SAPinsider

June 2024

DETAILED FINDINGS

From The Benchmark Report:

Cybersecurity Threats and Challenges to SAP Systems

By Robert Holland

Sponsored by

ONAPSIS rubrik splunk>

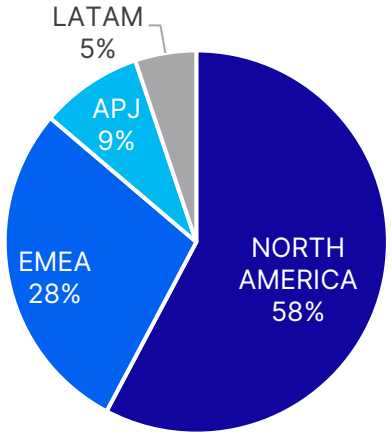
SAPinsider

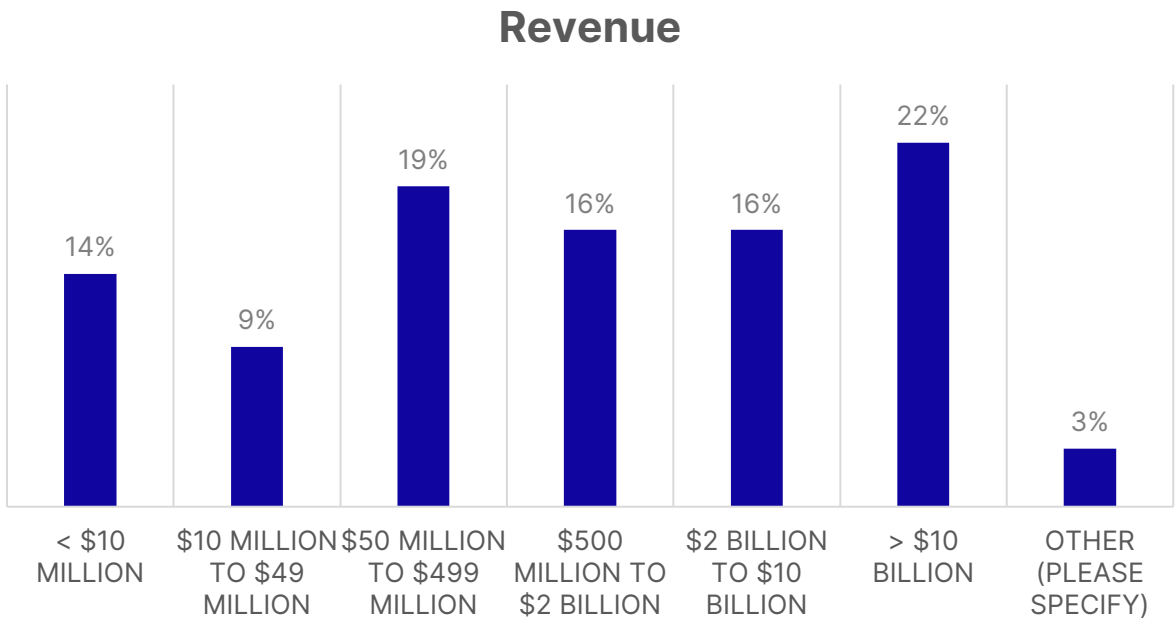
1

Between March and June 2024, SAPinsider surveyed 173 members of its community.

Survey participants from various geographical regions worldwide represented diverse organization sizes, contributing to a comprehensive dataset.

The primary objective of the survey was to gather insights from professionals who play a pivotal role in making cybersecurity decisions within their respective organizations.





© Copyright 2024 SAPinsider. All rights reserved.

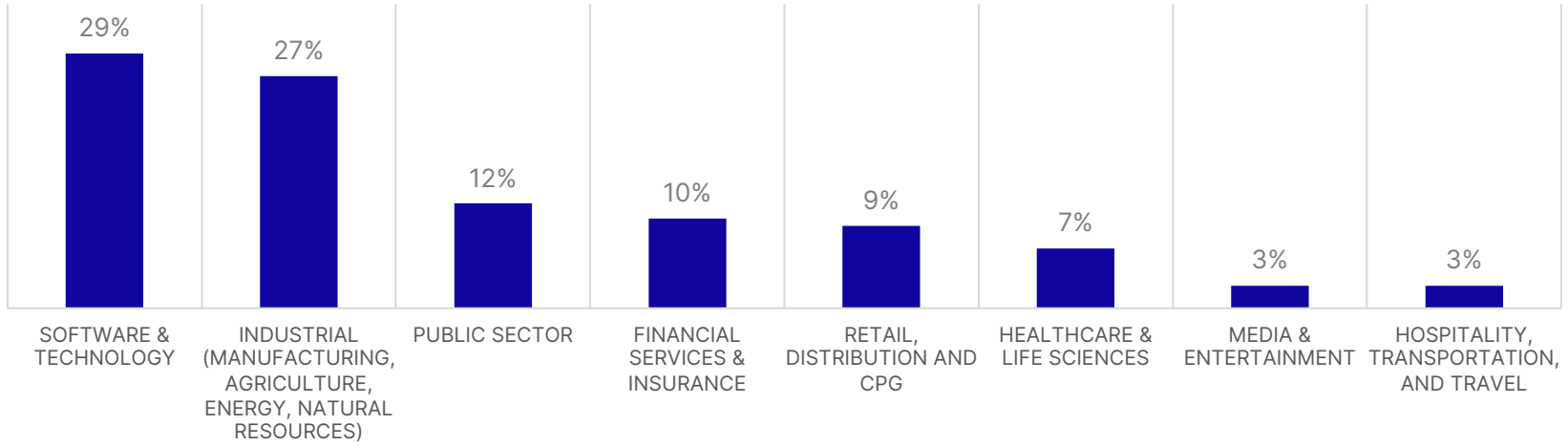
SAPinsider

2

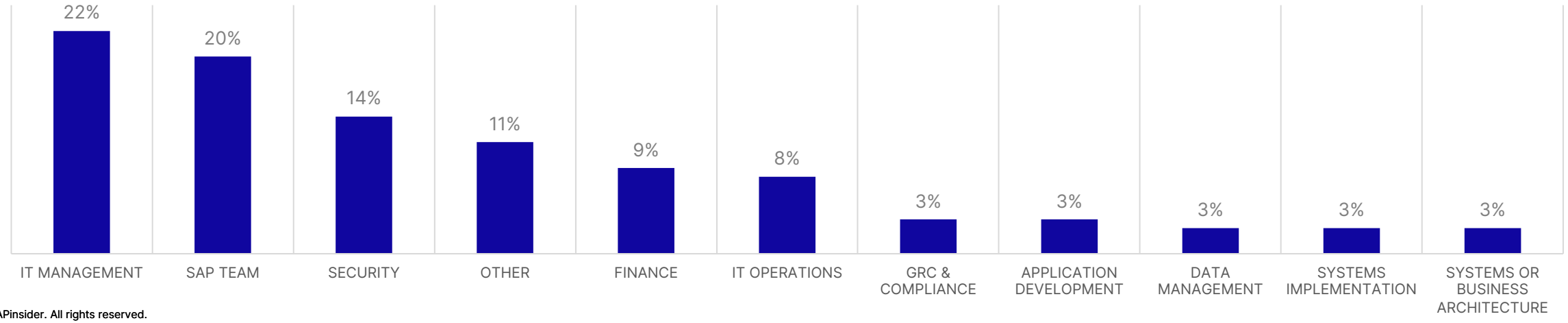
The participants were asked about cybersecurity, and the security strategies being implemented in their organizations.

They were also asked about their organizational roles and the market sector in which their organizations operated.

Market Sector



Role



© Copyright 2024 SAPinsider. All rights reserved.

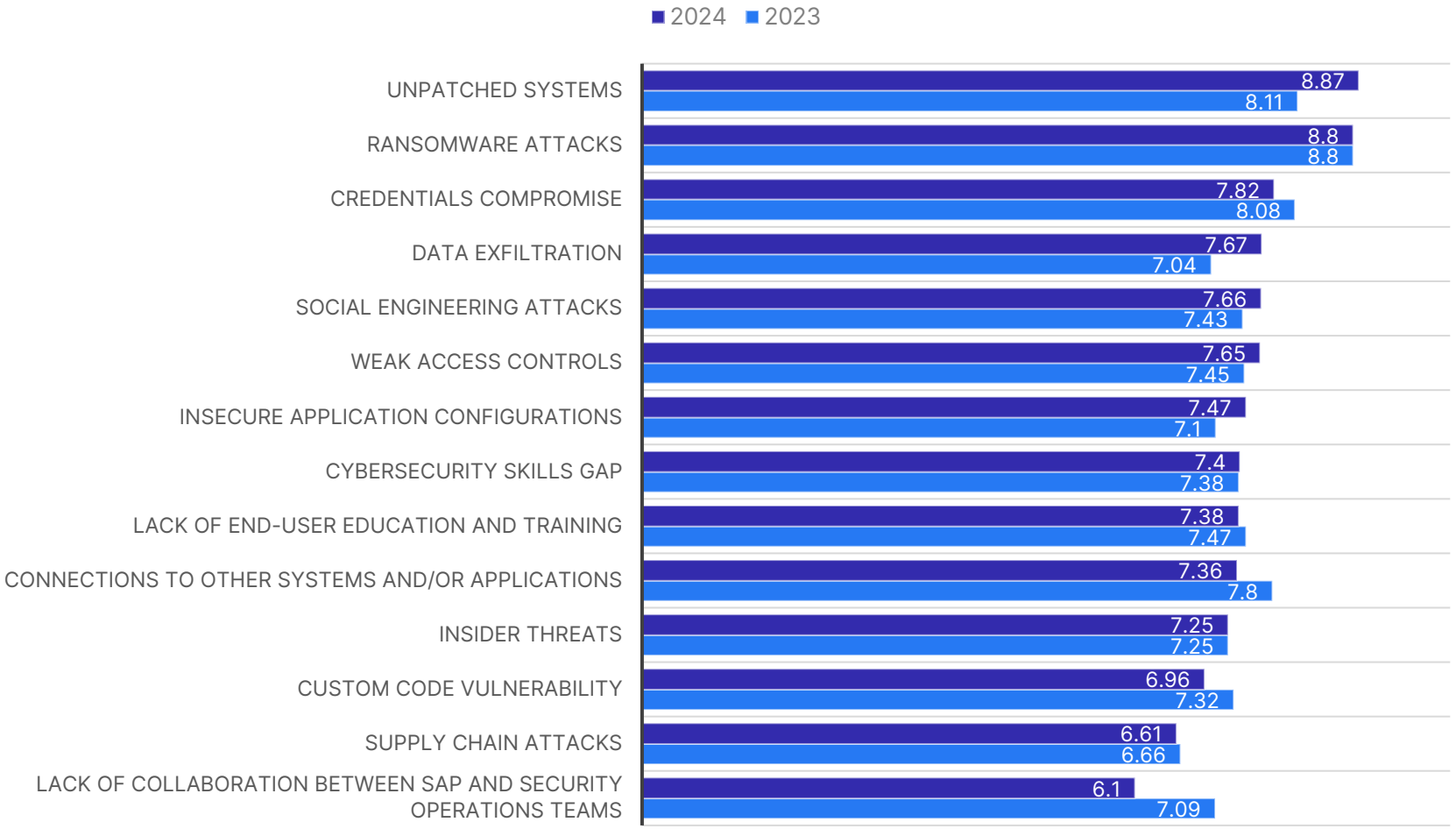
SAPinsider

3

For the last two years respondents considered ransomware attacks the biggest threat to their SAP systems, though unpatched systems was a close second. This year, unpatched systems is at the top of the list.

Organizations must develop and implement a comprehensive strategy for regular patching. Although maintaining this practice can be challenging in complex environments—especially when balancing the need for continuous system availability—regular patching is essential for safeguarding systems against vulnerabilities and threats.

Top Cybersecurity Threats to SAP Systems



© Copyright 2024 SAPinsider. All rights reserved.

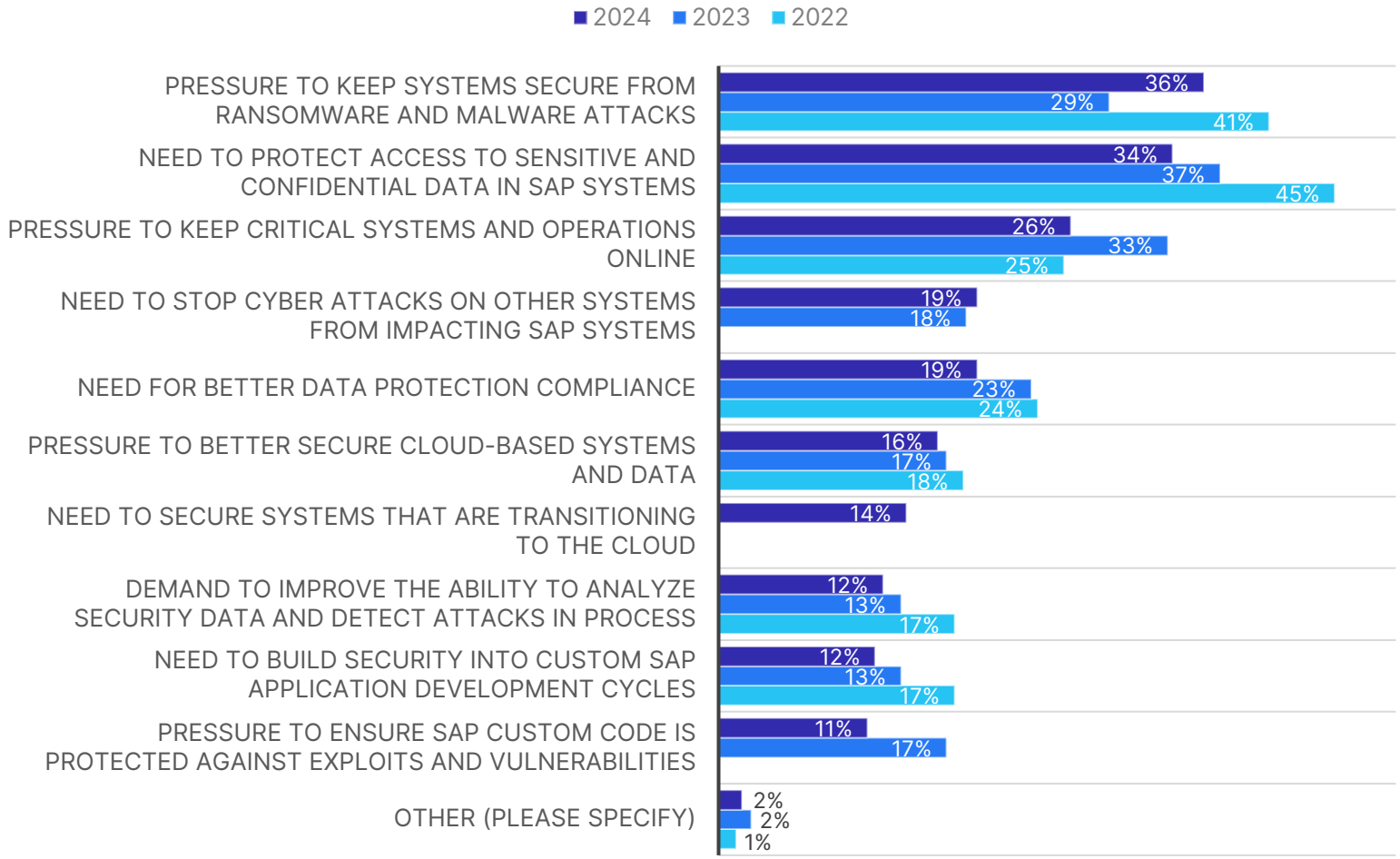
SAPinsider

4

The need to protect systems from ransomware and malware attacks was driven predominantly by smaller organizations that placed a lower emphasis on protecting the data in their SAP systems. However, organizations of all sizes want to keep systems and operations online.

Whether organizations focus on protecting systems from ransomware attacks or more generally protecting the data in those systems, it is vital that SAP systems are as secure as possible.

Factors Driving SAP Cybersecurity Strategy



© Copyright 2024 SAPinsider. All rights reserved.

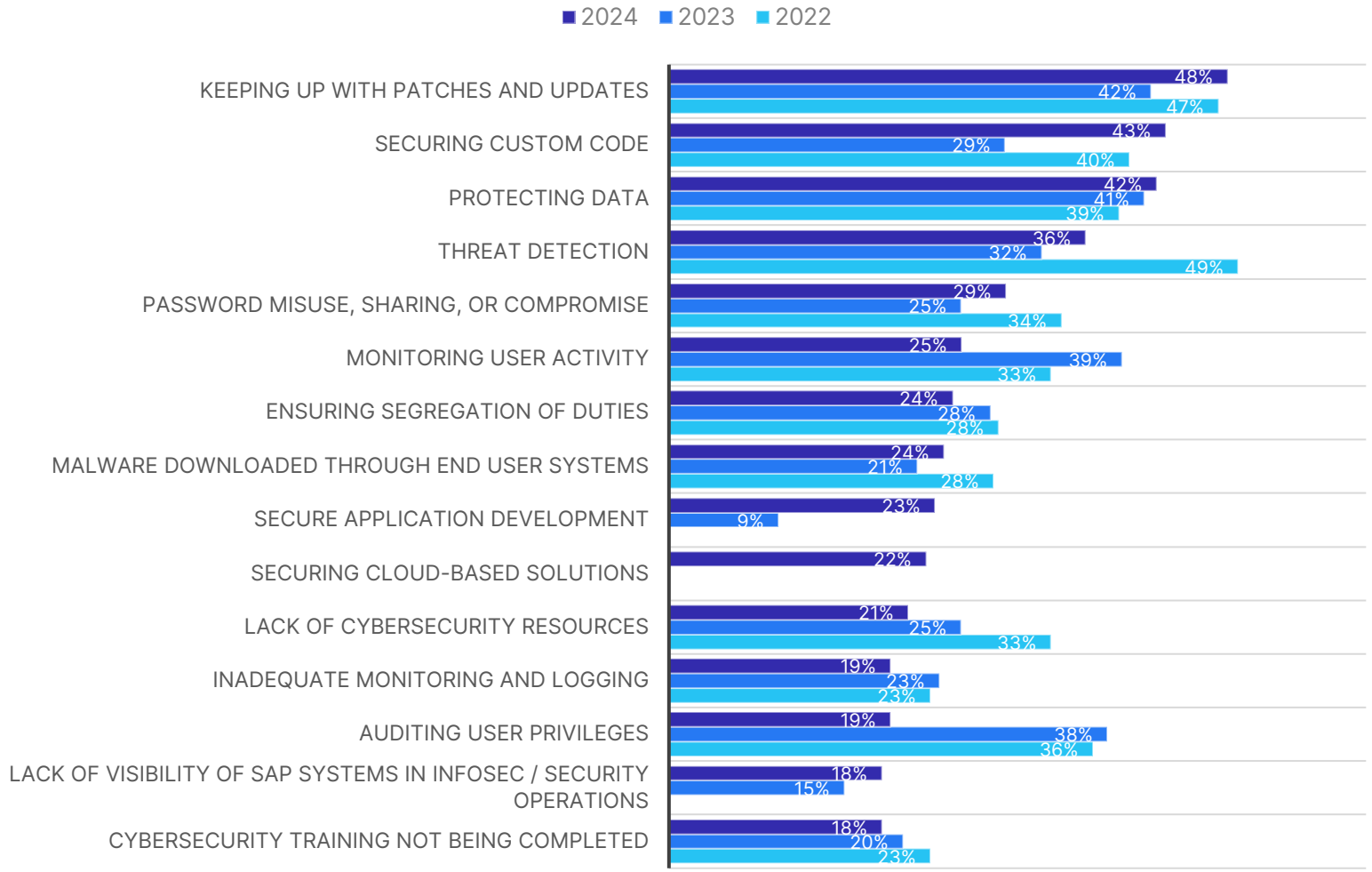
SAPinsider

5

With unpatched systems being one of the key threats to SAP systems, it is no surprise that keeping up with patches and updates is the biggest challenge faced by those securing their systems. Also seeing a jump in importance this year is the need to secure custom code.

Having a cybersecurity program brings together capabilities from across the organization to ensure that systems are protected. Every organization should expand the parameters of their security planning to ensure that that have an effective cybersecurity program.

Challenges Faced in Securing SAP Systems



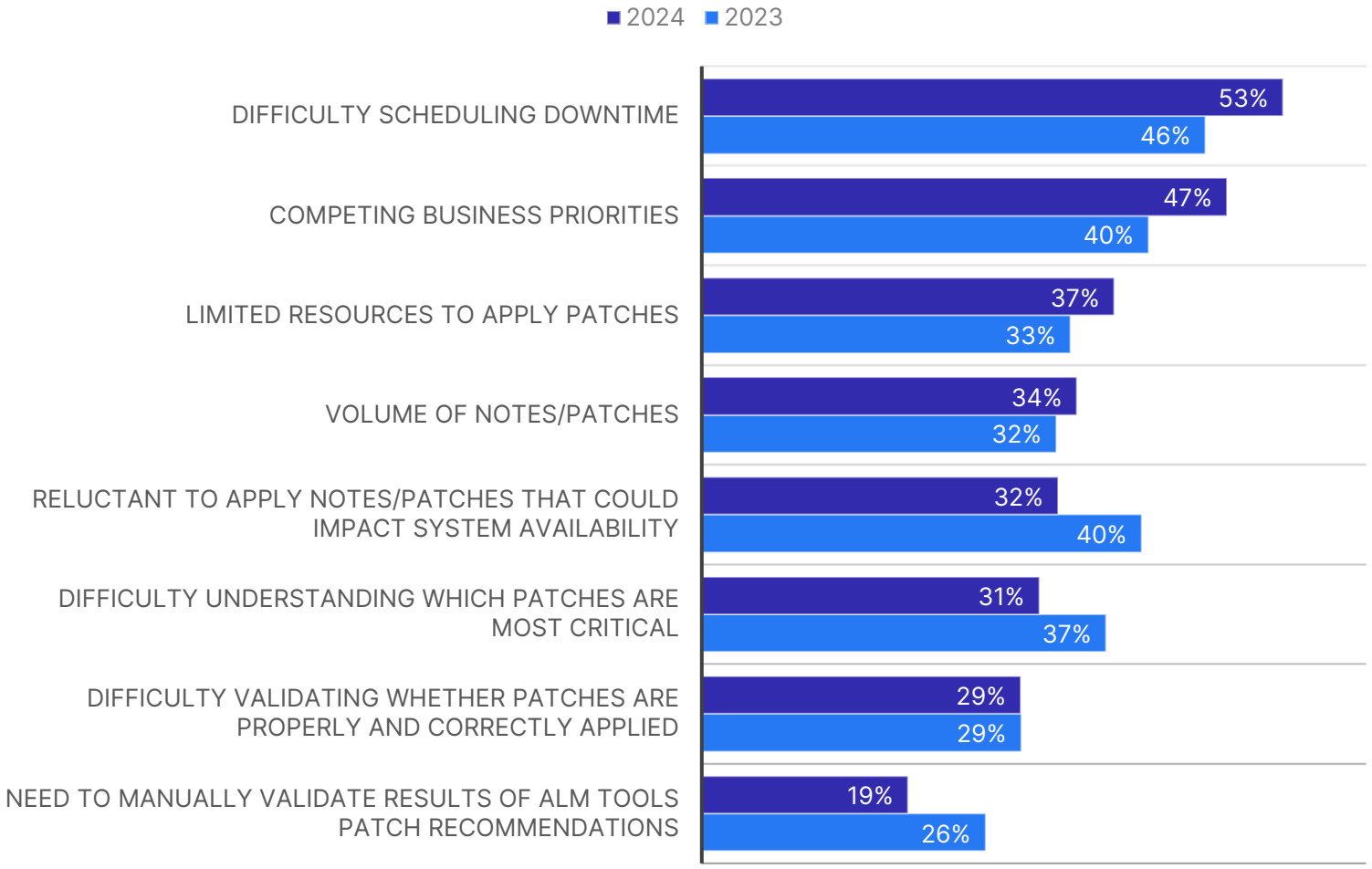
© Copyright 2024 SAPinsider. All rights reserved.

6

Of those that reported they had problems keeping up with patches and updates, the two most significant challenges related to scheduling. This is because competing business priorities are just as much a scheduling issue as regularly scheduled downtime.

Organizations need to flag patching difficulties to IT and security leadership so that these issues can be addressed. If they are not, vulnerabilities have the potential to be exploited.

Issues Leading to Patching Backlogs



© Copyright 2024 SAPinsider. All rights reserved.

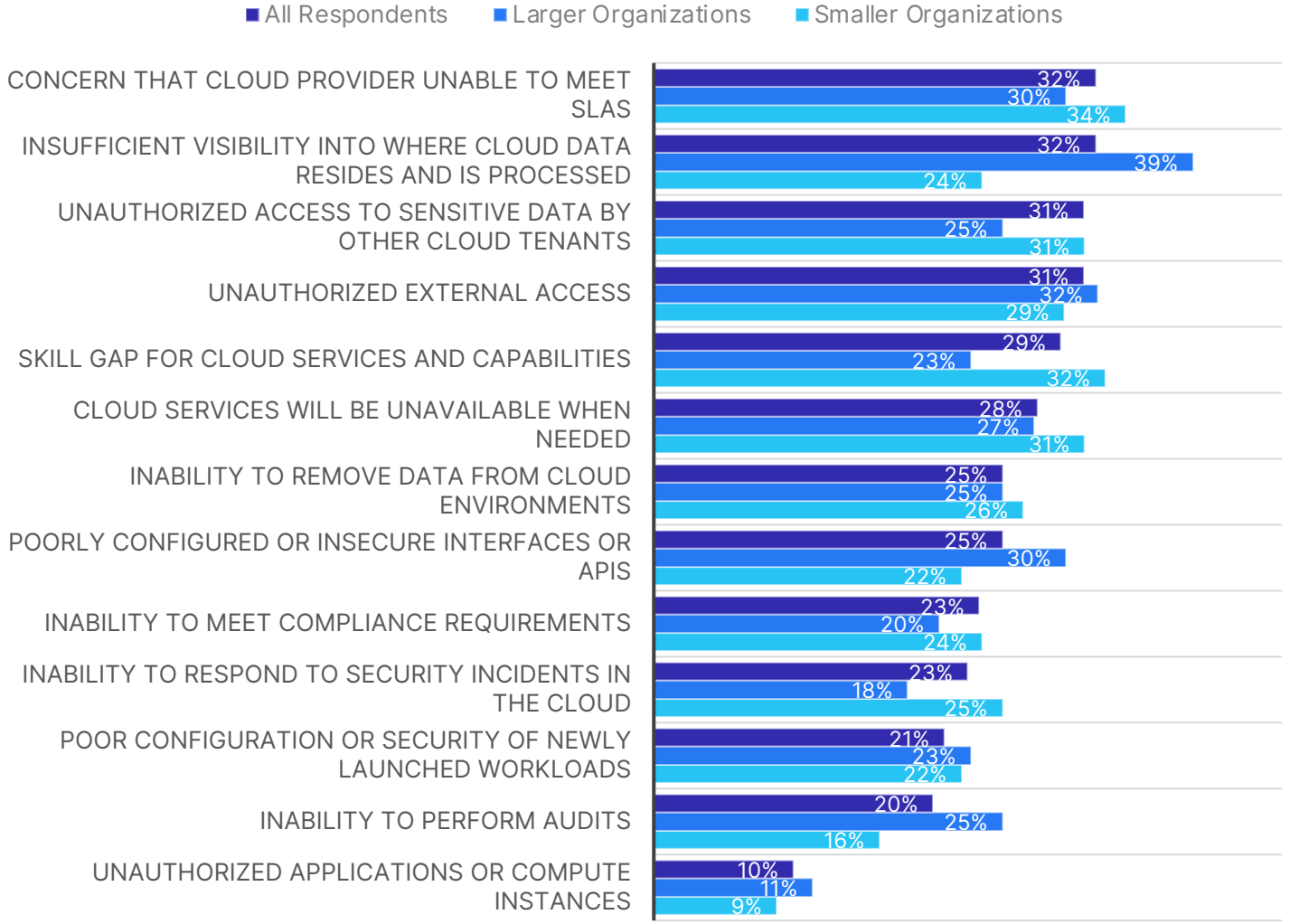
SAPinsider

7

While being unable to meet SLAs was the biggest potential cloud concern for respondents, the next two most important concerns were related to data. Data residency is a major topic for many organizations as is the potential access to data by other tenants in cloud system.

Working closely with cloud providers is an important way to remediate these concerns. This will not only better educate internal teams but will ensure that there is a better understanding of the cloud environments the organization is using.

Concerns With Using Cloud-Based Solutions



© Copyright 2024 SAPinsider. All rights reserved.

DART
MODEL FRAMEWORK

Strategy and Needs for Cybersecurity

DRIVERS

- Pressure to keep systems secure from ransomware and malware attacks (36%)
- Need to protect access to sensitive and confidential data in SAP systems (34%)
- Pressure to keep critical systems and operations online (26%)v

ACTIONS

- Training end-users to protect credentials from social engineering and other attacks (44%)
- Regularly implementing patches and updates (43%)
- Conducting regular audits and security assessments (36%)

REQUIREMENTS

- Real-time monitoring and logging capabilities (81%)
- Fully patched and updated systems (79%)
- Regular training and education programs for all employees (79%)
- Safe password practices (78%)
- Cybersecurity protection for cloud-based solutions (77%)
- Cybersecurity tools that provide consistent protection across cloud and on-premise environments (77%)

TECHNOLOGIES

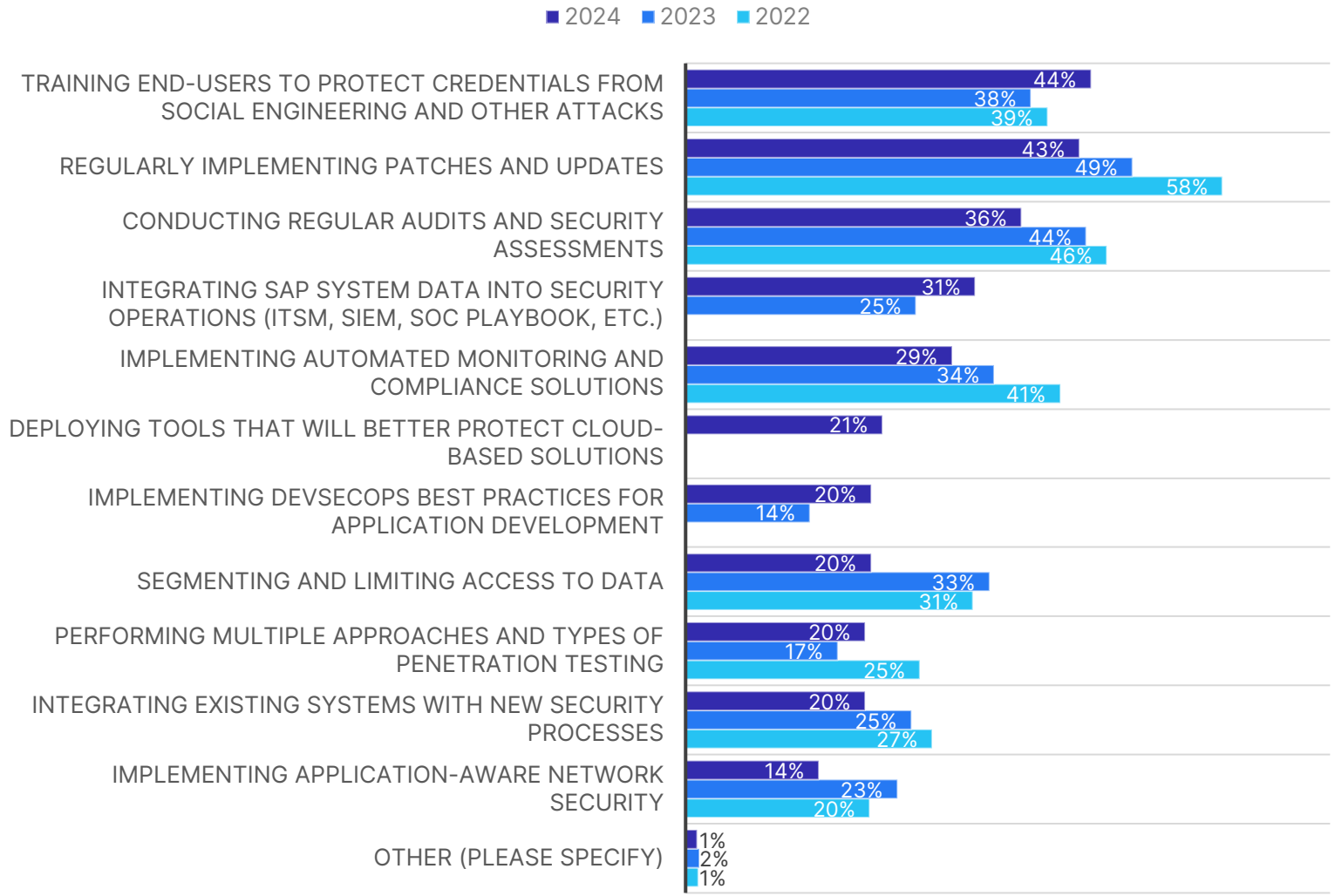
- Encrypted/Secure Connectivity (61%)
- Continuous Monitoring (59%)
- Data Encryption (57%)
- Vulnerability Management (49%)
- Security-Driven Networking (43%)
- Code Vulnerability Analysis (34%)
- Dynamic Authorization and Least Privilege (34%)
- Application-Aware Network Security (32%)
- Threat Intelligence Feeds (32%)
- Automated Testing for Compliance (32%)
- Embedded Hardware Authentication (30%)
- Automated Code Vulnerability Testing Tools (29%)
- Zero-Trust Models (25%)
- UI Masking (25%)
- Behavioral Analytics (21%)

8

In response to being concerned about ransomware and malware attacks impacting SAP systems, respondents are educating users. There is also an emphasis on patching regularly, although this has dropped slightly in importance from last year.

Focusing on user training can help shut down some of the most likely routes for threat actors — those using the systems. The more users know about ways that attacks can happen, the less likely they are to be socially engineered.

Actions Taken to Support Cybersecurity Strategies



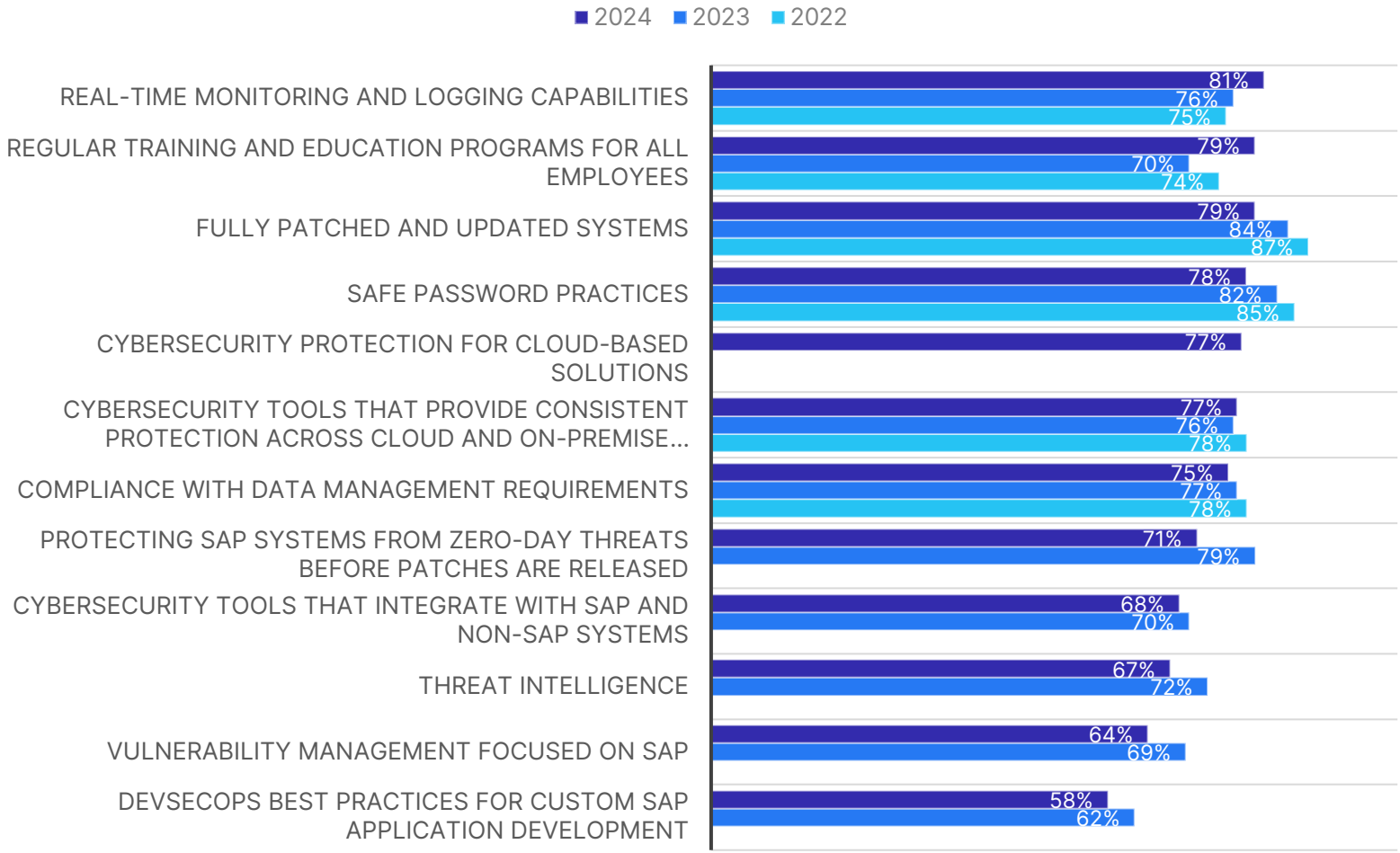
© Copyright 2024 SAPinsider. All rights reserved.

9

With a concern about ransomware attacks and users being exploited, real-time monitoring and logging can help detect unusual behavior in systems. This allows those tasked with securing systems to react to the early phases of an attack.

Regular training helps keep users up-to-date about phishing attacks and changing attack vectors, although users can be deterred from completing cybersecurity training when it is repetitive.

Requirements for Cybersecurity Strategies



© Copyright 2024 SAPinsider. All rights reserved.

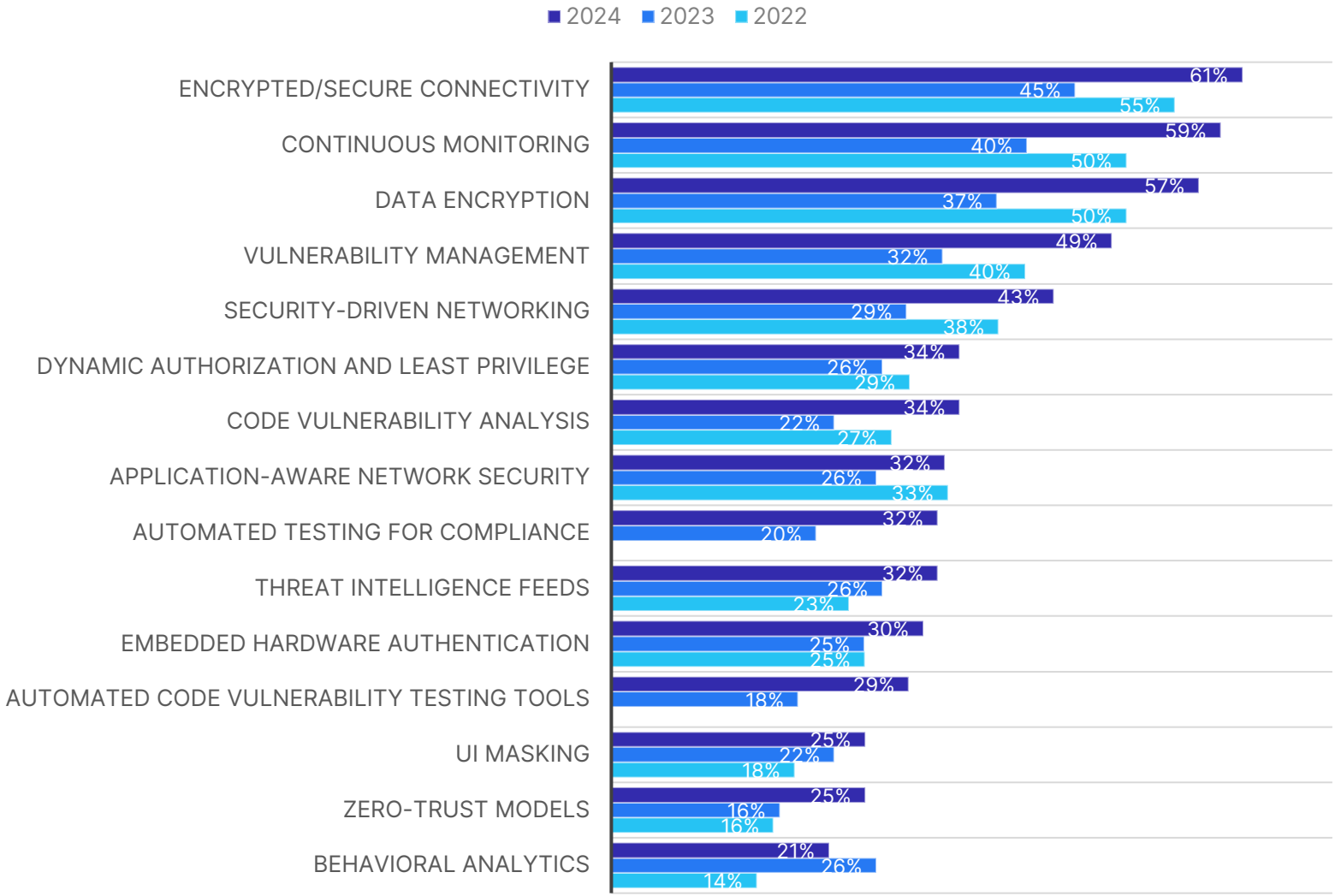
SAPinsider

10

Secure connectivity, continuous monitoring, and data encryption are the three most used technologies today.

Secure connectivity and data encryption help organizations make sure that data is secure when it is stored and during transit. Continuous monitoring is intended to reveal any unusual activity in systems. Combined, these three technologies provide a starting point for any cybersecurity strategy.

Technologies in Use Supporting Cybersecurity



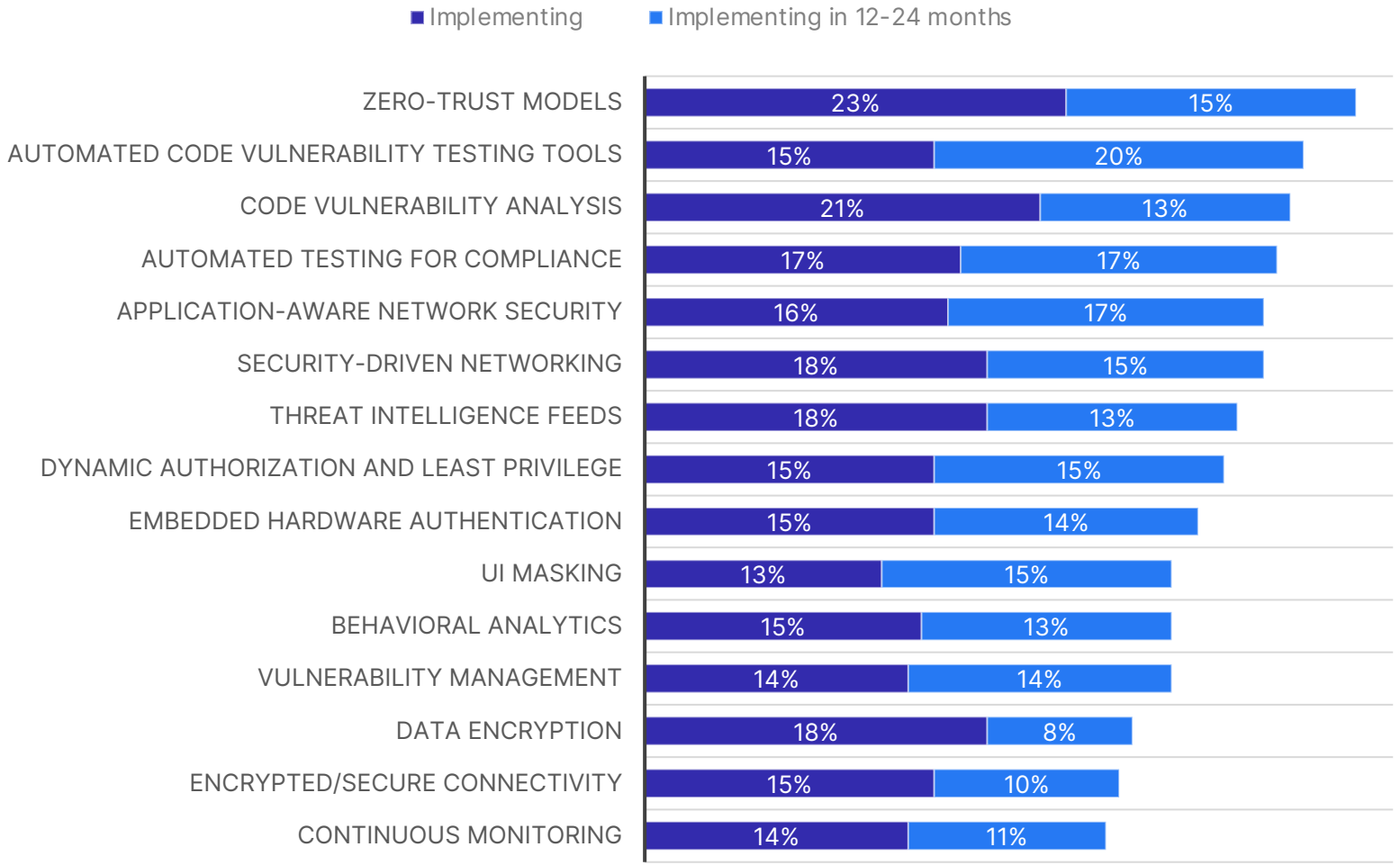
© Copyright 2024 SAPinsider. All rights reserved.

SAPinsider

11

Over the next two years, one of the biggest investment areas is reducing the vulnerabilities in custom code. Nearly all SAP environments have some customizations, while many have tens of thousands of lines of customized code. Since much of this may be infrequently used or developed by those no longer with the organization, having tools that help analyze and remediate potential vulnerabilities is crucial. This is especially true for organizations that are in the process of moving to SAP S/4HANA.

Technologies Being Implemented for Cybersecurity

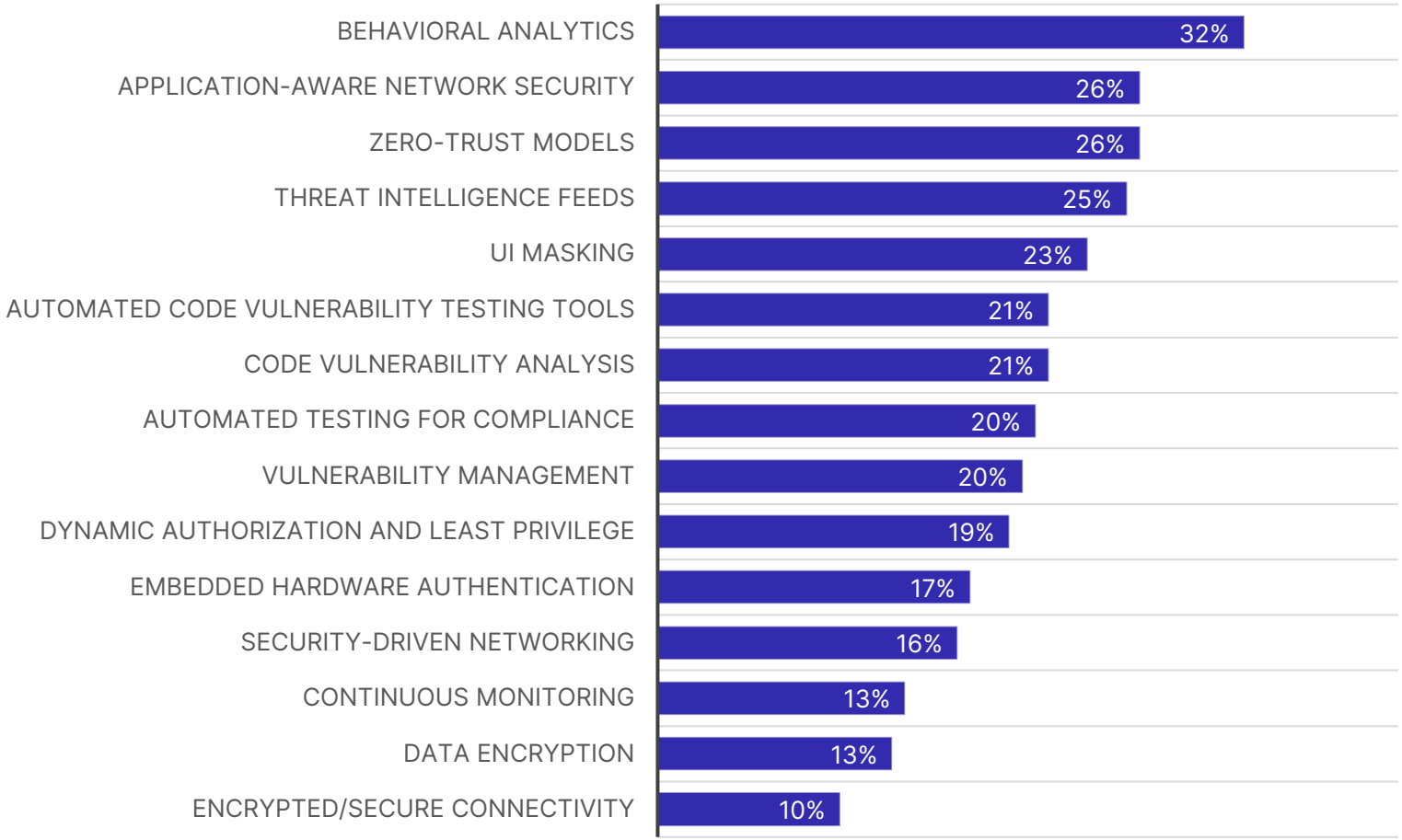


© Copyright 2024 SAPinsider. All rights reserved.

12

Behavioral analytics provides insight into the actions taken by users in systems. From a cybersecurity standpoint, this is helpful as it can quickly reveal when unusual activities are being performed by a specific account. Because any sort of account compromise would result in this type of unusual activity, having behavioral analysis makes it possible to detect breaches much earlier. This can then prevent some of the most significant damage from being done.

Technologies Being Evaluated for Cybersecurity

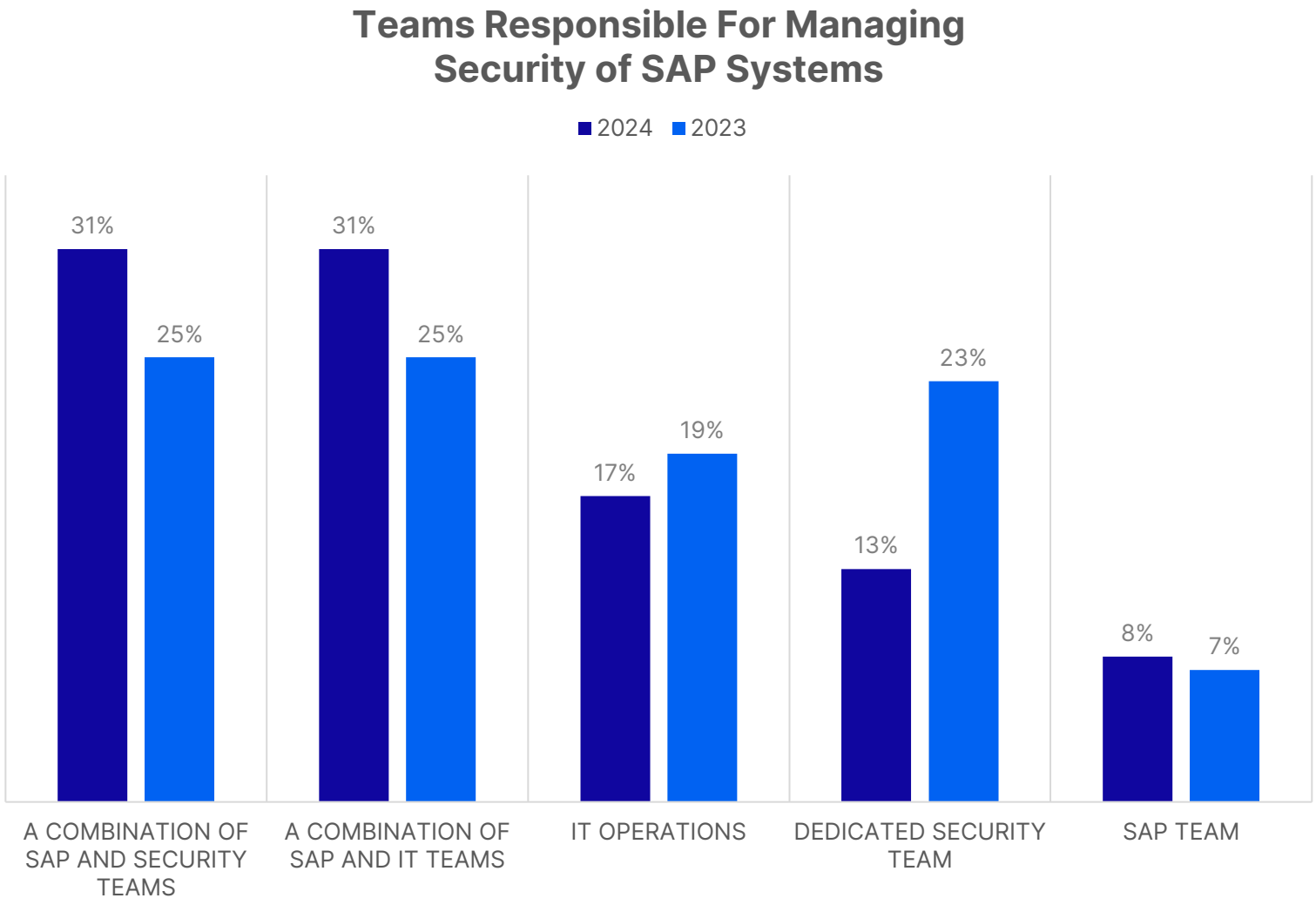


© Copyright 2024 SAPinsider. All rights reserved.

SAPinsider

13

Historically, the security of SAP systems was largely invisible to dedicated security teams. This is because it was normally managed entirely by the SAP team. This has shifted over the last few years. This year, nearly two-thirds of respondents report their SAP teams either working in combination with their security team or IT team to ensure that SAP systems are protected. This can ensure that SAP systems, and particularly those that they are integrated with, are much better protected.



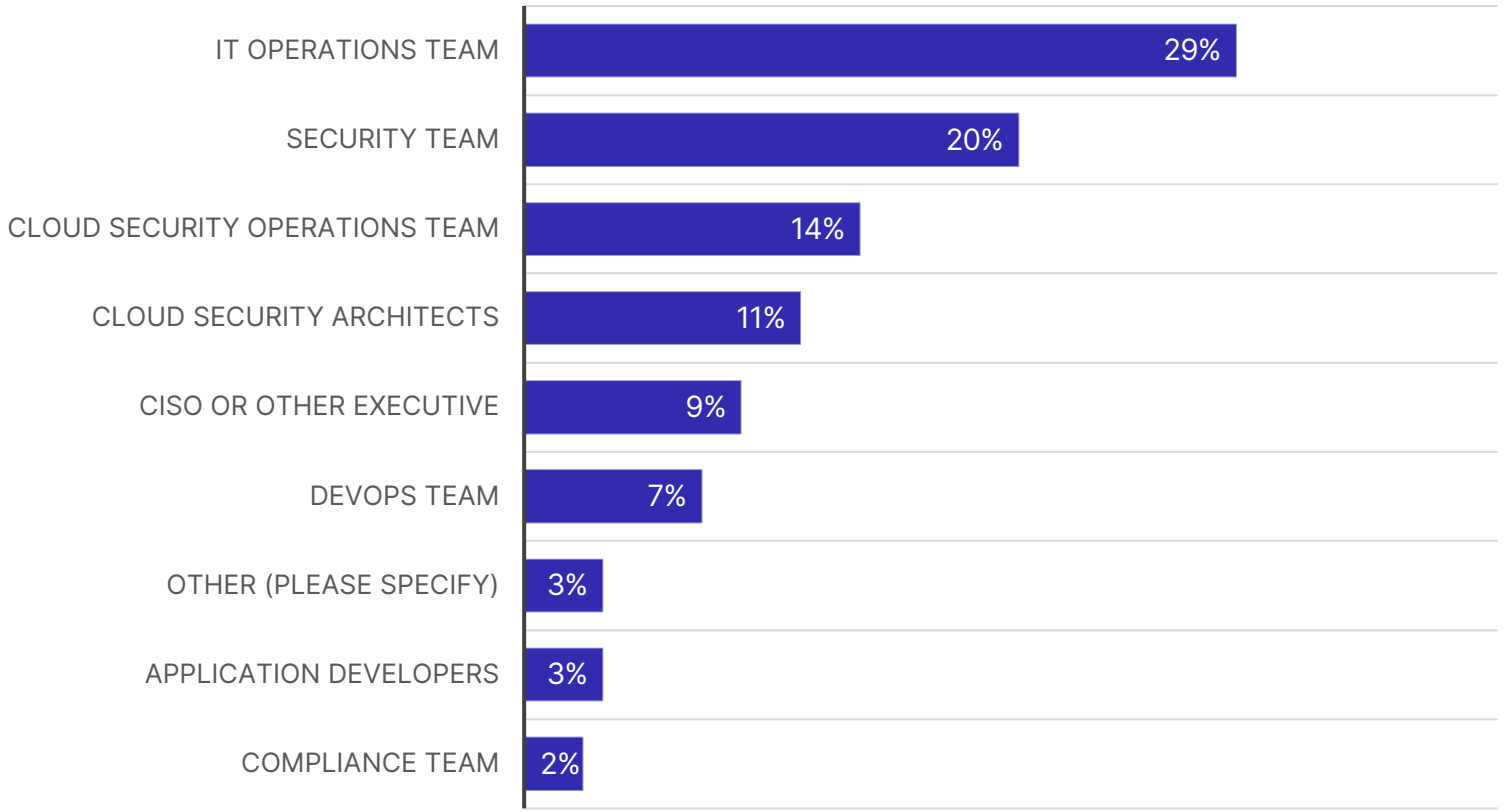
© Copyright 2024 SAPinsider. All rights reserved.

14

Moving to the cloud can be a challenge for many organizations as they may face a skills gap when it comes to cloud technologies. When security is not being managed by dedicated teams, this skill gap can sometimes be multiplied as a limited pool of resources can be overstretched.

Larger organizations were more likely to rely on a dedicated Cloud Security Operations team, but smaller organizations may not have the resources to staff a dedicated group, which is why they rely primarily on IT operations.

Responsible for Managing Security of Solutions Moving to the Cloud



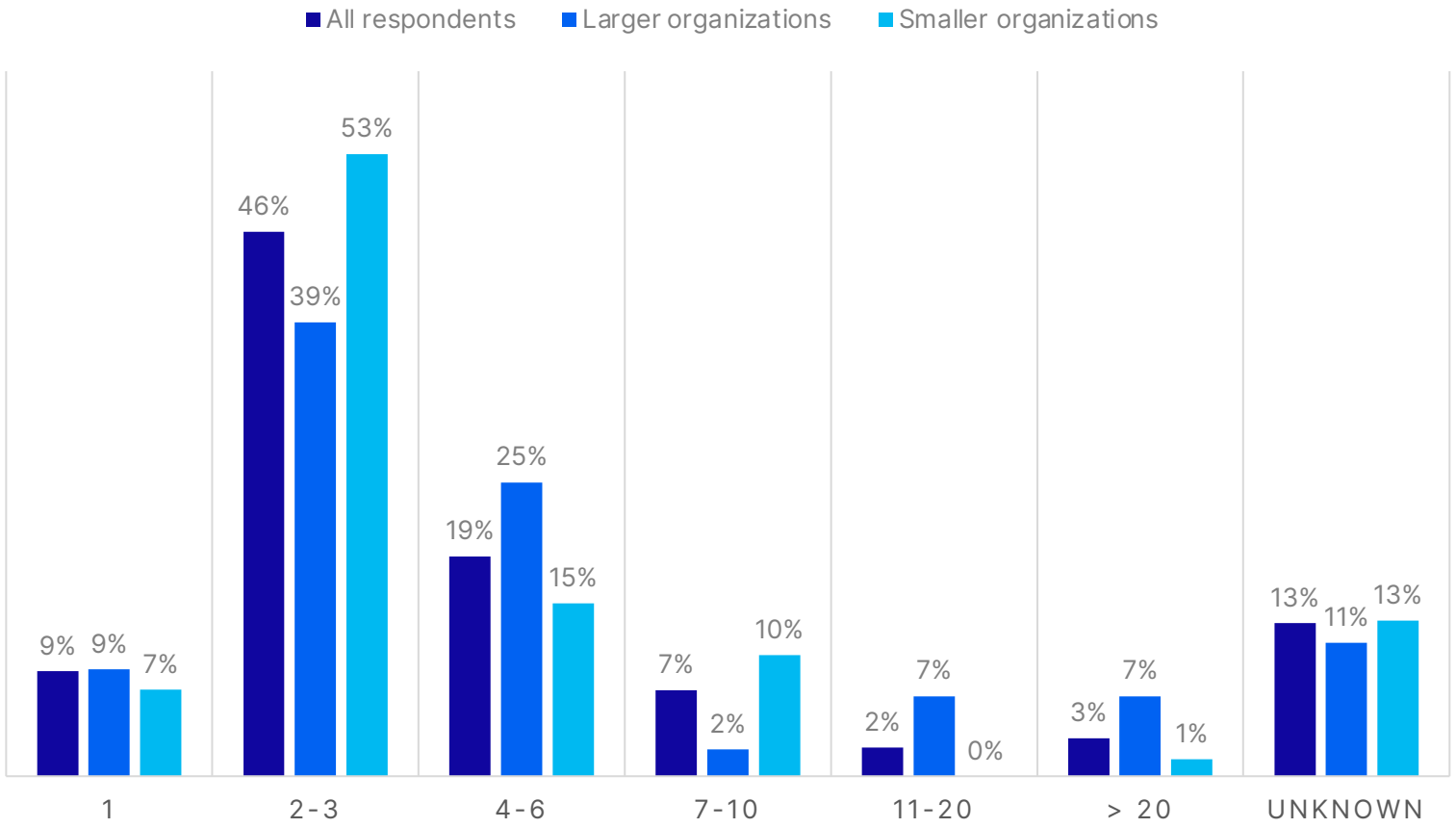
© Copyright 2024 SAPinsider. All rights reserved.

15

Most organizations rely on multiple cloud providers, and this trend is even more pronounced in larger organizations. For example, 41% of larger organizations report using at least four cloud providers.

The more cloud providers in use the more complex the security environment and the greater the potential attack surface. This means, it is vital for security teams to be well trained and knowledgeable about current attack trends.

Cloud Providers Used for Enterprise Workloads, Communications, Security, Integration, and Other Operations

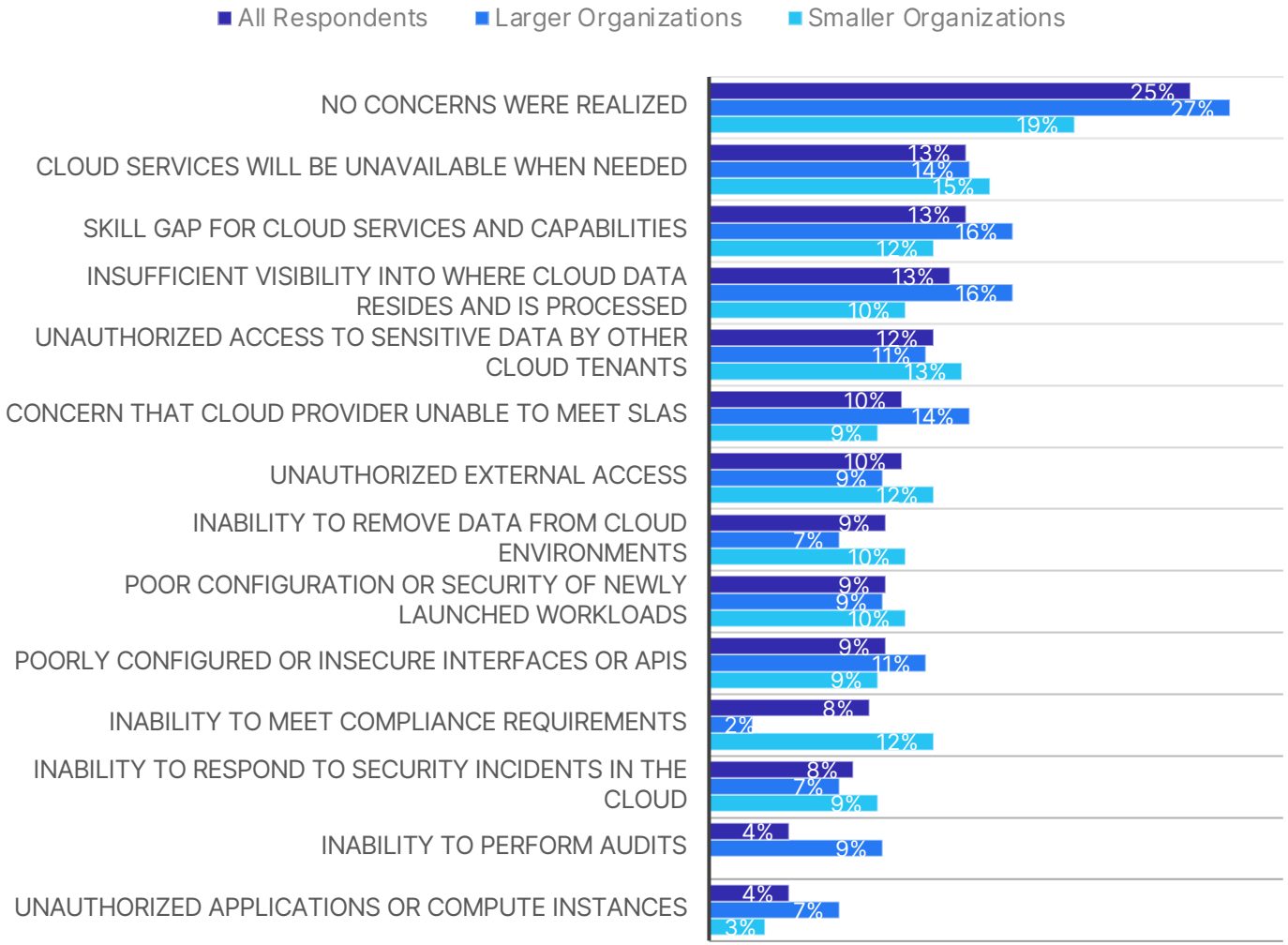


© Copyright 2024 SAPinsider. All rights reserved.

16

We previously examined the concerns that respondents had about using cloud environments, but the reality is that many of these concerns were not realized. The skill gap for cloud services and capabilities was listed fifth in potential threats, and cloud services being unavailable when needed was listed sixth. Yet, these ended up being the mostly likely concerns to be realized. This is where education and training are paramount for both staff and leadership so that organizations can dedicate resources in the most productive areas.

Cloud Concerns Realized in the Past Year

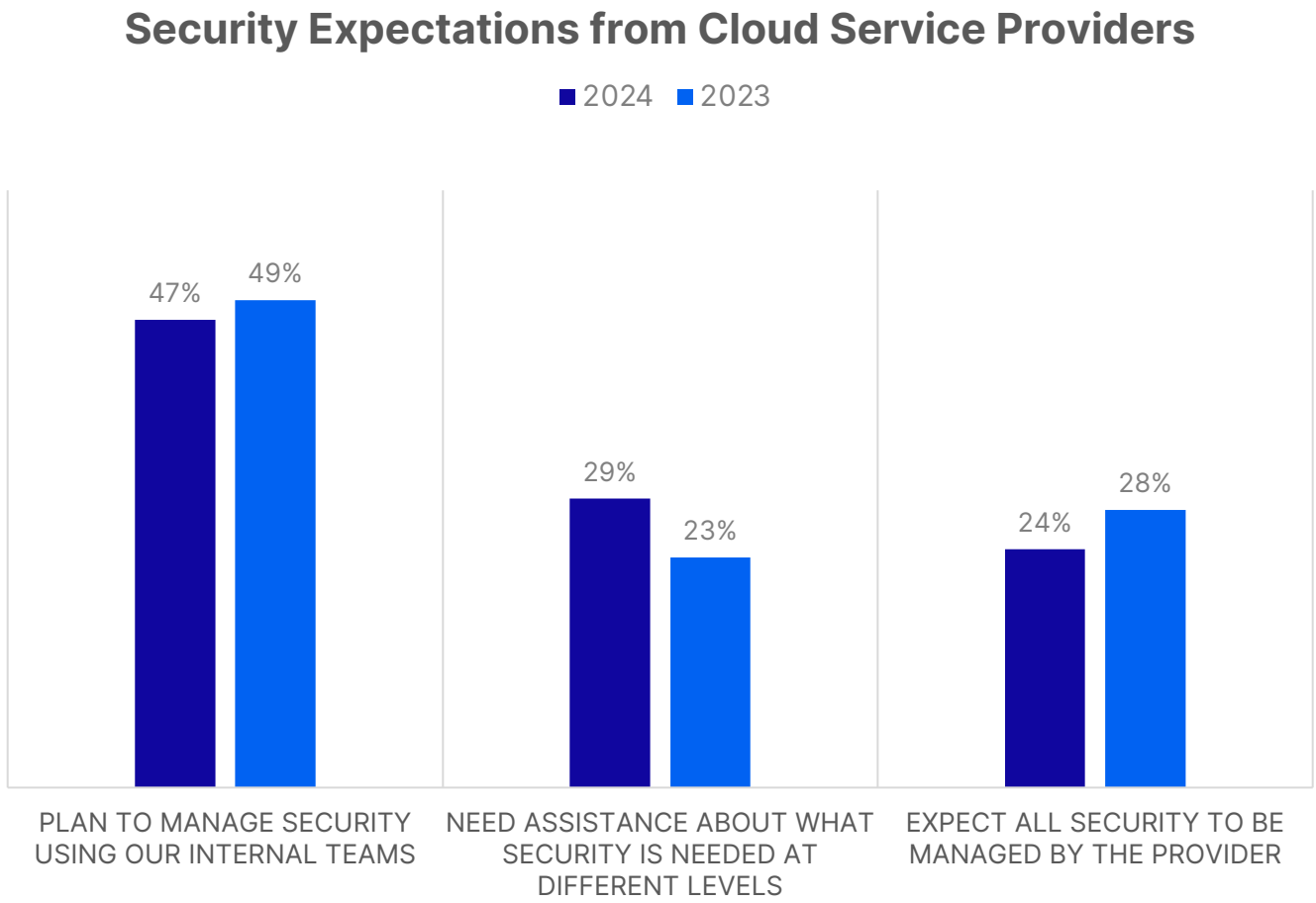


© Copyright 2024 SAPinsider. All rights reserved.

17

There were no major changes in the security expectations for cloud service providers between 2023 and 2024, although an increased number of respondents reported that they needed assistance about what security is needed at different levels.

This is another area where education and training can help make a significant difference with internal teams. Having experienced teams will reduce the confusion when it comes to what security will be managed by providers and how that management needs to be done.



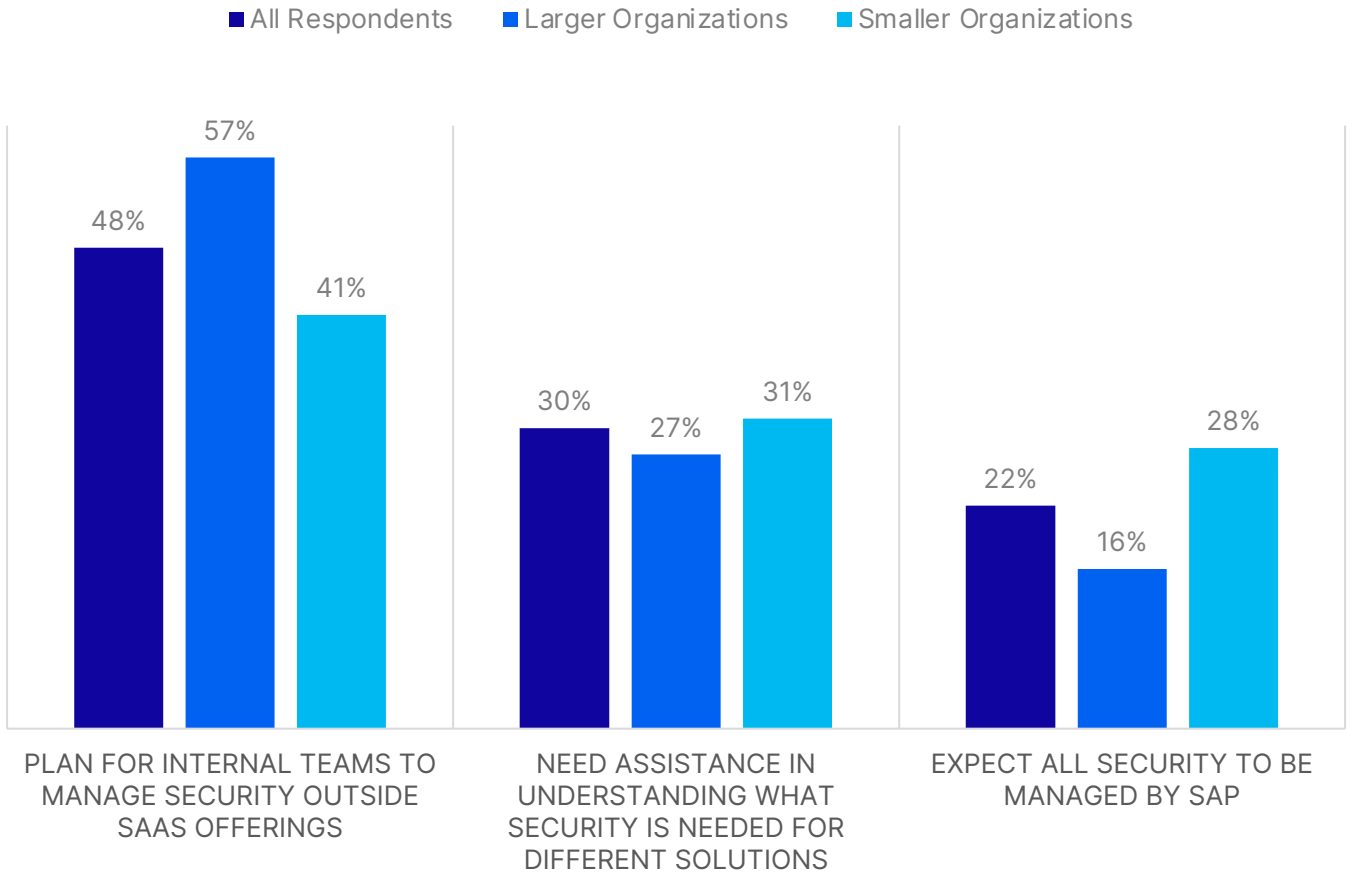
© Copyright 2024 SAPinsider. All rights reserved.

18

When it comes to SAP offerings, there is slightly more confusion about who is responsible for security than for the cloud in general. This is likely because information on cloud security is more generally available while securing cloud-based SAP offerings may require more specialized knowledge.

Organizations need to dedicate resources to working with SAP to understand who is responsible for different security aspects so that they can ensure that their systems are effectively protected.

Security Expectations for SAP Cloud Offerings and Solutions



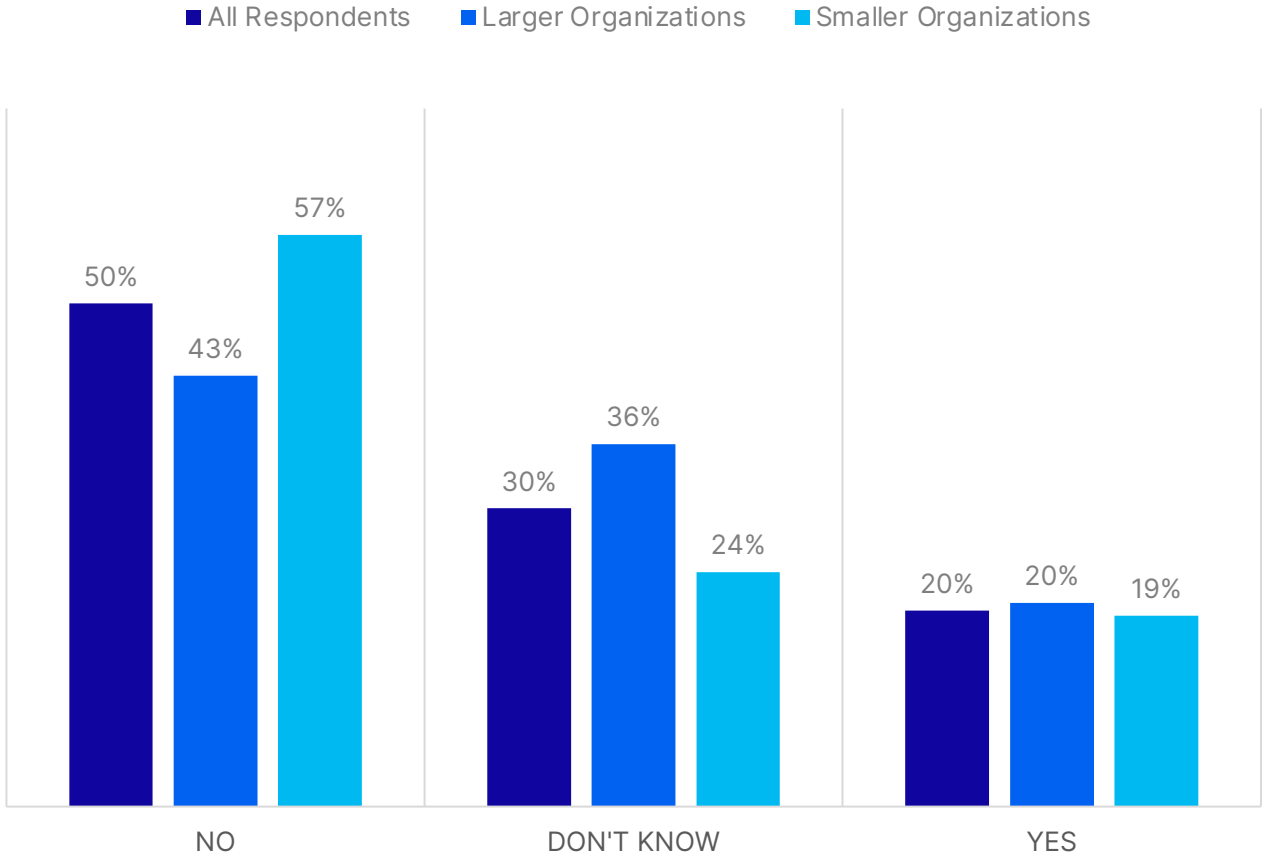
© Copyright 2024 SAPinsider. All rights reserved.

SAPinsider

19

There was no significant difference in the likelihood of an attack impacting a cloud provider between organizations of different sizes, although respondents from larger organizations were more likely to have no information. This is because of the size and complexity of the IT teams and the fact that those in the SAP team may be unaware of activities impacting systems outside of their purview.

Has Your Organization Been Subject to an Attack on a Cloud Provider in the Past Year



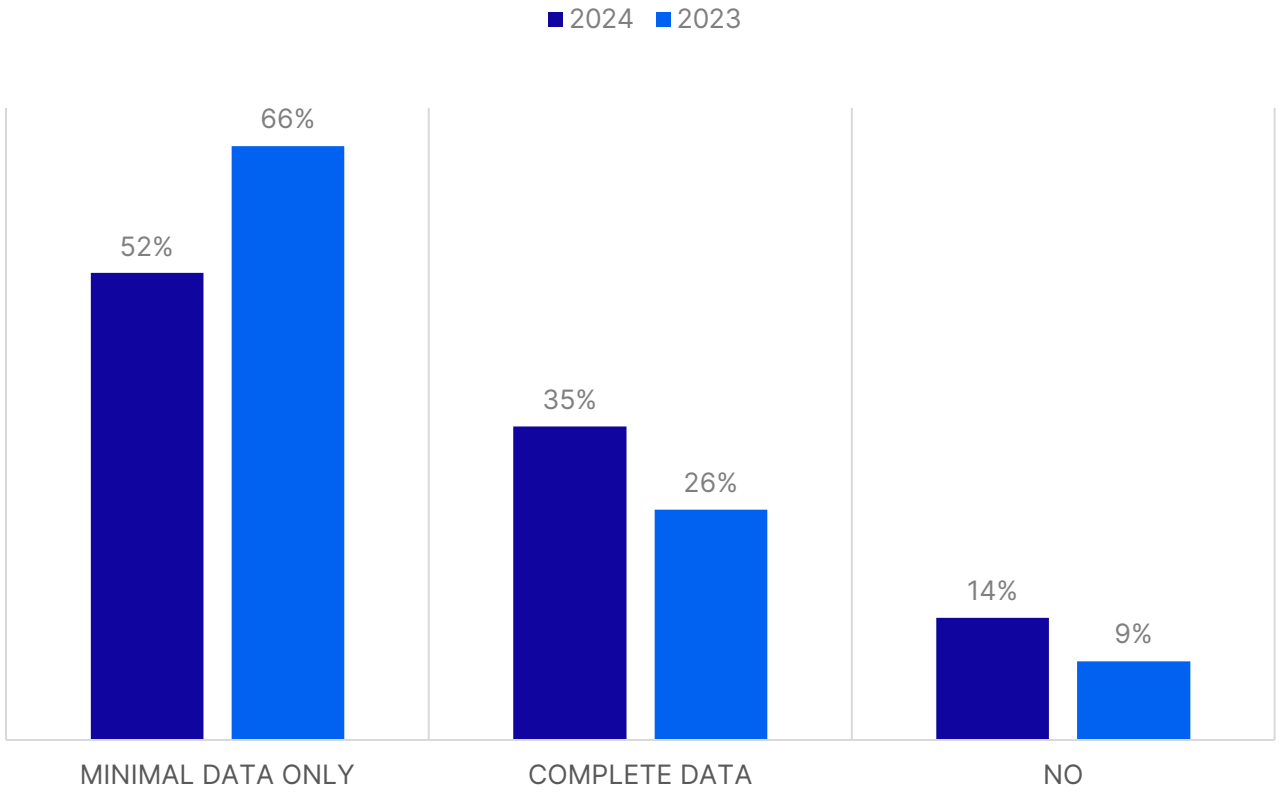
© Copyright 2024 SAPinsider. All rights reserved.

SAPinsider

20

One of the ways of determining whether a breach has occurred is to analyze system activity, particularly user behavior. If a user starts running transactions that they have never used before, it may indicate that the account has been compromised. However, while 35% of respondents reported that their organization was logging complete data, and increase of 10% from last year, more than half are only logging minimal user activity data.

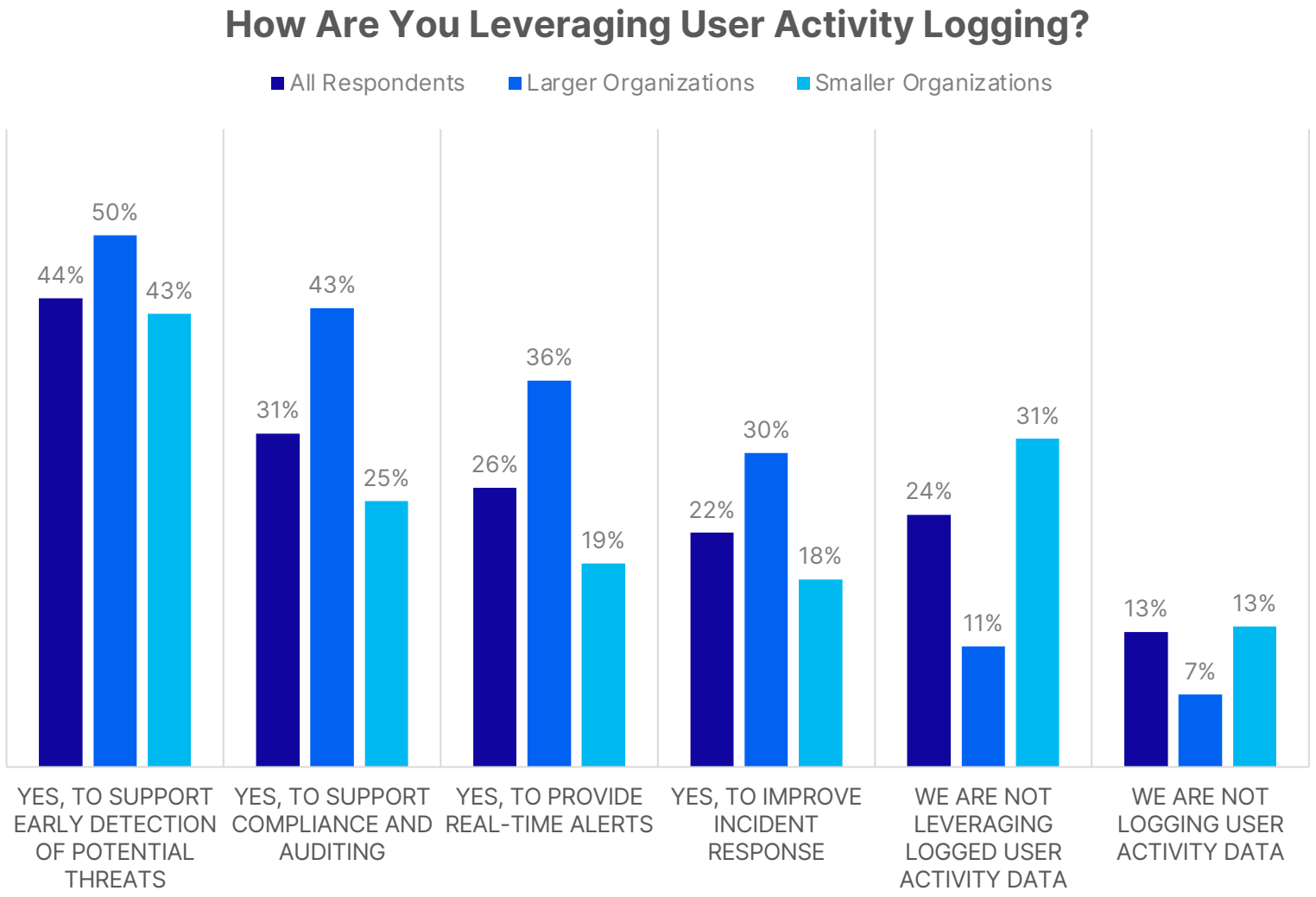
Are You Currently Logging User Activity for SAP Systems?



© Copyright 2024 SAPinsider. All rights reserved.

21

For organizations logging user activity, the primary purpose is often the early detection of potential threats. Other key scenarios include supporting audit and compliance, providing real-time alerts, and enhancing incident response. However, a concerning finding from the survey is that a quarter of respondents, particularly from smaller organizations, admitted to logging user activity data but not utilizing it effectively.



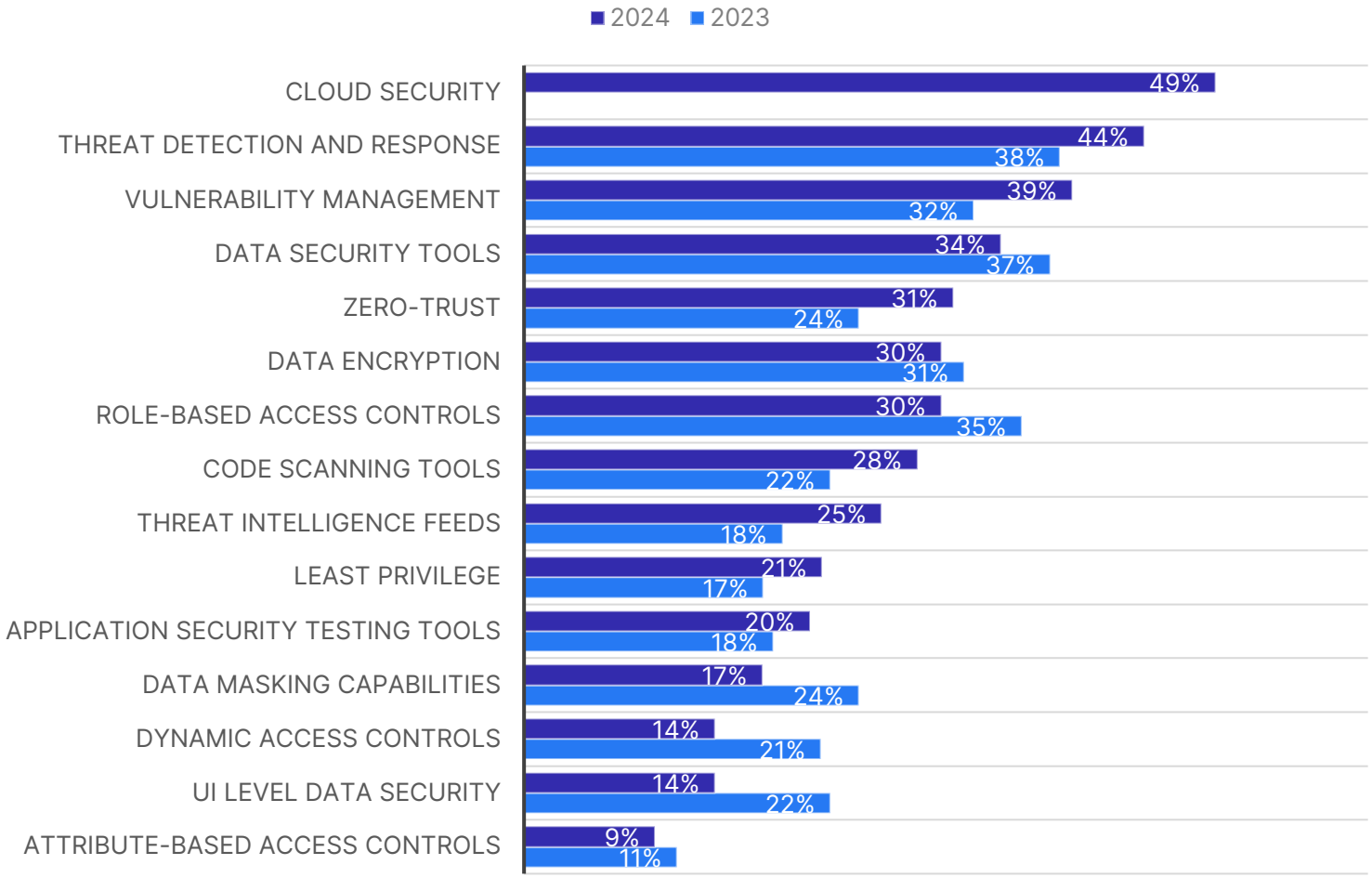
© Copyright 2024 SAPinsider. All rights reserved.

22

Cloud security is the most likely area to receive investment from respondent organizations, though there is increased investment for threat detection and response and vulnerability management when compared to last year. With an accelerating move to the cloud, this is unsurprising.

Organizations need to plan and prioritize their security budgets to ensure that new investments are being secured. This is particularly true for the cloud.

Planned Areas for Security Investment



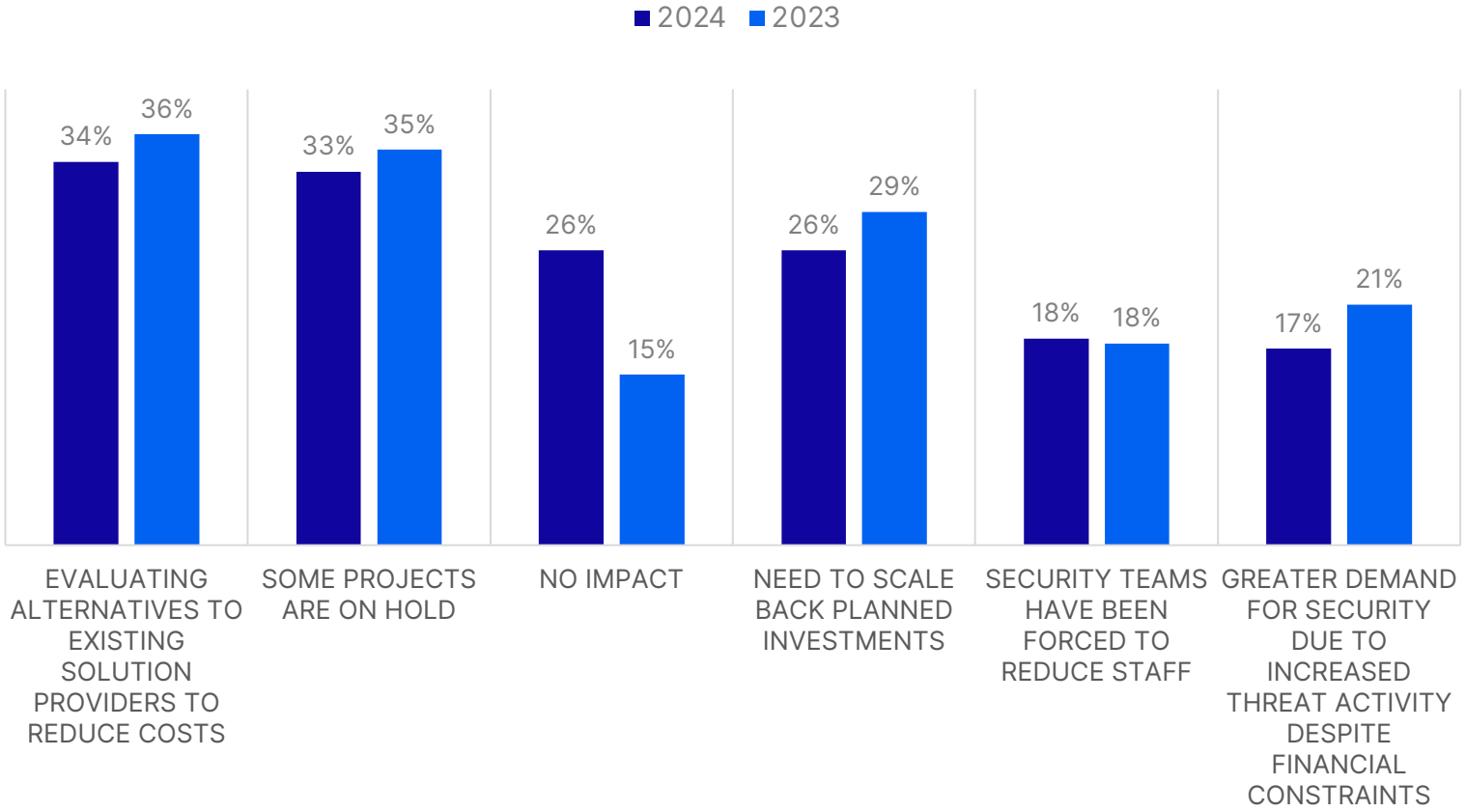
© Copyright 2024 SAPinsider. All rights reserved.

23

While investments persist, the global macroeconomic climate continues to affect security spending. Many respondents report the need to cut costs by exploring alternatives to their current solution providers, or by putting security projects on hold.

Although an increasing number of respondents see no impact this year, fewer are witnessing a rise in demand for security despite the growing frequency of breaches.

Impact of Current Economic Climate on Security Objectives



© Copyright 2024 SAPinsider. All rights reserved.

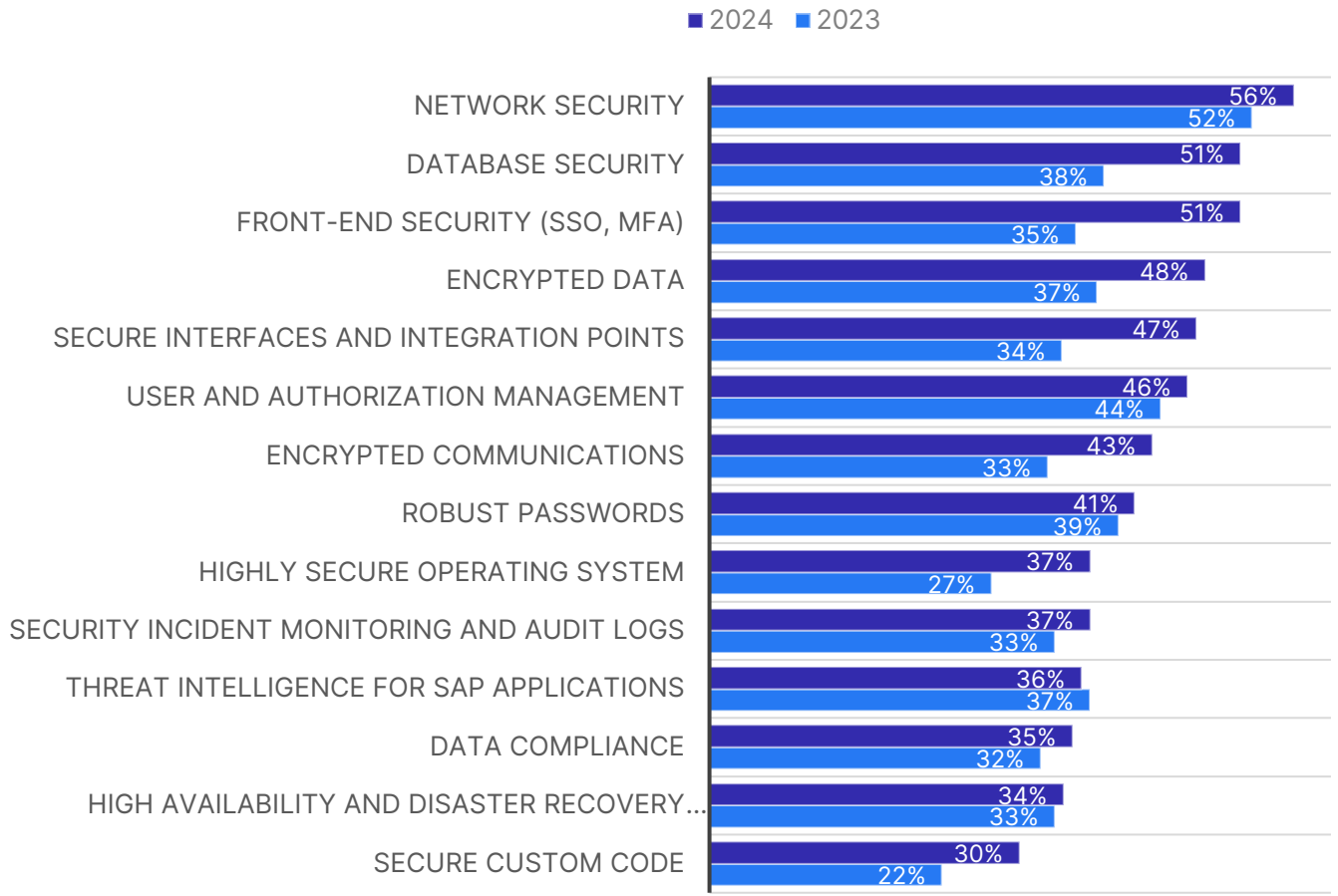
SAPinsider

24

Securing SAP systems can be complex since they are nearly always online and are connected to most other parts of the enterprise. They can also have specific security needs and patching requirements.

Network security helps secure the interconnectedness of systems while the next three required elements are about protecting the data in SAP systems. This reflects that protecting data in SAP systems is of paramount importance.

Elements Required to Make a Secure Environment for SAP Systems

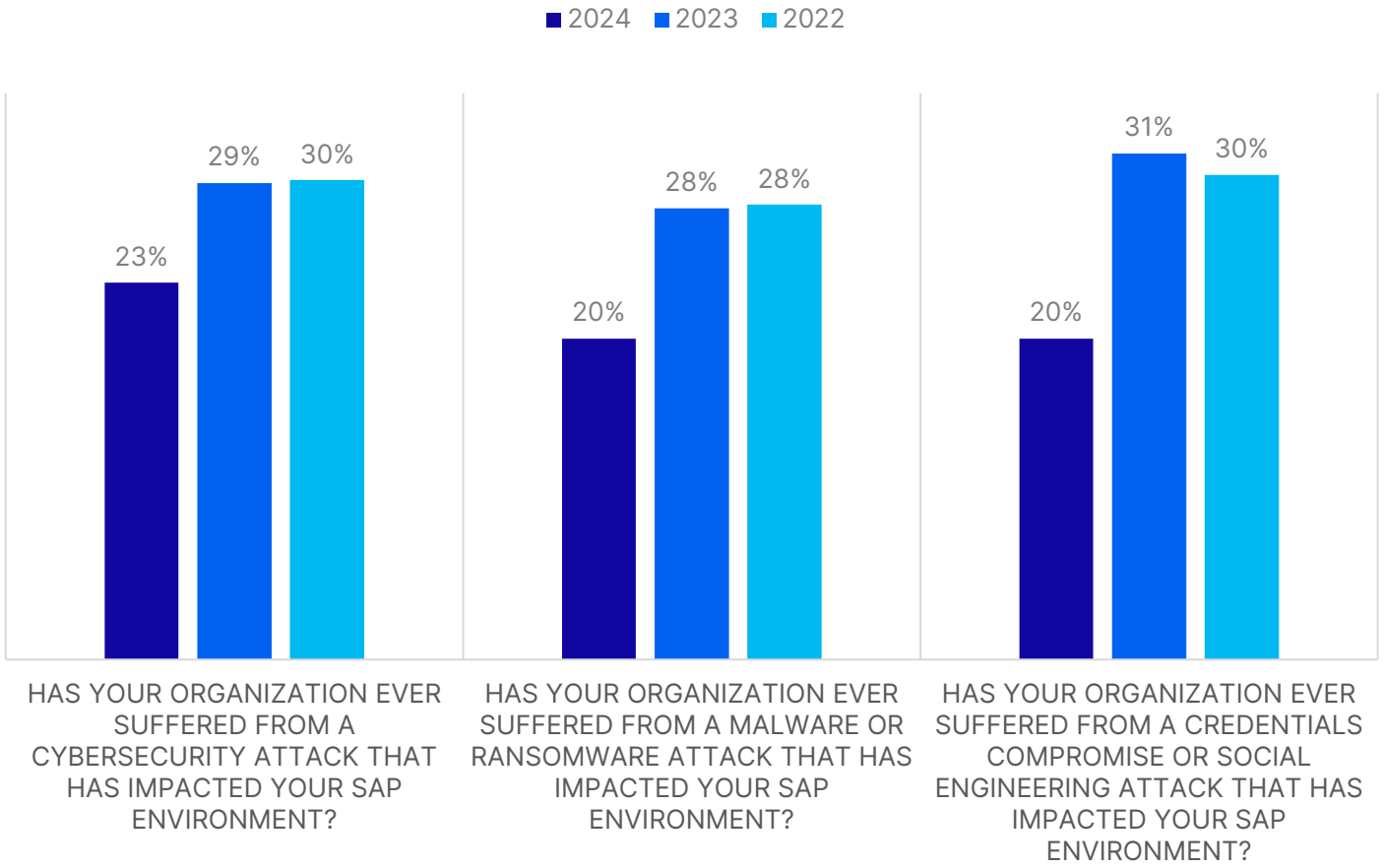


© Copyright 2024 SAPinsider. All rights reserved.

25

The decrease in the number of respondents reporting successful attacks on their systems can likely be attributed to the higher proportion of respondents from North America. Over the past two years, respondents from APJ and EMEA have been more likely to experience cyberattacks impacting their SAP systems compared to those in North America. This year, with nearly 60% of respondents located in North America, this shift in geographical representation may explain the observed decline in reported attacks.

Impact of Attacks Targeted at SAP Systems



© Copyright 2024 SAPinsider. All rights reserved.

THANK YOU

Robert Holland

Vice President, Research

robert.holland@sapinsider.org

SAPinsider.org

PO Box 982Hampstead, NH 03841

Copyright © 2024 Wellesley Information Services. All rights reserved.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. All other product and service names mentioned are the trademarks of their respective companies. Wellesley Information Services is neither owned nor controlled by SAP SE.