FORRESTER®

# Leaders Are Now Committed To Zero Trust

Zero Trust Is A Digital Business Enabler For All Size Firms

Get started ⟶

FORRESTER OPPORTUNITY SNAPSHOT: A CUSTOM STUDY COMMISSIONED BY CLOUDFLARE | OCTOBER 2020

# Securing Change Is The New Normal

Companies' first priorities in 2020 were obvious: protect revenue, serve customers, and enable employees. However, as firms sprint toward a cloud-enabled end state, they must do so securely. The COVID-19 pandemic has proven to be both a crisis and an opportunity for increased adoption of Zero Trust security architectures.[1] Contrary to popular thinking, there are few meaningful differences between the challenges that firms of different sizes face and the ways they are evolving their security practices.

In September 2020, Cloudflare commissioned Forrester to explore the impact of the disruptions on security strategy and operations among companies of all sizes. We surveyed 317 global security decision-makers and found that firms were not prepared, but the disruptions have made security a board-level conversation. Executives have bought into IT security investments to ensure business success moving forward, and many security leaders have identified Zero Trust as the best approach to meet this goal.

## Key Findings

The COVID-19 pandemic has shifted the way the world operates. As a result, companies are accelerating their digital transformation efforts with security in mind.

No one was prepared for this year's disruptions. Even with increased executive buy-in to change security culture and approach, firms face resource constraints and operational challenges.

Security leaders expect Zero Trust adoption to enable digital business transformation, improve network visibility, and enhance employee experience (EX).

# The New Normal Leads To Increased Security Buy-In

It is no secret that companies, customers, and employees are operating in fundamentally different ways than they did pre-pandemic. Seventy-five percent of survey respondents said they've experienced "extreme" or "significant" change in 2020. The pandemic has had the biggest impact on their revenue and planning (64%), and it's changed how customers do business with them (53%) and accelerated the shift to a distributed working model (52%).

In response to these changes, executive leaders — and not just security leaders — are investing in acceleration of their digital transformation efforts and adopting Zero Trust security.

**"Which of the following changes have impacted your organization the most in 2020?"**
(Showing top 3 ranked)


The impact of COVID-19 on our company's revenue and planning


Changes to how our customers do business with us


The shift to a distributed working model

**"How has this change impacted your organization's IT security approach?"**

| | | | |
|---|---|---|---|
| **CHANGE** | Impact of COVID-19 on our revenue and planning | Changes to how our customers do business with us | Shift to a distributed working model |
| **BIGGEST IMPACT** | Increased executive buy-in to accelerate our digital transformation efforts | Increased executive buy-in to accelerate our digital transformation efforts | Accelerated our shift to adopting a Zero Trust approach |



Base: 317 global director + security decision-makers at midsize and large companies
Source: A commissioned study conducted by Forrester Consulting on behalf of Cloudflare, September 2020

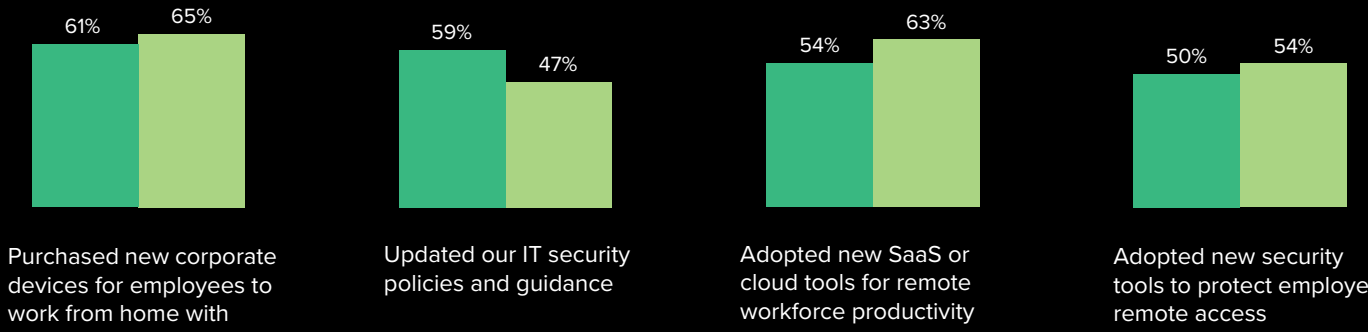
# Employee Enablement Drives Security Investments

Security teams have taken decisive action to evolve their operations. Regardless of company size, firms increased investment in software-as-a-service (SaaS)-based tooling and new devices to facilitate secure remote work, as well as updated security policies and guidance.

Although all of the surveyed companies are spending money on technology, smaller companies (<1000 employees) are being a bit more frugal. Larger organizations (1,000+ employees) are more likely to buy point solutions, while smaller organizations tend to be more strategic in their spending.

**"What changes has your IT security organization made so far in 2020?"**
(Select all that apply)

- Less than 1000 employees
- 1000+ employees




FORRESTER OPPORTUNITY SNAPSHOT:

Base: 317 Global Director + security decision makers at mid-size and large companies.
Source: A commissioned study conducted by Forrester Consulting on behalf of Cloudflare, September 2020

# Your Most Valuable Assets Are At Risk

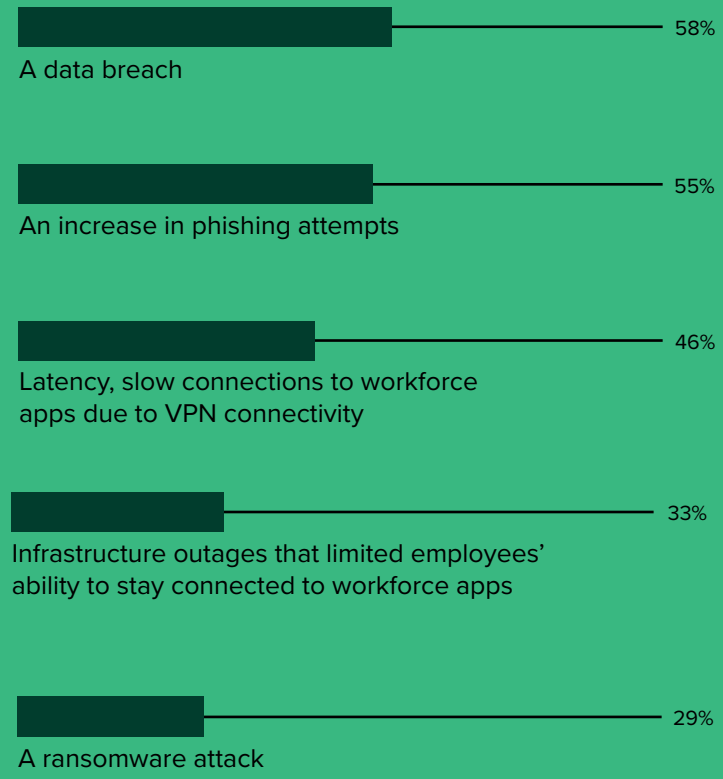
All companies big or small have critical assets to protect, including customer data and differentiating intellectual property that would cause business damage or market setback if stolen.[2] These assets are even harder to protect in a digital business ecosystem, and that's a reality that attackers are all too aware of. As such, 58% percent of respondents experienced a data breach in 2020, and 55% experienced an increase in phishing attempts.

Employee downtime is also costly to business. Thirty-three percent of respondents reported that infrastructure outages have limited employees' abilities to stay connected to workforce apps, and 46% reported latency issues due to VPN connectivity.

As remote work becomes the new norm, firms must evolve their security approaches to secure their most valuable assets: their data and their employees.



**"Did your organization experience any of the following in 2020?"**
(Select all that apply)



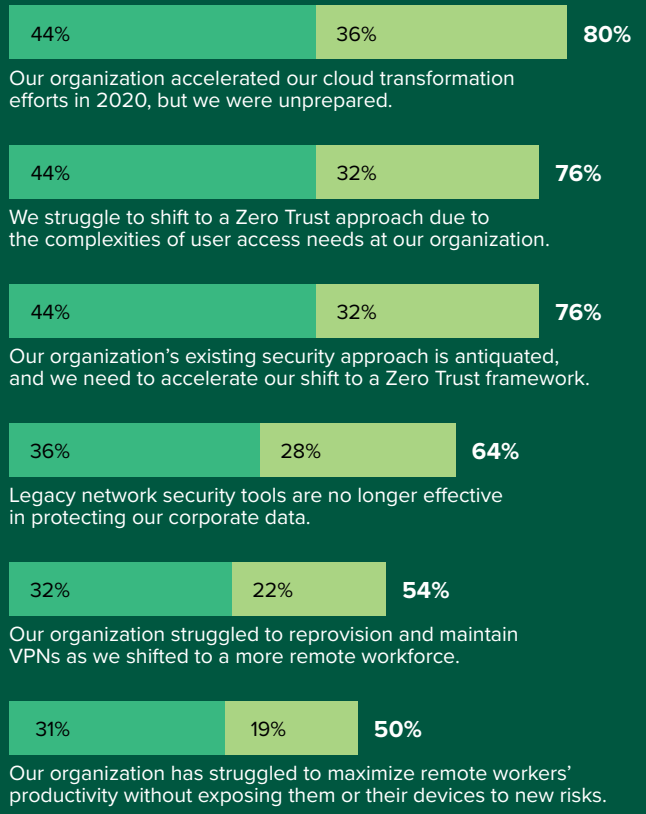

Base: 317 global director + security decision-makers at midsize and large companies
Source: A commissioned study conducted by Forrester Consulting on behalf of Cloudflare, September 2020

# Firms Struggle To Keep Up With 2020

The sudden shift to remote work and digital customer interaction forced progress on cloud transformation efforts, but it continues to be a painful journey. Eighty percent of security leaders said their organizations accelerated cloud transformation efforts in 2020, but they were unprepared to manage such an overhaul.

Going into the pandemic, many firms' existing IT practices hindered their abilities to support employee productivity without security tradeoffs. As such, 76% of firms want to accelerate their shift to a Zero Trust framework, but the adoption won't come without challenges. An equal share of firms identified identity and access management (IAM) complexity as a blocker for Zero Trust adoption. And 76% of respondents said designing around the complexities of employee access needs is a challenge for their firms.

**"Please rate your level of agreement with the following statements."** ● Agree ● Strongly agree

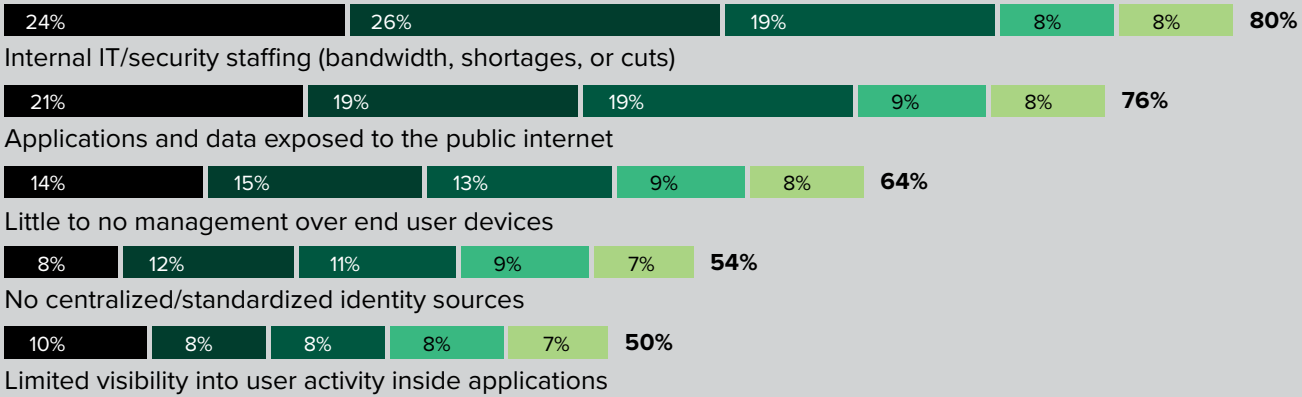



Base: 317 global director + security decision-makers at large and midsize companies
Source: A commissioned study conducted by Forrester Consulting on behalf of Cloudflare, September 2020

# Security Faces A Resource Shortage When It Needs It Most

As security teams struggle to support a remote workforce while accelerating their cloud and security transformation efforts, it should come as no surprise that respondents from firms big and small indicated a lack of people resources as their top security risk. The hastened cloud adoption also has security leaders concerned about valuable data being increasingly exposed to the public internet (76%). They are also concerned about their inabilities to manage end user devices (64%), likely due to more employees using personal devices for work outside of the office.

**"What are the biggest risks associated with your current security approach?"**
(Showing top 5 ranked)






Base: 317 global director + security decision-makers at large and midsize companies
Source: A commissioned study conducted by Forrester Consulting on behalf of Cloudflare, September 2020

# Room To Grow: Zero Trust Interest Exceeds Adoption Levels

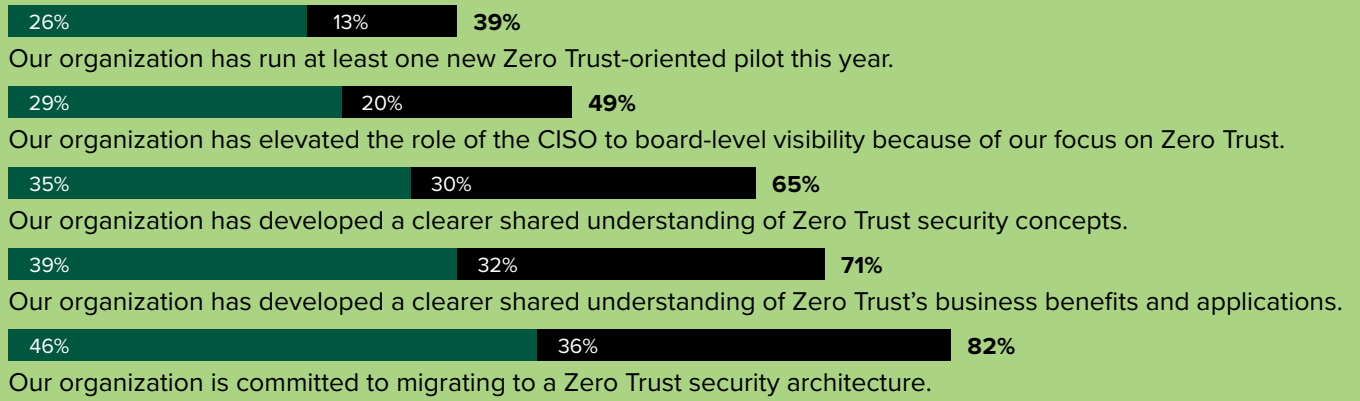
Zero Trust is no longer the sparkle in the eye of a lonesome security leader. Eighty-two percent of respondents said they are committed to migrating to a Zero Trust security architecture, and their interest in Zero Trust has elevated the role of CISO to board-level visibility at 49% of organizations. That said, only 39% of surveyed firms have run a Zero Trust-oriented pilot this year.

This commitment to Zero Trust adoption is not isolated to large enterprises. In fact, 71% of respondents from small-to-midsize businesses (<1,000 employees) said their organization plans on adopting Zero Trust as large enterprises and the US government have indicated there are significant strategic benefits to this new approach.

Zero Trust finally has the ear of the board. How long until it has their vote?

**"Please rate the following statements about how your organization's thinking on Zero Trust has changed in 2020."**

- Agree
- Strongly agree






Base: 317 global director + security decision-makers at large and midsize companies
Source: A commissioned study conducted by Forrester Consulting on behalf of Cloudflare, September 2020

# Zero Trust Is A Digital Business Enabler

As companies evolve to deal with permanent change, they expect Zero Trust to empower their businesses and employees. Respondents from small and large firms alike said enabling digital business transformation is the top Zero Trust benefit. These firms also expect Zero Trust to improve EX via easier, more secure, and faster access to applications. Zero Trust can enhance the technology experience by enabling fast, secure access from a broader array of corporate devices, and ease access to information by removing the need for VPN.[3] Network security starts and ends with visibility, and Zero Trust gives firms unprecedented visibility into user activity and patterns. With Zero Trust, visibility, detection, and prevention work together to secure firms' most sensitive and valuable data assets.[4] Smaller firms can also turn to Zero Trust to reduce the scope and cost of compliance initiatives.

## Top 5 Zero Trust Benefits

**LESS THAN 1,000 EMPLOYEES**

- Enabled digital business transformation
- Improved network visibility
- Reduced scope and cost of compliance initiatives
- Improved employee experience via easier, more secure, and faster access to applications
- Improved flexibility to extend access to third parties securely

**MORE THAN 1,000 EMPLOYEES**

- Enabled digital business transformation
- Improved employee experience via easier, more secure, and faster access to applications
- Increased data awareness and insights
- Improved network visibility
- Prevented malware propagation

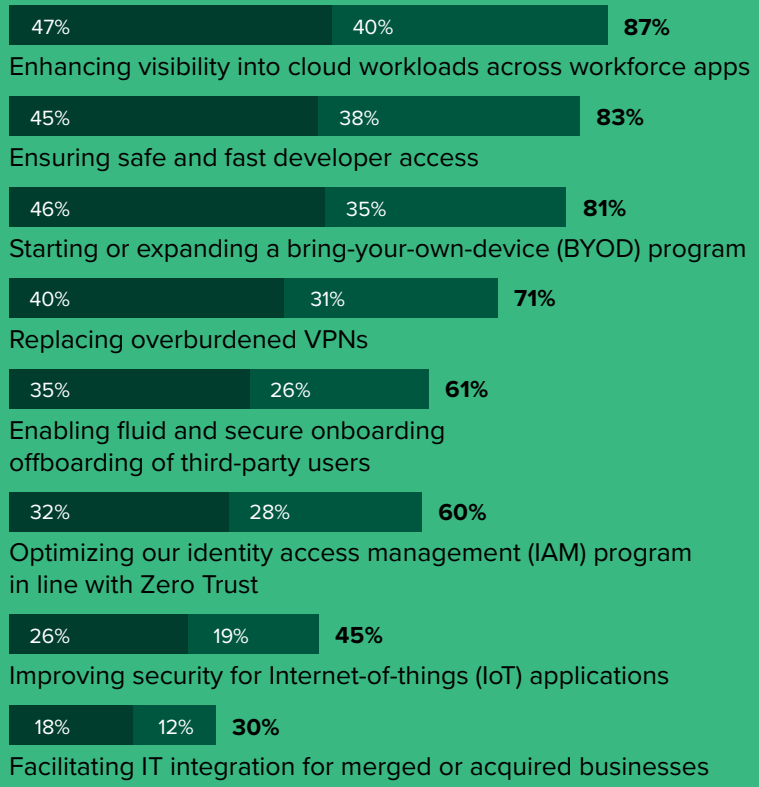


Base: 317 global director + security decision-makers at large and midsize companies
Source: A commissioned study conducted by Forrester Consulting on behalf of Cloudflare, September 2020

# Zero Trust Is A Critical Lever To Improve EX

For years, companies have sacrificed end user experience in the name of security, which impeded productivity, bred frustration, and led to higher attrition. But the Zero Trust model extends beyond the traditional network focus to include workloads, data, devices, and users. This means firms can start using Zero Trust in new ways to improve EX.

In fact, the most important Zero Trust use cases to respondents are enhancing visibility into cloud workloads across workforce apps (87%), ensuring safe and fast developer access (83%), and starting or expanding bring-your-own-device (BYOD) programs (81%). Seventy-one percent also plan to turn to Zero Trust to replace overburdened VPNs. Employees in a Zero Trust model don't launch VPN clients, they don't have to remember passwords, and they don't worry they're going to get fired for accessing files with sensitive information. In short, Zero Trust helps relieve employees of the burden of dealing with security.[5]




Base: 317 global director + security decision-makers at large and midsize companies
Source: A commissioned study conducted by Forrester Consulting on behalf of Cloudflare, September 2020

# Conclusion

In the wake of the pandemic, every business had to become a digital business overnight. In response, security leaders are:

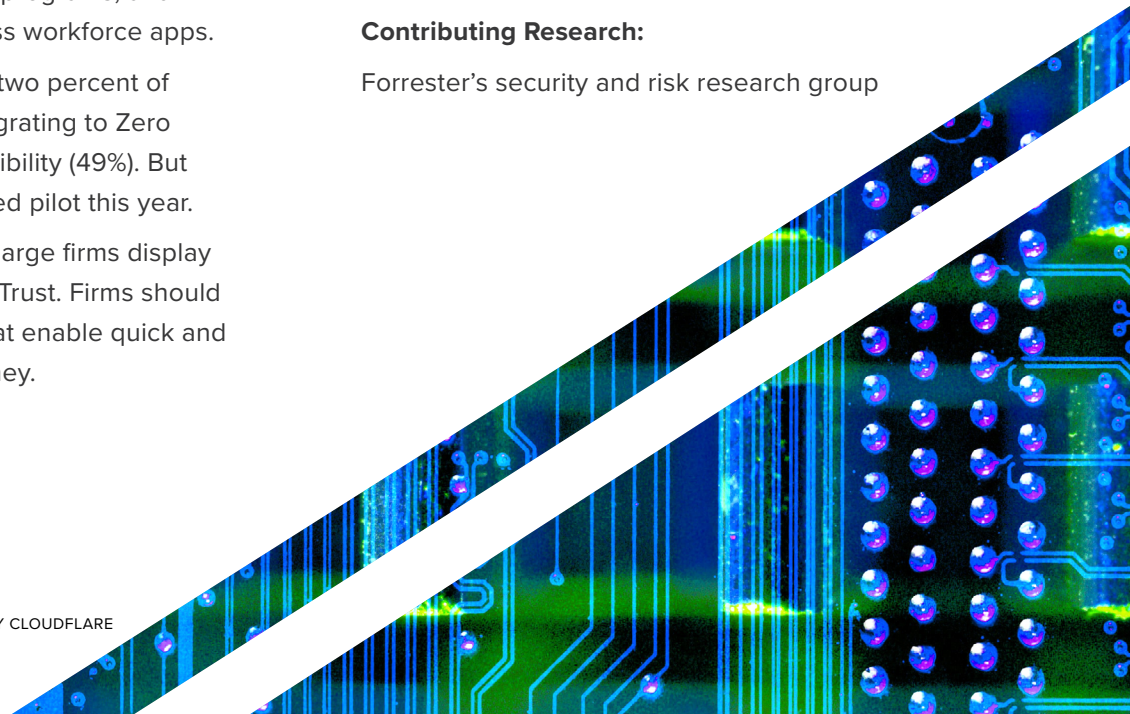
- Adopting Zero Trust to improve EX: Firms plan to focus on secure developer access, implementing better BYOD programs, and enhancing visibility into cloud workloads across workforce apps.
- Beginning to take Zero Trust seriously: Eighty-two percent of respondents said their firm is committed to migrating to Zero Trust, and this has given CISOs board-level visibility (49%). But only 39% of firms have run a Zero Trust-oriented pilot this year.
- Seeking short- and long-term wins: Small and large firms display the same level of motivation to embrace Zero Trust. Firms should prioritize cloud-delivered security solutions that enable quick and incremental progress along the adoption journey.

**Project Director:**

Mandy Polacek, Market Impact Consultant

**Contributing Research:**

Forrester's security and risk research group



# Methodology

This Opportunity Snapshot was commissioned by Cloudflare. To create this profile, Forrester Consulting conducted an online survey of 317 global security decision-makers. The custom survey began and was completed in September 2020. Although the graphics are representative of all of the survey respondents, we found few differences between small and large organizations. Where there were significant differences, we displayed the different segments side-by-side.

**ENDNOTES**

[1] Source: Chase Cunningham, "Our Newest Round Of ZTX Evaluations Is Out," Forrester Blogs (go.forrester.com/blogs/our-newest-round-of-ztx-evaluations-is-out/).

[2] Source: "The Forrester Tech Tide™: Zero Trust Threat Prevention, Q3 2020," Forrester Research, Inc., September 18, 2020.

[3] Source: "Enhance EX With Zero Trust," Forrester Research Inc., July 13, 2020.

[4] Source: "The Eight Business And Security Benefits Of Zero Trust," Forrester Research, Inc., September 25, 2019.

[5] Ibid.

**ABOUT FORRESTER CONSULTING**

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit forrester.com/consulting.



FORRESTER OPPORTUNITY SNAPSHOT: A CUSTOM STUDY COMMISSIONED BY CLOUDFLARE
OCTOBER 2020

# Demographics

**COMPANY SIZE (EMPLOYEES)**

| | |
|---|---|
| 34% | < 1,000 |
| 34% | 1,000 to 4,999 |
| 32% | > 5,000 |

**REGION**

| | |
|---|---|
| 33% | North America |
| 33% | EMEA |
| 34% | APAC |

**CYBER SECURITY STRATEGY RESPONSIBILITY**

| | |
|---|---|
| 14% | Final decision-maker |
| 31% | Part of a team making decisions |
| 55% | Decision influencer |

**INDUSTRY (SHOWING TOP 5)**

| | |
|---|---|
| 8% | Technology and/or technology services |
| 7% | Retail |
| 6% | Electronics |
| 6% | Education and/or nonprofits |
| 6% | Consumer product goods and/or manufacturing |


FORRESTER®