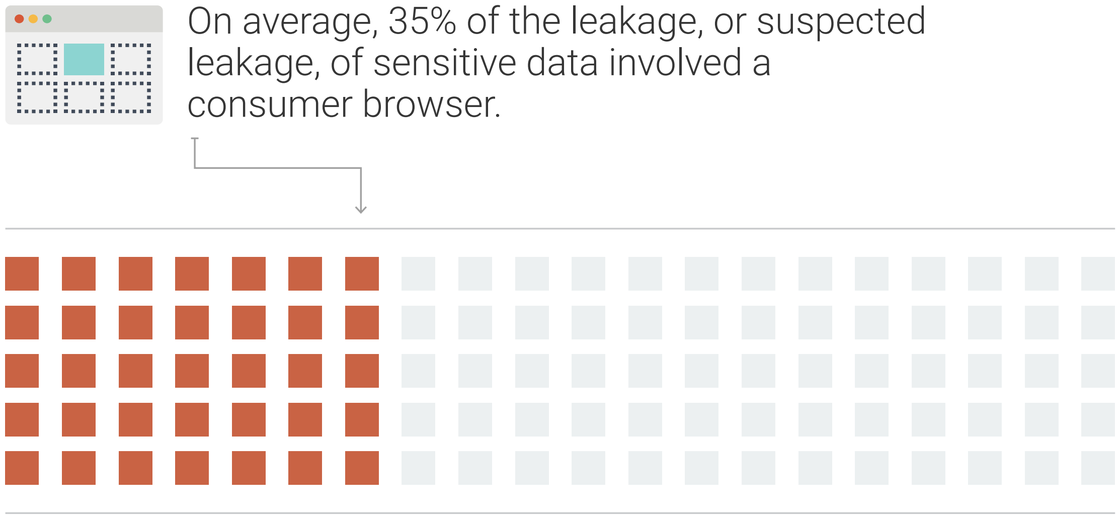
While browsers excel at providing seamless access to applications and data, the only available options in the early phase of the browser-app era were general-purpose consumer browsers. To make them work more effectively with enterprise workloads and regulations, organizations built additional security and management capabilities around them.

Despite this, an average of **35% of sensitive data leakage events involve browser access,** reflecting both the volume of sensitive data flowing through browsers and the complexity of securing this traffic across diverse environments.

This extensive reliance on browsers for sensitive data access, combined with the growing adoption of browser-based applications and the high amount of data leakage through the browser, suggests an opportunity to revisit how organizations approach browser deployment and management.

The Browser Is Increasingly Used to Access Sensitive Information.





BACK TO CONTENTS

Evolving Browser Security for Modern Needs

The importance of modernization becomes even more pronounced when looking at the likelihood of future data leakage events organization-wide. 59% of organizations said they expect to experience a data leakage event in the future—a number that should serve as a wake-up call.

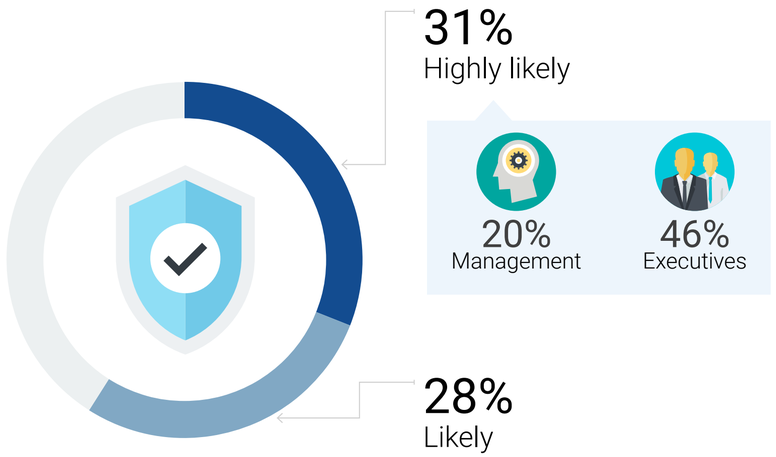
For the 81% of organizations that have reported 10 or more data leakage events in the past year involving a browser, the consequences, both long- and short-term, have been significant:

- Short-term effects include increased security measures (61%) and operational disruptions (46%).
- Long-term effects include reputational damage (39%) and competitive disadvantage (33%).

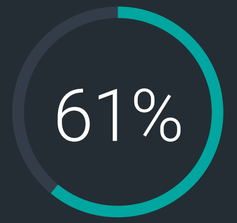
These outcomes highlight the complexity of securing access to applications and data and often tie directly to aspects of technical debt that stem from using legacy security and access technologies to deliver modern workloads.

Because the future of access to apps and data revolves around the browser, organizations need to consider modern approaches that can amplify the benefits of browsers while improving security and compliance to mitigate risk.

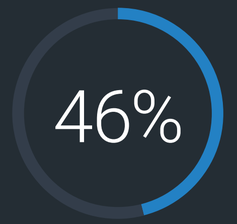
Likelihood of Data Leakage Occurring Based on Current IT and Security infrastructure.



Top Business Impacts Due to Sensitive Data Loss Events Over the Last 12 Months.

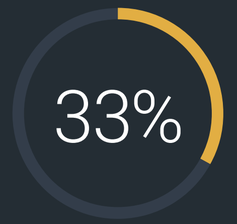


Increased security measures



Operational disruption

Reputation damage



Competitive disadvantage

BACK TO CONTENTS

Browser-based Access: Unlocking New Possibilities

Browser-based application access represents a significant advantage for organizations, with 85% agreeing that delivering applications through browsers improves the end-user experience. This makes sense since users already know how to use browsers, making them an ideal platform for application delivery.

The appeal extends beyond user experience to infrastructure optimization. 72% of organizations want to move away from desktop and application virtualization workloads that were deployed primarily to deliver access to web-based applications. This shows a clear desire to reduce costs and eliminate complex infrastructure that was necessary in the past but may no longer align with modern needs.

With browsers now the primary method of app delivery, the industry has reached a point where a need to modernize browser and browser app delivery has emerged. While it's been possible to secure access and centrally configure some aspects of consumer browsers (e.g., general purpose browsers like Chrome, Firefox, Edge, and Safari) as if they were any other native OS application using classic secure access technologies, these tactics don't always do enough to address the needs of delivering modern browser-based apps, their sensitivity, or the sensitivity of the data. Worse, they may, in fact, contribute to technical debt.

As such, a new approach has emerged that combines the familiarity of the browser with modern secure access, compliance, and management capabilities called the enterprise browser. The next section explores how enterprise browsers are helping organizations achieve their objectives.

User Experience, Simplification, and Security Highlight the Need for Modernized Application Access.

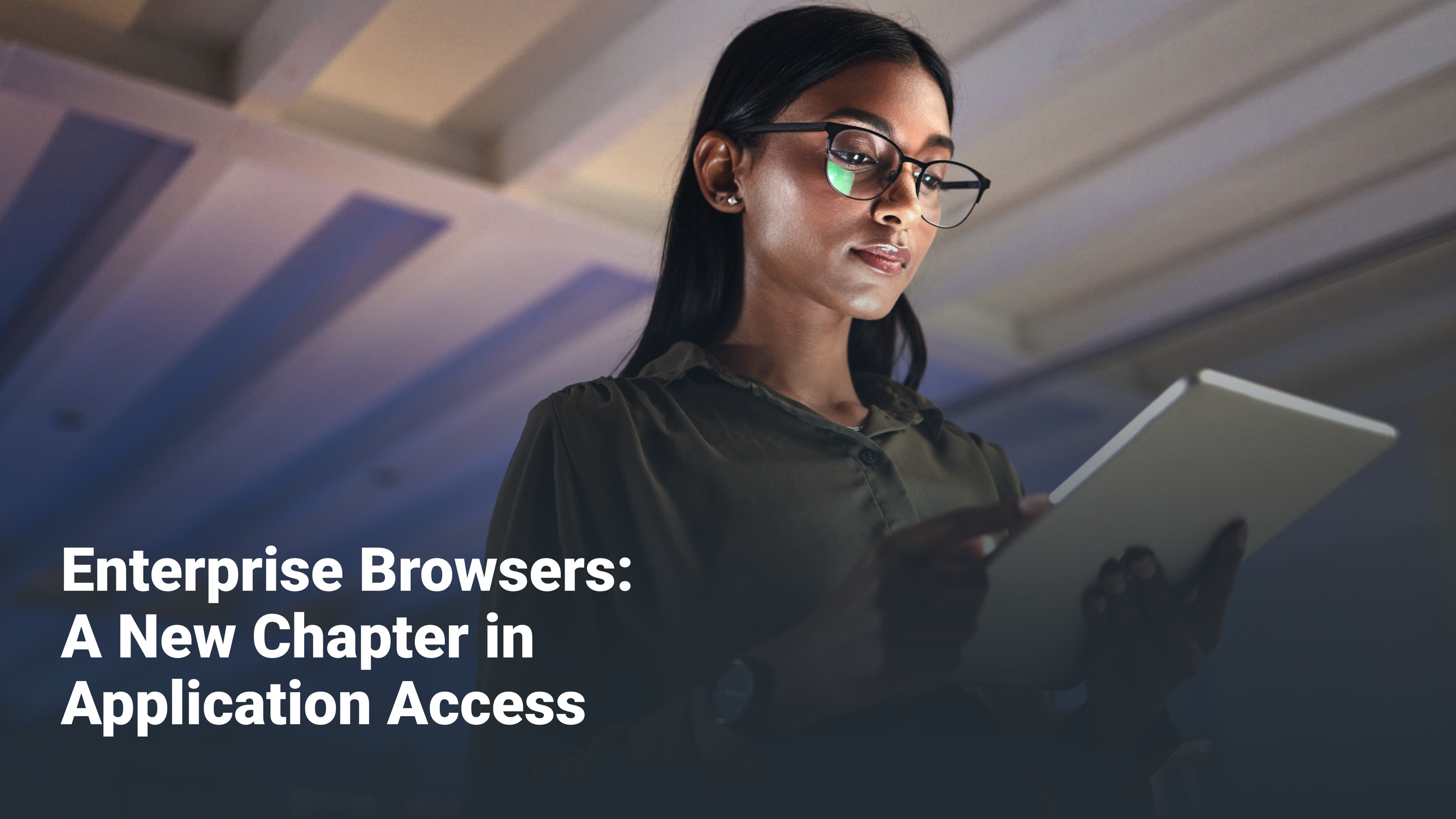
85%

I believe end-user experience would improve if we used a browser to access all of our applications (N=500)

72%

We want to eliminate desktop and app virtualization (e.g. VDI, remote browser isolation, etc.) as a mechanism to access web applications (N=241)

BACK TO CONTENTS



Enterprise Browsers: A New Chapter in Application Access

Enterprise Browsers: A New Chapter in Application Access

Organizations are clearly looking for alternative paths that are much simpler for their application delivery needs. One alternative—the enterprise browser—offers centralized management and built-in security tools that enable organizations to provide a familiar browser interface to end users, while enforcing security and compliance policies through centralized configuration.

What's particularly interesting about enterprise browsers is that, while the category itself is only about four years old, many organizations report having used them for much longer. This would indicate that, though organizations have experience with basic browser management through GPOs and other centralized settings or remote browser isolation techniques, true enterprise browsers, with their full suite of built-in security and management capabilities, represent something entirely new.

This also helps explain the acceleration observed in the market. As organizations learn more about enterprise browsers as a distinct category, interest continues to grow. Among organizations that haven't yet deployed an enterprise browser, 58% plan to do so in the next 12 months, with 88% planning deployment within two years.

This growth is exceptional, and it's driven by both the enormous need to deal with issues around browser security and technical debt, as well as the outcomes that enterprise browsers offer.

Plans to Deploy Enterprise Browsers.

- **20%** Less than 6 months
- **38%** Between 6 to 11 months
- **30%** 1 to 2 years
- **8%** 3 to 5 years
- **2%** More than 5 years

"What's particularly interesting about enterprise browsers is that, while the category itself is only about four years old, many organizations report having used them for much longer."

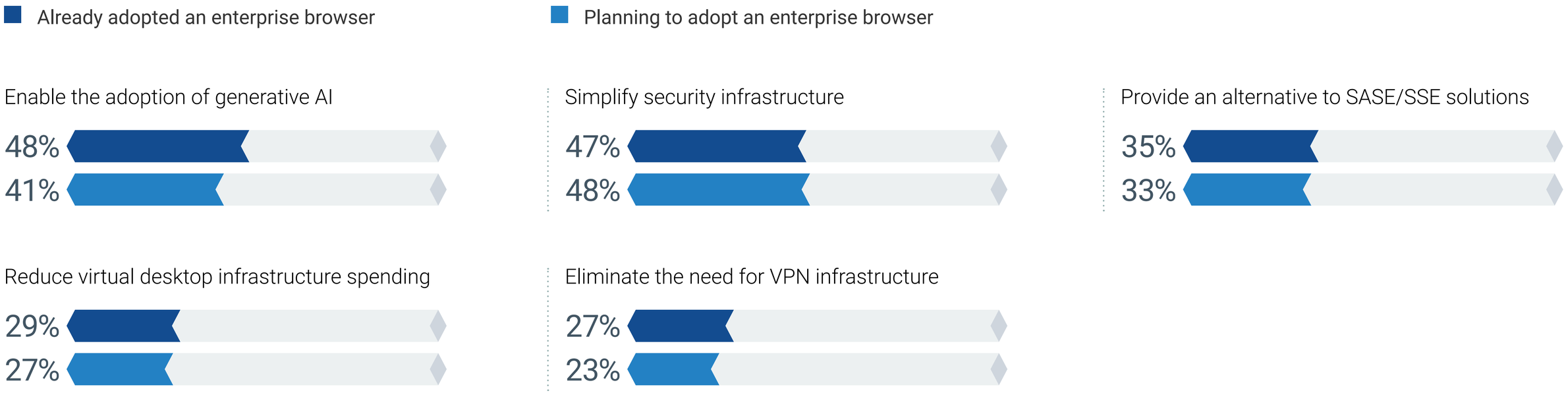
Enterprise Browsers Exceed Expectations

The growth and interest in enterprise browsers is even more impressive given the high-profile expectations that adopters had, which range from simplifying security infrastructure and providing alternatives to SASE/SSE solutions to eliminating the need for VPNs or desktop virtualization. These are all key elements to reducing technical debt and optimizing IT and security processes.

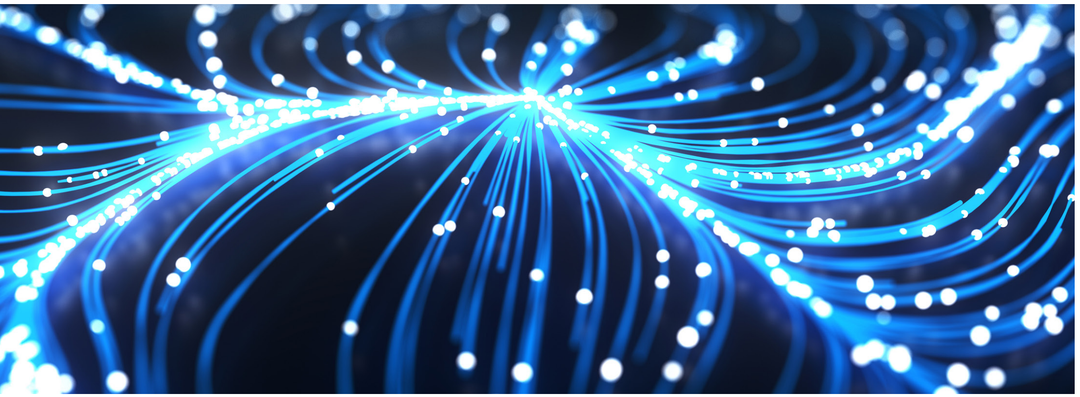
Interest extends beyond traditional secure access use cases. One particularly interesting finding is that 48% of organizations believe enterprise browsers enable their adoption of generative AI technologies. This is likely driven by concerns over the sensitive data that can be exchanged via browser-based AI tools and the need for enterprise-grade security controls at the browser level to mitigate these risks.

It's also a great example of the value of modernization, addressing today's application delivery needs, eliminating complexity and technical debt, and positioning organizations to confidently embrace emerging technologies.

Use Cases Organizations Want to Solve With the Adoption of an Enterprise Browser.



BACK TO CONTENTS



Enterprise Browsers Deliver Clear Value

Organizations that have already adopted enterprise browsers have reported overwhelmingly positive results that live up to their high expectations:

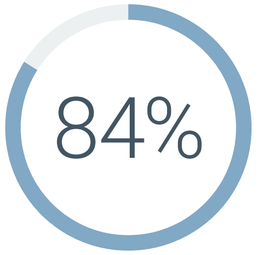
- 88% said enterprise browsers enabled their organization to solve use cases that were previously difficult to address.
- 85% said they believed the right enterprise browser could help reduce technical debt.
- 84% planned to increase their investments in enterprise browsers over the next 12 months.

It's clear that enterprise browsers are not just a tactical security measure. Rather, an enterprise browser can be a strategic enabler for IT modernization, as evidenced by clear improvements in security and operational efficiency, along with the belief that it can help reduce technical debt and enable new use cases.

Enterprise Browsers Are Seen as a Strategic Solution.

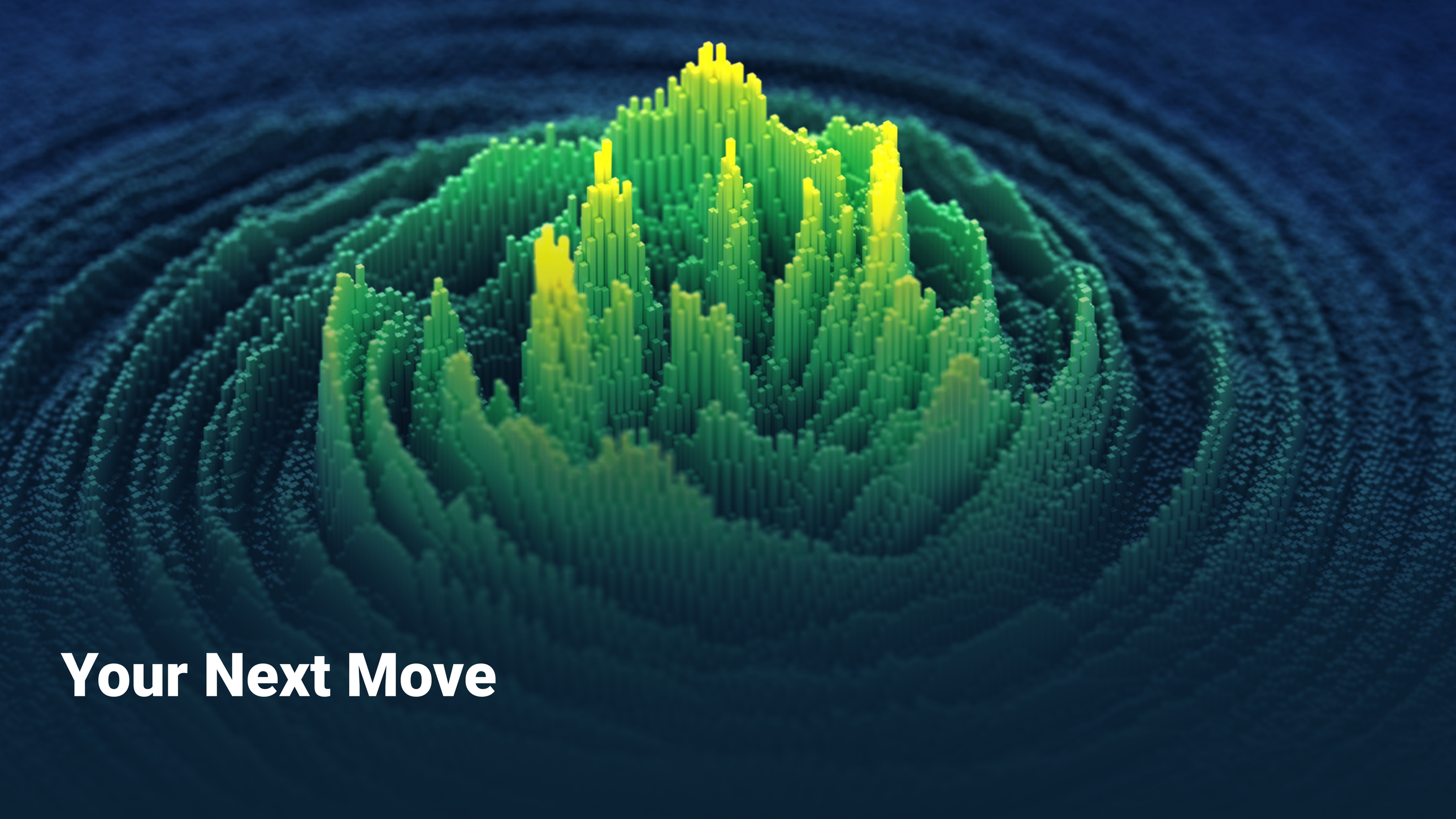
Enterprise browsers enabled our organization to solve use cases that were previously difficult to address

We believe the right enterprise browser can help us reduce technical debt at our organization



We plan to increase our investments allocated toward enterprise browser over the next 12 months

BACK TO CONTENTS



Your Next Move

Final Thoughts

This research highlighted how application access strategies evolve from one “best available” solution to another over time and how yesterday’s best available solution might be contributing to complexity, costs, and risk today in the form of technical debt.

One data point, in particular, speaks volumes: 26% of operating costs can be attributed to maintaining existing technology infrastructure described by respondents as “technical debt.” This is the result of years of implementing tools and solutions to meet business requirements—each the right choice for its time but collectively contributing to growing complexity.

Browser-based applications represent the latest evolution in application access, with 53% of sensitive data already accessed through browsers and 75% of organizations expecting browser-based application usage to increase over the next 24 months. To date, this has mostly been accomplished with general-purpose browsers, coupled with various existing security and management approaches. While effective compared to doing nothing, the research shows that 35% of data leakage events still involve a browser, so a modern alternative is needed.

Enterprise browsers have emerged as a new option in application access, offering built-in security and management capabilities while maintaining familiar interfaces. What’s more, enterprise browsers meet—and exceed—customer expectations, which is leading to its rapid adoption, with 84% of organizations planning to increase investments in enterprise browsers this year.

While considering application access strategies, especially as they relate to the browser, IT and security leaders should ask themselves:

- How does the organization’s current application access strategy align with where the organization is headed?
- What opportunities exist to reduce complexity while improving security and user experience?

With the introduction of enterprise browsers, organizations now have new options to modernize their application delivery strategy, while maintaining the flexibility to embrace emerging technologies and use cases.

BACK TO CONTENTS

Island

How Island Can Help

Island's Enterprise Browser technology provides a secure, centrally managed alternative to consumer browsers and remote browser isolation that helps organizations protect sensitive data, simplify IT operations, and improve productivity.

LEARN MORE

RESEARCH METHODOLOGY AND DEMOGRAPHICS

To gather data for this eBook, Enterprise Strategy Group conducted a comprehensive online survey of 500 IT and cybersecurity decision-makers involved with their organizations' purchase process for endpoint devices.

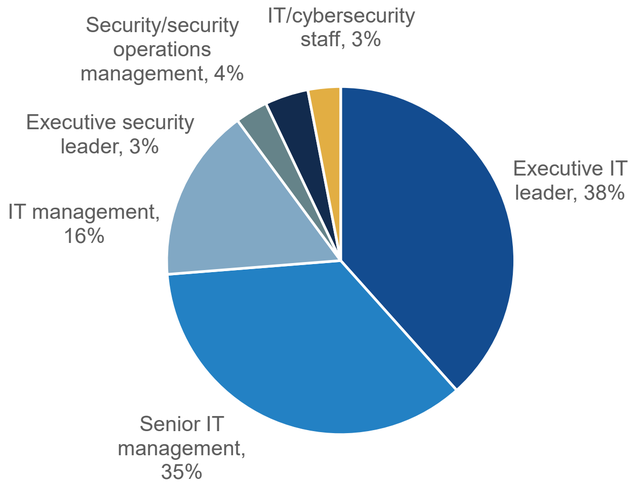
All organizations represented were in the enterprise market segment (i.e., greater than 1,000 employees) and span all private- and public-sector verticals.

The survey was fielded between October 15, 2024 and November 18, 2024.

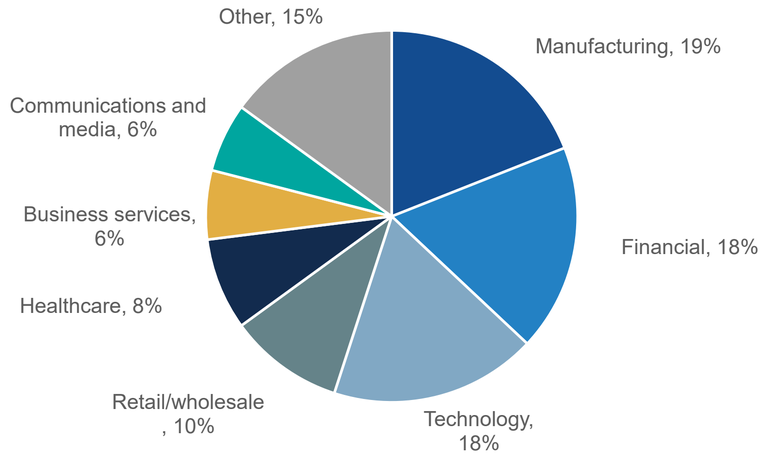
The margin of error at the 95% confidence level for this sample size is + or - 7 percentage points.

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

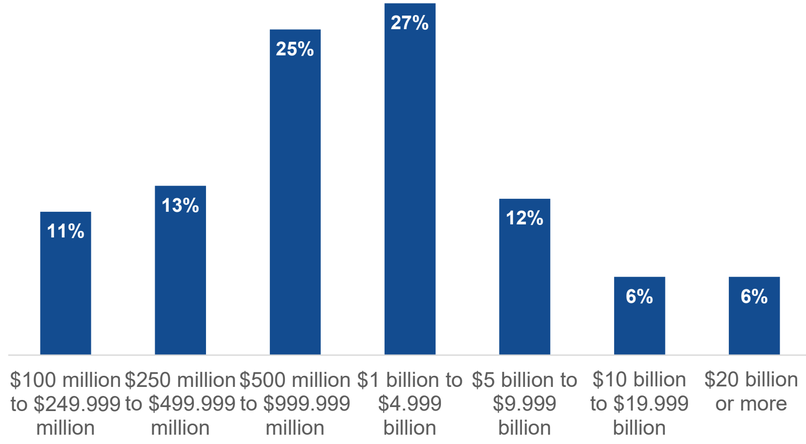
Respondents by Job Title/Level.



Respondents by Primary Industry.



Respondents by Total Annual Revenue.



BACK TO CONTENTS

Enterprise Strategy Group, now part of 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.

This Enterprise Strategy Group eBook was commissioned by Island Technology, Inc. and is distributed under license from TechTarget, Inc.