nagomi

The 2025 CISO Pressure Index

The Pressures, Challenges, and Opportunities Facing Today's Security Leaders

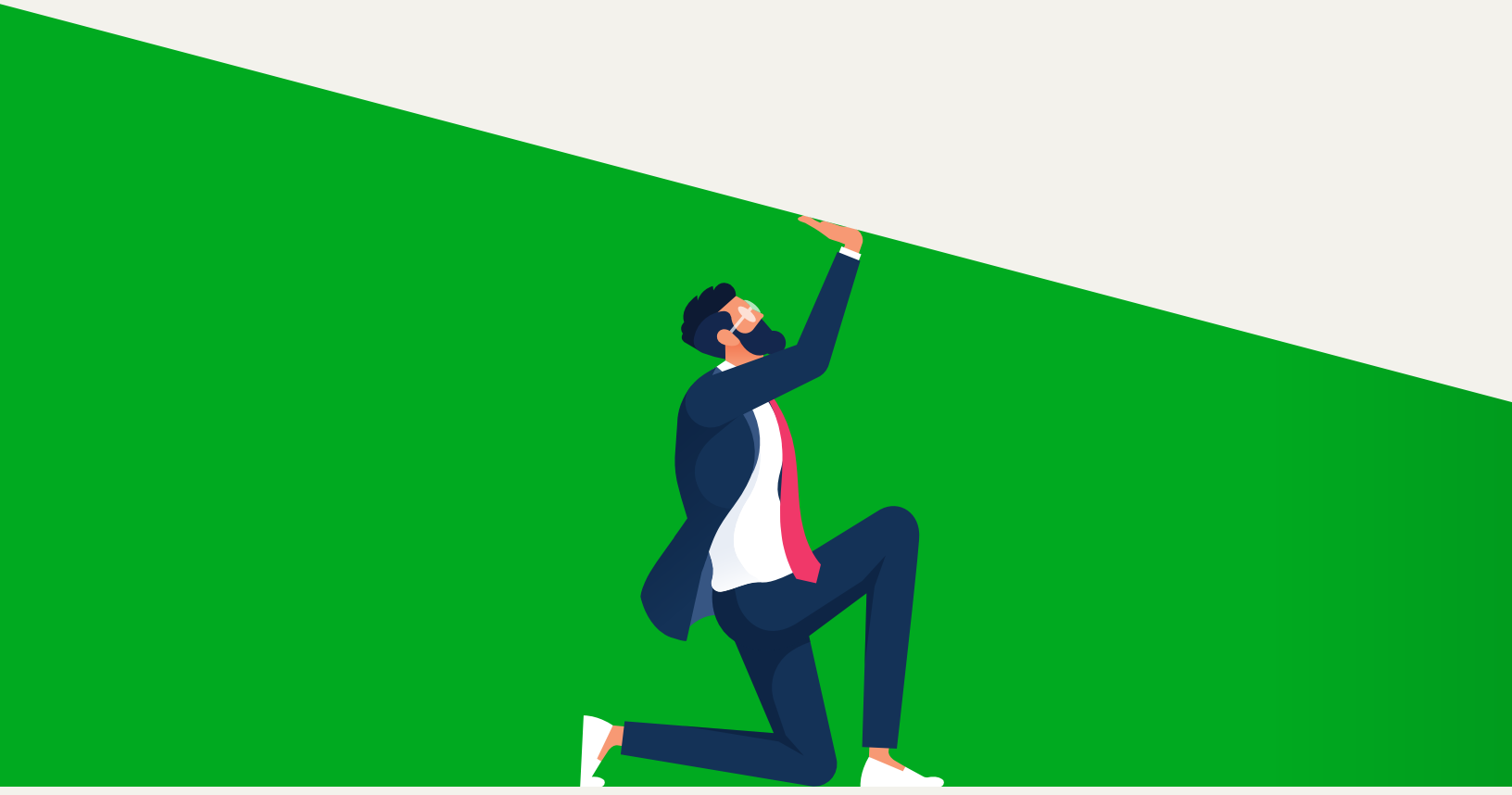


Table of Contents

Introduction

Every breach puts the business at risk. Every breach puts the Chief Information Security Officer (CISO) on the line. This cycle has become unsustainable.

CISOs are operating in one of the most difficult environments in memory. Cyber incidents are escalating in volume and impact, fueled by rapid advances in agentic AI and emboldened threat actors. At the same time, boards are demanding clearer risk metrics, regulators are raising expectations, and companies are cutting costs, often expecting CISOs to do more with fewer resources.

This convergence of pressures has made the role of the CISO uniquely high stakes. Leaders are accountable for every incident, regardless of whether it was preventable, and the professional toll is mounting. The 2025 Nagomi CISO Pressure Index captures this moment with hard data: the daily strain on security leaders, the widening gap between security investment and outcomes, and the cultural challenges that leave CISOs carrying responsibility they cannot, and should not, shoulder alone.

This report explores the state of the profession today: the relentless pressure CISOs face, the failures of sprawling tool stacks, the rising expectations of boards, and the paradox of AI as both top threat and promised efficiency driver. It also highlights where organizations must act to better support their leaders and strengthen resilience. **And while CISOs are at the center of this story, they cannot carry it alone.**

For the Wider Security Community...Security is a team sport.

For IT leaders, risk managers, compliance officers, and other executives, these findings are a reminder to share responsibility: to build alignment, provide resources, and create a culture where security leaders are supported. This data is also a tool for understanding the true weight CISOs carry and why that weight must be shared if organizations want to stay resilient.

Executive Summary

The data does not sugarcoat the reality: CISOs are under extraordinary strain, and the consequences are serious.

It isn't just burnout...

80% of CISOs report being under high or extreme pressure today.

87% say that pressure has increased over the past 12 months.

67% report being burned out weekly or daily.

40% have considered leaving their roles altogether.

44% say it has already affected their ability to prepare for breaches, exposing organizational vulnerability at the worst possible moment.

Incidents are constant...

73% of respondents experienced a major security event in the past six months.

>50% say they are personally blamed always or often when breaches occur.

60% fear their job would be at risk following a major incident.

58% say the cyber incident happened even though a tool was in place to stop it.

Meanwhile, CISOs manage ever-larger tool stacks...

65% of CISOs oversee 20 or more security tools. But most report gaps in integration and limited ROI. These tool failures compound the pressure, not relieve it.

Boardroom pressure now rivals threat pressure...

44% say expectations from the board/ executives are their top stress point, more than those citing external threats (33%).

82% feel confident quantifying risk, but over half lack standardized, business-relevant metrics that leadership reliably understands.

And then there's AI...

59% fear agentic AI attacks as their top threat for the next 12 months.

Almost 20% of recent incidents were AI-related.

But the paradox is acute:

82% also report pressure to reduce staff using AI-driven automation. CISOs are now fighting new AI threats while being asked to cut the very resources needed to defend.

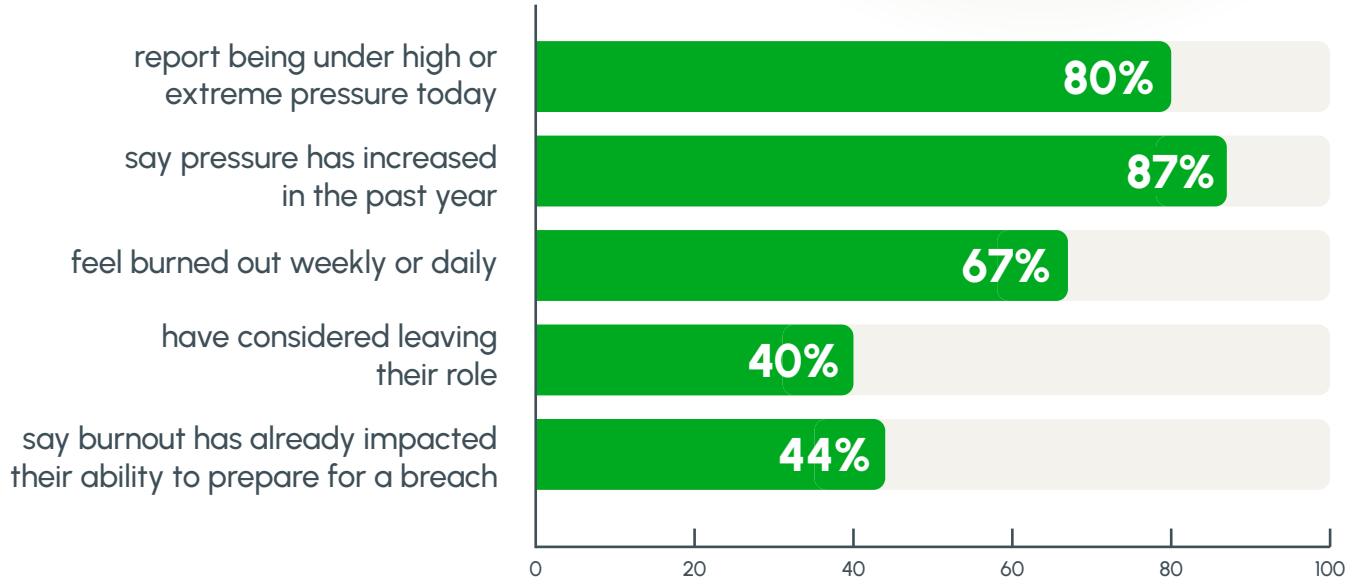
These findings make one thing clear: this is a turning point. Organizations must respond.

Closing the gap between security investment and outcomes, giving boards clearer risk metrics, consolidating tool stacks, and treating CISOs as partners, not scapegoats, are essential. Because when CISOs burn out or fail, the rest of the business is next.

Nagomi surveyed 100 Chief Information Security Officers across the United States.

Pressure Point #1

CISOs Are Operating at Unsustainable Pressure Levels



The implications are stark. Security leaders are expected to maintain constant vigilance, respond to incidents at any hour, reassure boards and executives, and manage sprawling tool stacks with shrinking teams and resources. The role rarely allows time to recover. The cost is not only human: when CISOs are overextended, the organizations they protect are less prepared for inevitable attacks.

The numbers show a role pushed to the edge. What started as a technical craft is now consumed by nonstop alerts, executive pressure, and the silent truth that one breach can trigger corporate damage and personal fallout. Without a shift, this churn will keep draining seasoned leaders when their judgment is needed most.

Pressure Point #2

Incidents Are Routine and CISOs Take the Blame

Seventy-three percent of CISOs faced a major security incident in the past six months. For most, these events are not anomalies but part of the job. Yet more than half (56%) say they are personally blamed always or often when breaches occur, and 60% fear their job would be at risk if a major breach happened on their watch.

This personal accountability is striking when you consider the reality: many incidents occur despite defenses and extensive cybersecurity tooling being in place. Fifty-eight percent of CISOs say they experienced at least one incident that their existing tools were supposed to prevent but didn't. The gap between investment and outcome is leaving security leaders to answer for failures that are often outside their control.

For CISOs, the message is clear, every breach is both a technical challenge and a career risk. This relentless cycle of incident, blame, and fear erodes trust between CISOs and the organizations they serve. It also drives short-term decision-making, as leaders weigh not just what's best for security, but what will protect their own standing if the worst happens.

Career Risk = Business Risk

73% of CISOs experienced a significant incident in the past six months.

56% are personally blamed always or often when breaches occur.

60% say their job would be at risk following a major breach.

Most common types of incidents

29% data breaches

22% ransomware

19% AI-related incidents

Pressure Point #3

Sprawling Tool Stacks Fail at Critical Moments

58% of CISOs experienced incidents that their tools should have prevented.

CISOs are managing sprawling, fragmented security stacks that too often leave them exposed when it matters most. Sixty-five percent oversee 20 or more tools, and more than 1 in 10 juggle 50 or more. Instead of reducing risk, these bloated stacks often add complexity, waste, and blind spots.

The most troubling finding: 58% of CISOs say they've experienced incidents that their tools were specifically meant to prevent. These failures cut to the core of the trust gap between investment and protection — organizations are spending more, but not necessarily getting the value they hoped to defend better.

Integration and visibility are recurring pain points. More than half (56%) report that their tools don't integrate fully, forcing teams to patch together workflows and manually connect the dots. Most (58%) say that fewer than half of their tools show measurable ROI. The result is wasted resources, duplicated effort, and security teams forced to fight advanced threats with an incomplete picture.

CISOs are clear about what they need: less clutter, more clarity. They want better integration across platforms, centralized oversight, and consolidated reporting. Without it, tool sprawl will keep eroding both defenses and the people tasked with maintaining them.

Bloated security stacks

65% of CISOs manage 20+ tools

13% of CISOs manage 50+ tools

CISO Wishlist

55% want better integration

49% want centralized oversight

32% want consolidated reporting

Pressure Point #4

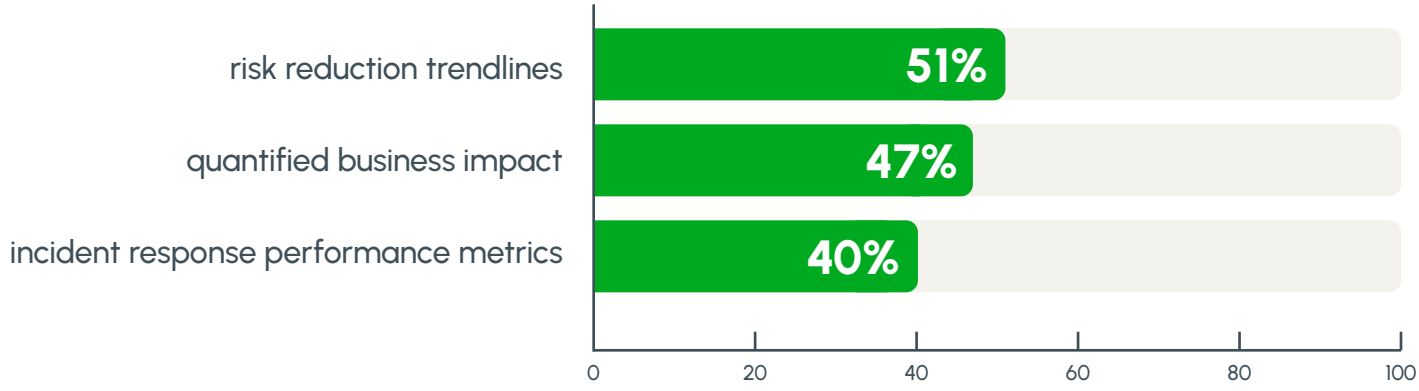
Boards Are Now the Top Source of Pressure

For many CISOs, the greatest pressure isn't coming from cybercriminals outside the walls of the organization. It is coming from inside the boardroom. Forty-four percent say expectations from boards and executives are their number one source of stress, compared with 33% who point to external threats. That shift shows how much the role has evolved. CISOs are now business leaders first and foremost, expected to guide strategy, explain risk, and safeguard the organization at every level.

The real challenge is not a lack of leadership. CISOs are already leading. The problem is the absence of a shared language for risk. Eighty-two percent feel confident they can quantify risk, yet more than half (54%) admit they lack the business-relevant metrics that can cut through with leadership. Boards want clear trendlines that show risk is going down, numbers that tie incidents to business impact, and performance measures that reflect how quickly and effectively teams respond when something goes wrong. Without these shared measures, conversations can feel like two sides speaking past each other.

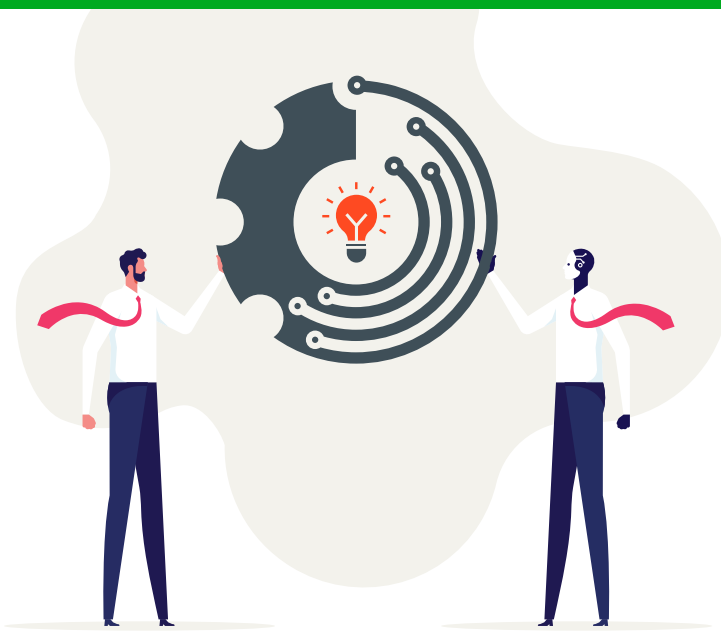
This disconnect creates strain on both sides. CISOs are held accountable when incidents occur, yet too often they are left without the clarity or support that comes from true alignment. Closing this gap is not just a matter of reporting. It is about ensuring boards and CISOs share a common framework for risk, so security leaders can do their jobs with the trust, backing, and resources they need.

Top 3 metrics boards want most



Pressure Point #5

AI Is Both the Top Threat and a Cost-Cutting Mandate



CISOs are caught in a paradox. On one hand, agentic AI attacks are now seen as the most urgent near-term threat: 59% say they fear these attacks more than any other over the next 12 months. Nearly one in five recent incidents were already AI-related, highlighting how fast the threat has moved from hypothetical to real. Looking ahead, 47% expect agentic AI to be their top concern within the next two to three years.

At the same time, 82% of CISOs face pressure from boards or executives to increase efficiency using AI-driven automation. Twenty-eight percent already have a formal mandate in place, while more than half report informal pressure to cut costs this way. That means CISOs are being asked to rely on the same technology that is actively arming attackers and to do it while reducing the resources their defenses depend on.

59% of CISOs cite agentic AI as their top near-term threat.

47% expect agentic AI to be their top concern within the next two to three years.

CISOs face pressure to increase efficiency

82%
face pressure to reduce staff with AI

28%
already have a formal mandate

54%
report informal pressure

This contradiction puts CISOs in a no-win position. They cannot ignore AI's potential to improve efficiency, but every adoption decision must be balanced against its role in fueling more sophisticated attacks. Until organizations approach AI with both urgency and caution — investing in augmentation rather than replacement — the imbalance will leave CISOs stretched thinner and adversaries with the upper hand.

Conclusion: Turning Pressure Into Progress

The 2025 Nagomi CISO Pressure Index makes one thing clear: the current trajectory CISOs are on is unsustainable. CISOs are being asked to do the impossible — defend against a wave of escalating attacks, manage sprawling tool stacks with questionable ROI, and satisfy rising board expectations — all while navigating burnout and the threat of personal blame.

These findings are not just about the state of the profession. They are about the resilience of every organization. When 58% of incidents happen despite a tool being in place to stop them, when 60% of CISOs fear losing their job after a breach, and when nearly half admit burnout is already impacting breach readiness, the conclusion is unavoidable: business risk has become inseparable from CISO risk.

But the message of this report is not defeat. It is a call to act. Organizations must:

1. **Close the gap between tools and outcomes** by validating that defenses work as intended, reducing sprawl, and focusing investment where it delivers measurable results.
2. **Empower CISOs with meaningful board alignment** by adopting risk metrics that are standardized, business-relevant, and transparent.
3. **Build resilience into culture** by shifting from blame to shared accountability, ensuring leaders are supported rather than scapegoated.
4. **Address the AI paradox** by defending against agentic AI threats while using AI responsibly to augment human expertise, not replace it.

CISOs are the frontline protectors of modern business, but they cannot and should not carry this weight alone. The next era of cybersecurity will be defined by organizations that recognize this, that support their leaders with integrated defenses, clear visibility, and a culture of partnership.

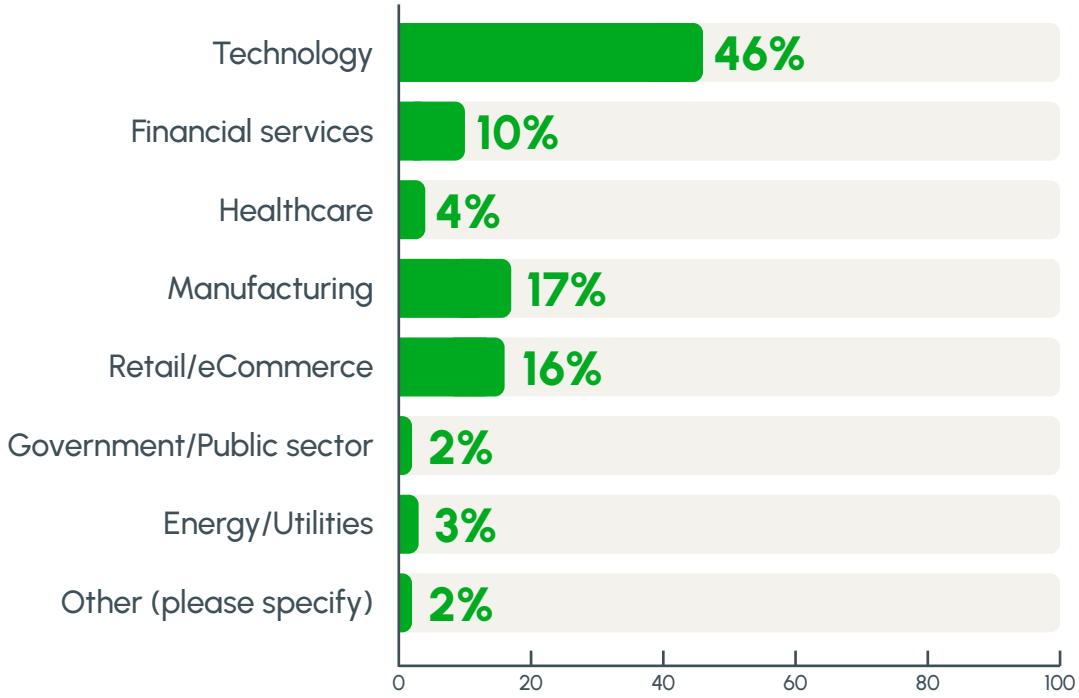
Validating exposure and effectiveness — not just buying more tools — will be the new standard. Organizations that embrace this shift will not only protect their CISOs, they'll protect their entire business.

For CISOs, boards, and the broader security community, the path forward is simple: take these pressures seriously, and turn them into progress.

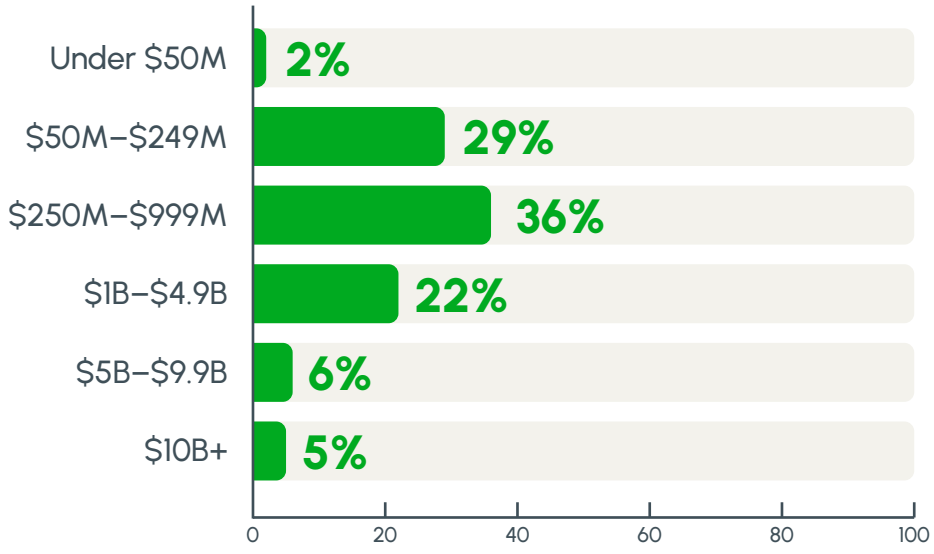
Methodology & Demographics

The 2025 Nagomi CISO Pressure Index is based on a September 2025 online survey of 100 CISOs across the United States. Respondents represented mid-market to global enterprises in industries including technology, financial services, healthcare, retail, and manufacturing.

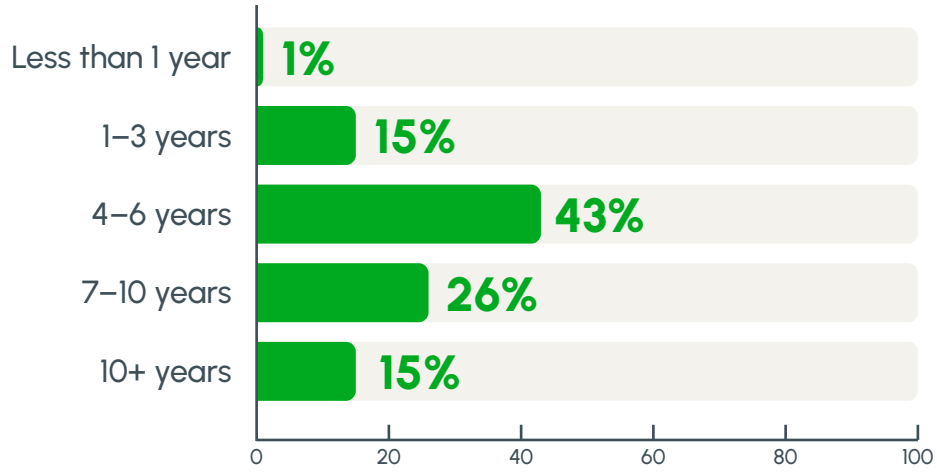
Which best describes your company's primary industry?



Annual company revenue



Years you have served as a CISO (or equivalent)



About Nagomi Security

Nagomi Security gives enterprise security teams the control to eliminate exposure, faster and at scale. As the execution layer of Continuous Threat Exposure Management (CTEM), Nagomi unifies asset visibility, contextual prioritization, remediation guidance, and performance reporting in a single platform. At its core is Exposure Lens, the only engine that correlates assets, controls, vulnerabilities, and threats to show risk in context across subsidiaries and business units. By validating defenses and directing fixes to the right owners, Nagomi ensures issues are resolved instead of tracked, closing exposures faster, strengthening defenses continuously, and delivering measurable progress for both security and business leaders. Recognized by Gartner® as a Cool Vendor, Nagomi is a pioneer in Automated Security Control Assessment (ASCA), helping organizations operationalize exposure management and drive down risk with the tools they already own.

nagomi

Learn more at: nagomisecurity.com