JULY 2026

SAPinsider

DETAILED FINDINGS

From The Benchmark Report:

# Cybersecurity Threats and Challenges to SAP Systems 2026

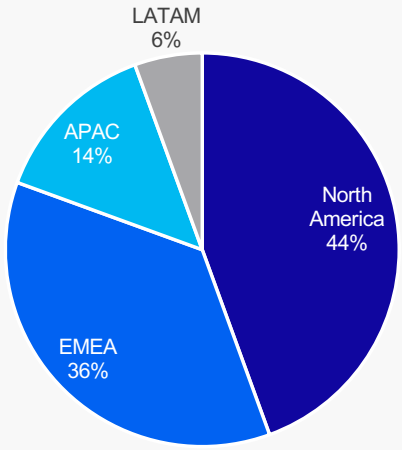
By Robert Holland

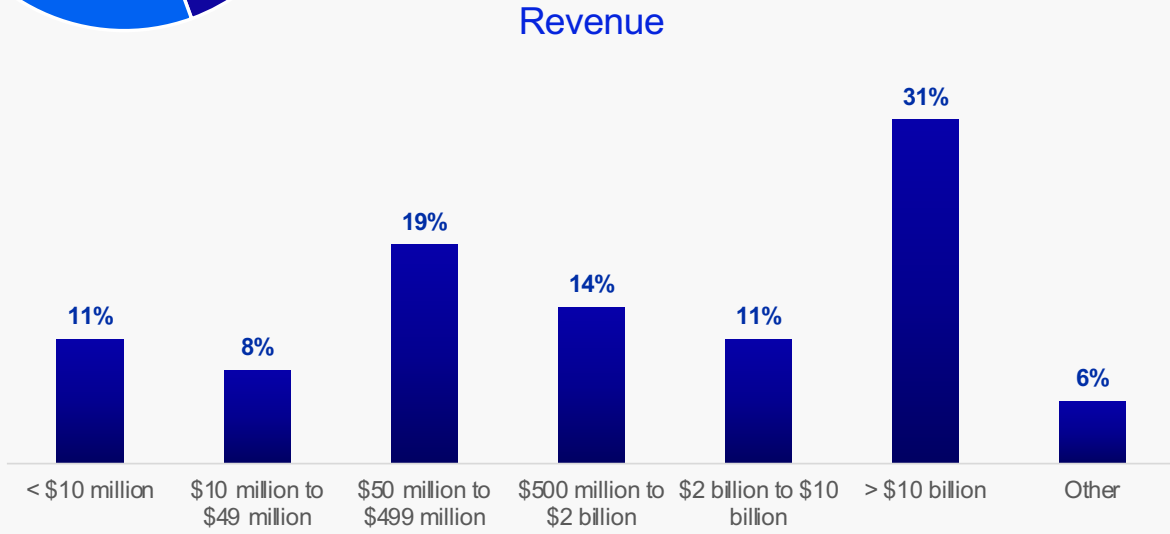
RESEARCH PARTNER SAP | SPONSORED BY ONAPSIS

1

**Between April and June 2026, SAPinsider surveyed its community members to gain deeper insights into their cybersecurity strategy and plans.**

**The survey explored the biggest cybersecurity challenges they face, the factors influencing their cybersecurity strategy, whether they were moving to SAP Cloud ERP, the challenges they face in implementing cybersecurity for SAP, and where they plan their cybersecurity investments for the future.**

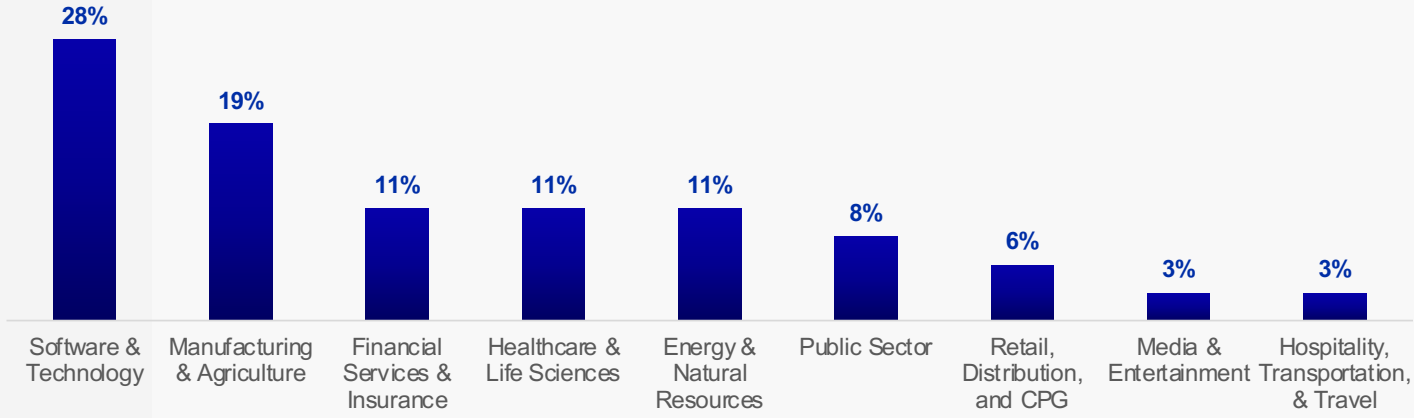


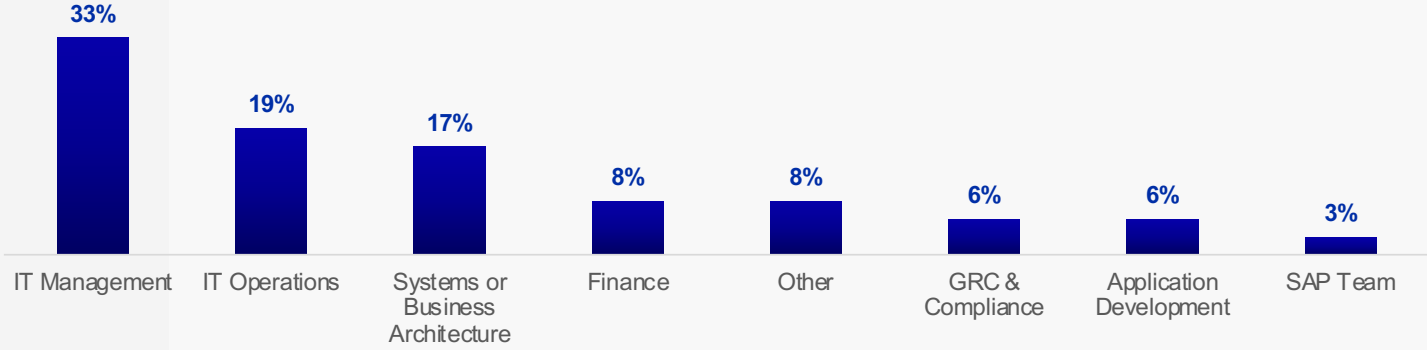
2

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

## Industry




## Role

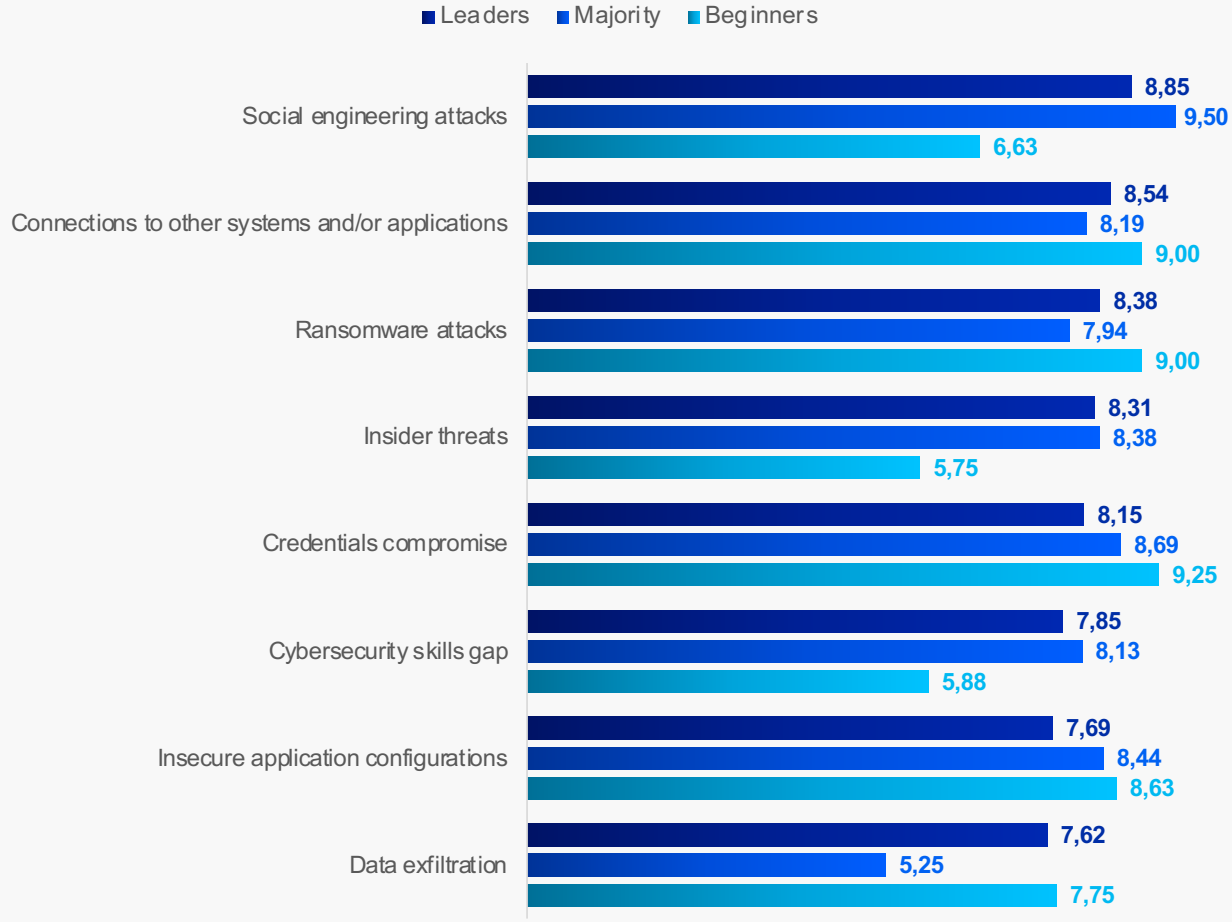


3

**Data this year suggests a shift from data-centric concerns to identity or connectivity-centric threats. With social engineering attacks, insider threats, credentials compromise, connections to other systems, and insecure application configurations all being in the top eight biggest potential threats, identity and connectivity-centric concerns are certainly front and center for respondents.**

**This does not mean that data-related threats are not important as more than half (51%) of the respondents to this year's survey reported that they regarded the business processes and data supported by SAP applications as mission-critical, and that any disruptions would severely impact revenue, operations, or compliance obligations.**

## Top Cybersecurity Threats to SAP Systems

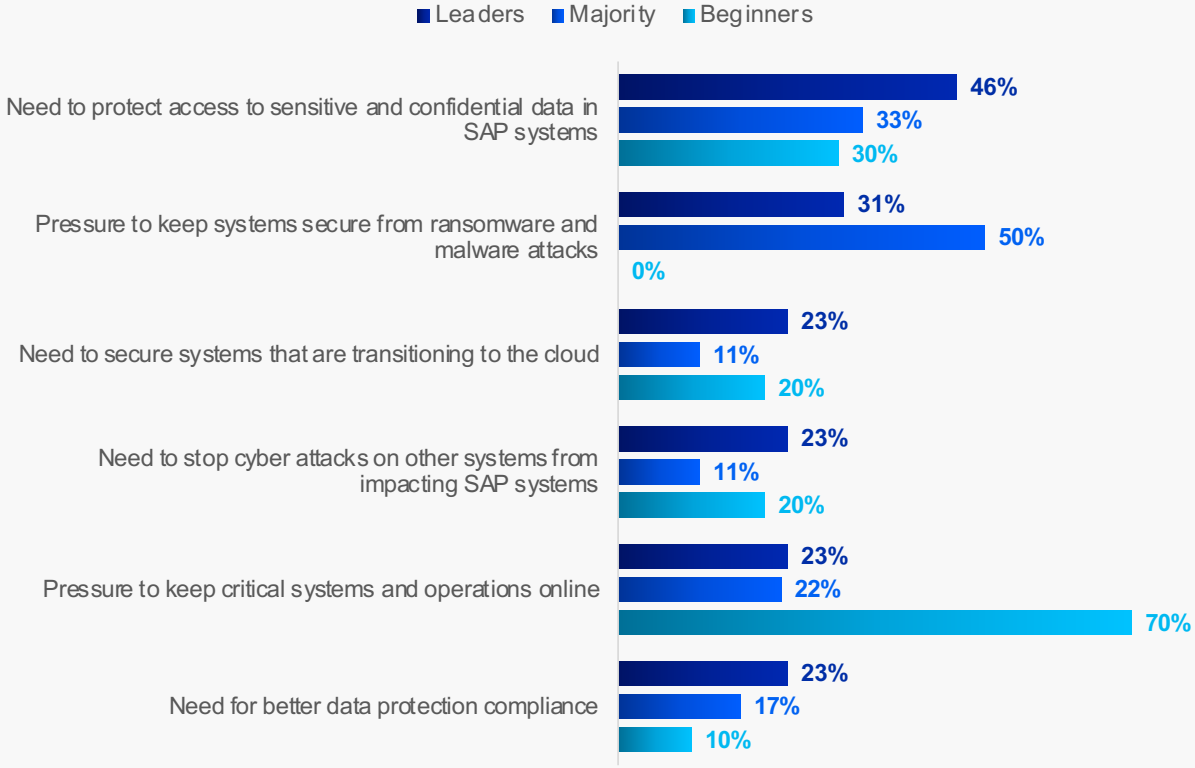


# 4

**The most important factor driving cybersecurity strategy for security leaders continues to be a need to protect access to the sensitive and confidential data in SAP systems (46%).**

**Protecting the data in SAP systems has been the most important factor driving cybersecurity strategy in four of the past five years. Although important, the shift to credentials and connectivity-related threats is only starting and has not yet displaced the overarching need to protect the data and processes stored in SAP systems.**

## Factors Most Responsible for Driving Strategy and Plans for Cybersecurity

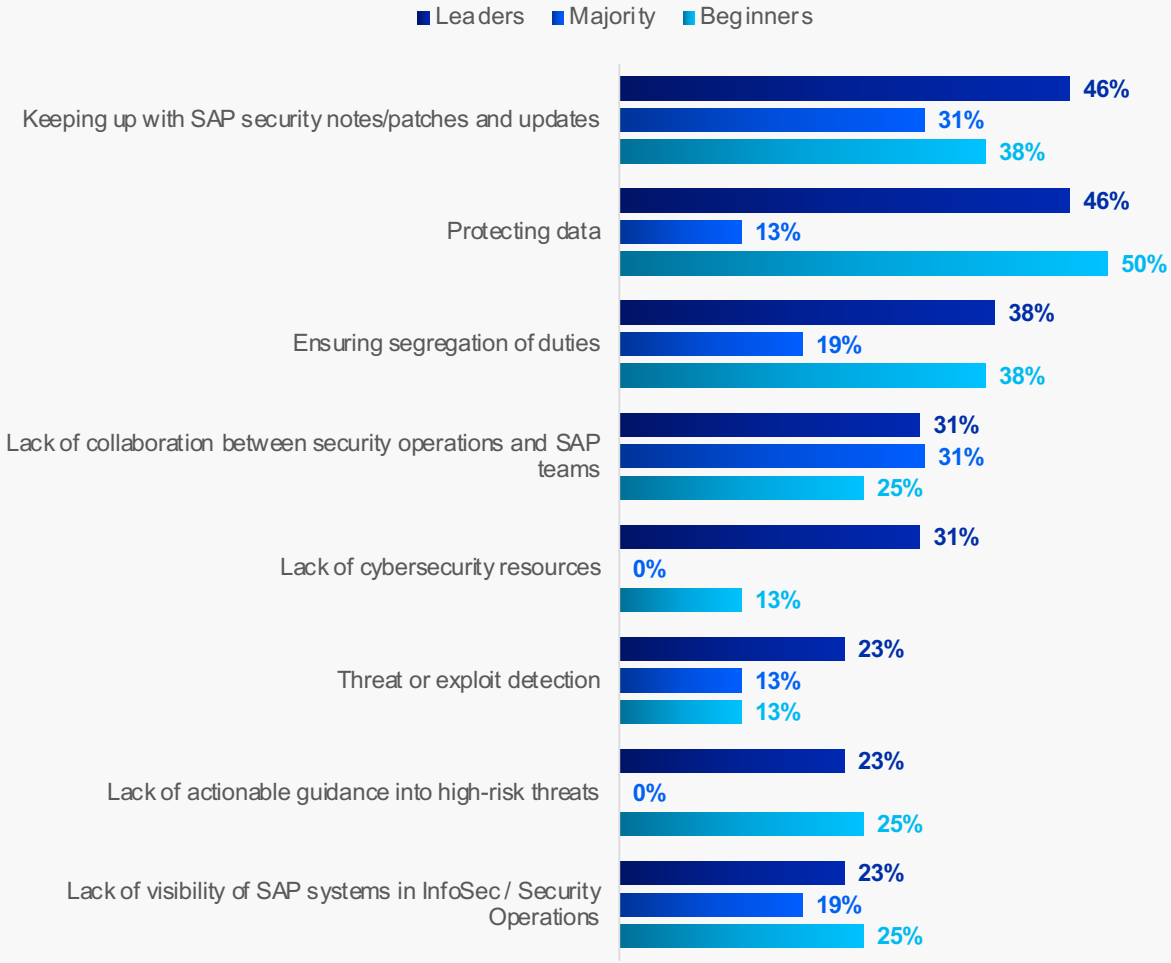


5

**As has been the case for several years, security leaders and the respondent majority report that keeping up with SAP security notes, patches, and updates remains the biggest obstacle. It is the second most important challenge for beginners in security.**

**In some ways this is surprising, as security experts and vendors have been talking about solving patching challenges for years. However, with the number of patches released by SAP last year, it becomes easier to see why applying them in a timely manner continues to be an issue.**

## Biggest Challenges Faced in Securing SAP Systems



6

**For many organizations, scheduling patching can be difficult, particularly in a global organization. A lack of resources in prioritizing, verifying, and validating patches only makes this even more problematic.**

**The concern that this brings is that, even when critical patches are released, a significant proportion of the SAP community may not be able to apply them for some time.**

**Given that at least one vulnerability last year was under active exploitation before it was patched, this is hugely concerning from a cybersecurity perspective.**

## Issues Experienced That Lead to Patching Backlog

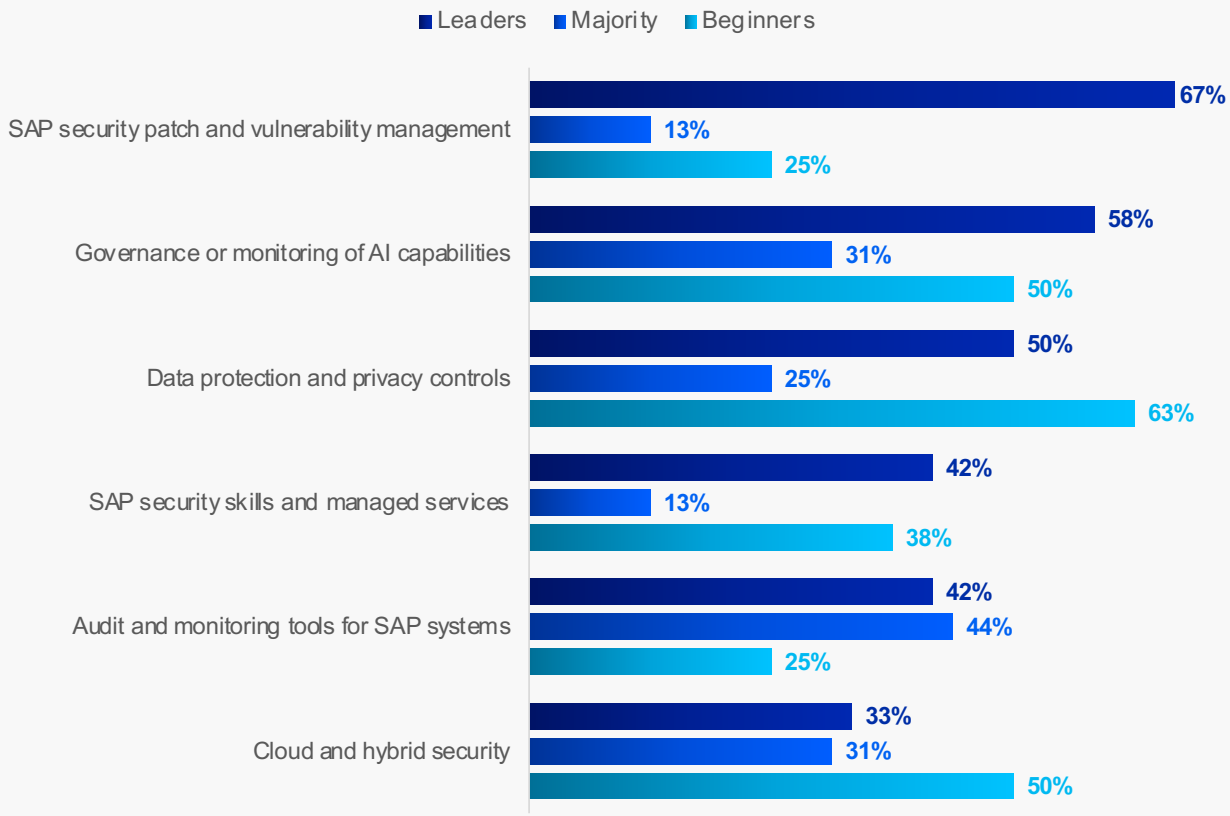
7

**For security leaders, there is an obvious focus on patch and vulnerability management. This is higher than the resources planned for any other group.**

**Additionally, security leaders are investing in governance and monitoring of AI capabilities. While this is a topic that seems to be falling more under the oversight of traditional GRC teams, it is a crucial one for organizations.**

**For the respondent majority, the largest planned investment area is in audit and monitoring tools for SAP systems. Security beginners plan their greatest investment in data protection and privacy controls.**

## Areas of Planned SAP-Specific Cybersecurity Investments

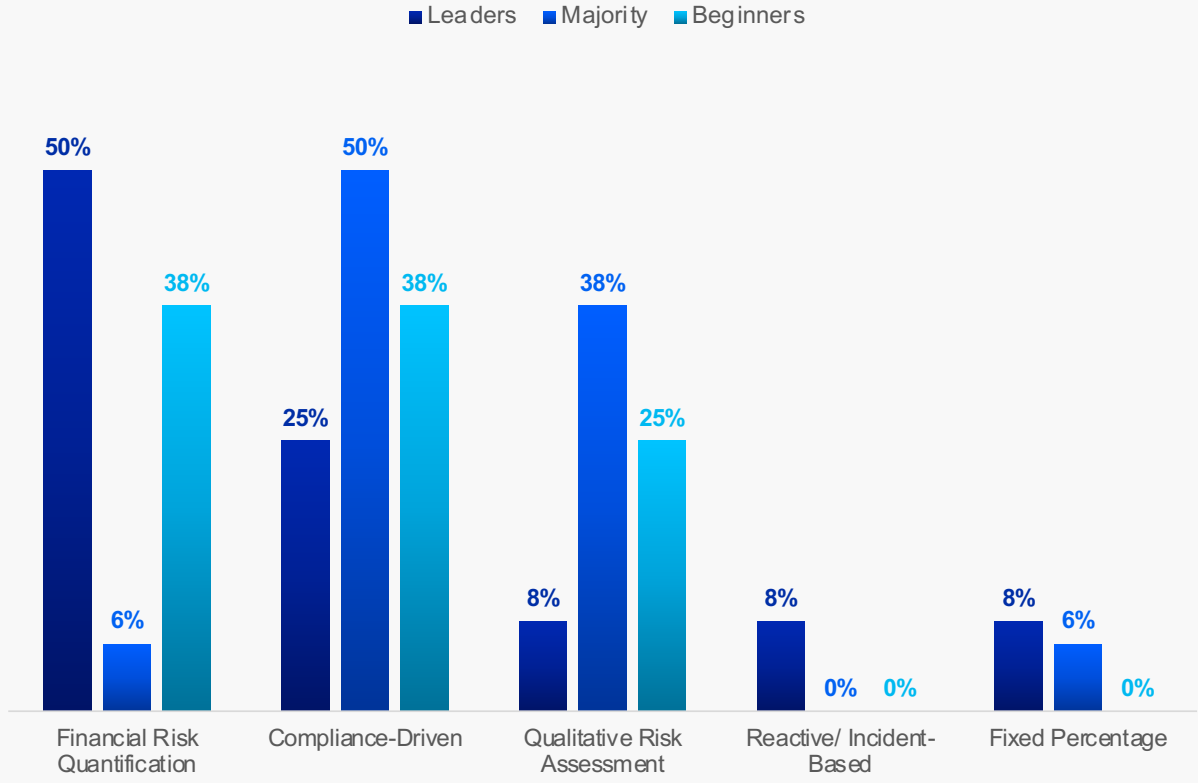


8

**Cybersecurity funding can be based on several factors. These include:**

- **Financial Risk Quantification: Budget is based on the calculated financial impact of potential data breaches or system downtime (e.g., Value at Risk).**
- **Compliance-Driven: Funding is secured primarily to meet regulatory or audit requirements (e.g., SOX, GDPR).**
- **Qualitative Risk Assessment: Budget is based on a "High/Medium/Low" threat landscape determined by leadership.**
- **Reactive/Incident-Based: Funding is typically released in response to a specific security incident or a failed audit.**
- **Fixed Percentage: SAP security is a fixed, non-negotiable part of the broader ERP or IT budget.**

## How Funding and Resources are Justified for SAP Cybersecurity



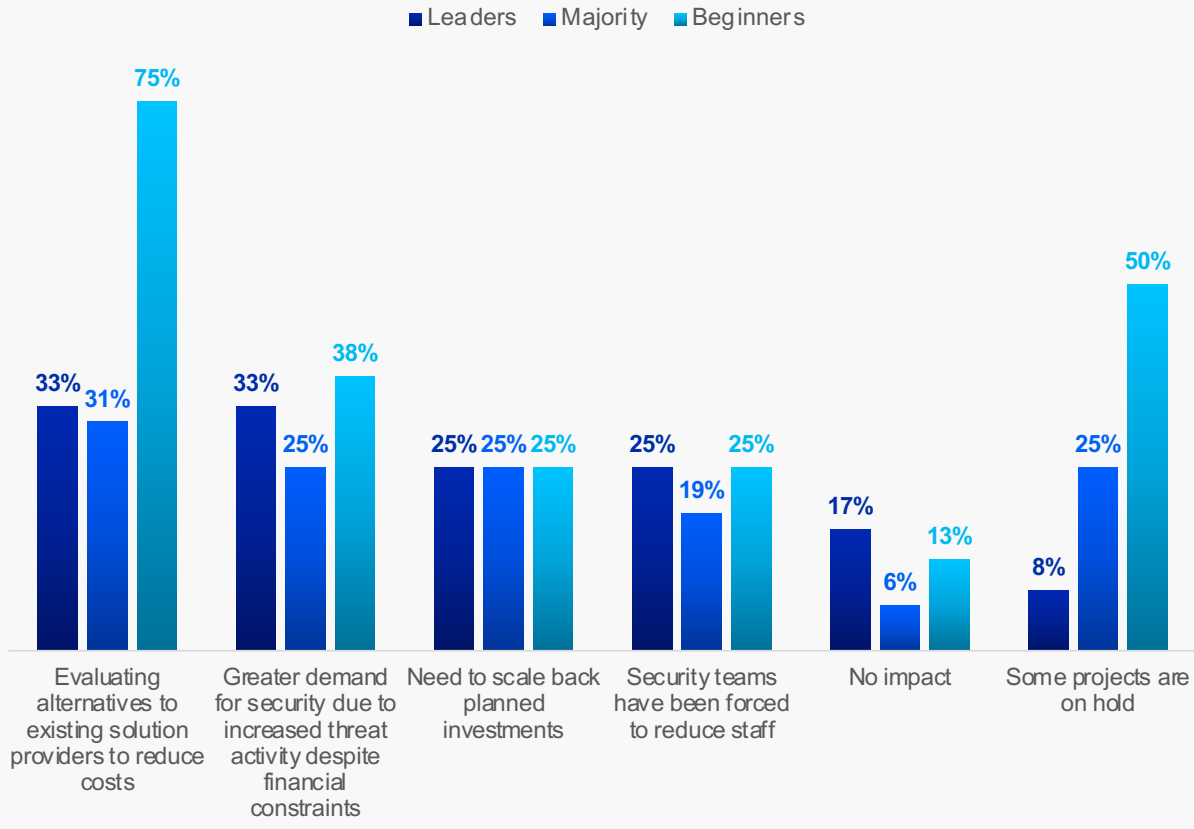
9

**The current economic climate is creating challenges for all respondents. The most likely scenario for all groups is to evaluate alternatives to existing solution providers to reduce costs.**

**While this is much more likely for security beginners than other groups, a third of both security leaders (33%) and the respondent majority (31%) report they are in the same situation.**

**Similarly, a quarter of all respondent groups report that they need to scale back any planned investments, and almost as many report that their security teams have been forced to reduce staff.**

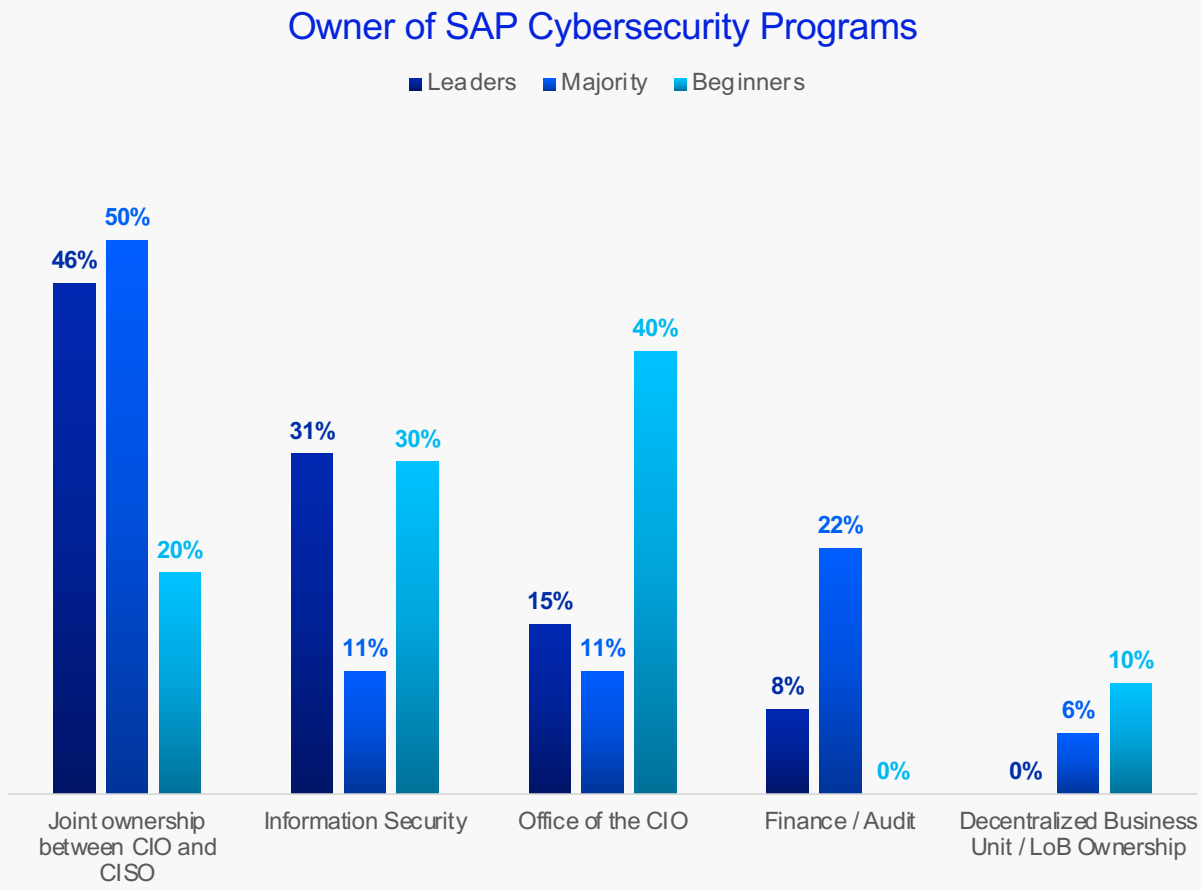
## Impact of Current Economic Climate on Security Objectives



10

**Both cybersecurity leaders and the respondent majority report they have joint ownership of their cybersecurity programs between their CIO and CISO.**

**This level of collaboration is extremely important because SAP teams are more likely to be part of the CIO's organization while information security teams bring broader cybersecurity expertise. All respondents should aim on moving toward this level of collaboration.**



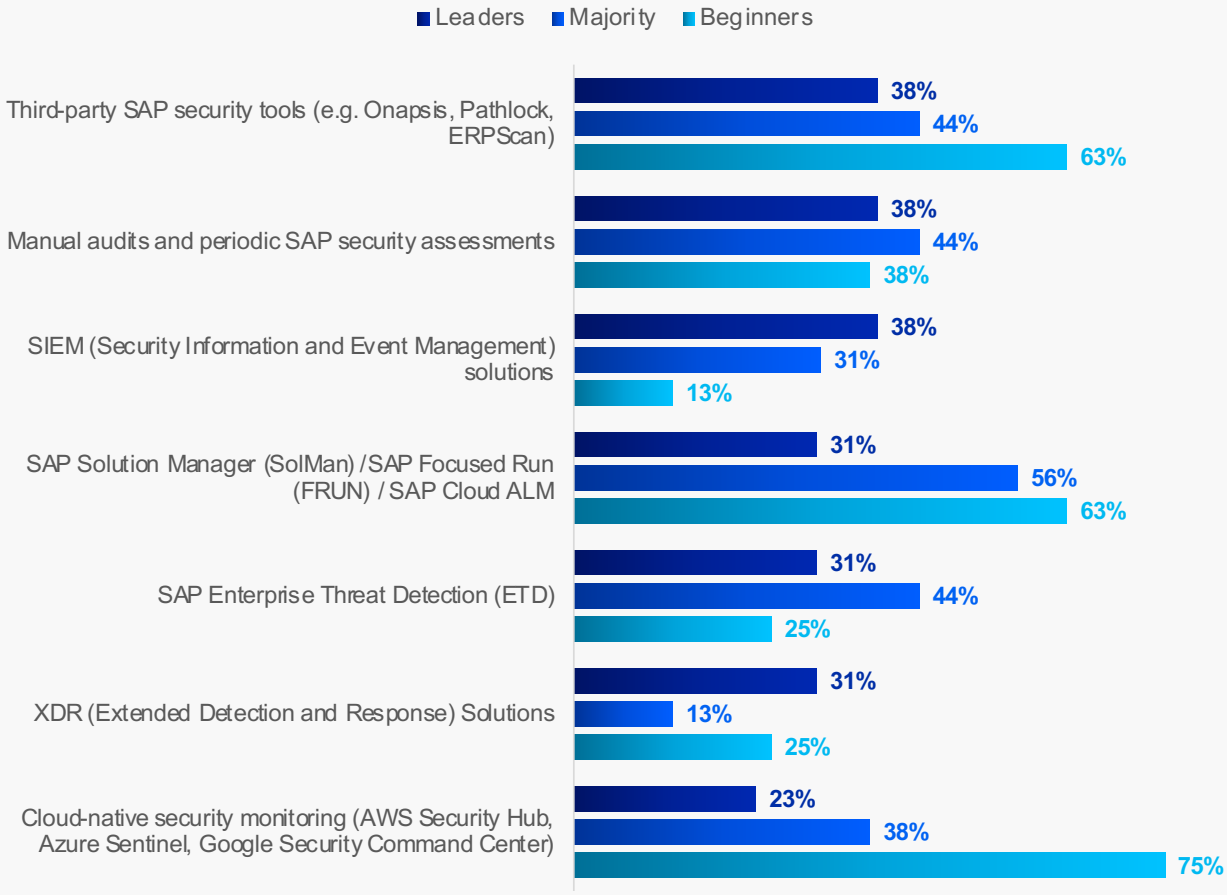
11

**Security leaders use a variety of methodologies when it comes to detecting and monitoring threats in SAP environments. Some are using third-party tools while others have integrated SIEM solutions, SAP tools, or even XDR.**

**The respondent majority is primarily using out of the box solutions such as SAP Solution Manager, SAP Cloud ALM, and SAP Focused Run. While these are helpful, they do not provide the same level of insight or, more importantly, evaluation as dedicated cybersecurity solutions.**

**Security beginners are also using a variety of tools and solutions to detect threats, but may in the future need to focus on specific areas rather than utilizing a multiplicity of solutions.**

## How Threats are Detected and Monitored in SAP Environments

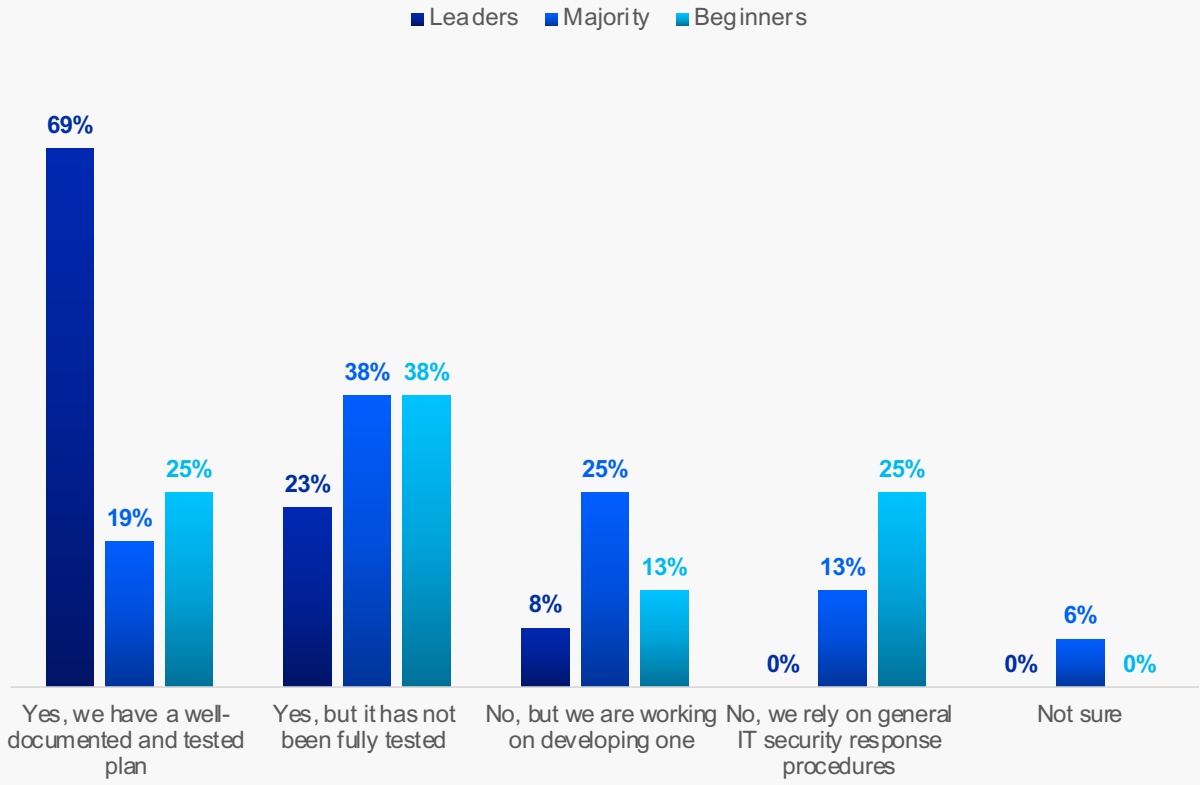


12

**More than two thirds (70%) of respondents report that their organization has an incident response plan specifically for SAP-related cyber incidents.**

**Only 38% report that they have tested this plan, but this is a significant increase over last year when only those with the most mature cybersecurity posture reported having a plan. What is even more positive is that another 16% are developing a plan and only 10% rely on general IT security response procedures.**

## Status of Incident Response Plan for SAP-Related Cyber Incidents

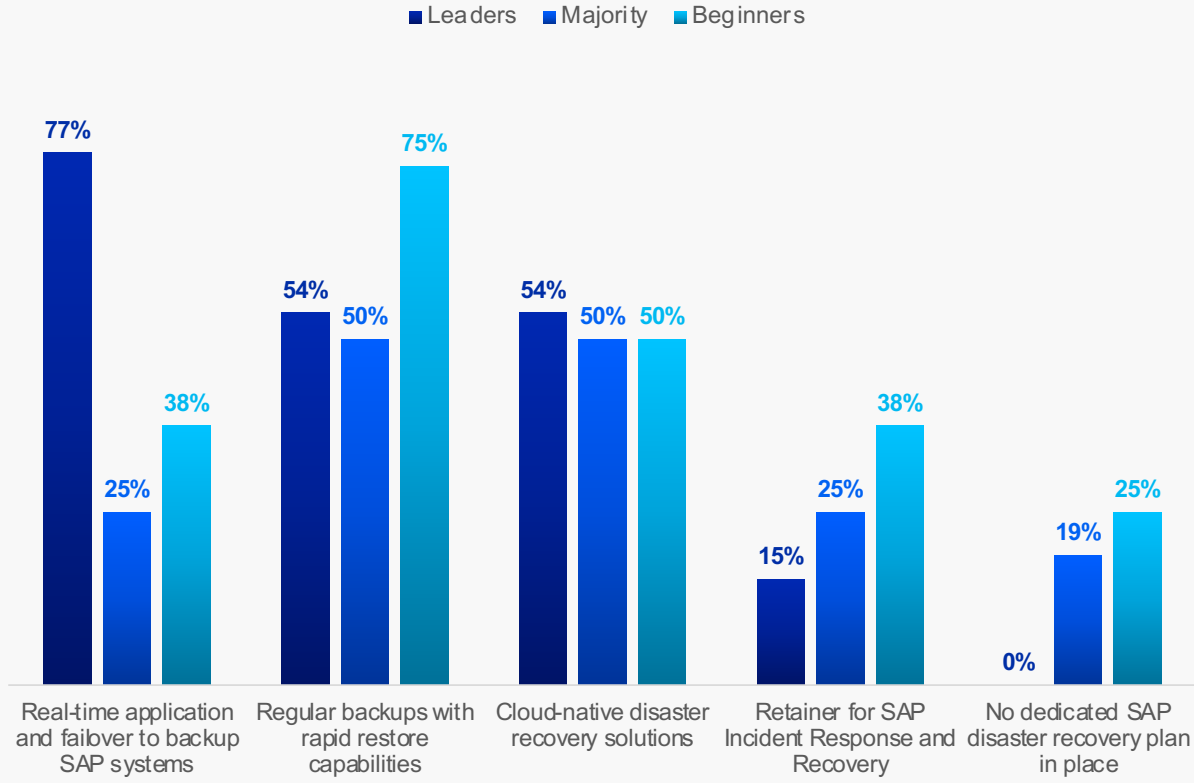


13

**Only security leaders are likely to have real-time application failover and backup capabilities when it comes to disaster recovery (DR) for SAP workloads following a security breach. Most respondents have at least regular backups while a good proportion are using cloud-native DR solutions.**

**What is concerning is the significant proportions of both the respondent majority and security beginners that have no dedicated disaster recovery plan in place for their SAP environments.**

## Ways of Handling Disaster Recovery for SAP Workloads in Case of a Security Breach



14

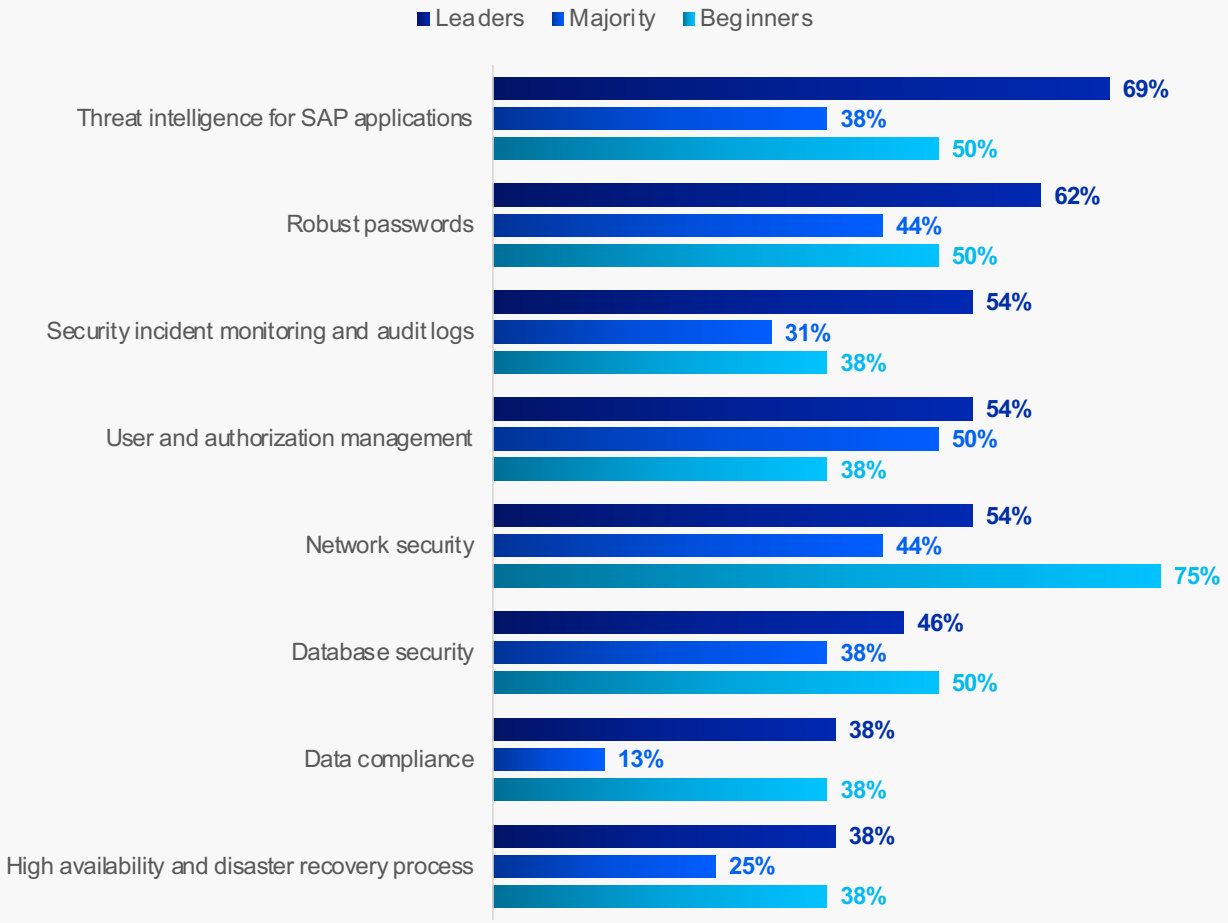
**Respondents were asked to select from 18 different elements that they believed were required to create a secure environment for their SAP systems.**

**Security leaders focused on threat intelligence, robust passwords, security incident monitoring, user and authorization management, and network security.**

**Beyond threat intelligence and robust passwords, security beginners were most focused on network security, database security, as well as encrypted data and communications. This reflects that they are still focused on more reactive capabilities.**

**The respondent majority are also behind the curve when it comes to capabilities, such as threat intelligence, and remain focused on user and authorization management issues.**

## Most Important Elements Required to Make a Secure Environment for SAP Systems



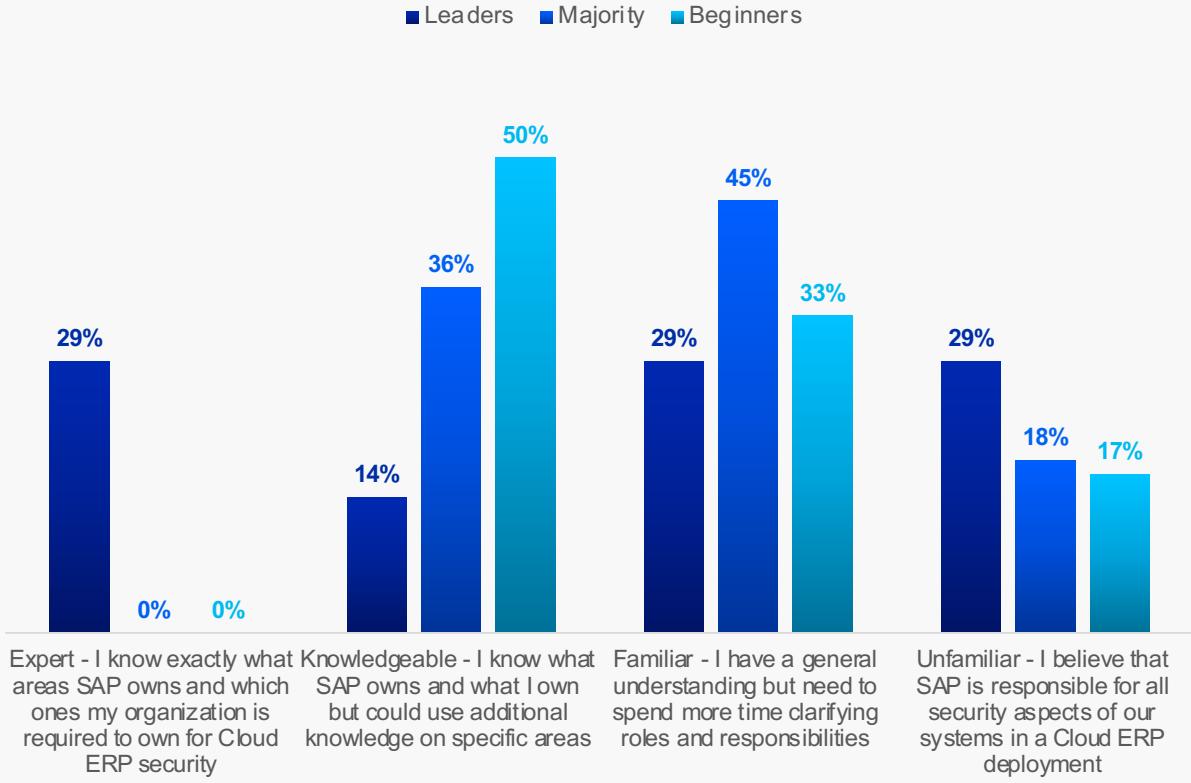
15

**Two thirds of respondents plan on moving to SAP Cloud ERP Private (formerly RISE with SAP). Those that plan on moving were asked about their level of knowledge when it came to the Shared Responsibility Model. What is notable is just how little respondents were familiar with that model.**

**While security leaders had the greatest average level of knowledge, less than half of all respondents (42%) had more than a general understanding of their role under the Shared Responsibility Model.**

**It is crucial that organizations dedicate time to educating teams on the Shared Responsibility Model and their role in it if they are to keep their SAP Cloud ERP Private environments secure.**

## Knowledge About Security Ownership and Roles Under the Shared Responsibility Model for SAP Cloud ERP Private






* Only asked of those planning on moving to SAP Cloud ERP Private

16

**The SAP Cloud ERP Private model can be very different from more familiar environments.**

**However, security leaders have identified areas of real threat, including securing both existing and legacy systems in parallel, agentic AI, and SAP BTP security. These respondents are even concerned about understanding which security notes need to be prioritized.**

**The respondent majority, less informed about SAP Cloud ERP Private, are most concerned with vulnerability management, SAP access to the technology stack, and cloud infrastructure. Both this group and cloud beginners need to learn more about SAP Cloud ERP Private so they can more effectively evaluate potential threats.**

## Most Concerning Areas of Cybersecurity in SAP Cloud ERP Private




* Only asked of those planning on moving to SAP Cloud ERP Private

DART
MODEL FRAMEWORK

# Strategy and Needs Cybersecurity Plans for SAP

## DRIVERS

- Need to protect access to sensitive and confidential data in SAP systems (37%)
- Pressure to keep critical systems and operations online (34%)
- Pressure to keep systems secure from ransomware and malware attacks (32%)

## ACTIONS

- Regularly implementing patches and updates (46%)
- Integrating SAP system data into Security Operations (44%)
- Training end-users to protect credentials from social engineering and other attacks (37%)
- Segmenting and limiting access to data (32%)

## REQUIREMENTS

- Fully patched and updated systems (88%)
- Safe password practices (88%)
- Real-time monitoring and logging capabilities (85%)
- Cybersecurity tools that integrate with SAP and non-SAP systems (80%)
- Regular training and education programs for all employees (80%)
- Protecting SAP systems from zero-day threats before patches are released (80%)

## TECHNOLOGIES

- Encrypted/Secure Connectivity (59%)
- Continuous Monitoring (54%)
- Vulnerability Management (51%)
- Dynamic Authorization and Least Privilege (49%)
- Data Encryption (46%)
- Security-Driven Networking (35%)
- Automated Code Vulnerability Testing Tools (32%)
- Code Vulnerability Analysis (30%)
- Threat Intelligence Feeds (30%)
- Application-Aware Network Security (30%)
- Automated Testing for Compliance (27%)
- Embedded Hardware Authentication (22%)
- Zero-Trust Models (22%)

17

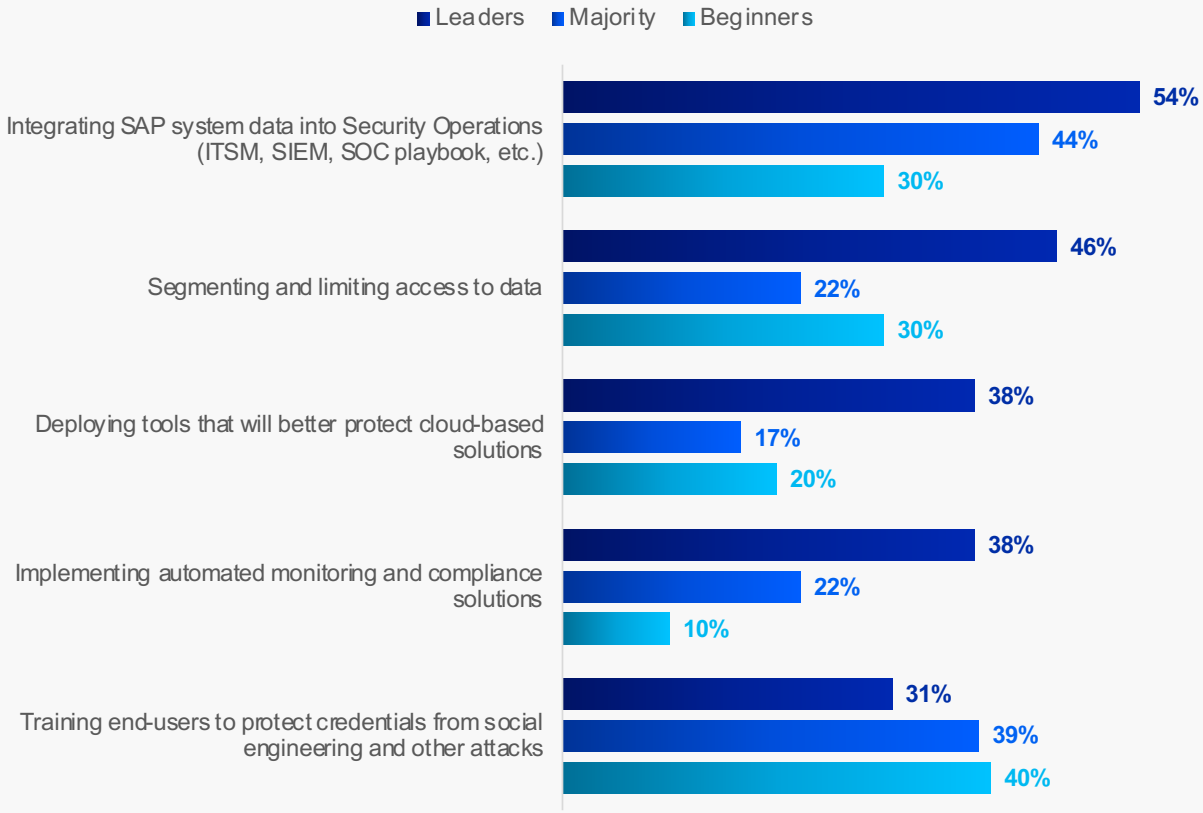
**Connecting SAP systems data with tools being used by Security Operations teams helps provide a consistent level of monitoring for those applications.**

**An example of this type of integration is currently being positioned by Microsoft Sentinel, but other partners such as Splunk have been integrating SAP systems with their SIEM tools for many years.**

**This strategy directly connects to the pressure to keep critical systems and operations online and the pressure to protect them from ransomware and malware attacks.**

**The more a standard baseline can be established, the more readily any exceptions can be detected.**

## Strategies Employed to Support SAP Cybersecurity Needs



18

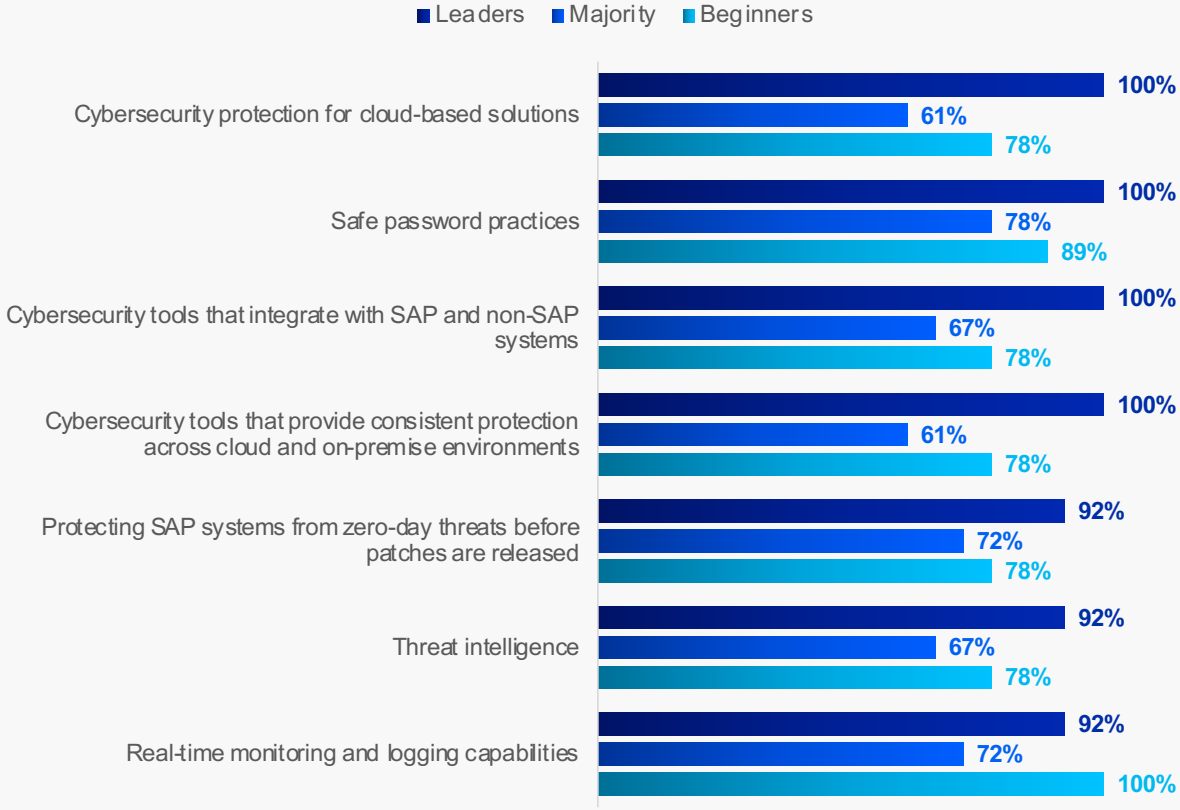
**Strategies are important, but organizations must fulfill specific requirements to implement strategies.**

**This year, respondents emphasized protection for cloud-based systems, safe password practices, cybersecurity tools that integrate SAP and non-SAP systems, and cybersecurity tools that provide consistent protection across cloud and on-premise environments.**

**These requirements connect directly to the strategy of deploying tools that better protect cloud-based solutions, and doing more with less when it comes to budget, since tools will work across the enterprise landscape rather than being solution specific.**

**Safe password practices also support the need to protect against identity-centric threats.**

## Requirements for Cybersecurity for SAP Systems



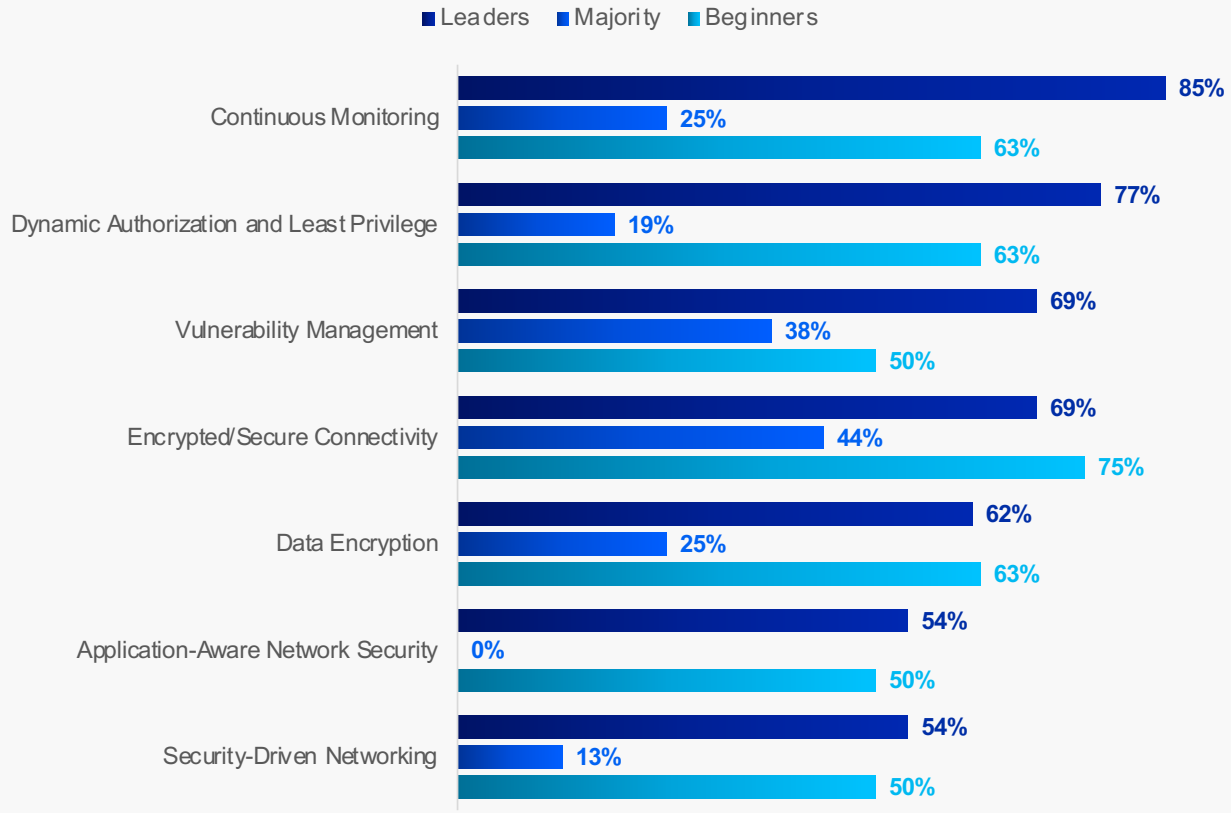
19

**Security leaders are already using the technologies that will provide them with a real-time status on SAP systems and help protect the data in those systems.**

**The respondent majority is lagging significantly in the implementation of these technologies, as they are still moving from a reactive to proactive posture.**

**Interestingly, security beginners are more likely to have some technologies deployed than the respondent majority, though they are still more focused on setting up existing environments than moving to technologies that will provide a more proactive foundation.**

## Technologies Being Used to Support Cybersecurity Strategy



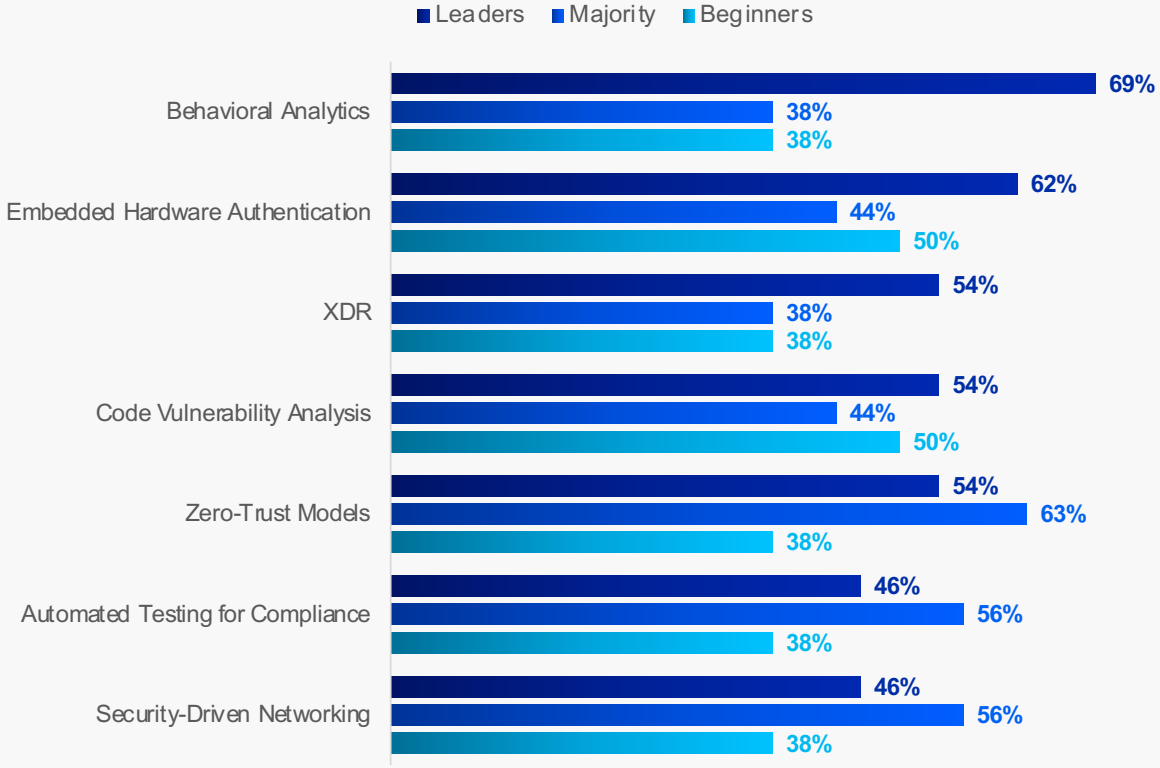
20

**Security leaders are already starting to deploy capabilities like behavioral analytics, embedded hardware authentication, and XDR that will continue to expand SAP systems monitoring.**

**The respondent majority is focused on catching up with what they are not already running today. This includes zero-trust models, automated testing for compliance, and security-driven networking, all tools that security leaders are already leveraging.**

**Cybersecurity beginners are most focused on code vulnerability analysis, vulnerability management, and embedded hardware authentication as they race to catch up and build a foundation that provides more proactive insights.**

## Technologies Being Implemented to Support Cybersecurity Strategy



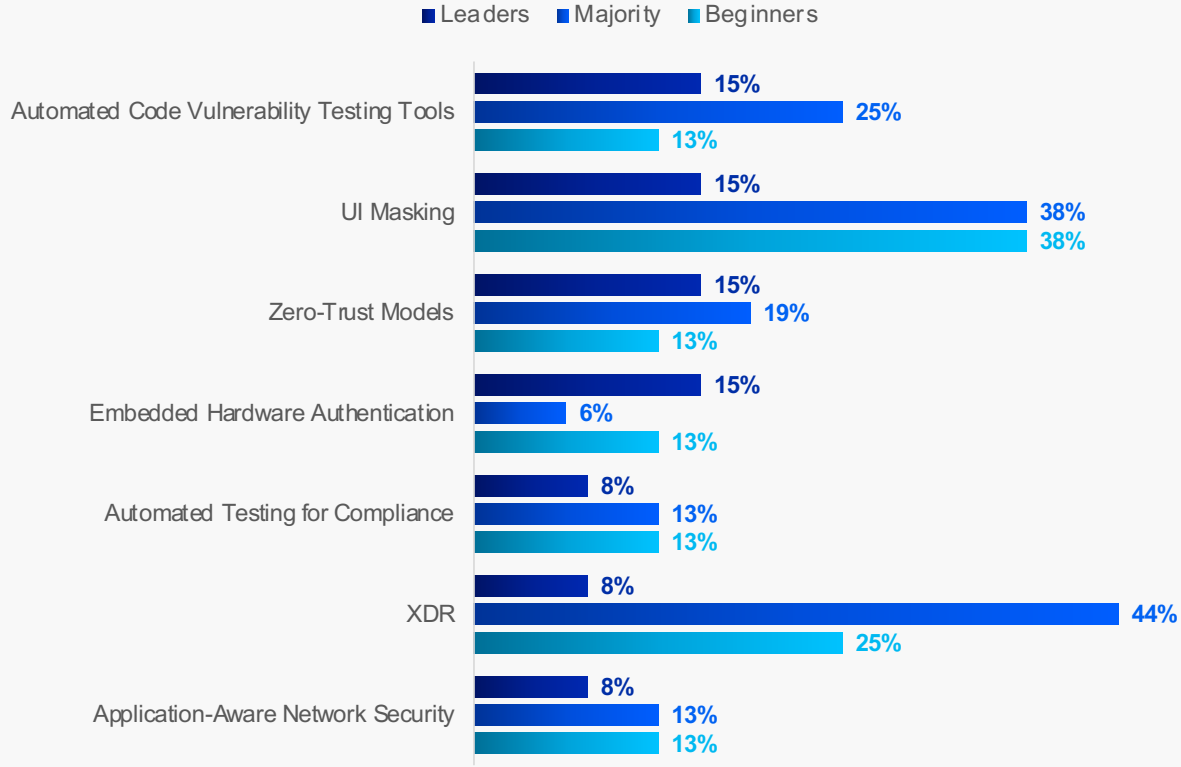
21

**Since security leaders are more likely to be using or implementing many of these technologies, they are less likely to be evaluating them for future usage.**

**The respondent majority are focused on evaluating technologies like XDR, UI masking, and behavioral analytics, which will help transition to a more proactive posture.**

**Security beginners continue to chase some of these technologies. Their primary focus is on UI masking, XDR, Threat Intelligence, and Behavioral Analytics. However, respondents in this group need to find a way to jump start their cybersecurity strategy or they will become even more vulnerable.**

## Technologies Being Evaluated to Support Cybersecurity Strategy



SAPinsider

# THANK YOU


**Robert Holland**
Chief Research Officer

robert.holland@sapinsider.org


**SAP insider.org**


PO Box 982Hampstead, NH 03841