PORTNOX REPORT

CISO Perspectives for 2025

The surprising views of cybersecurity leaders on Zero Trust's false promises, MFA's limitations, the shifting sands of compliance and cyber insurance, job security (or lack thereof), and more.

TABLE OF CONTENTS

RESEARCH OBJECTIVES & METHODOLOGY

What We Did

Portnox partnered with Wakefield Research on custom quantitative research to:

- Understand the cybersecurity environment and pressures CISOs face;
- Identify which trends CISOs believe have promise and which ones do not;
- Gauge interest and progress in moving towards Passwordless Authentication.

How We Did It

The Portnox Survey was conducted by Wakefield Research (www.wakefieldresearch.com) among 200 US CISOs at companies with a minimum annual revenue of $500m with representative quotas set for company size, between August 29th and September 9th, 2024, using an email invitation and an online survey.

Results of any sample are subject to sampling variation. The magnitude of the variation is measurable and is affected by the number of interviews and the level of the percentages expressing the results. For the interviews conducted in this particular study, the chances are 95 in 100 that a survey result does not vary, plus or minus, by more than 6.9 percentage points from the result that would be obtained if interviews had been conducted with all persons in the universe represented by the sample.

portnox

Key Findings

KEY FINDINGS

CISOs are concerned about security breaches, and also their own job, as they seek to balance security with the employee experience.

CISOs are worried about a cyber-attack breaching their organization's security defenses and concerned about the consequences, including potentially costing them their job. As a result, they have a more scrutinizing view of cybersecurity trends as they seek protection while under pressure to maintain the employee experience and minimize costs.

For example, many have a positive view of Zero Trust, but fewer than half view it as the future of cybersecurity in an unqualified light. Nearly a quarter don't believe it's a good fit for all organizations, and even 15% consider it more hype than value. This perspective may also be driven by the fact that half of CISOs report their organization needs a significant upgrade, if not a complete overhaul, to implement Zero Trust. Similarly, CISOs agree that Multi-Factor Authentication can't keep pace with evolving threats.

This comes as most CISOs try to balance security with the employee experience; just 42% feel they can consider the employee experience as secondary to security. They hear from employees as well, particular about disruptions caused by interference with their work or constant requests to update their password.

KEY FINDINGS

CISOs view compromised passwords or authentication as a vulnerability, and most are looking at Passwordless Authentication to improve security.

High-profile security breaches happen all the time, and in these events CISOs are likely to believe it was a compromised password or authentication behind it. As a result, many are looking at options to shore up this vulnerability.

Enter Passwordless Authentication, which nearly a third of CISOs have already begun implementing and another 38% are planning to. Just 6% haven't considered it, making it a promising trend that CISOs believe can make a difference. In particular, CISOs believe it will result in stronger access control and reduced risk of common password exploits.

However, to fully implement they need to overcome potential barriers; most notably is the need to preserve the employee experience. The risk of employee lockout is the most common hesitancy to adopt Passwordless Authentication (53%), and another 45% are concerned about employee resistance to change. Fortunately, half of CISOs also believe that Passwordless Authentication would improve the employee experience (50%) and also increase productivity (42%).

KEY FINDINGS

Adding to the challenges CISOs face are ever-changing regulations and pressures to keep costs down.

Just 10% of CISOs feel fully prepared for the new NIS2 regulations in the EU; around a third (31%) feel somewhat prepared at best. This reflects the challenge of a dynamic regulatory environment. In fact, all CISOs agree that even the most agile companies cannot keep up to date with every regulation.

On top of these pressures, CISOs constantly face pressure to reduce security costs. For example, CISOs report that there are frequent evaluations of new solutions to lower cyberinsurance premiums; two-thirds (68%) report these evaluations happen often or all the time. This approach comes as CISOs don't have a firm understanding of everything their cyberinsurance covers, adding to the uncertainty.

To view the full data from the survey, including a complete breakdown of respondent demographics please visit:
www.portnox.com/2025-ciso-perspectives-report-data/

portnox

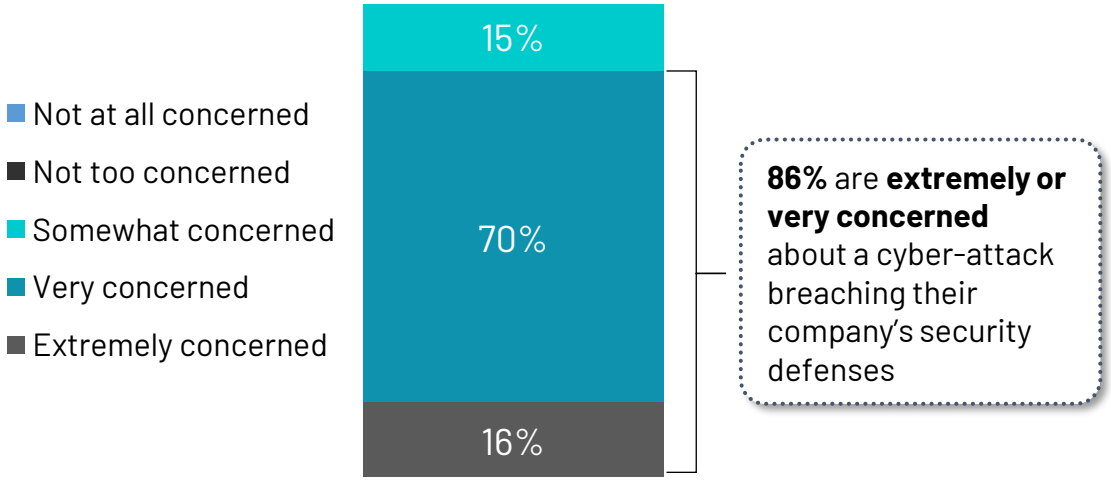
Detailed Research Findings

CISO CONCERNS

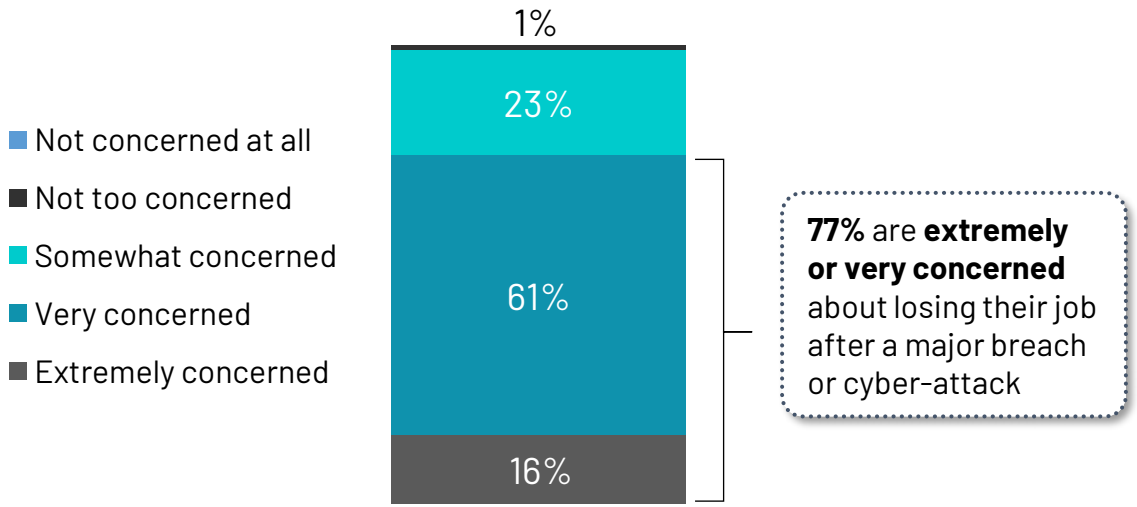
CISOS CONCERNED ABOUT BREACHES & THEIR OWN JOBS

CISOs aren't taking their security for granted; all CISOs are concerned about a cyber-attack breaching their defenses, including 86% who are very or extremely concerned. After a spate of high-profile terminations, they also fear that the next major breach could cost them their job.

CONCERNS OF A CYBERSECURITY ATTACK
N=200



CONCERNS OF JOB LOSS AFTER CYBERSECURITY ATTACK
N=200

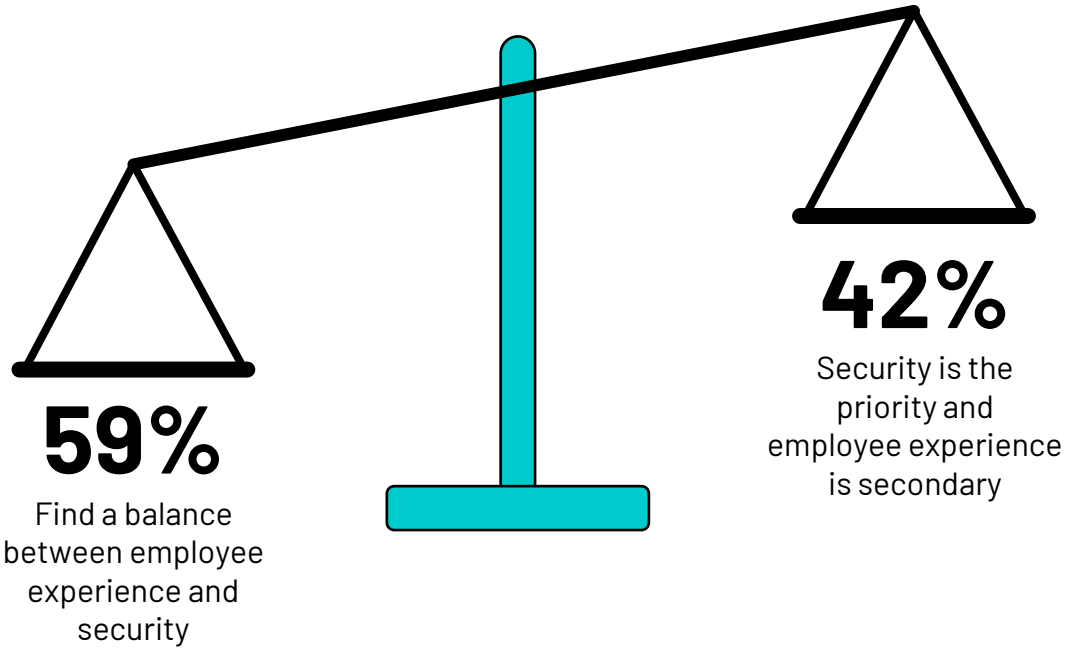


Q3. How concerned are you about a cyber-attack breaching your organization's security defenses? / 18. How concerned are you that you may lose your job if your organization faces a major breach or cybersecurity attack?

MOST STRIVE TO BALANCE SECURITY & EXPERIENCE

Accommodating the employee experience is a necessary component of any cybersecurity approach. Over half of CISOs aim to find a balance between it and security; the other 42% considers the employee experience a secondary concern.

CYBERSECURITY APPROACH FOR EMPLOYEE EXPERIENCE
N=200



1. How does your organization approach cybersecurity with regards to the employee experience?

EMPLOYEE COMPLAINTS FOCUSED ON DISRUPTIONS TO WORK

No matter the approach, employees will have complaints about the process. These complaints focus on disruptions to their day-to-day, specifically anything that interferes with their work (51%) or frequent password changes (51%).

EMPLOYEE SECURITY MEASURE COMPLAINTS
N=200

51%
Interferes with or slows work

51%
Password changes are too frequent

46%
Takes too long to resolve issues

45%
Not adequately trained on how to use them

43%
Difficult to understand

41%
Use tedious processes

2. What complaints do employees have about your organization's security measures?

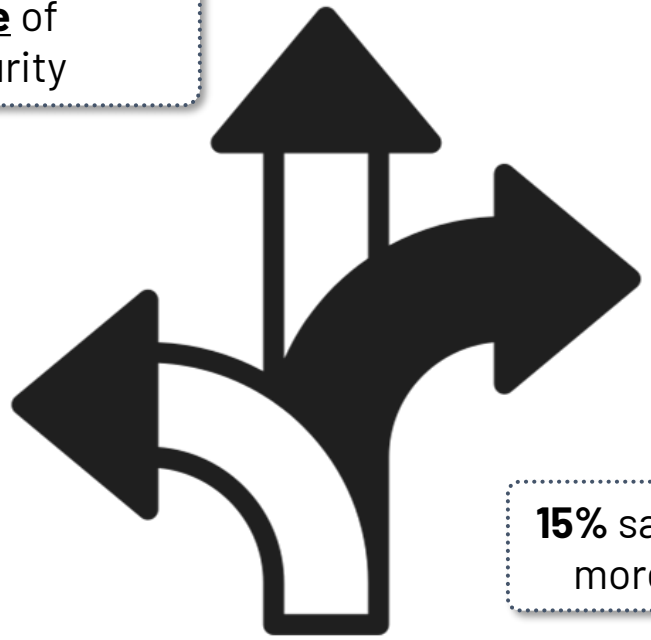
ZERO TRUST HAS PROMISE FOR SOME BUT PERHAPS NOT ALL

Several years in, CISOs have yet to form a consensus around Zero Trust. While 38% see it as the future and another 26% see promise despite the challenges to implement it, a similar 22% don't believe it can work for every organization. Another 15% dismiss it as more hype than value.

OPINION ON ZERO TRUST
N=200

38% view Zero Trust as the **future** of cybersecurity

26% see **promise** in Zero Trust, but organizations face difficulty to implement it



22% believe Zero Trust can work for some organizations, but **not all**

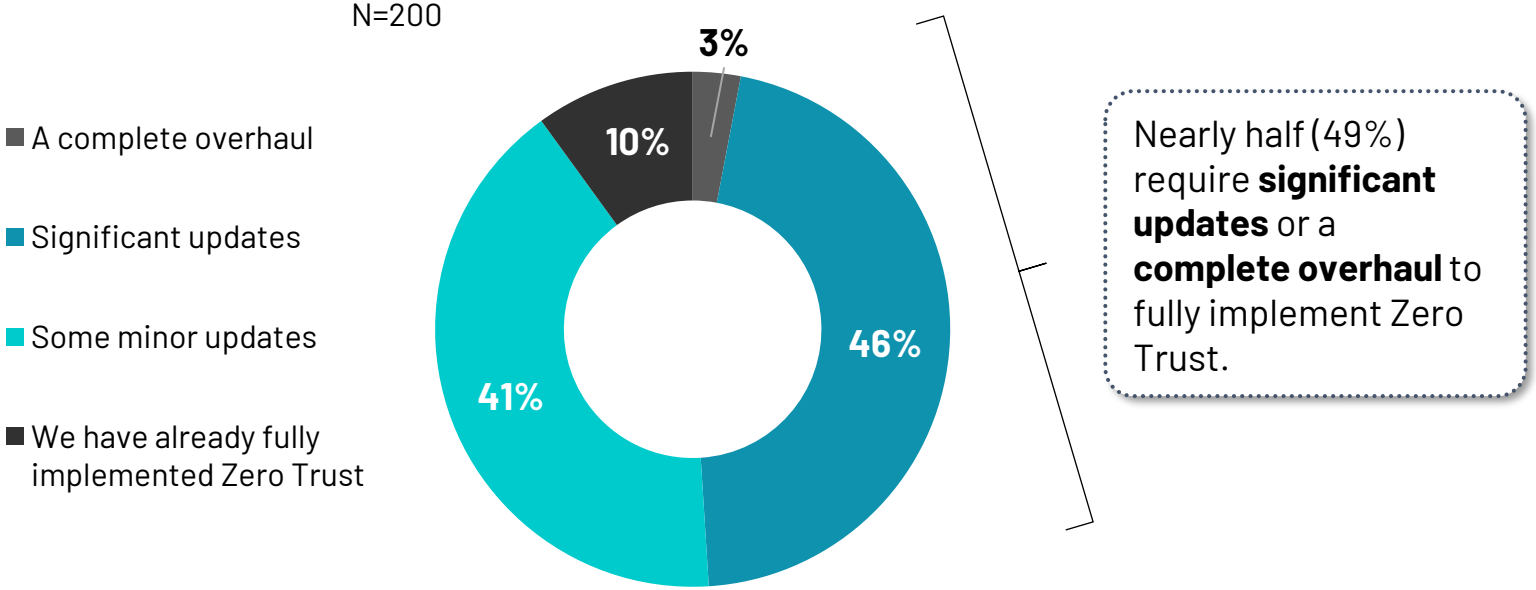
15% say that Zero Trust is more **hype** than value

7. Which comes closest to your opinion about Zero Trust?

ORGANIZATIONS REQUIRE A LOT OF WORK TO REACH ZERO TRUST

One reason CISOs may be skeptical of adopting a Zero Trust framework is the amount of work required at their organization to implement it. Nearly half say it would require significant updates, if not a complete overhaul. Just 10% of companies have fully implemented Zero Trust, showing that the discussion over whether to invest in it – and how much – continues across organizations.

REQUIREMENTS FOR ZERO TRUST IMPLEMENTATION
N=200



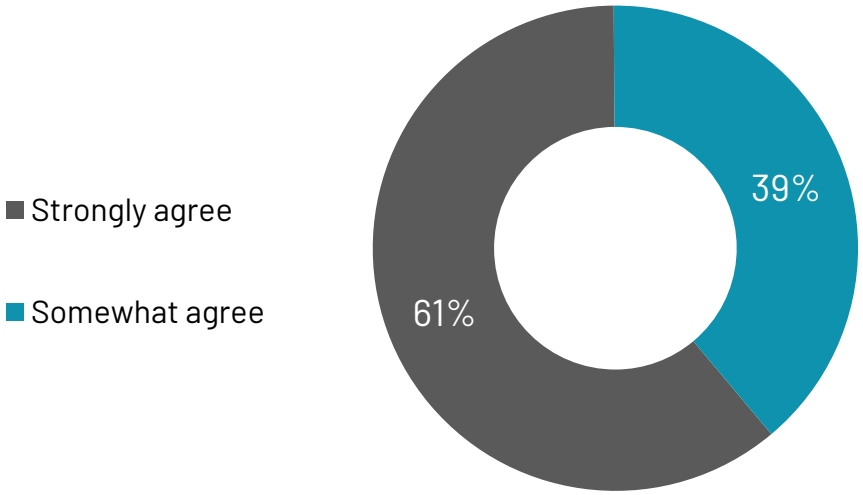
Nearly half (49%) require **significant updates** or a **complete overhaul** to fully implement Zero Trust.

6. What would be required to fully implement Zero Trust at your organization?

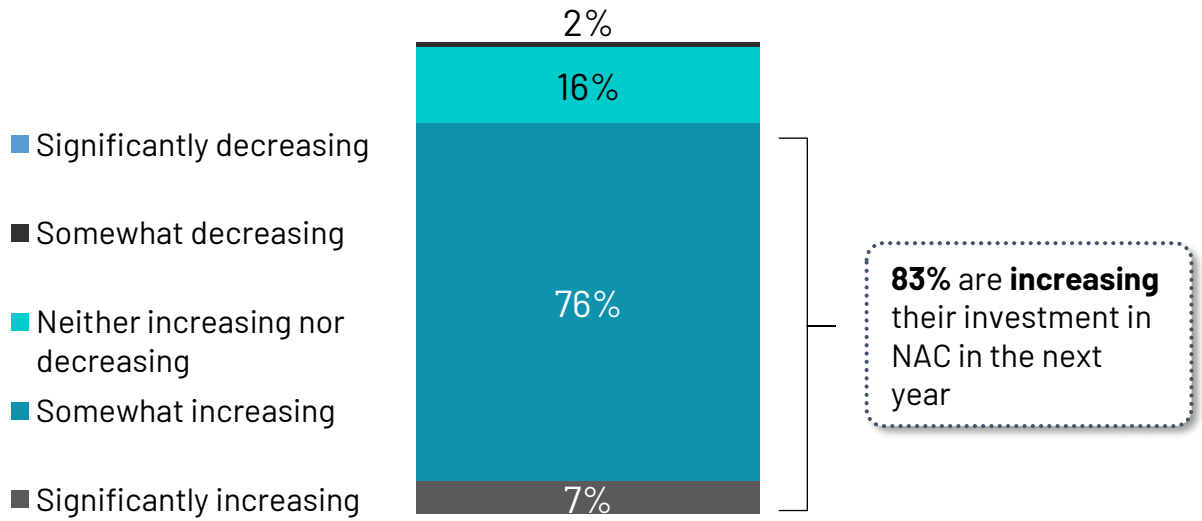
NAC IS CRITICAL & ORGANIZATIONS ARE INCREASING INVESTMENT

Regardless of their views of Zero Trust, CISOs understand that Network Access Control (NAC) is a critical component of any framework they put in place. Reliance on NAC is growing, as more than 4 in 5 are increasing their investment in the next year.

NAC IS CRITICAL COMPONENT FOR ZERO TRUST
N=200



ORGANIZATIONAL INVESTMENT IN NAC IN THE NEXT YEAR
N=200

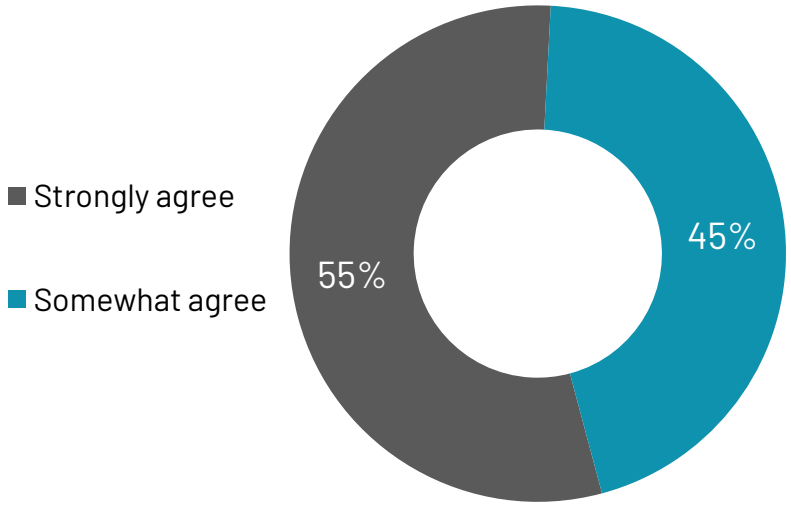


8. How strongly do you agree or disagree with the following statement: Network Access Control (NAC) is a critical component of any Zero Trust framework. / 9. Will your organization be increasing or decreasing investment in NAC in the next year?

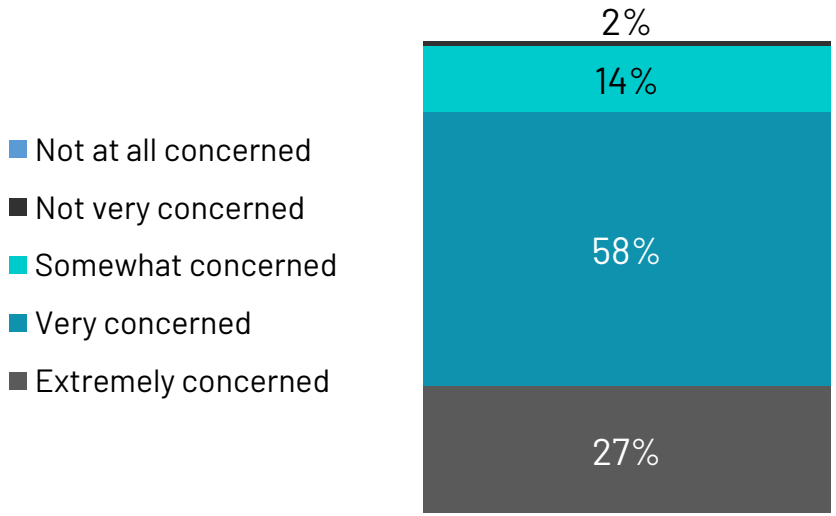
CISOS AGREE THAT MFA ISN'T SUFFICIENT AS PROTECTION

All CISOs agree that Multi-Factor Authentication cannot keep pace with evolving threats, which is why nearly all (98%) are concerned that MFA doesn't do enough to protect employees.

LEVEL OF AGREEMENT FOR MFA NOT KEEPING PACE WITH EVOLVING THREATS
N=200



LEVEL OF CONCERN OVER MULTI-FACTOR AUTHENTICATION EMPLOYEE SECURITY
N=200



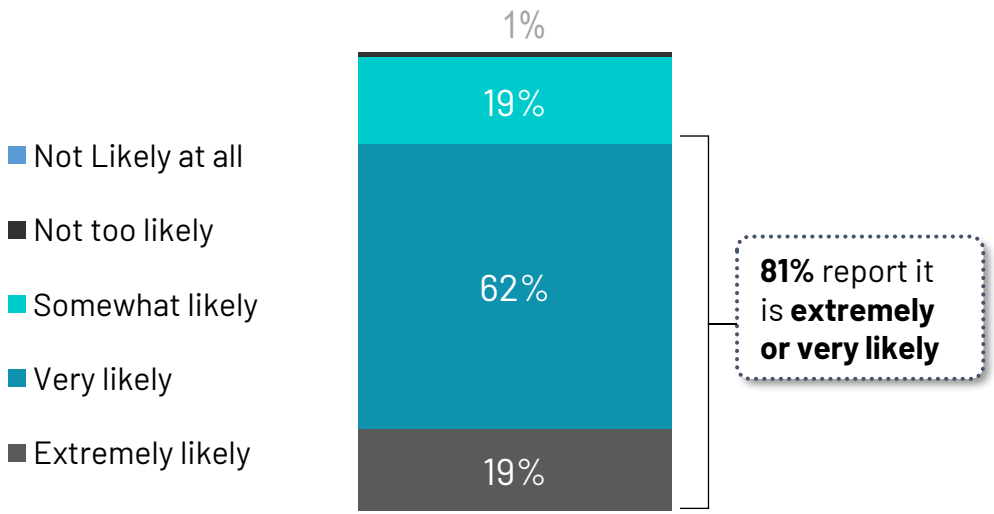
5. How strongly do you agree or disagree with the following statement: MFA can't keep pace with evolving threats. / 4. How concerned are you that security provided by Multi-Factor Authentication does not do enough to protect employees?

A PASSWORDLESS FUTURE

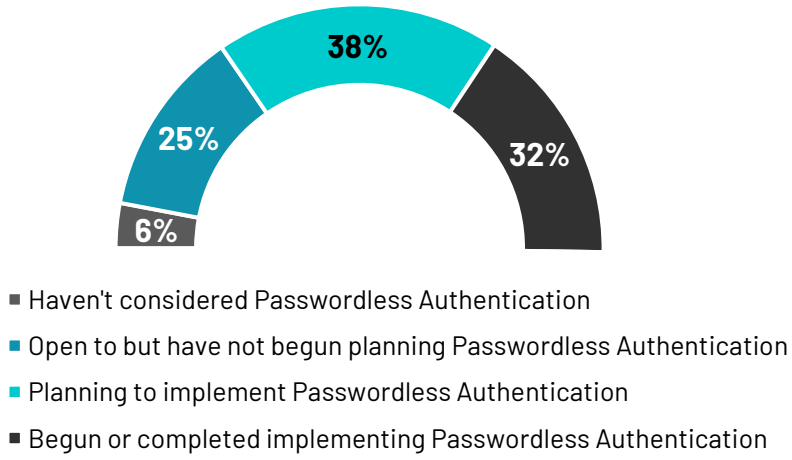
MOST ARE WORKING TOWARDS PASSWORDLESS AUTHENTICATION

When CISOs hear about a high-profile breach, they are likely to believe that it was the result of a compromised password of authentication. This understanding of organizational vulnerabilities is likely driving interest in Passwordless Authentication: nearly a third (32%) have already begun implementing this approach, and another 38% plan to.

LIKELINESS OF BREACH CAUSED BY COMPROMISED PASSWORD OR AUTHENTICATION
N=200



CURRENT ORGANIZATIONAL STANDING WITH PASSWORDLESS AUTHENTICATION IMPLEMENTATION
N=200



10. When you hear of a high-profile security breach or hack, how likely do you think it is due to a compromised password or authentication? / 11. Which describes where your organization currently stands with the implementation of Passwordless Authentication?

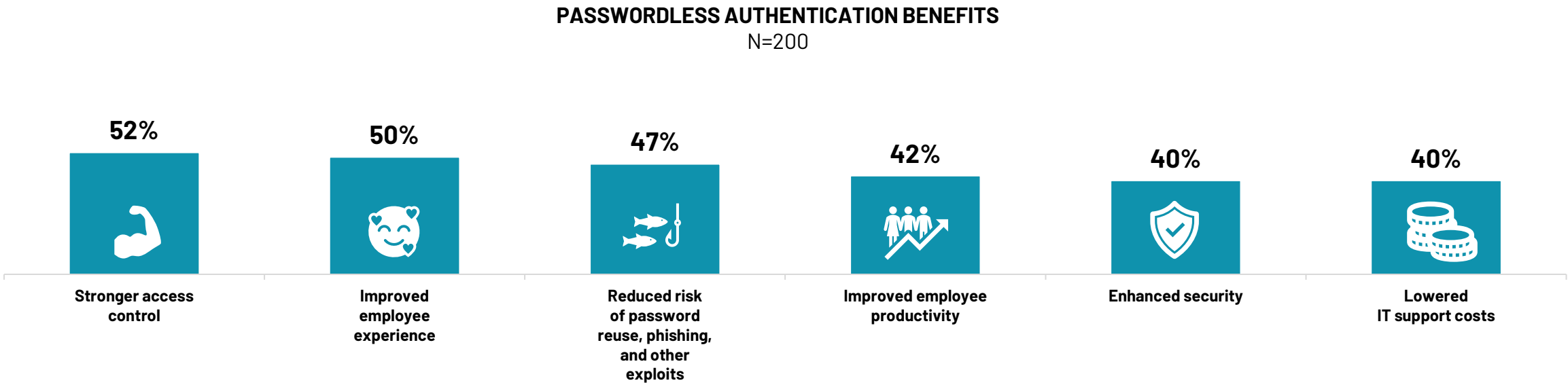
EMPLOYEE EXPERIENCE LEADS THE CONCERNS OVER PASSWORDLESS

CISOs cite a number of factors that could cause organizations to hesitate in moving towards Passwordless Authentication. Concerns over the employee experience lead the way, including a risk of lockout (53%) and resistance to change (45%).

12. What hesitancies are there to implementing Passwordless Authentication in your organization?

HALF SAY PASSWORDLESS WOULD IMPROVE EMPLOYEE EXPERIENCE

On the other hand, in addition to stronger access control (52%), half of CISOs (50%) cite an improved employee experience as a top benefit of using Passwordless Authentication and 42% believe it would increase employee productivity. CISOs also feel they would benefit from a reduced risk of exploits (47%) and enhanced security (40%).



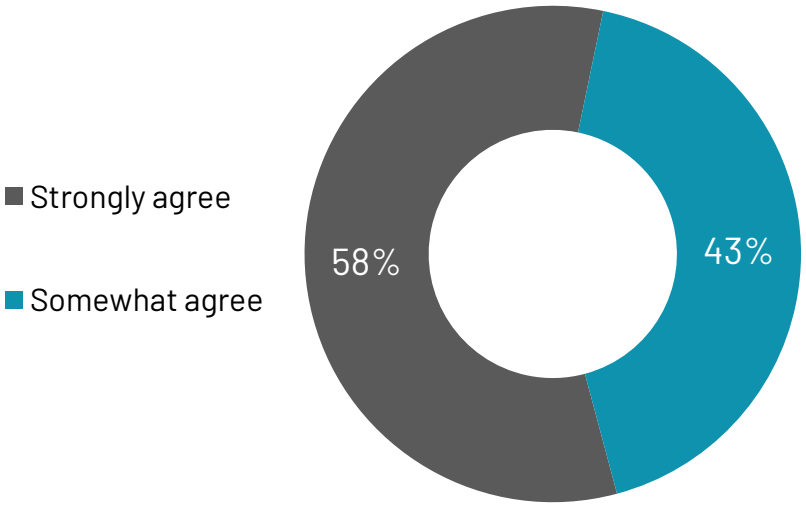
12. What hesitancies are there to implementing Passwordless Authentication in your organization?

SECURITY CHALLENGES

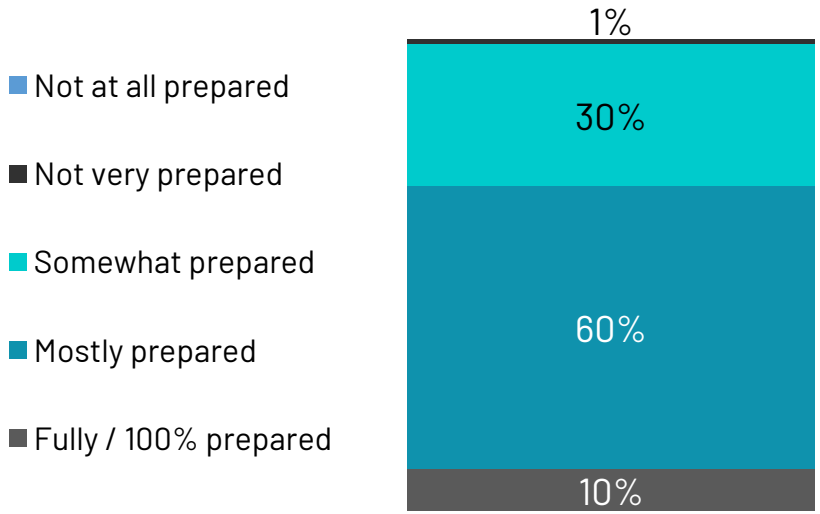
CHANGING REGULATIONS ADD TO THE PRESSURE

With 90% not fully prepared for NIS2, all CISOs agree even the most agile companies can't keep up with every regulation in a rapidly changing landscape.

IMPOSSIBLE FOR EVEN THE MOST AGILE COMPANY TO KEEP UP TO DATE WITH EVERY REGULATION
N=200



LEVEL OF PREPAREDNESS FOR NIS2
N=200



17. How much do you agree or disagree with the following statement? It is impossible for even the most agile company to keep up to date with every regulation in a rapidly changing landscape. / 16. How prepared is your organization for NIS2?

ZTNA ISN'T WORKING AS WELL AS PROMISED

Just 8% of CISOs have completed a move to ZTNA without issue. Another 8% have completed the move but found it difficult, while most CISOs have just begun a move (46%) or are still in planning stages (38%). Adoption may not got as planned, as all CISOs agree that ZTNA does not work as well as has been promised, based on what they've seen.

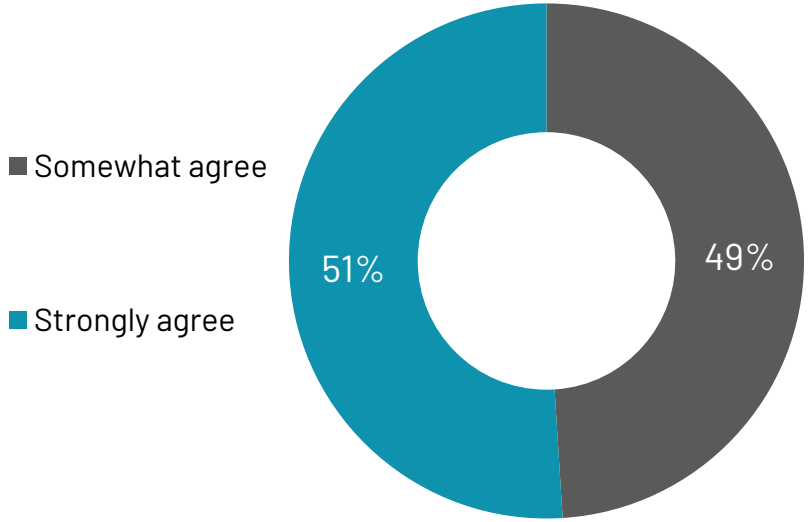
CURRENT ORGANIZATIONAL STANDING WITH ZTNA ADOPTION
N=200

16%
have completed a move to ZTNA, though half (8%) found it difficult to implement

46%
have begun to move to ZTNA, and it is too early to tell how difficult it will be

38%
plan to move to ZTNA but haven't begun yet

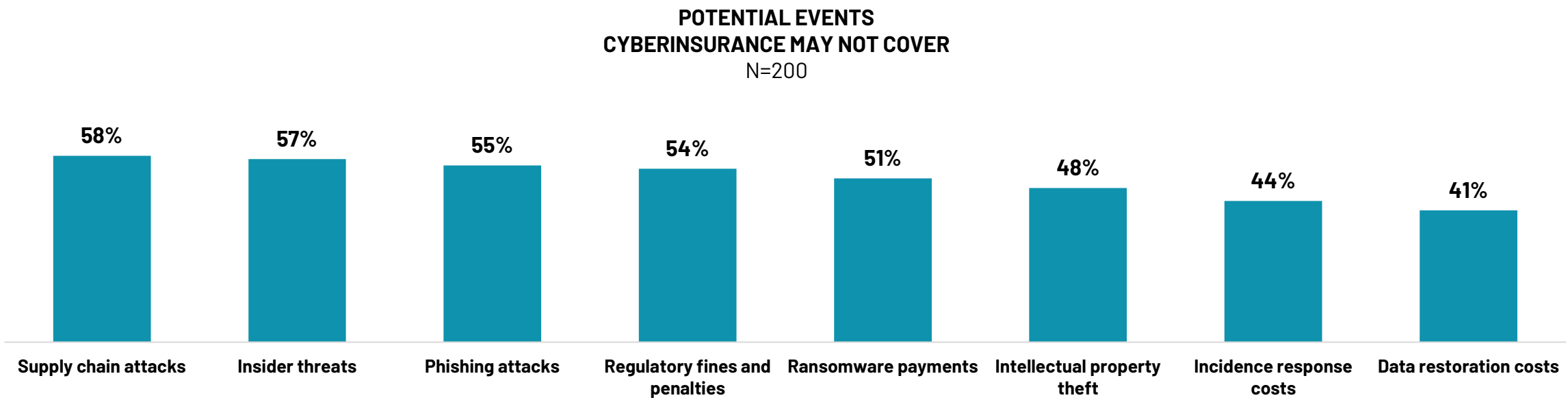
ZTNA NOT WORKING AS WELL AS PROMISED
N=200



14. Which of the following describes where your organization currently stands with the implementation of Zero Trust Network Access (ZTNA) adoption? / 15. How strongly do you agree or disagree with the following statement: Based on what I've seen and heard, ZTNA does not work as well as has been promised.

QUESTION MARKS ABOUND ABOUT CYBERINSURANCE COVERAGE

CISOs aren't fully certain how covered their organization would be across a number of different fronts, most commonly supply chain attacks (58%) and insider threats (57%), but also across several other vulnerabilities and consequences as well.

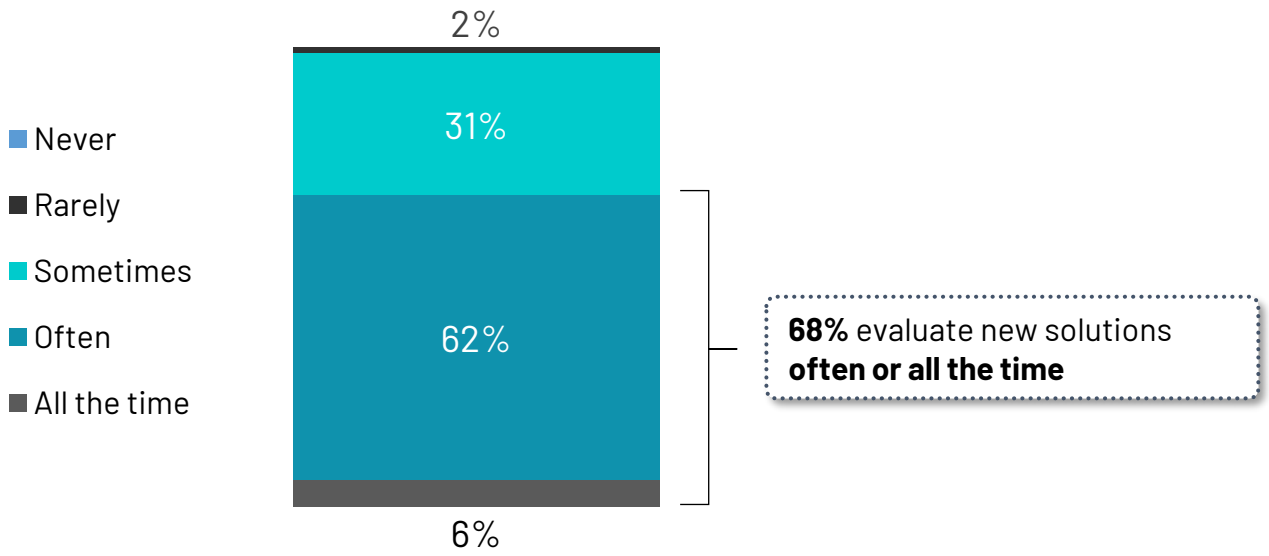


19. Which of the following, if any, are you not 100% sure your current cyberinsurance would cover?

CISOS UNDER PRESSURE TO LOWER CYBERINSURANCE COSTS

On top of the concerns over a breach, CISOs are also under pressure to reduce costs, as evidenced by the constant evaluation of new solutions to lower their cyberinsurance premiums. Nearly all (98%) report this happens, with two-thirds (68%) say this evaluation happens often or all the time.

FREQUENCY OF EVALUATING NEW SOLUTIONS TO LOWER CYBERINSURANCE PREMIUMS
N=200



20. How often does your organization evaluate new solutions to lower cyberinsurance premiums?

portnox

Appendix

GENDER, AGE, REGION, EMPLOYMENT, EDUCATION

GENDER	TOTAL *N=200*
Male	92%
Female	8%
Non-binary	-

EMPLOYMENT	TOTAL *N=200*
Employed full-time	100%
Employed part-time	-
Unemployed	-
Retired	-
Stay-at-home / do not work	-

AGE	TOTAL *N=200*
18 to under 50	50%
50 or older	51%

REGION	TOTAL *N=200*
Northeast	32%
South	26%
Midwest	17%
West	26%

EDUCATION	TOTAL *N=200*
Grade school	-
Some high school	-
Graduated from high school or equivalent	-
Some college	-
Associate degree	-
Bachelor's degree	49%
Graduate or post-graduate work	52%

What is your gender please? / What is your age? / REGION / What is your employment status? / What is the highest level of formal education you have completed?

GENDER, AGE, REGION, EMPLOYMENT, EDUCATION

LEVEL	TOTAL *N=200*
Owner or Equivalent (Partner, Principal, etc.)	-
C-Level Executive (CEO, CFO, CISO, etc.)	100%
Vice President	-
Director	-
Senior Management	-
Mid-Management (Manager, Supervisor, etc.)	-
Non-management	-
Admin / Support Staff	-

ROLE	TOTAL *N=200*
CEO	-
CFO	-
CIO	-
CISO	100%
COO	-
CXO	-
Other	-

COMPANY	TOTAL *N=200*
Publicly held	11%
Privately held	89%

EMPLOYEES	TOTAL *N=200*
1,000 to under 5,000	56%
5,000 to 50,000	44%

How would you describe your current level or title at your company? / Which of the following best describes your role at your company? / Is your company publicly or privately held? / How many employees does your company have?

INDUSTRY

INDUSTRY	TOTAL *N=200*
Accounting	1%
Automotive	2%
Banking / finance	6%
Business and management services	2%
Communications	2%
Construction	3%
Consulting	2%
Education	1%
Entertainment	2%
Energy	3%
Government / policy / public sector	-
Healthcare / medicine / pharmaceuticals	2%

INDUSTRY (cont.)	TOTAL *N=200*
Hospitality / restaurant / service industry	2%
Information Technology (IT) / software	37%
Insurance	3%
Journalism / media / publishing	2%
Law	2%
Manufacturing	16%
Non-profit	-
Real estate	3%
Retail	7%
Sales	-
Science / engineering	2%
Utilities	3%
Other	-

Which of the following best describes the industry in which your company operates?

REVENUE, YEARS AT COMPANY, YEARS IN BUSINESS

REVENUE	**TOTAL** *N=200*
Under $100 million	-
$100 million to under $250 million	-
$250 million to under $500 million	-
$500 million to under $1 billion	50%
$1 billion to under $2.5 billion	24%
$2.5 billion to under $5 billion	14%
$5 billion to under $10 billion	7%
$10 billion to under $15 billion	3%
$15 billion to under $25 billion	2%
$25 billion or more	2%

YEARS AT COMPANY	**TOTAL** *N=200*
Under 10	72%
10 or more	29%

YEARS IN BUSINESS	**TOTAL** *N=200*
Under 35	61%
35 or more	40%

To view the full data from the survey, including a complete breakdown of respondent demographics please visit: www.portnox.com/2025-ciso-perspectives-report-data/

Which of the following categories includes your company's annual sales revenue? / For how many years have you been at your current company? / For how many years has your current company been in business?

portnox

ABOUT PORTNOX

Portnox offers cloud-native zero trust access control and cybersecurity essentials that enable agile, resource-constrained IT teams to proactively address today's most pressing security challenges: the rapid expansion of enterprise networks, the proliferation of connected device types, the increased sophistication of cyberattacks, and the shift to zero trust. Hundreds of mid-market and enterprise companies have leveraged Portnox's award-winning security products to enforce powerful access, endpoint risk monitoring and remediation policies to strengthen their organizational security posture. By eliminating the need for any on-premises footprint common among traditional information security systems, Portnox allows companies – no matter their size, geo-distribution, or architecture – to deploy, scale, enforce and maintain these critical zero trust security policies with unprecedented ease.

For more information, please visit www.portnox.com.