



The State of the Security Team 2022

Can security teams meet stakeholders' requirements?



Contents

01	Executive Summary	3
02	Key Findings	4
	Section 1: Security is No Longer an Internal Affair; Customers and Partners Now Demand Higher Standards	5
	Section 2: High Security Team Stress and Turnover Are Leading to Higher Security Risk	8
	Section 3: Companies Lack a Strategy for Adding New Security Capabilities That Improve Security While Reducing Stress	12
03	Conclusion	15
04	Methodology	16
	About LogRhythm	17
	About Dimensional Research	18

Executive Summary

Cybersecurity has become a business imperative; however, the demands from stakeholders such as customers, partners, and government regulators continue to evolve and overwhelm security teams. And, a persistent shortage of skilled professionals, along with the complexity of security solution sprawl, adds more pressure to security teams and leads to higher security risk. To meet stakeholder demands, alleviate stress, and reduce risk, executives must prioritize hiring and solution integration, rather than be lured into the trap of deploying unnecessary technology.

While many vendors regularly release data on these challenges, LogRhythm sought to understand the current stressors security professionals face, as well as the ways they overcome them. LogRhythm partnered with Dimensional Research, a leading independent research firm, to conduct a global survey of 1,175 security professionals and executives. The research investigates security solution capabilities, deployment strategies, security gaps, and the value of tool consolidation. The survey also includes insightful data collected by LogRhythm and Dimensional Research in 2020 to establish trends.

Compared to our 2020 research initiative, we also expanded the global reach of this survey. Initially, we thought this might glean interesting differences by country and region, driven by access to technology, resources, skills, and defense sophistication. Instead, we found a global perspective in which the challenges faced by security teams, their stressors, and the ability to deal with them are strikingly similar.

To meet stakeholder demands, alleviate stress, and reduce risk, executives must prioritize hiring and solution integration, rather than be lured into the trap of deploying unnecessary technology.

Key Findings

LogRhythm's initial iteration of the research in 2020 found significant misalignment between executives and their security teams. In fact, only 43% of respondents indicated they received enough executive support with regards to budget, strategic vision, and buy-in. In contrast, the 2022 research concludes executive teams are more informed and educated about cybersecurity. As a result, executive support nearly doubled over the last two years. In fact, the majority of respondents (83%) said they now receive enough executive support, indicating a significant improvement in understanding the importance of cybersecurity initiatives and alignment between executive leadership and their security teams.

Still, the research found that many challenges remain. The top drivers of stress are largely unchanged and investment in overlapping tools continues. Security teams notice they must answer not only to internal stakeholders, but also to external stakeholders like partners, customers, and government regulators, or risk losing business because of an inability to meet security expectations. Instead of implementing more tools to address these challenges, security teams seek skilled team members and integrated solutions.

Section 1

Security is No Longer an Internal Affair; Customers and Partners Now Demand Higher Standards

Cybersecurity is no longer an internal affair as 91% admit their company's security strategy and practices must now align to customers' security policies and standards (Chart 1). Partners also exert control with 85% stating their company must provide proof of meeting partners' security requirements (Chart 2).

Have your customers ever asked your company to provide proof that they meet specific security requirements?

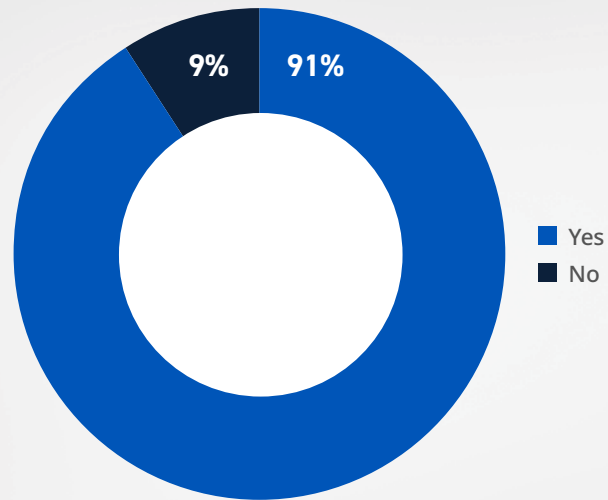


Chart 1

Have your partners ever asked your company to provide proof that specific security requirements are met?

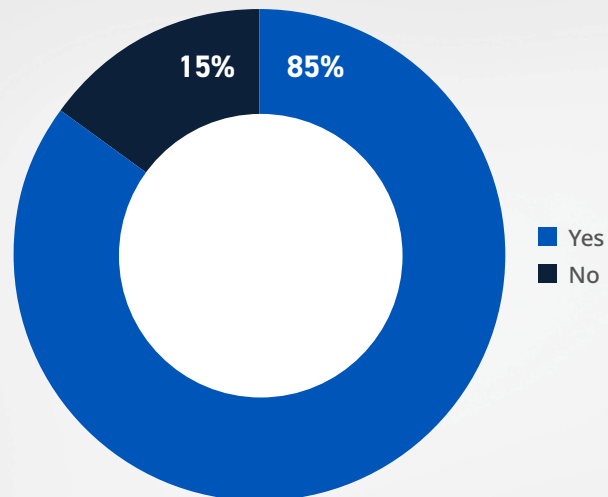


Chart 2

Meeting these partner and customer security requirements is not just a paper exercise, as two out of three companies (67%) admitted to losing deals by failing to meet specified security requirements (Chart 3).

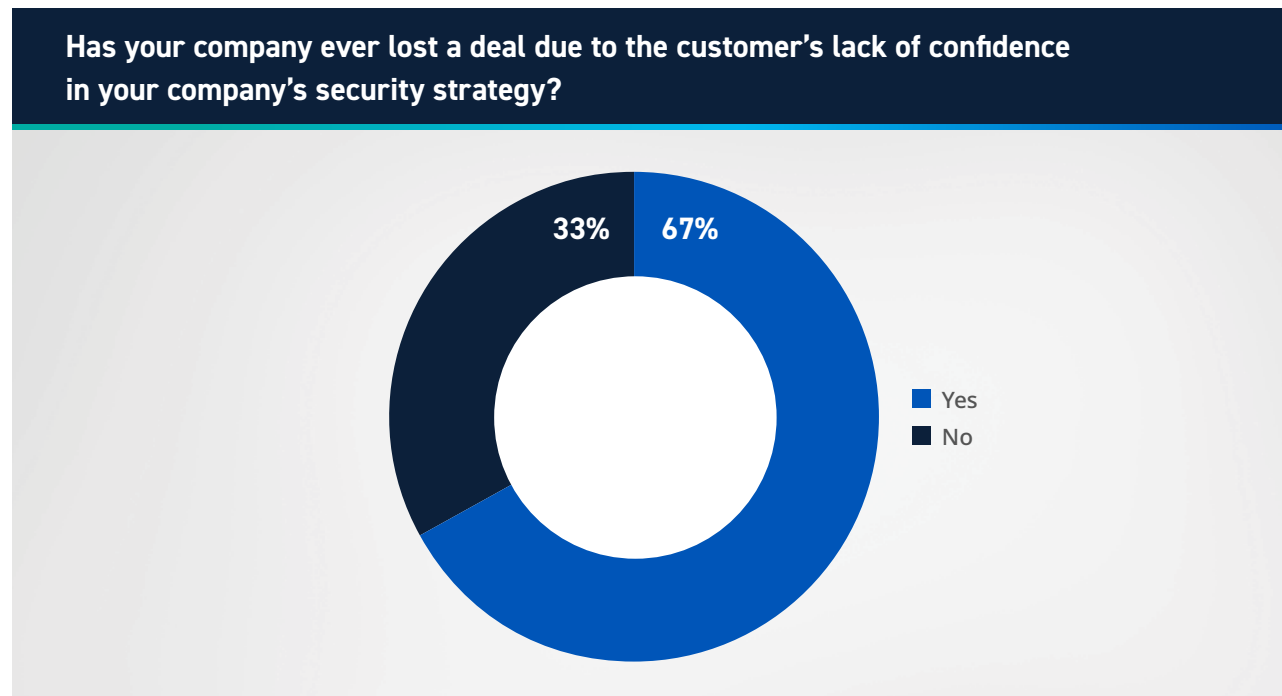


Chart 3

When asked, “Which of the following challenges is your company lacking proper solutions to address?” the top three most commonly selected answers included the tools to properly manage digital supply chain security, defend the increasing defense perimeter driven by remote employees and expanding cloud utilization, and manage the risk of employees who intentionally or inadvertently breaks security protocols (Chart 4).

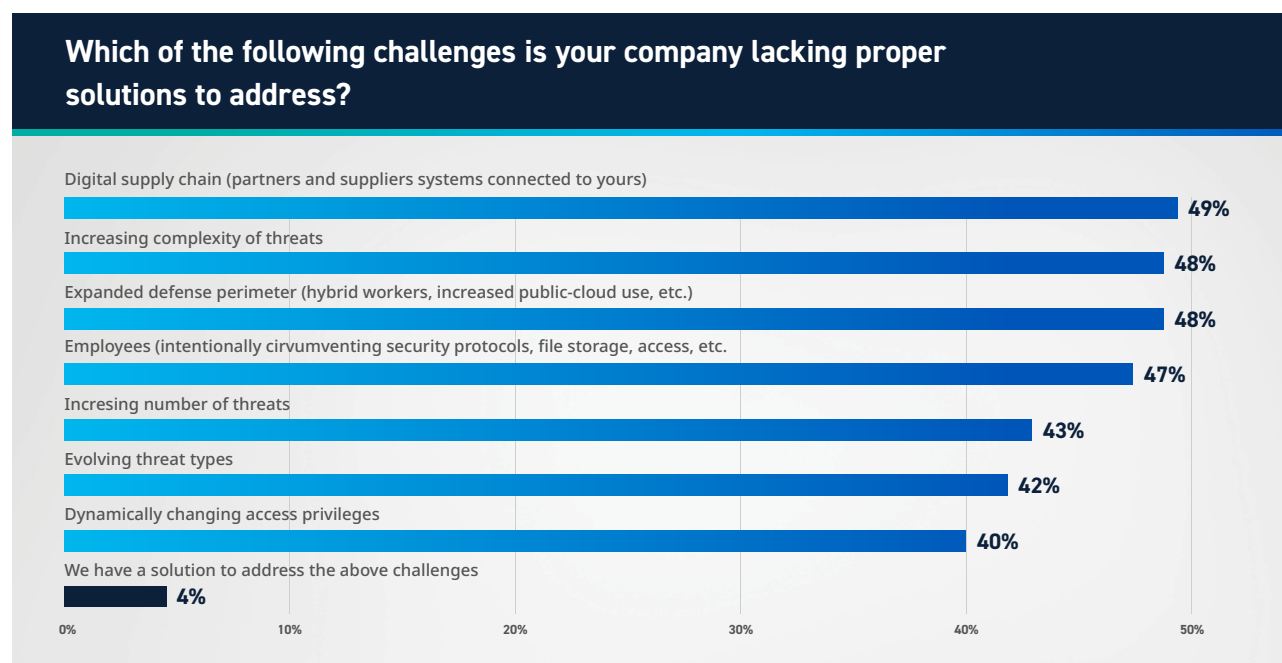


Chart 4

Section 2

High Security Team Stress and Turnover Lead to Higher Security Risk

77% of executive participants stated employee turnover compromises security team effectiveness (Chart 5). Work-related stress for the security team is increasing for nearly seven in ten companies, with 30% reporting a significant increase (Chart 6), indicating many companies may be trying to do more with less amidst budget constraints.

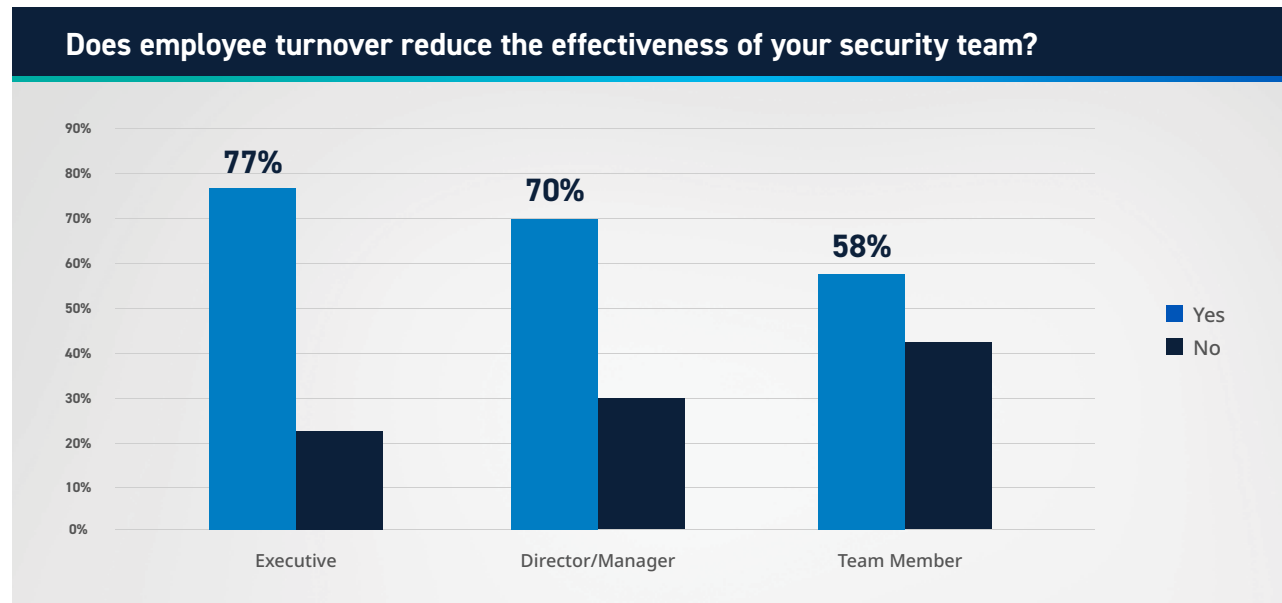


Chart 5

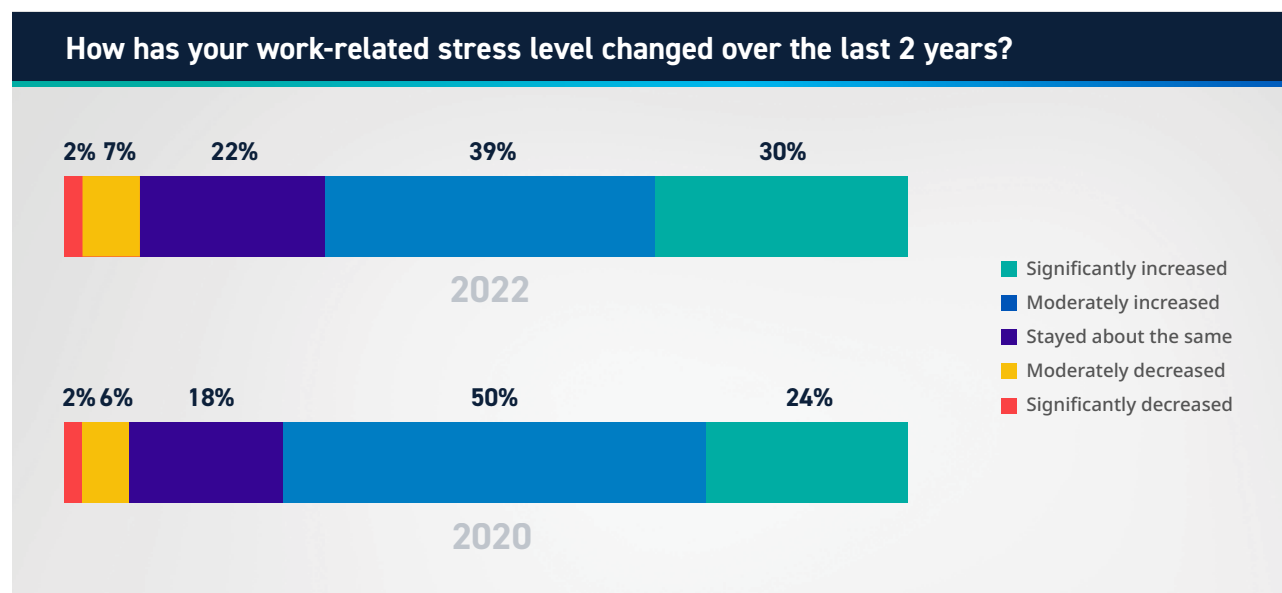


Chart 6

Growing attack sophistication and frequency, combined with more responsibilities and regulatory compliance, are increasing stress. In 2020, factors such as attack sophistication and frequency, and meeting regulatory requirements like GDPR, had a strong lead over other challenges that increased stress. In 2022, it appears that security teams are overall more worried about an increasing number of complex security challenges (Chart 7).

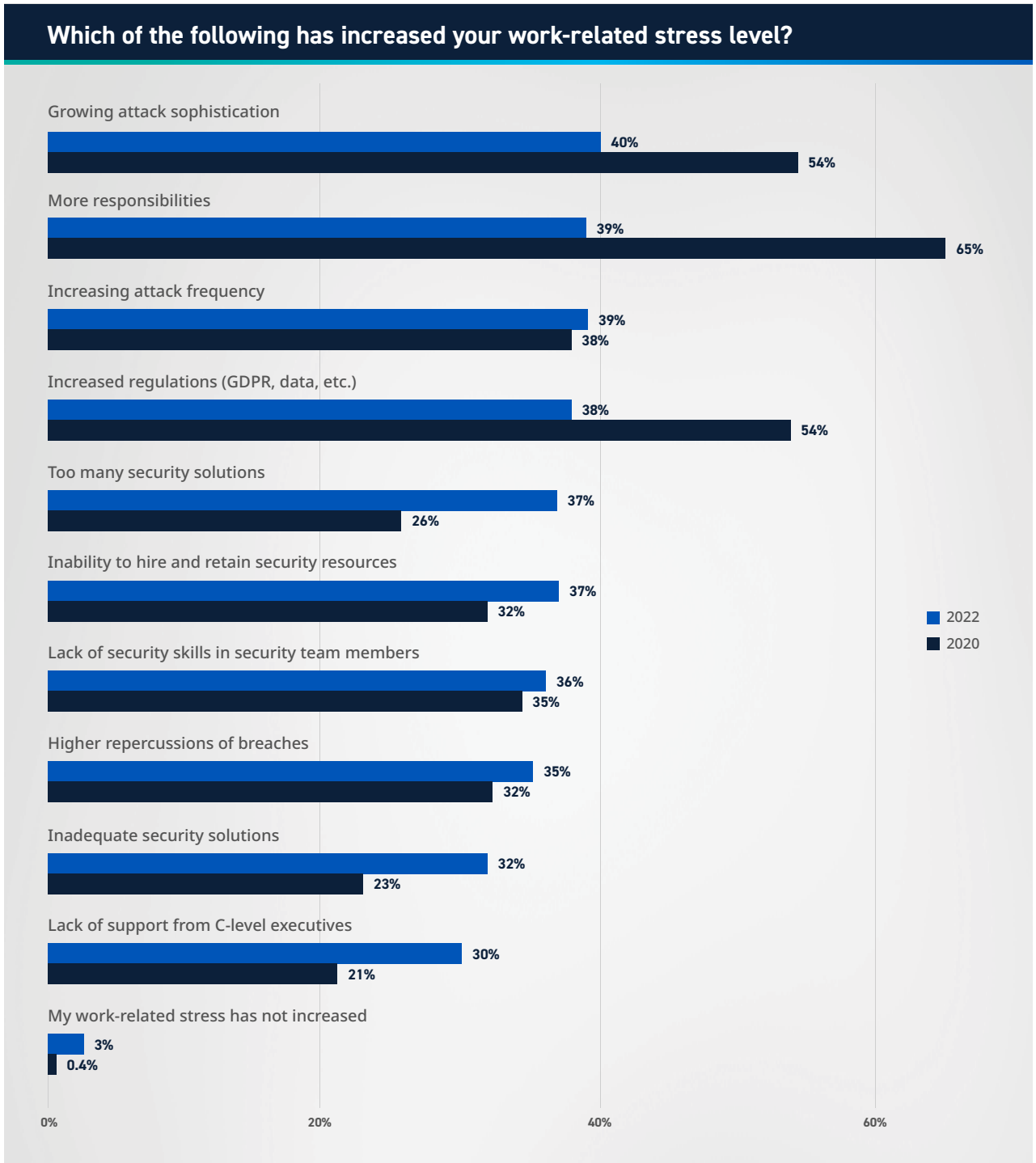


Chart 7

When asked what would reduce stress, participants indicated a few key items, such as more experienced team members, support from other IT teams, and better integrated security tools (Chart 8).

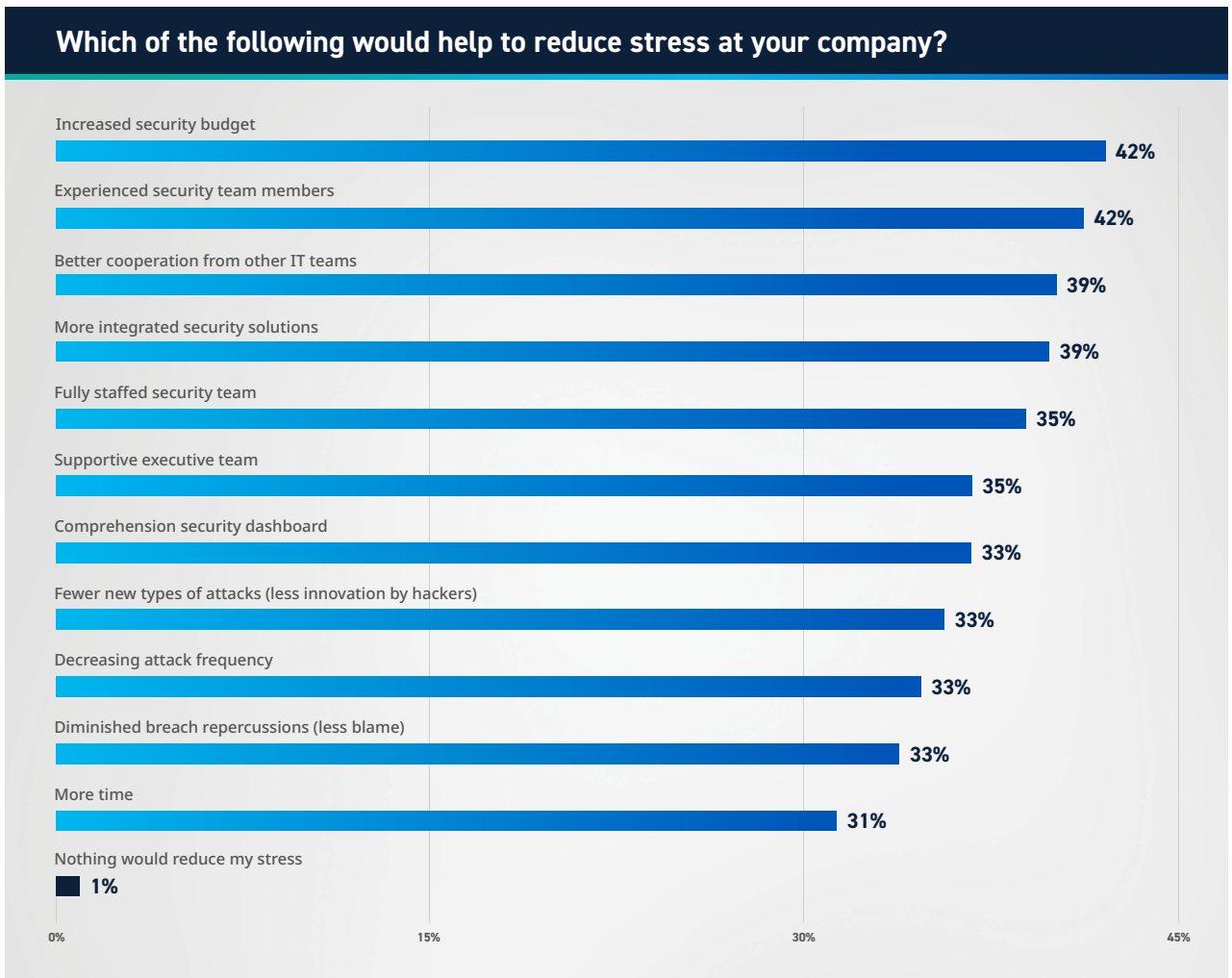


Chart 8

Section 3

**Companies Lack a Strategy
for Adding New Security
Capabilities That Improve
Security While Reducing Stress**

The research then focused on security tools and found 85% of companies have an increasing trend of overlapping security solutions (Chart 9), but a majority of tool overlap is accidental (Chart 10). As a result, security teams face additional work to deploy and maintain duplicative tools, which can be particularly frustrating because these efforts won't necessarily yield better security defenses or improve response times.

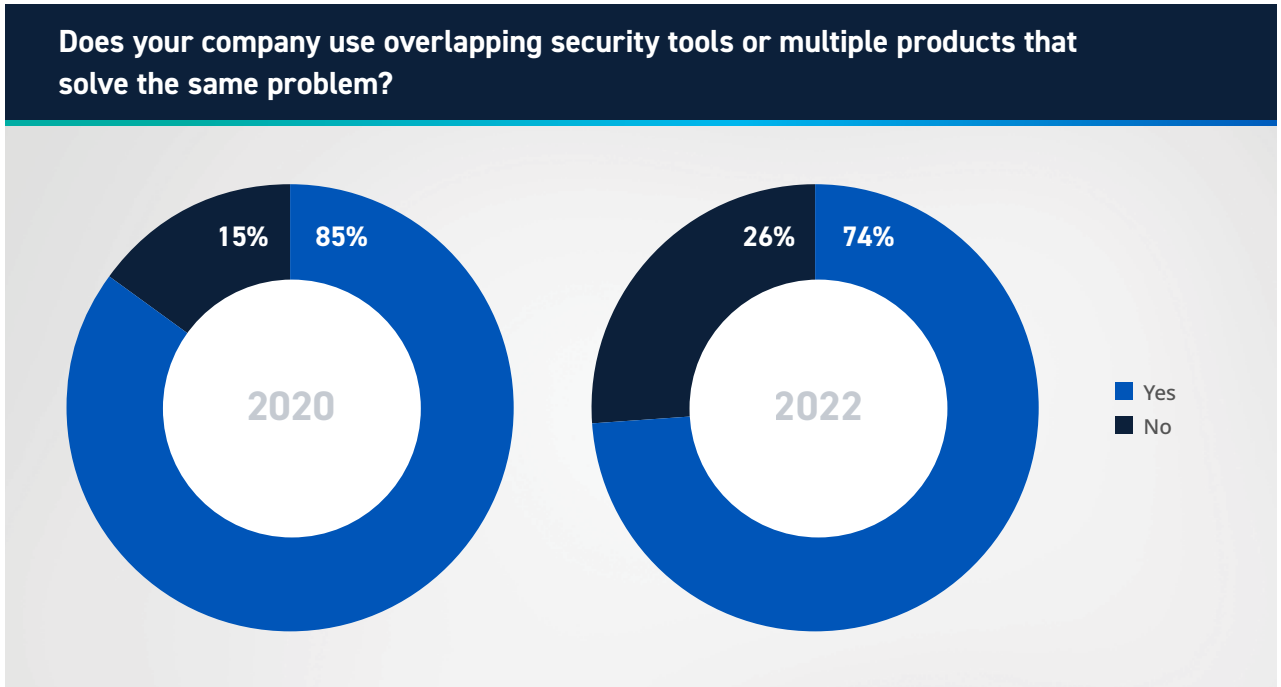


Chart 9

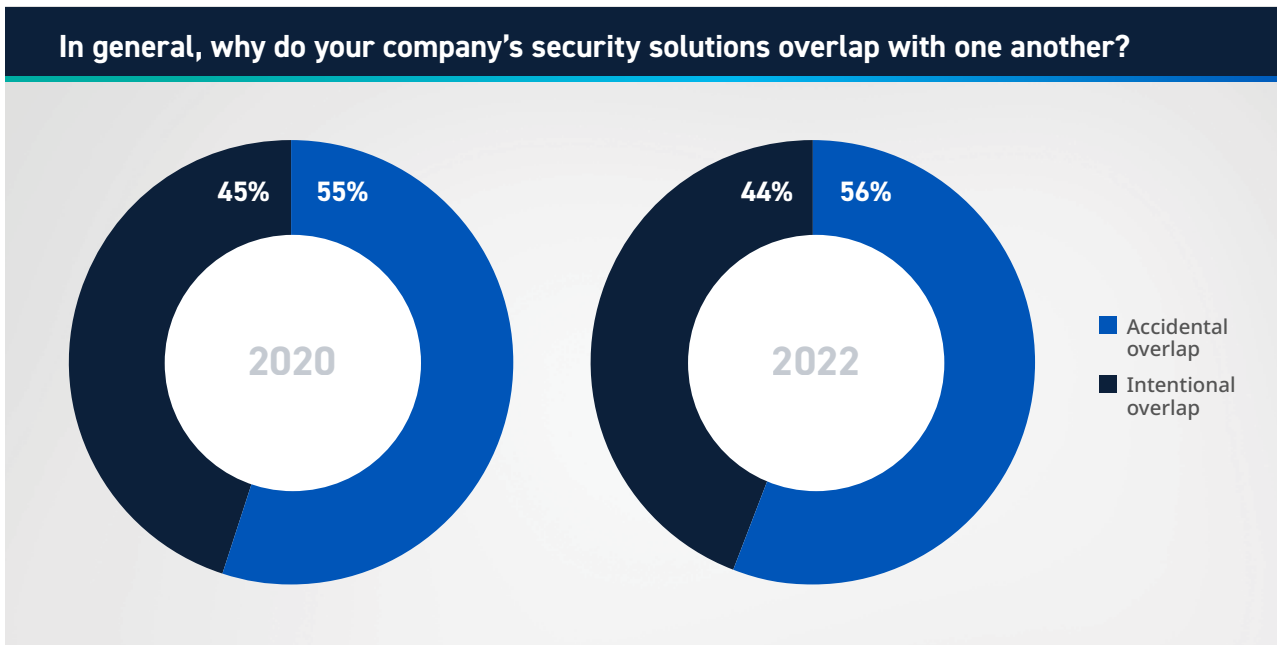


Chart 10

Yet in spite of that, one of the top three objectives for security teams in 2022 is the deployment of even more security tools (Chart 11).

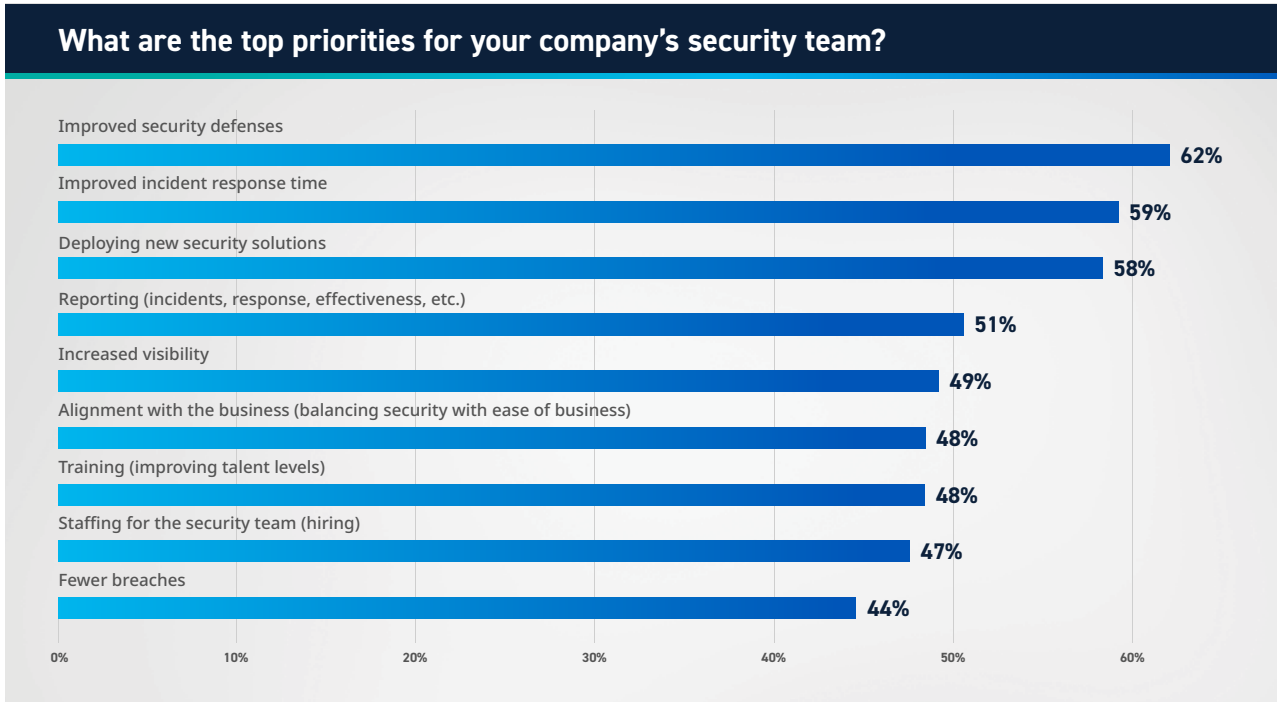


Chart 11

When security experts were asked directly about the benefits of integrated security tools, they responded with faster security issue notification, identification, and resolution, delivering an overall improved security posture. In short, consolidated security tools lead to faster issue detection, identification, and resolution, yielding improved security posture (Chart 12).

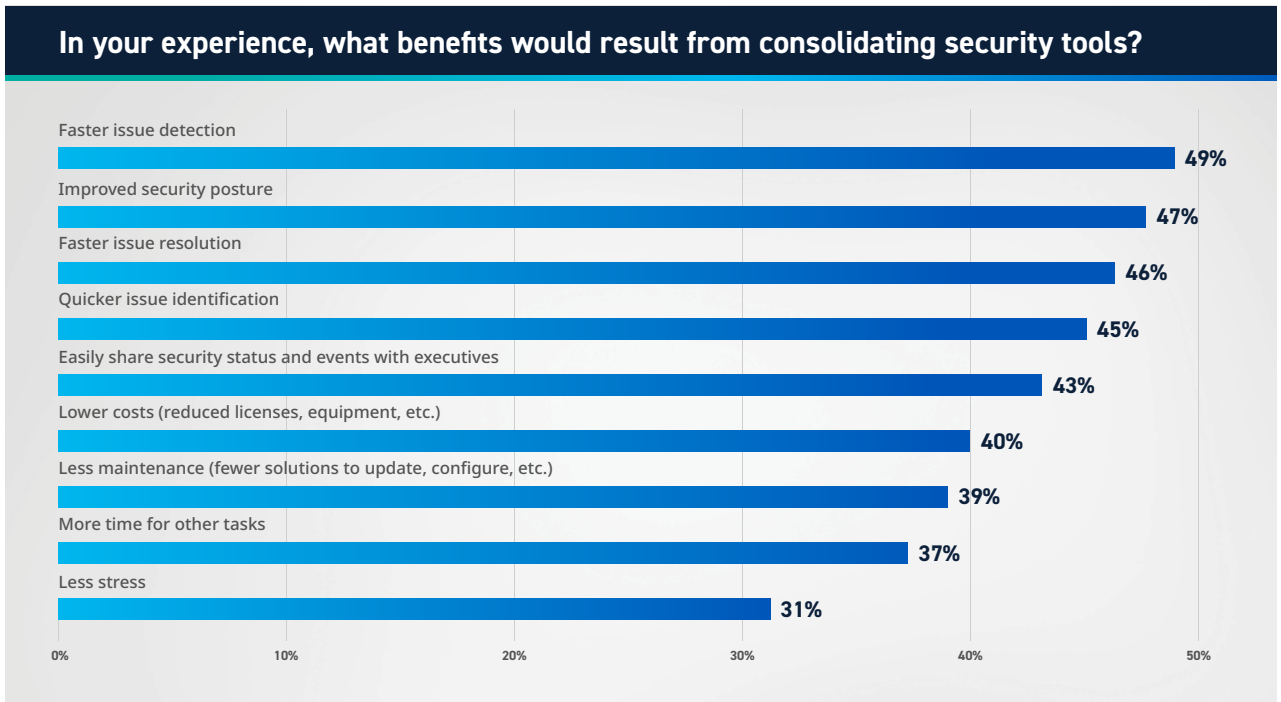


Chart 12

Conclusion

Security teams face challenges on every front; digital transformation continues to expand the attack surface; external stakeholders are becoming more focused on the efficacy of cybersecurity in their supply chains, and overlapping cybersecurity tools cause stress on already stretched security teams.

Executives need to pay more attention to the priorities of frontline security professionals and focus on consolidation, training, and staff retention. It is equally important to ensure security teams are armed with the appropriate resources to meet regulatory compliance requirements, as well as internal and external stakeholder demands.

04 —

Methodology

Security and IT professionals at medium to enterprise companies representing all seniority levels were invited to participate in a survey on their company's security practices. The survey was administered electronically, and participants were offered a token compensation for their participation. A total of 1,175 qualified participants completed the survey in 2022 and 308 in 2020. All participants had enterprise security responsibilities. Participants were from five continents representing a global view.



About LogRhythm

LogRhythm helps busy and lean security operations teams save the day—day after day. There's a lot riding on the shoulders of security professionals—the reputation and success of their company, the safety of citizens and organizations across the globe, the security of critical resources—the weight of protecting the world.

LogRhythm helps lighten this load. The company is on the frontlines defending against many of the world's most significant cyberattacks and empowers security teams to navigate an ever-changing threat landscape with confidence. As allies in the fight, LogRhythm combines a comprehensive and flexible security operations platform, technology partnerships, and advisory services to help SOC teams close the gaps.

Together, LogRhythm and our customers are ready to defend.
Learn more at logrhythm.com.





About Dimensional Research

Dimensional Research® provides practical market research for technology companies. We partner with our clients to deliver actionable information that reduces risks, increases customer satisfaction, and grows the business. Our researchers are experts in the applications, devices, and infrastructure used by modern businesses and their customers.

For more information, visit www.dimensionalresearch.com.





www.logrhythm.com // info@logrhythm.com

United States: 1.866.384.0713 // United Kingdom: +44 (0)1628 918 330
Singapore: +65 6222 8110 // Australia: +61 2 8019 7185

© LogRhythm Inc. | BR210822-12