ManageEngine

The State of Cybersecurity in Latin America 2024

www.manageengine.com

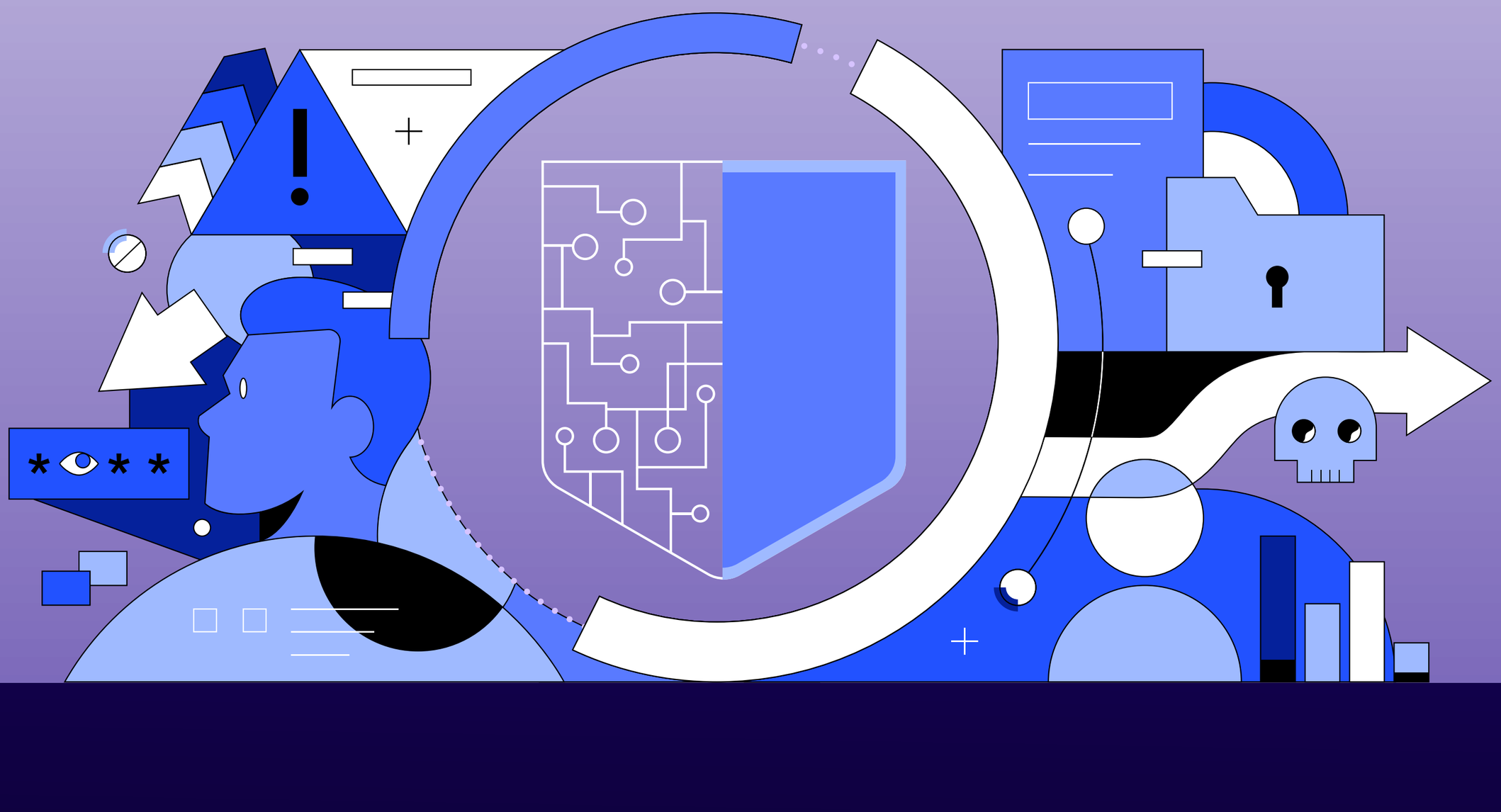


Table of index

A regional survey of executives and security professionals

Introduction

This paper provides a brief synopsis of a regional research survey focusing on the state of IT security in Latin America and the impact of AI on security defense and on security team members. The research also investigated the use of cybersecurity insurance and the ability to meet data management requirements.

A total of 705 qualified executives and security professionals at small businesses to large enterprises completed the survey. Participants were in seniority positions, manager level and above, and were directly responsible for their organisations' security defense and strategies.

This research investigated trends across all types of industries in the following countries:

Brazil

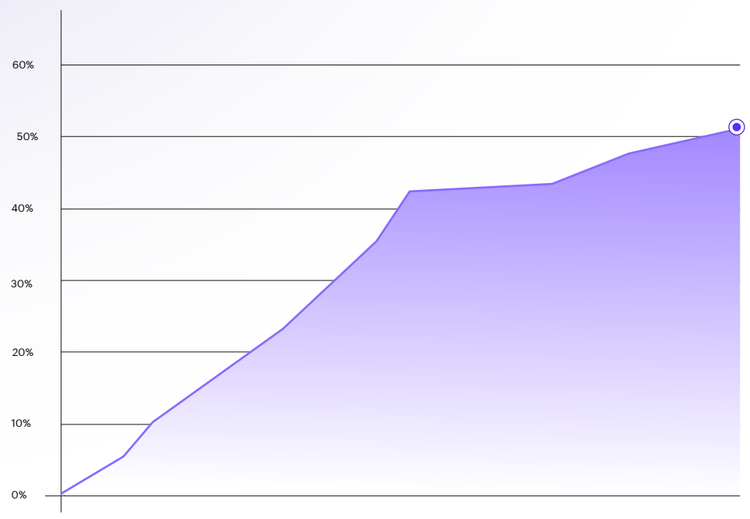
Mexico

Colombia

Argentina

Key highlights

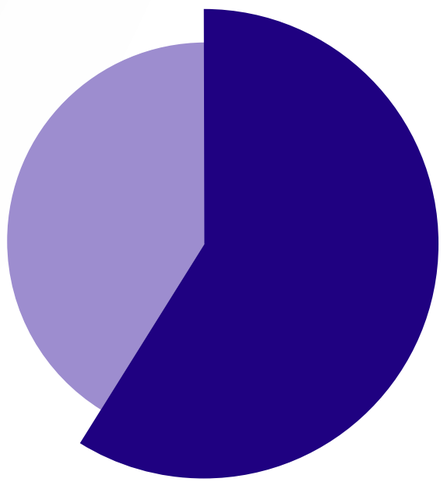
AI-empowered attacks usher in a new era of security threats with increased effectiveness



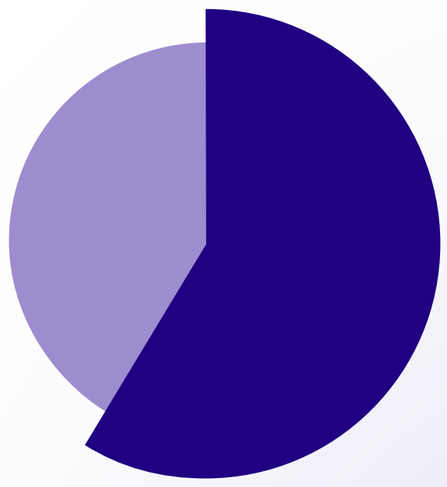
51%

of companies stated that generative AI played a significant role in cyberattacks

Employees remain one of the weakest links in security defenses



65% of security professionals said new employees who do not receive security training create significant risk to the business



64% of security professionals state their stress level is rising

ManageEngine

Key highlights

AI-enabled security solutions are critical for defending the business in 2024

92% share AI-enabled security solutions are critical for defending their company

89% indicate that half or more of all their security solutions will be AI-powered by the end of 2024

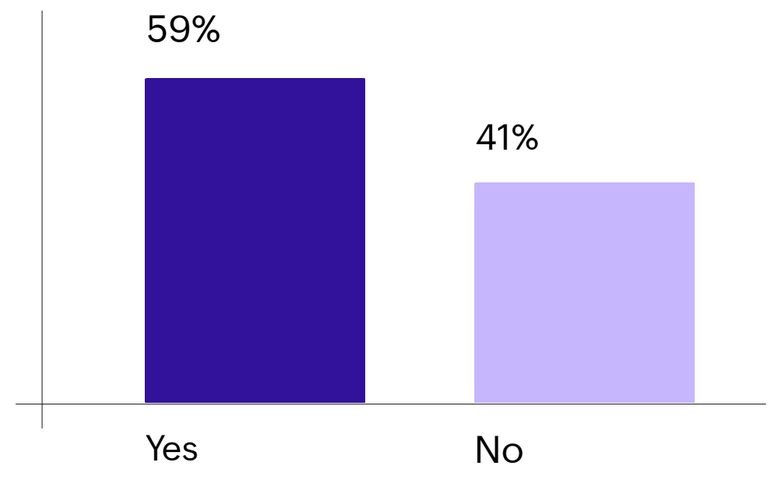
86% unilaterally trust AI-enabled security tools to make changes and implement actions

Section 1: Threats and impact

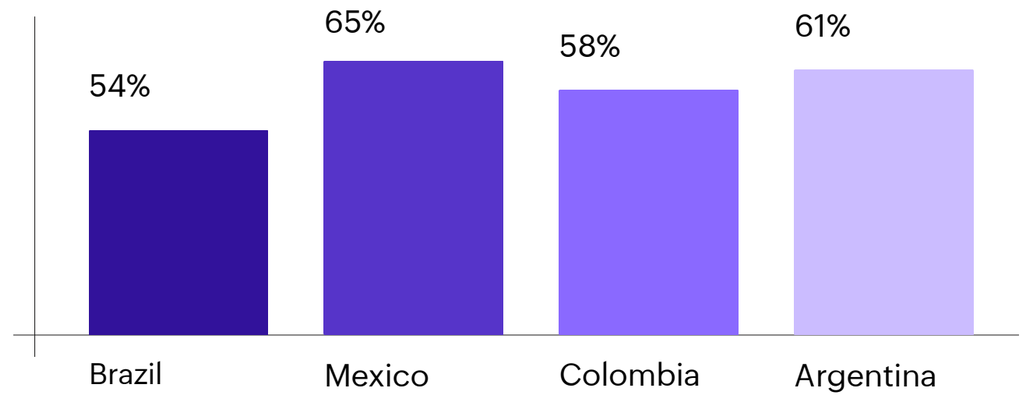
In 2023, more than half (51%) of LATAM companies stated that generative AI played a significant role in **cyberattacks against** their companies.

In 2023, 59% of respondents acknowledged that their companies encountered an increase in cybersecurity breaches compared to previous years. However, attacks resulting in **substantial financial losses** were low.

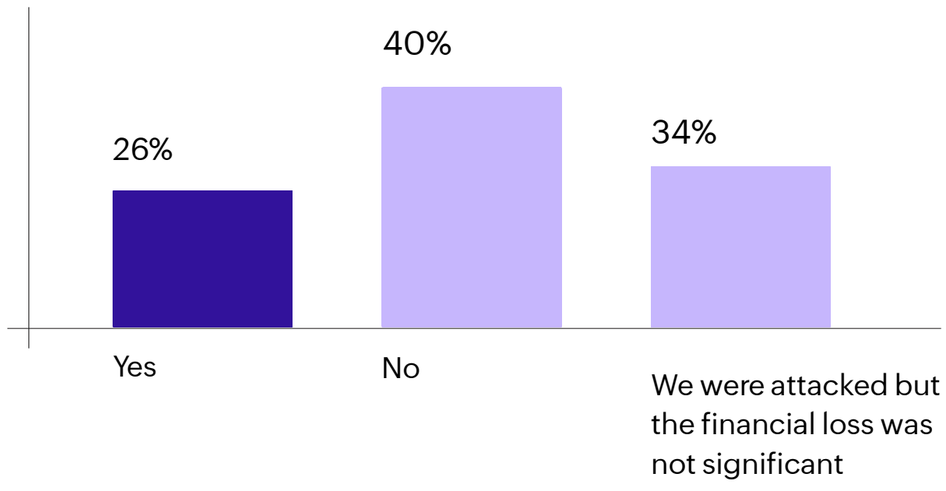
Did your company experience more cybersecurity breaches (successful attacks) in 2023 compared to previous years?



Companies in the following regions experienced more cybersecurity breaches in 2023 compared to previous years:

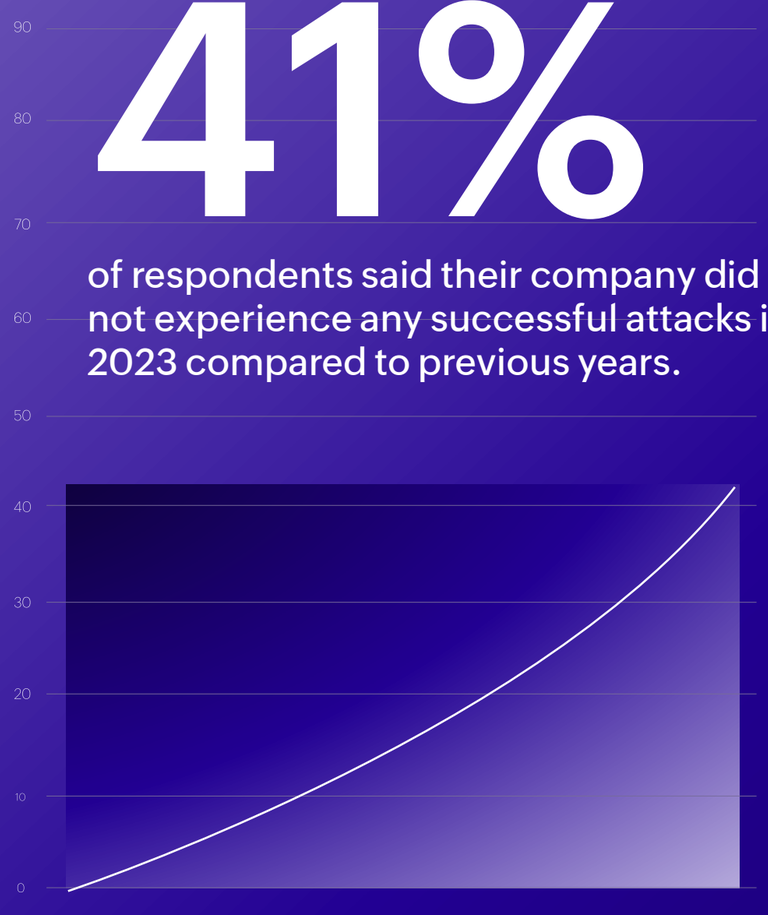


In 2023, did your company experience a cybersecurity attack that resulted in significant financial loss?

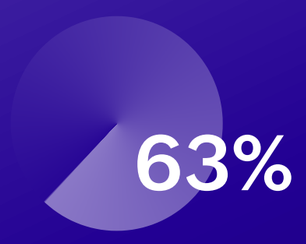


41%

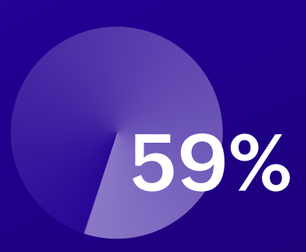
of respondents said their company did not experience any successful attacks in 2023 compared to previous years.



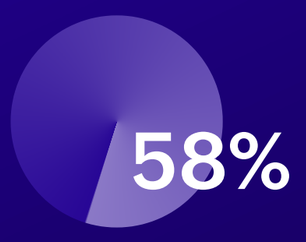
What contributed to your company experiencing fewer breaches in 2023?



Comprehensive security solutions in place



Improved security awareness among employees

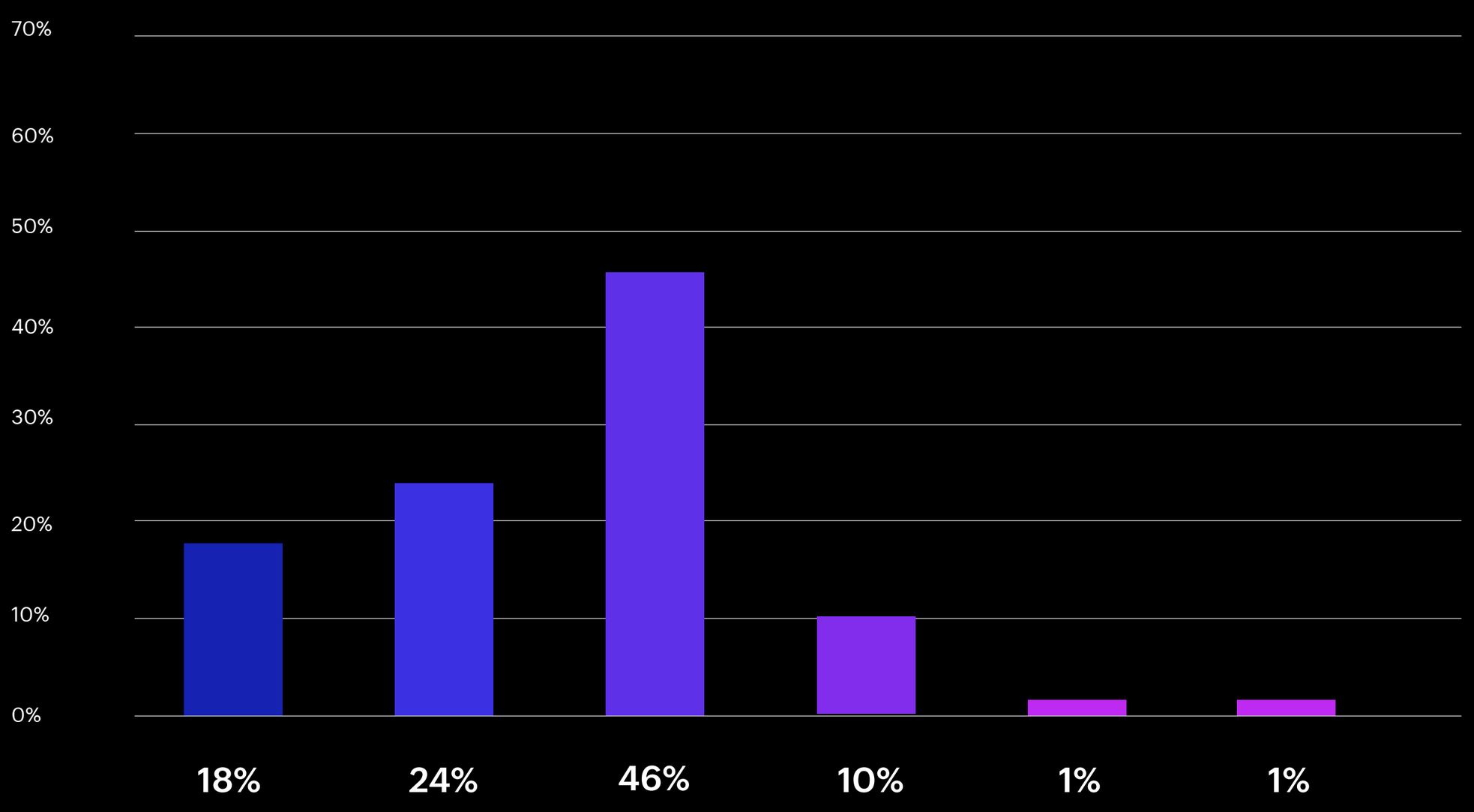


Increased budget allocation for cybersecurity

Section 2: Cybersecurity insurance

In LATAM, 99% of companies reported having cybersecurity insurance, yet only 42% found obtaining such insurance easy or very easy.

Q	How easy would you describe the process of purchasing cybersecurity insurance?



Very Easy: 18%

Easy: 24%

Moderate (neither easy nor difficult): 46%

Difficult: 10%

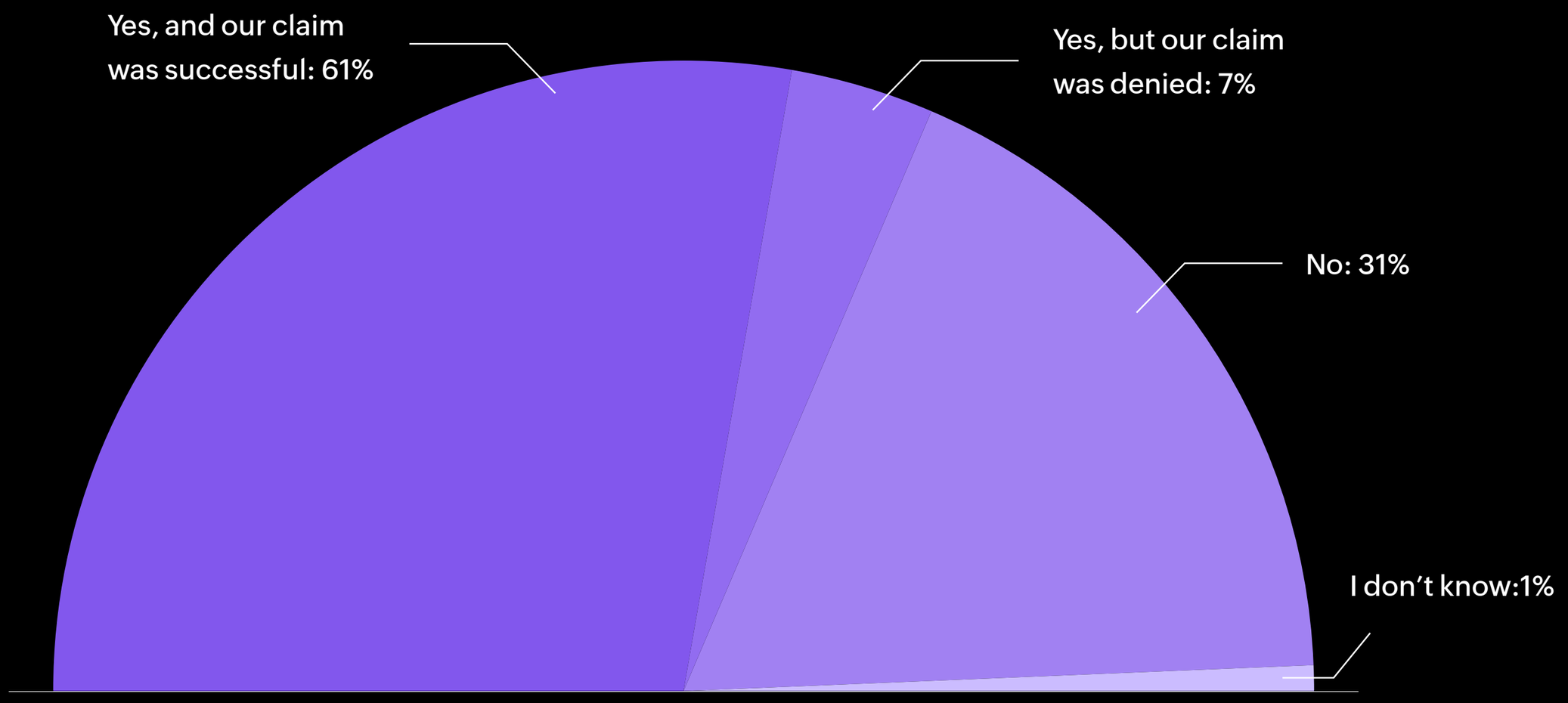
Very difficult: 1%

We don’t have cybersecurity insurance: 1%

ManageEngine

Only 27% of respondents reported that their organizations had experienced cyberattacks leading to a substantial financial loss, while 34% acknowledged being targeted by cyberattacks without experiencing significant financial harm. That said, more than six in ten respondents (62%) disclosed their companies were able to successfully secure insurance claims for the cyberattacks they faced in 2023.

Q Did your company make a cybersecurity insurance claim for any of the attacks it faced in 2023?

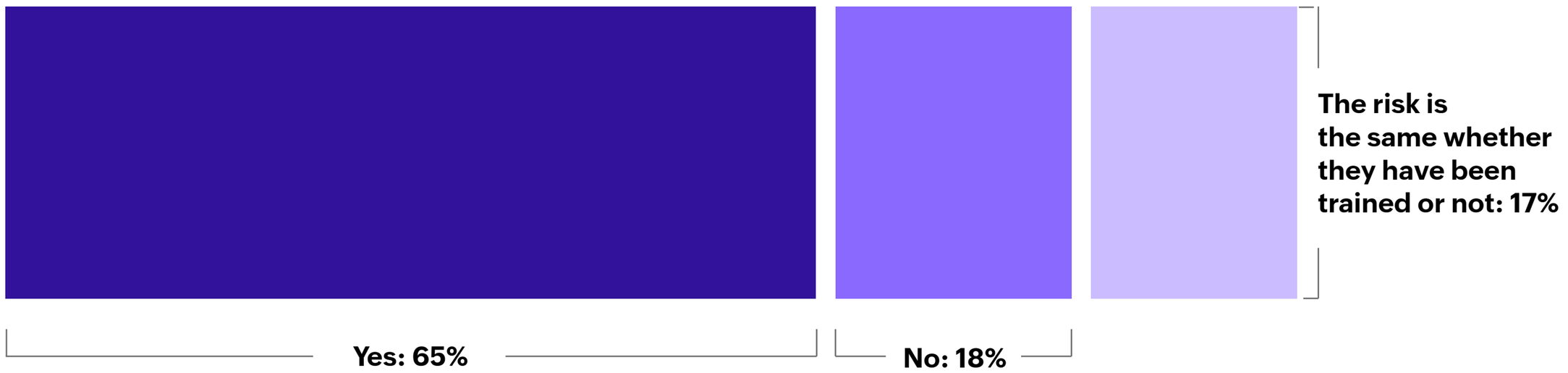


The strong insurance focus on employee security training is merited as the second and third leading security threat vectors in 2023 that included employees: accidental employee actions (64%) and willful employee actions or internal bad actors (39%). External entities, at 67%, barely beat out the employee threat. Analyzing the data revealed the employee risk grows with company size.

Section 3: Role of employees

In addition, 65% of security professionals said new employees who do not receive security training create significant risk to the business. Companies do understand the threat, as 97% of companies report employees are trained on security. However, given the many breaches companies experience, there is a concern about the quality of employee training. The data again showed AI-powered cyberattacks were even more effective against employees, as they can make phishing, deepfakes, and other employee-focused threats even more sophisticated and convincing. This makes training of employees, especially for those who have newly joined the organization, an absolute necessity.

Q	In your experience, do new employees who have not received cybersecurity training create significant risk for your company?



Section 4: Role of AI

Security professionals state AI-enabled security solutions are needed, with 92% stating it was critical for defending their company. This led to 89% indicating that half or more of all their security solutions will be AI-empowered by end of 2024. **Security teams having faced GenAI-powered attacks were three times more likely to say all their security needed to be AI-enabled.**

The research did reveal some controversial findings, as 86% unilaterally trust AI-enabled security tools to make changes and implement actions without the need of a human to review the proposed action. Perhaps this is due to the lack of experience noted previously. However, security professionals are aware of this risk, and 89% stated that an independent organization is needed to ensure the trustworthiness of AI-enabled security solutions.

The fact is, AI-empowered attacks are more effective, creating financial hardships and increasing stress on security teams. In 2024, companies will need AI-enabled tools and experienced professionals to defend the business and protect their data against the growing AI threats.

Q	In your opinion, will AI be critical to defending against cybersecurity attacks in 2024?

Q	In general, does your company trust AI-enabled cybersecurity solutions to make appropriate changes to your security defenses?

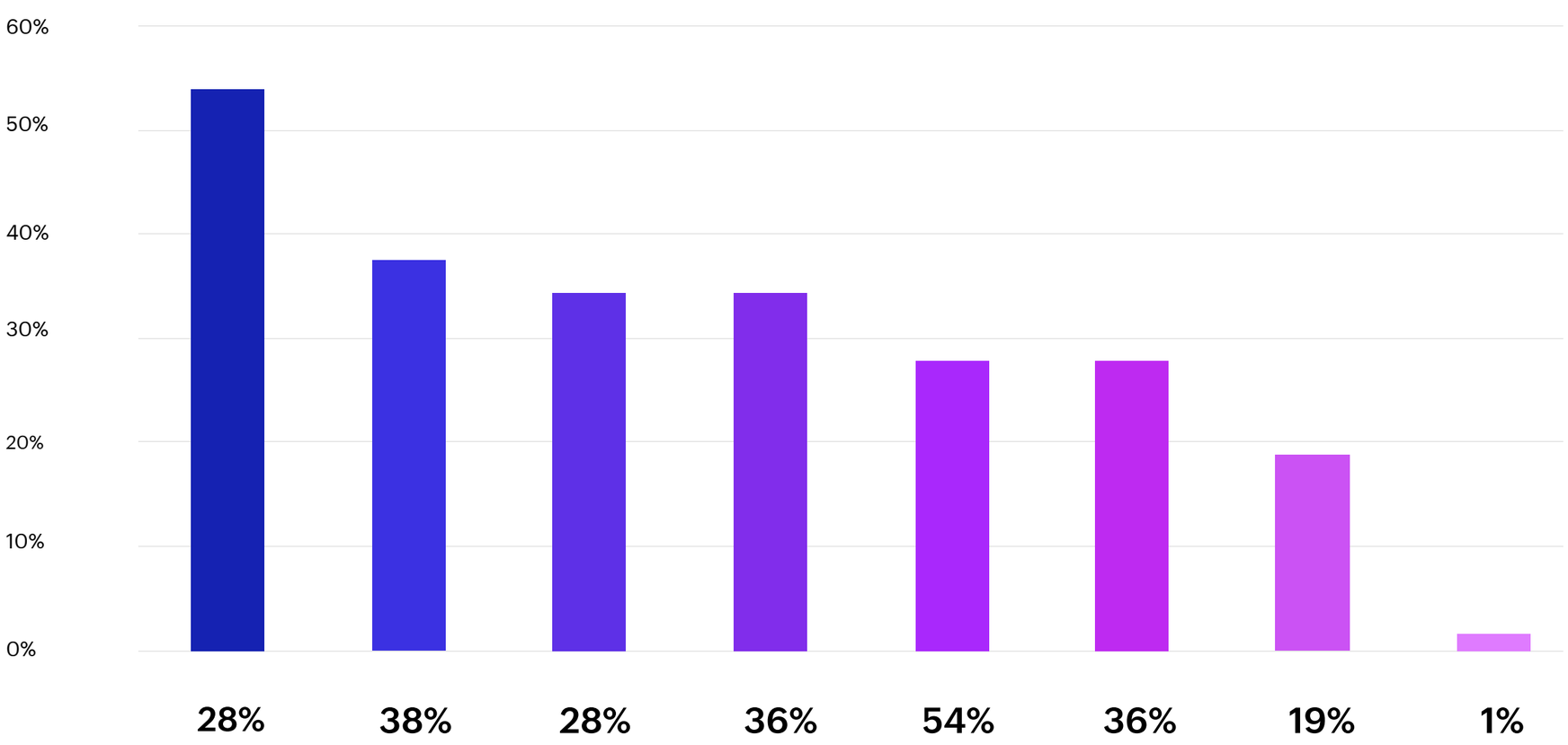
ManageEngine

Section 5: Rising stress in cybersecurity teams

The security challenge grows, as security professionals stated that by the end of 2024, 90% of LATAM companies will be facing GenAI-powered security attacks. This is driving 64% of security team members to admit their stress level is going up.

The top item driving their stress, at 54%, is the increasing number of security issues (attacks, breaches, patches, updates, false positives, etc.), followed by a lack of experienced team members (38%) likely compounded by emerging AI-enabled attacks. In third, at 38%, security professionals cite a lack of support from other teams within the business, often indicating willful neglect of security rules and policies, which makes their job even harder, as we recall employee are the second- and third-most pervasive threat vectors.

Q	What is causing your stress level to increase? Select all that apply.



Too few security team members 28%

Lack of experienced team members 38%

Lack of training 28%

Inadequate cybersecurity solutions 36%

Increasing number security issues (attacks, alerts, patches, etc.) 54%

Lack of support within the company (other employees, departments, etc.) 36%

Poor leadership (strategy, support, etc.) 19%

Other 1%

ManageEngine

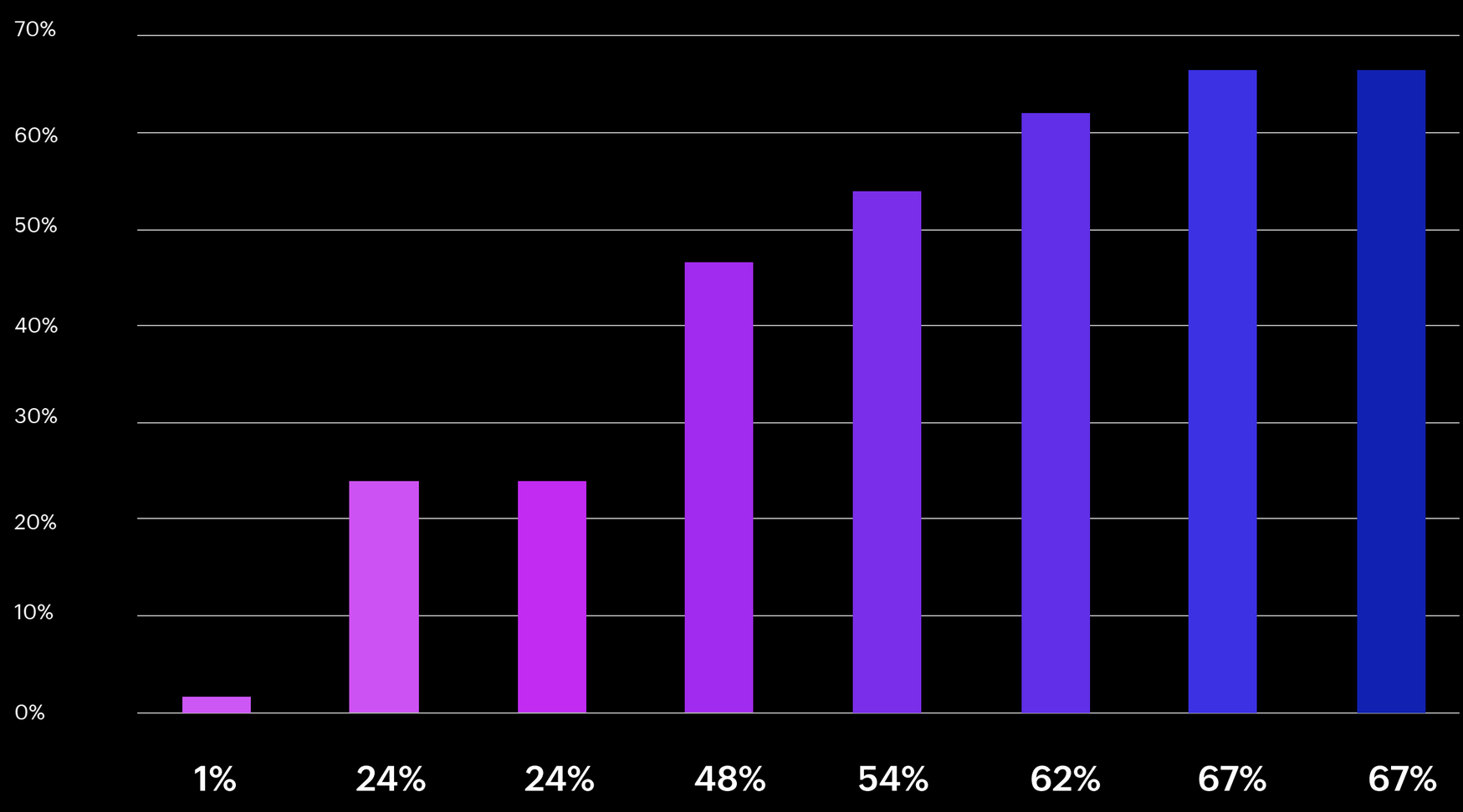
Section 6: Compliance

The need for cybersecurity insurance and meeting its requirements is driving a positive effect on companies, with 79% stating they are currently compliant with all data protection regulations. An additional 19% assert they will be compliant by the end of 2024.

Q To the best of your knowledge, is your company fully compliant with local and international data protection regulations?

Nearly all (99%) of insurance companies have specific requirements necessary to qualify for a cybersecurity policy, and “adherence to data protection regulations” was the top requirement according to respondents.

Q	Which requirements did your company have to meet in order to purchase cybersecurity insurance?



There were no specific requirements to purchase cybersecurity insurance: 1%

No previous breaches: 24%

No past insurance claims: 24%

Incident response plan: 48%

Regular employee training: 54%

Risk assessment and management: 62%

Security and access control policies: 67%

Adherence to data protection regulations: 67%

Conclusion

The findings of this regional survey shed light on the evolving cybersecurity landscape in Latin America. The study highlighted the challenges, opportunities, and potential patterns that business leaders must be attentive to in the region.

The increasing rate of AI-powered attacks signifies a significant shift in the nature and efficacy of cyberthreats. That said, it was interesting to find out there is a growing reliance on AI-enabled security solutions, with the vast majority of the respondents also recognizing the importance of using the technology in defending against future threats. Another key sentiment among respondents was their confidence in AI's ability to autonomously make cybersecurity decisions without human intervention. Nonetheless, they emphasize the necessity for independent oversight to guarantee the reliability and trustworthiness of AI-driven tools.

Employee behavior remains a prominent vulnerability in security defenses, emphasizing the need for comprehensive security training programs. While most companies report conducting employee training on security measures, there are concerns regarding the effectiveness and quality of these programs, particularly in the face of increasingly sophisticated AI-powered attacks.

Another crucial component that emerged while diving into understanding organizational resilience is cybersecurity insurance, with nearly all those surveyed claiming their companies possess such coverage. Although certain challenges persist in obtaining insurance, the correlation between insurance claims and adherence to data protection laws and regulations underscores the critical importance of navigating these challenges.

Looking ahead, companies must prioritize investments in AI-driven security solutions and robust training programs while addressing compliance requirements and supporting their security teams to effectively navigate the evolving threat landscape. By embracing these imperatives, businesses in Latin America can enhance their resilience and readiness to confront the challenges of cybersecurity in the digital age.

About ManageEngine

ManageEngine is a division of Zoho Corporation that offers comprehensive on-premises and cloud-based IT management solutions catering to a wide range of organizations, MSPs and MSSPs. Established and emerging enterprises—including 9 of every 10 Fortune 100 organizations—rely on ManageEngine's real-time IT management tools to ensure optimal performance of their IT infrastructure, including networks, servers, applications, endpoints and more. ManageEngine has offices worldwide, including in the United States, the United Arab Emirates, the Netherlands, India, Colombia, Mexico, Brazil, Singapore, Japan, China, Australia and the United Kingdom as well as 200+ global partners to help organizations tightly align their business and IT

ManageEngine

For more information, please visit the company site, follow the company blog and get connected on