FORRESTER®

Regaining Control With A Connectivity Cloud

How A New Type Of Cloud Can Tame IT And Security Complexity

A FORRESTER CONSULTING THOUGHT LEADERSHIP PAPER COMMISSIONED BY CLOUDFLARE, NOVEMBER 2023

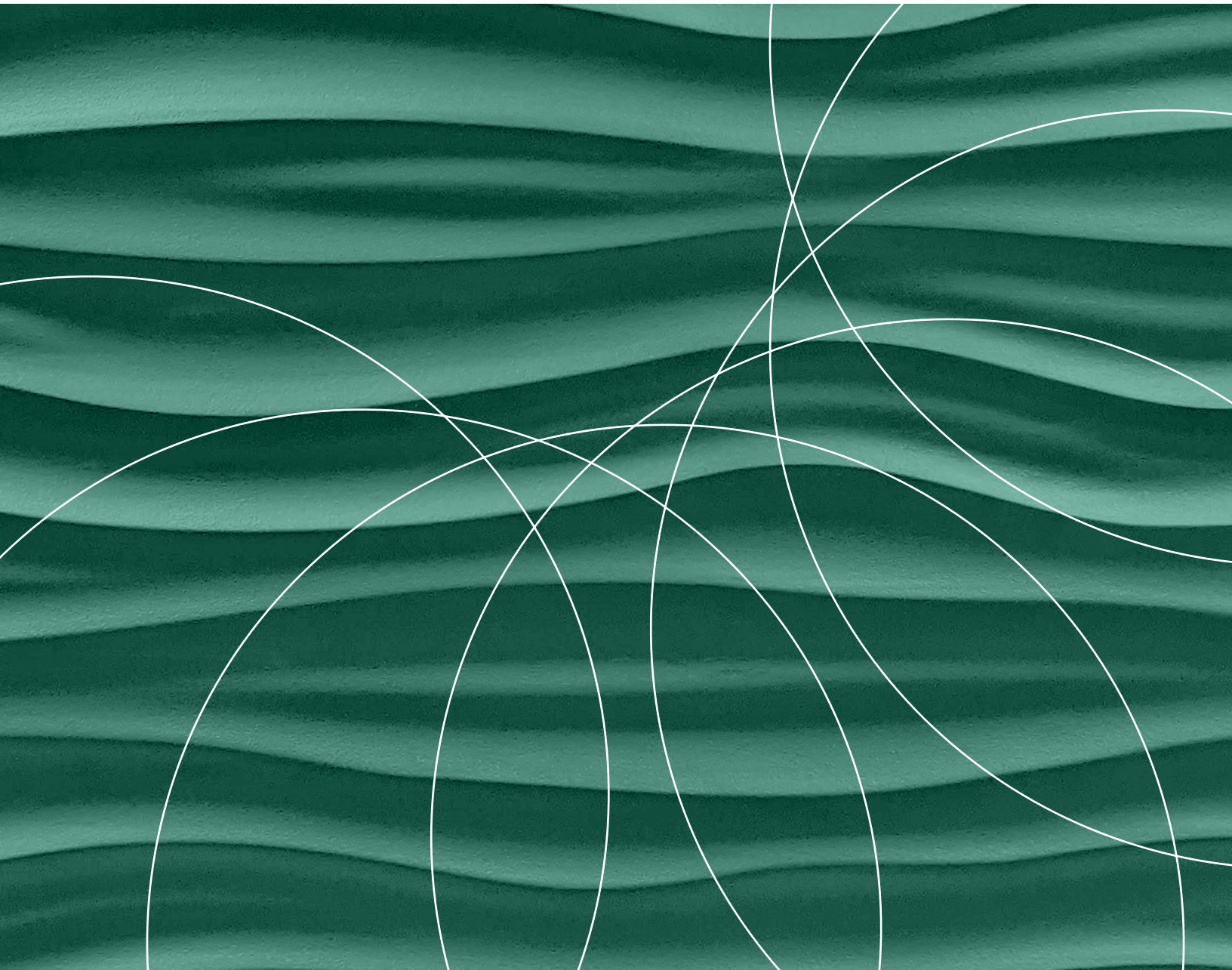


Table Of Contents

Project Team:

Vanessa Fabrizio,

Senior Market Impact Consultant

Jenna Bonugli,

Associate Market Impact Consultant

Contributing Research:

Forrester's Security & Risk research group

ABOUT FORRESTER CONSULTING

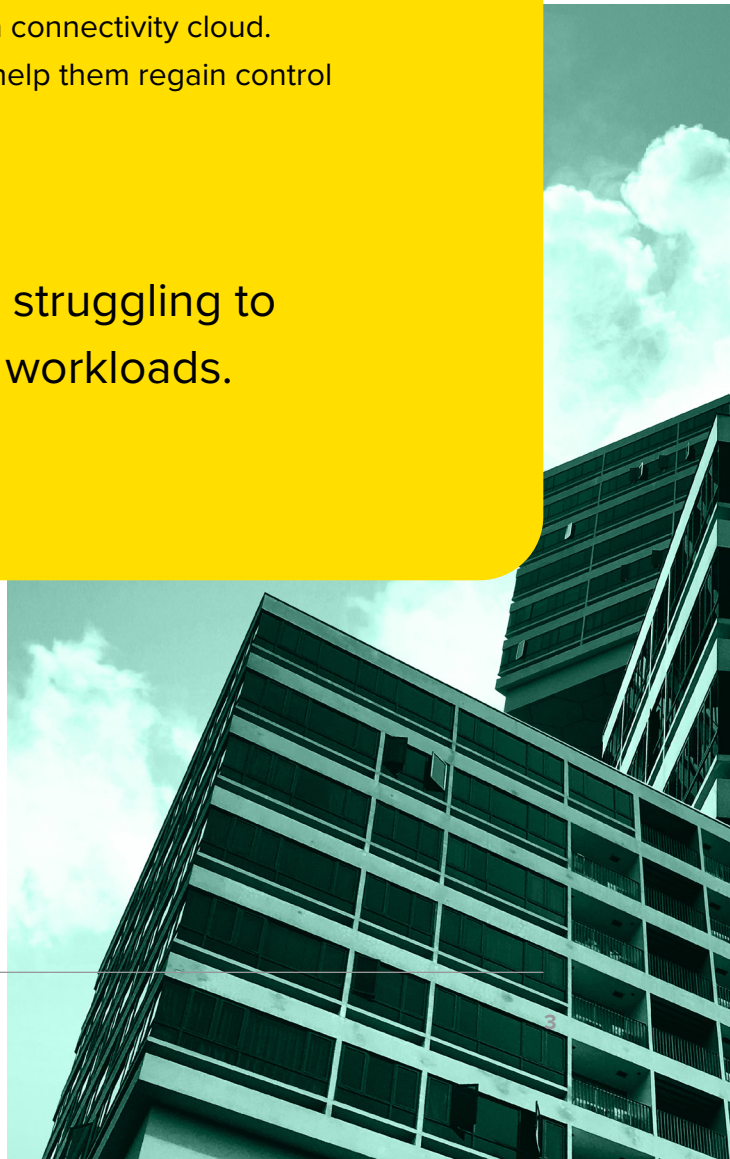
Forrester provides independent and objective research-based consulting to help leaders deliver key outcomes. Fueled by our customer-obsessed research, Forrester's seasoned consultants partner with leaders to execute their specific priorities using a unique engagement model that ensures lasting impact. For more information, visit forrester.com/consulting.

Executive Summary

The security landscape is rapidly evolving. Businesses once had a set number of locations to secure with on-premises operations in designated offices. Now, with the adoption of the public cloud, software-as-a-service (SaaS) applications, and anywhere work, security teams must secure and provide access to infinite locations. These new domains permit less visibility and control than the previous, on-premises environments and require more complex integration efforts.

In August 2023, Cloudflare commissioned Forrester Consulting to evaluate the growing complexity of IT and security teams. Forrester conducted an online survey with 449 global IT and security decision-makers and found that their responsibilities have significantly increased and grown in complexity in the last three years. This increased complexity has caused IT and security teams to lose control of their organizations' environments — and failure to regain control of the IT and security environment has significant business consequences. This paper discusses a solution — a connectivity cloud. Respondents believe that a connectivity cloud will help them regain control and accelerate digital transformation initiatives.

> IT and security respondents are struggling to manage their vast and complex workloads.



Key Findings

IT and security teams are losing control of their organizations' environment. Over the last five years, the responsibilities of IT and security teams have grown in number and in complexity. Respondents are struggling to adapt to their new, more complex environments.

Failure to regain control of the IT and security environment has massive business consequences. Respondents are not able to support the evolving user types and a growing number of users. Failure to address this challenge will impact customer experience, employee experience, productivity, competitive advantage, time to market, and the overall risk profile.

Today's business requires secure, performant connectivity. It also requires connectivity that promotes connection between people, apps, data, devices, networks, and clouds. This type of connectivity will solve IT and security teams' top challenges by supporting cloud and SaaS application strategies and an anywhere workforce.

A hypothetical solution, a connectivity cloud, might be the answer. Almost all (96%) of respondents said that a connectivity cloud would be valuable to their organization, and most are ready to invest.

IT And Security Responsibilities Have Increased In Number And Complexity

The IT and security landscape has expanded vastly. Previously, IT and security teams were focused on providing secure access for a set number of known locations. But now with widespread adoption of the public cloud and SaaS applications, anywhere work, and the increasing role of the public internet in corporate networking strategies, these teams are now responsible for providing network access and security anywhere an employee works and anywhere apps and data might reside. This growing complexity has caused companies to lose control of their IT and security environment. Forrester research found:

- **IT and security responsibilities have increased.** Respondents have a vast list of responsibilities, from ensuring security and connectivity to taking advantage of new sources of revenue (see Figure 1). Not only are these responsibilities multifaceted, but they are also new. Five years ago, respondents were not responsible for most of the things they are responsible for today. The top new responsibilities include ensuring compliance with government regulations, ensuring security for all workers, ensuring connectivity for in-office workers, and managing and securing applications in the public cloud (see Figure 2).
- **Responsibilities are more complex.** Not only are IT and security teams' responsibilities growing, but they are also becoming more complex. Almost half of respondents said ensuring connectivity for in-office workers is more complex than it was in 2020. And one-third of respondents said setting and enforcing access and security policies, adopting new technologies, and ensuring security for all workers is more complex.
- **IT and security respondents are losing control of their environment.** A remarkable 39% of respondents admitted their company is losing control of its IT and security environment. The main factors contributing to this decline in control are an increased number of applications (66%) and an increase of locations for applications (62%).

FIGURE 1

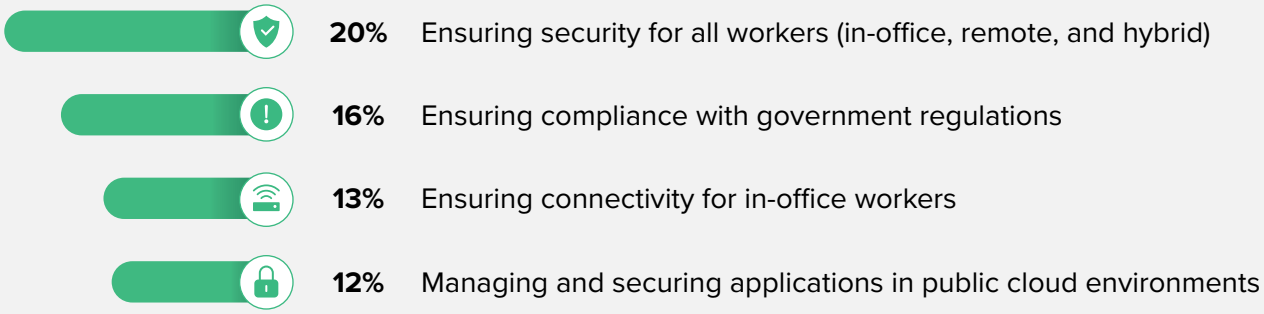
“Which of the following falls under the responsibility of the IT and security teams at your company?”

Base: 449 global decision-makers at the director level or higher who influence or direct their organizations choice of enterprise solutions
Note: Showing top 7 responses
Source: A commissioned study conducted by Forrester Consulting on behalf of Cloudflare, August 2023

FIGURE 2

IT And Security Team Responsibilities Increases Over The Last Five Years

(Showing “We were not responsible for this five years ago”)



Base: 449 global decision-makers at the director level or higher who influence or direct their organizations choice of enterprise solutions
Note: Showing four responses
Source: A commissioned study conducted by Forrester Consulting on behalf of Cloudflare, August 2023

IT And Security Teams Struggle To Manage Their New Workload

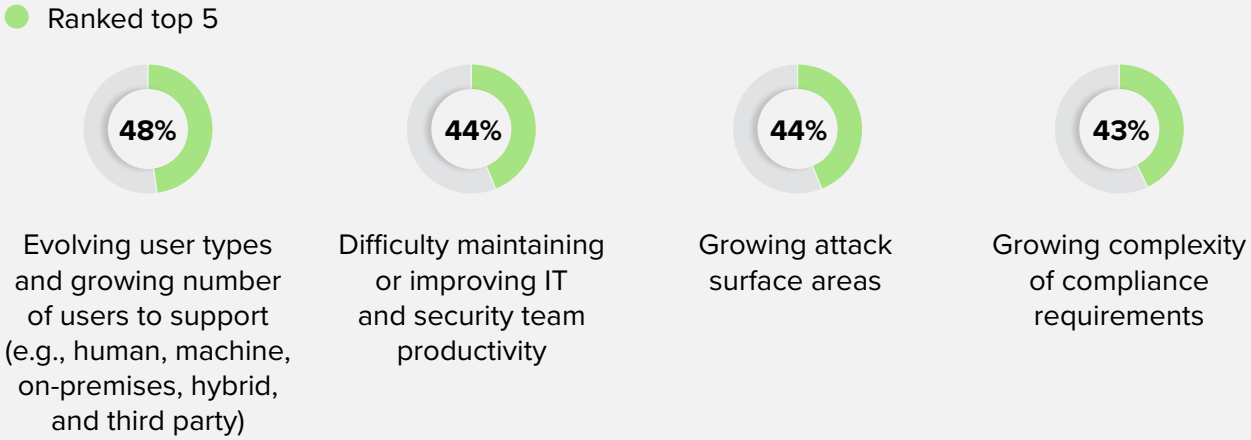
The driving forces of digital transformation — such as the adoption of cloud and SaaS, the growing importance of the web and public internet for enterprise application and networking strategies, and the evolution to anywhere work — have created a magnitude of challenges for IT and security teams. Forrester research found:

Respondents are struggling to support the evolving user types and a growing number of users.

- **IT and security respondents are struggling to support the new workforce.** Forty-eight percent of respondents say they are struggling to support evolving user types and a growing number of users. Further, respondents are challenged to manage the growing attack surface and comply with the growing complexity of compliance requirements (see Figure 3).
- **Failure to address these challenges will generate negative business impact.** Respondents indicate that a failure to address the above challenges will impact customer experience, employee experience, productivity, competitive advantage, time to market, and their organization's overall risk profile (see Figure 4).
- **Respondents are looking for help.** To mitigate the above challenges, respondents are planning to increase their number of dedicated resources (57%); consolidate vendors, platforms, and tools (51%); and outsource to managed service providers and system integrators (47%). IT and security teams know they can't effectively support anywhere work with their current set of resources and are looking for new approaches and solutions.

FIGURE 3

"What are the top challenges your organization's IT and security teams are currently facing?"



Base: 449 global decision-makers at the director level or higher who influence or direct their organizations choice of enterprise solutions
Note: Showing top 4 responses
Source: A commissioned study conducted by Forrester Consulting on behalf of Cloudflare, August 2023

FIGURE 4

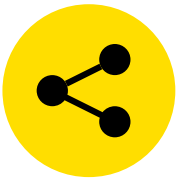
Challenges Will Affect Various Business Priorities If Not Adequately Addressed

CHALLENGE	IMPACTED BUSINESS PRIORITY		
	1	2	3
Evolving user types and growing number of users to support	Customer experience	Employee experience	Overall risk profile
Difficulty maintaining or improving IT and security team productivity	Productivity	Employee experience	Time to market
Growing attack surface areas	Productivity	Time to market	Overall risk profile
Growing complexity of compliance requirements	Competitive advantage	Productivity	Time to market

Base: 178 global decision-makers at the director level or higher who influence or direct their organizations choice of enterprise solutions
Note: Showing top responses
Source: A commissioned study conducted by Forrester Consulting on behalf of Cloudflare, August 2023

The Answer: A Connectivity Cloud

As the business landscape evolves to anywhere work, so must IT and security capabilities. Respondents believe that today's business requires secure and performant connectivity that promotes connection between people, apps, data, devices, networks, and clouds. This type of connectivity will help solve IT and security teams' top challenges by supporting an anywhere workforce. But how can this connectivity be accessed? We asked respondents to imagine a solution that:



Respondents believe that today's business requires secure, performant connectivity that promotes connection between people, apps, data, devices, networks, and clouds.

- Delivers secure, performant, "any-to-any" connectivity across on-prem, SaaS, cloud, and public internet environments.
- Integrates with any network.
- Offers full API-level programmability of all its services and functions.
- Delivers a unified view and policy control across on-prem, SaaS, cloud, and public Internet environments.

For the purpose of our research, we called this solution connectivity cloud and found:

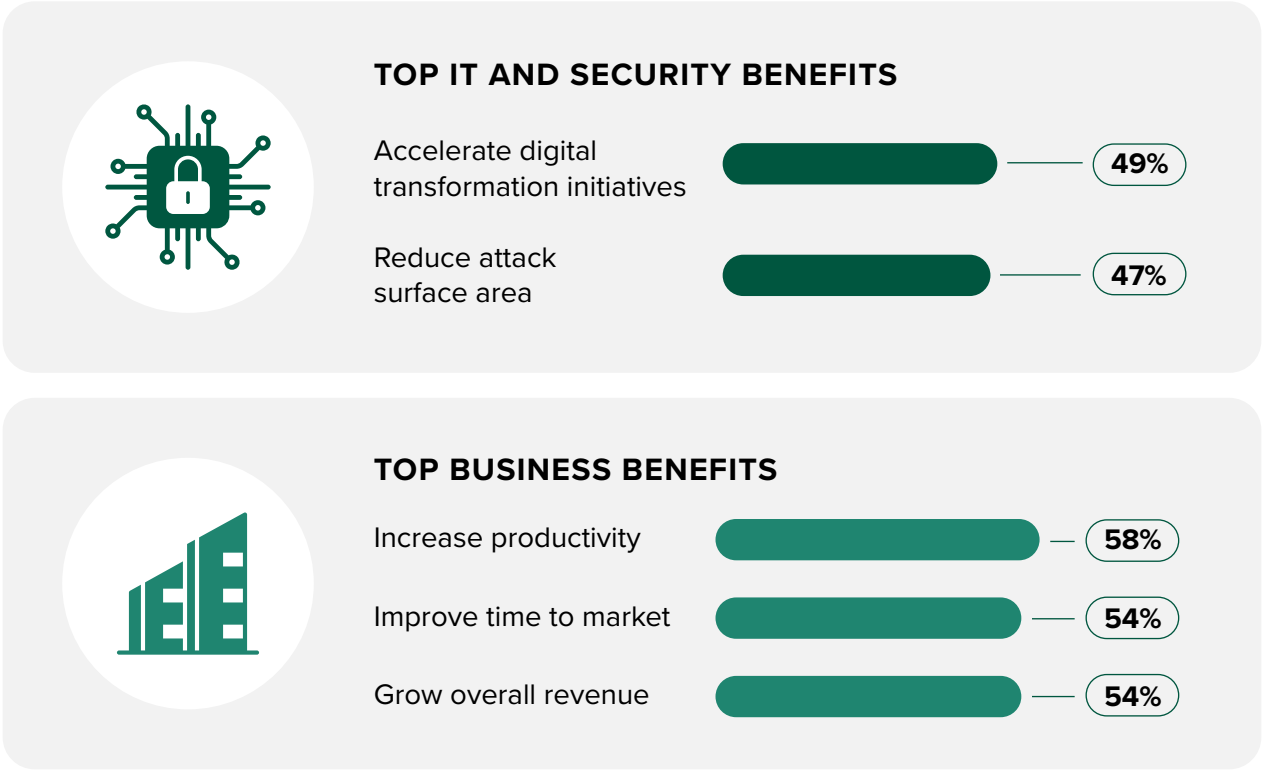
- **A connectivity cloud would be valuable to respondents' organizations.** Almost all (96%) of respondents say that a connectivity cloud would be valuable to their organization.
- **Respondents are ready to invest in a connectivity cloud.** On average, respondents indicate that they would invest 16% of their current IT and security budget for the solution.
- **A connectivity cloud would produce business benefits.** Respondents would expect a connectivity cloud to increase productivity, improve time to market, grow overall revenue,

accelerate digital transformation initiatives, and reduce the attack surface area, (see Figure 5).

Technology must evolve with the workplace. As we move to anywhere work, we must provide any-to-any access and security. Connectivity cloud would help IT and security teams regain control of their environment by providing access and security to all employees within one solution.

> On average, respondents would invest 16% of their current budget for a connectivity cloud solution.

FIGURE 5



Base: 449 global decision-makers at the director level or higher who influence or direct their organizations choice of enterprise solutions
Note: Showing top responses
Source: A commissioned study conducted by Forrester Consulting on behalf of Cloudflare, August 2023

Key Recommendations

Forrester's in-depth survey of 449 global decision-makers in IT and security yielded important recommendations:

Collaborate for secure cloud migration success

Many organizations are migrating infrastructure and workloads to the cloud, straining the IT and security organizations who are supporting the transitions. IT and security teams must partner early and stay engaged for these migrations to be successful, secure, and compliant. Identify key network and security integrations in your local environment and cloud ecosystem.

Reduce complexity to increase visibility and control

Security leaders cite IT complexity as a top concern. This is exacerbated by the move to the cloud and anywhere work. Regain control by looking for opportunities to simplify environments, consolidate vendors, and rationalize tech stacks. Gain visibility by integrating technologies and gathering and analyzing data.

Build a strategy to secure anywhere work and digital initiatives

Remote work and highly distributed infrastructure is here to stay. Your organization's security strategy has to evolve and scale to meet users and applications where they are across the globe. Work with vendors and partners to understand their roadmap for cloud connectivity capabilities and the digital business initiatives they have across their applications and users.

Appendix A: Methodology

In this study, Forrester conducted an online survey of 449 decision-makers who influence or direct their organizations choice of enterprise solutions at organizations in the United States, United Kingdom, Canada, Brazil, India, Australia, Singapore, France, Argentina, Germany, and Mexico to evaluate the experiences organizations have with the technology they utilize. Survey participants included decision-makers in IT and cybersecurity. Respondents were offered a small incentive as a thank-you for time spent on the survey. The study began in July 2023 and was completed in August 2023.

Appendix B: Demographics

COUNTRY	
United States	**29%**
United Kingdom	**8%**
Canada	**8%**
Brazil	**7%**
India	**7%**
Australia	**7%**
Singapore	**7%**
France	**7%**
Argentina	**7%**
Germany	**6%**
Mexico	**6%**

TOP 4 INDUSTRIES	
Financial services	**14%**
Retail	**13%**
Government	**9%**
Technology and/or technology services	**6%**

RESPONDENT DEPARTMENT	
IT	**52%**
Cybersecurity	**48%**

LEVEL OF RESPONSIBILITY IN IT AND SECURITY	
I oversee my company's security department and have strong visibility into our IT department.	**35%**
I oversee my company's IT department and have strong visibility into our security department.	**32%**
I oversee my company's IT and security departments.	**25%**
I have visibility into my company's IT and security departments, but I don't directly oversee either.	**8%**

RESPONDENT POSITION	
Director	**47%**
Vice president	**34%**
C-level executive	**19%**

NUMBER OF EMPLOYEES	
1,000 to 4,999 employees	**50%**
5,000 to 19,999 employees	**34%**
20,000 or more employees	**16%**

Note: Percentages may not total 100 due to rounding.

FORRESTER®