SAPinsider

DETAILED FINDINGS FROM
THE BENCHMARK REPORT

By Robert Holland May 2023

CYBERSECURITY THREATS TO SAP SYSTEMS

DETAILED FINDINGS

Sponsored by

LAYER SEVEN SECURITY Microsoft Azure ONAPSIS pathlock SUSE

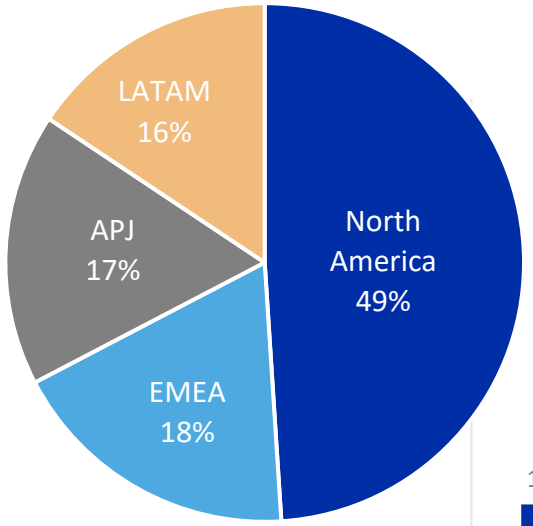
DETAILED FINDINGS

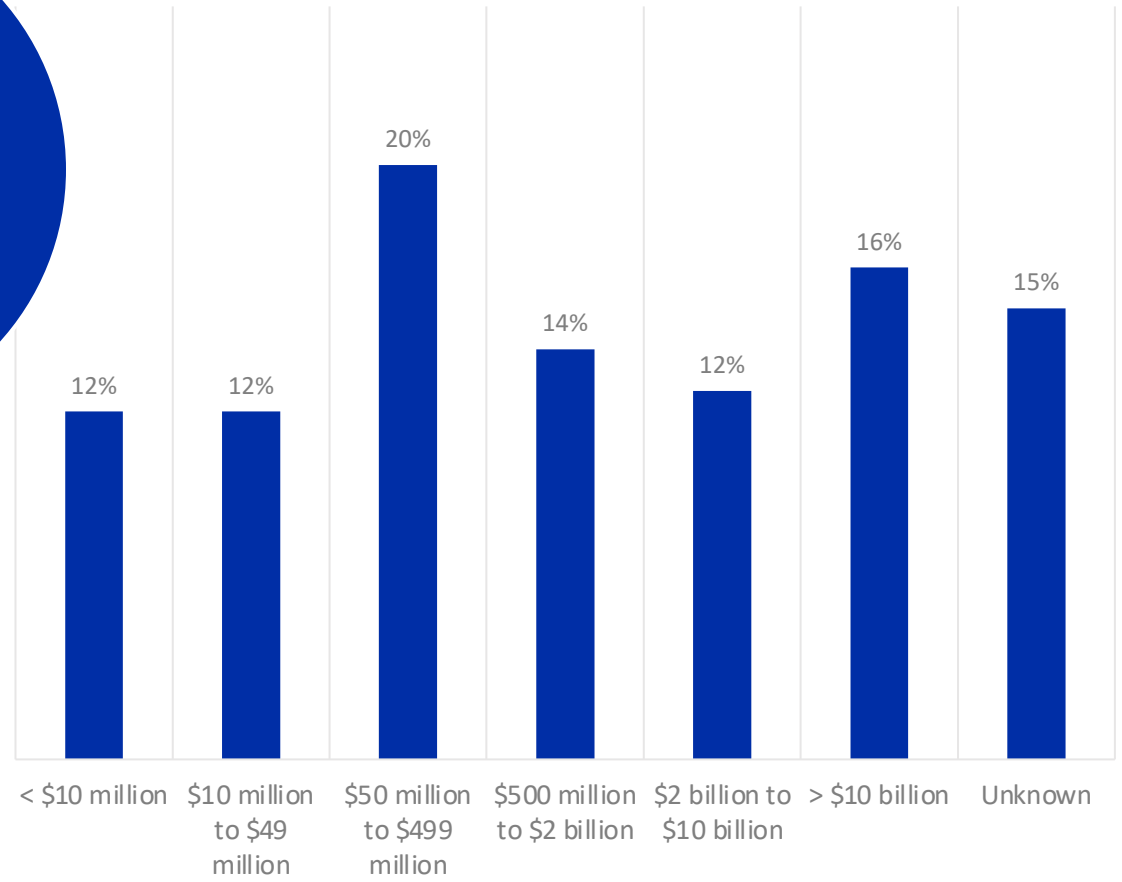
1

206 members of the SAPinsider community were surveyed between February and April of 2023.

Respondents were from different areas around the globe, and were employed by organizations of differing sizes.

The survey focused on those who were involved in cybersecurity or security decisions in their organizations, with a significant number of respondents having completed a previous survey.





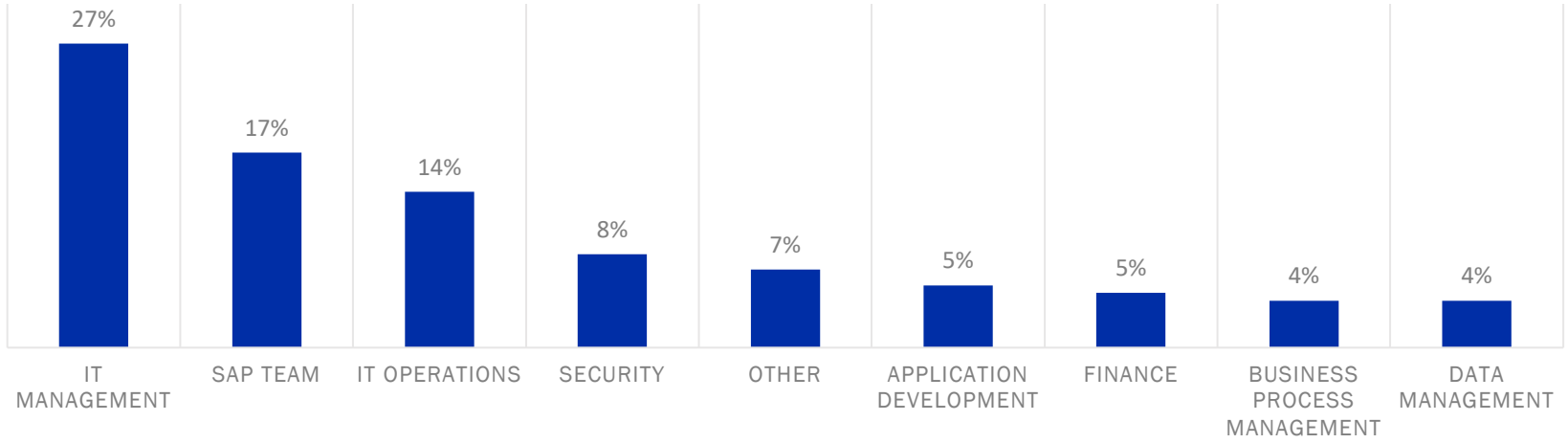
DETAILED FINDINGS

2

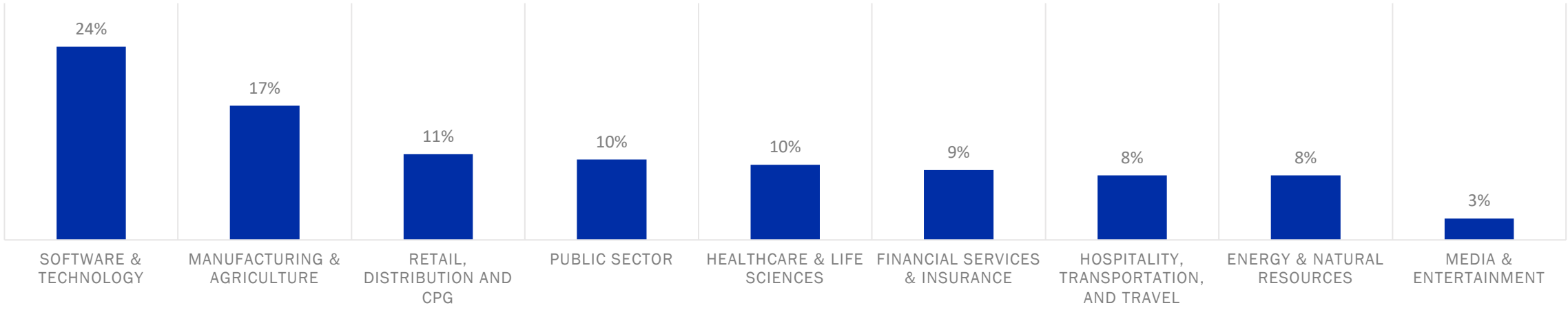
Respondents were asked about the cybersecurity threats to their SAP systems, and their plans to address those threats.

Respondents were also asked what role they played within their organization and what in what market sector their organization functioned.

Department or Functional Area



Industry



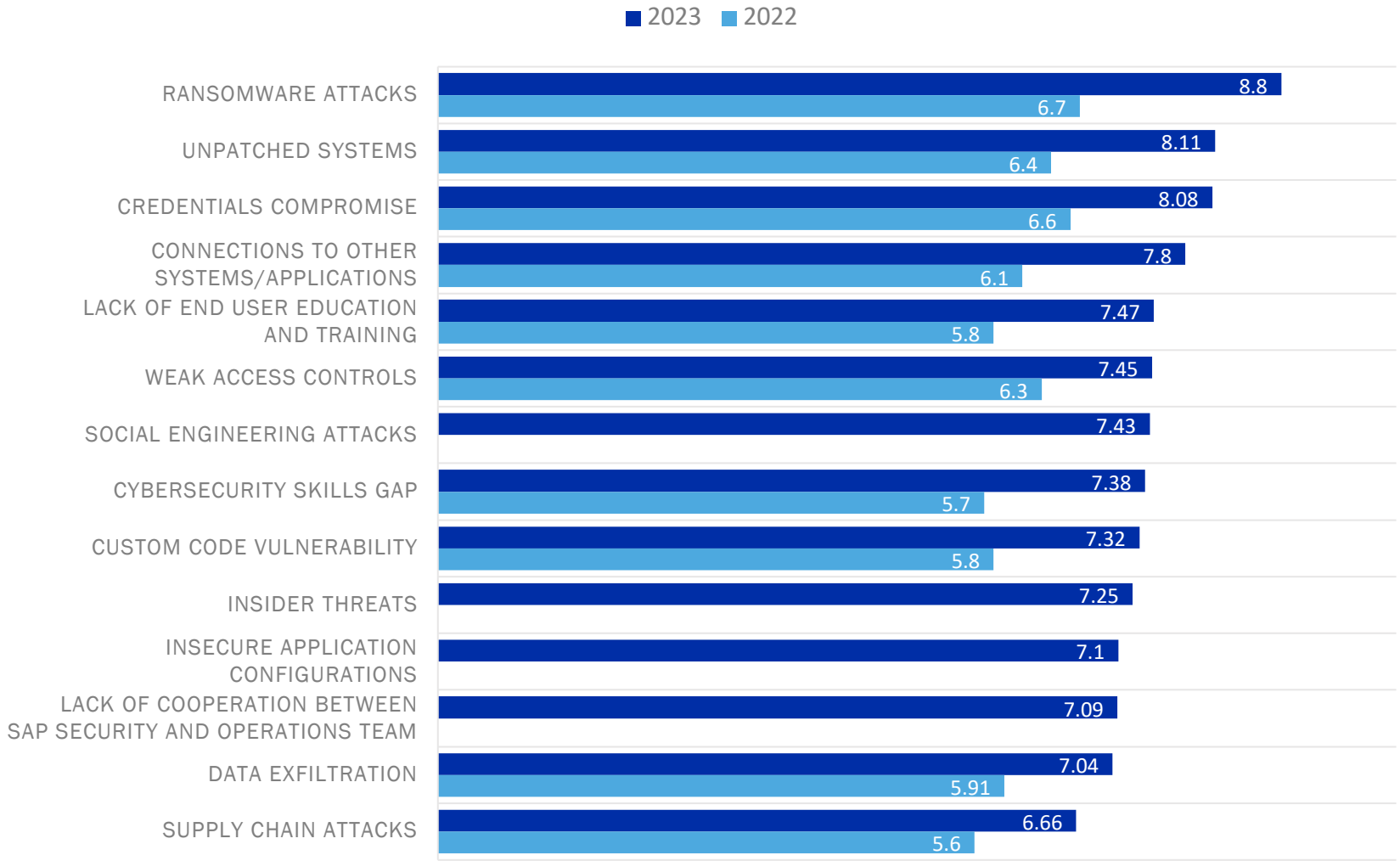
DETAILED FINDINGS

3

Ransomware attacks remain the biggest potential threat, but this is closely followed by unpatched systems and a potential credentials compromise — both of which potentially open SAP systems to attacks that can compromise or expose data.

Put a patching strategy in place that ensures that critical vulnerabilities are patched in a timely manner. Consider leveraging application lifecycle management tools to help automate patching processes.

Rank the Cybersecurity Threats to SAP Systems



DART MODEL FRAMEWORK

Cybersecurity Threats to SAP Systems

DRIVERS

- Protection for secure and confidential data (37%)
- Pressure to keep critical systems and operations online (33%)
- Pressure to keep systems secure from ransomware and malware attacks (29%)
- Need for better data protection compliance (23%)

ACTIONS

- Regularly implementing patches and updates (49%)
- Conducting regular audits and security assessments (44%)
- Training end-users to protect credentials from social engineering and other attacks (38%)
- Implementing automated monitoring and compliance solutions (34%)

REQUIREMENTS

- Fully patched and updated systems (84%)
- Safe password practices (82%)
- Cybersecurity tools that provide consistent protection across cloud and on-premise environments (76%)
- Real-time monitoring and logging capabilities (76%)
- Compliance with data management requirements (76%)

TECHNOLOGIES

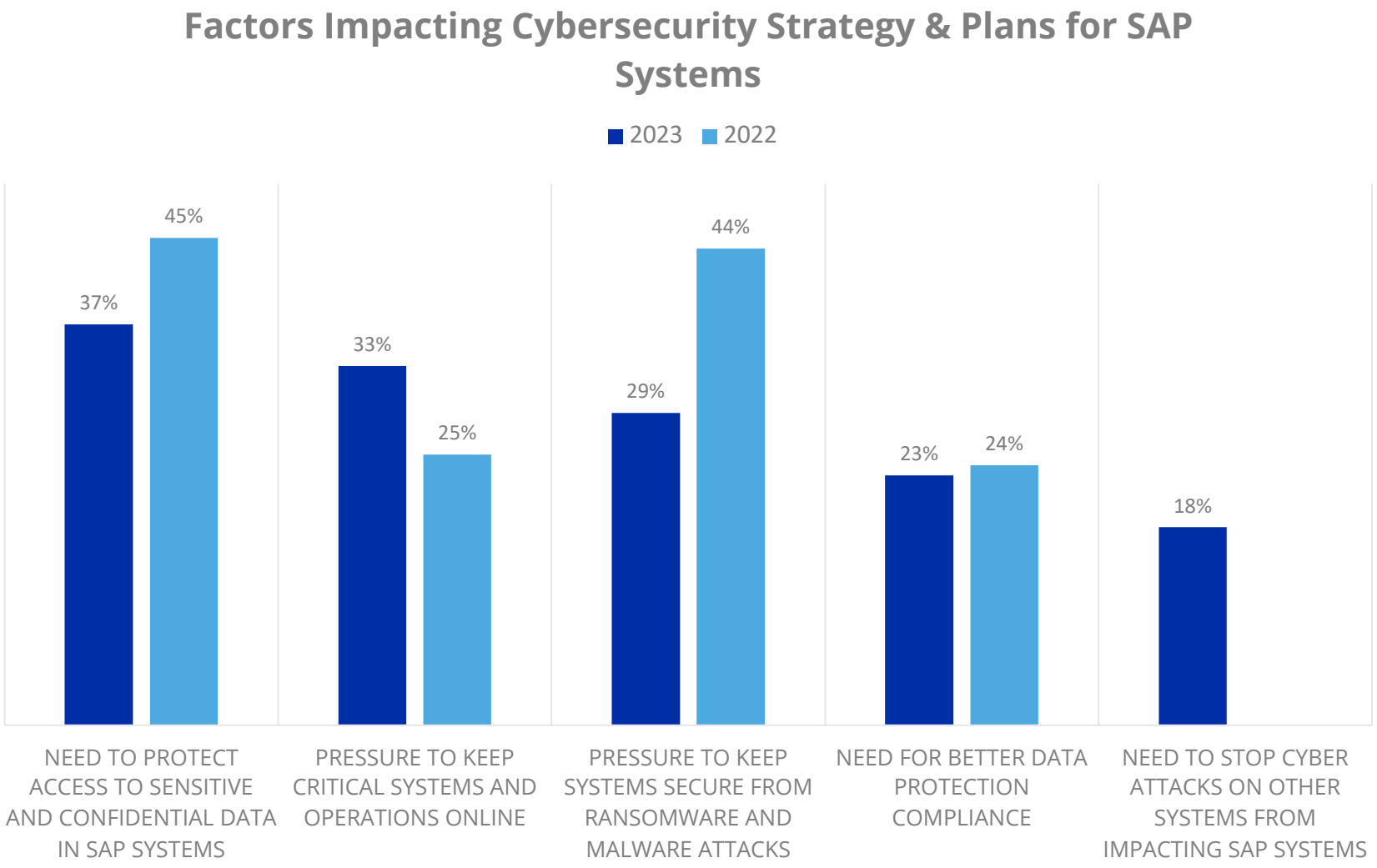
- Encrypted/Secure Connectivity (45%)
- Continuous Monitoring (40%)
- Data Encryption (37%)
- Vulnerability Management (32%)
- Threat Intelligence Feeds (26%)
- Behavioral Analytics (26%)
- Embedded Hardware Authentication (25%)
- UI Masking (22%)
- Code Vulnerability Analysis (22%)
- Zero-Trust Models (16%)

DETAILED FINDINGS

4

These factors indicate the increasing importance of data integrity and availability that is driving security concerns in the SAP landscape. SAP systems must remain available, and the data in them must be protected.

Review data protection, confidentiality, and security strategies and look for opportunities to improve. Data input validation, user access reviews, and data at rest protection can all have a significant impact without major investments being required.

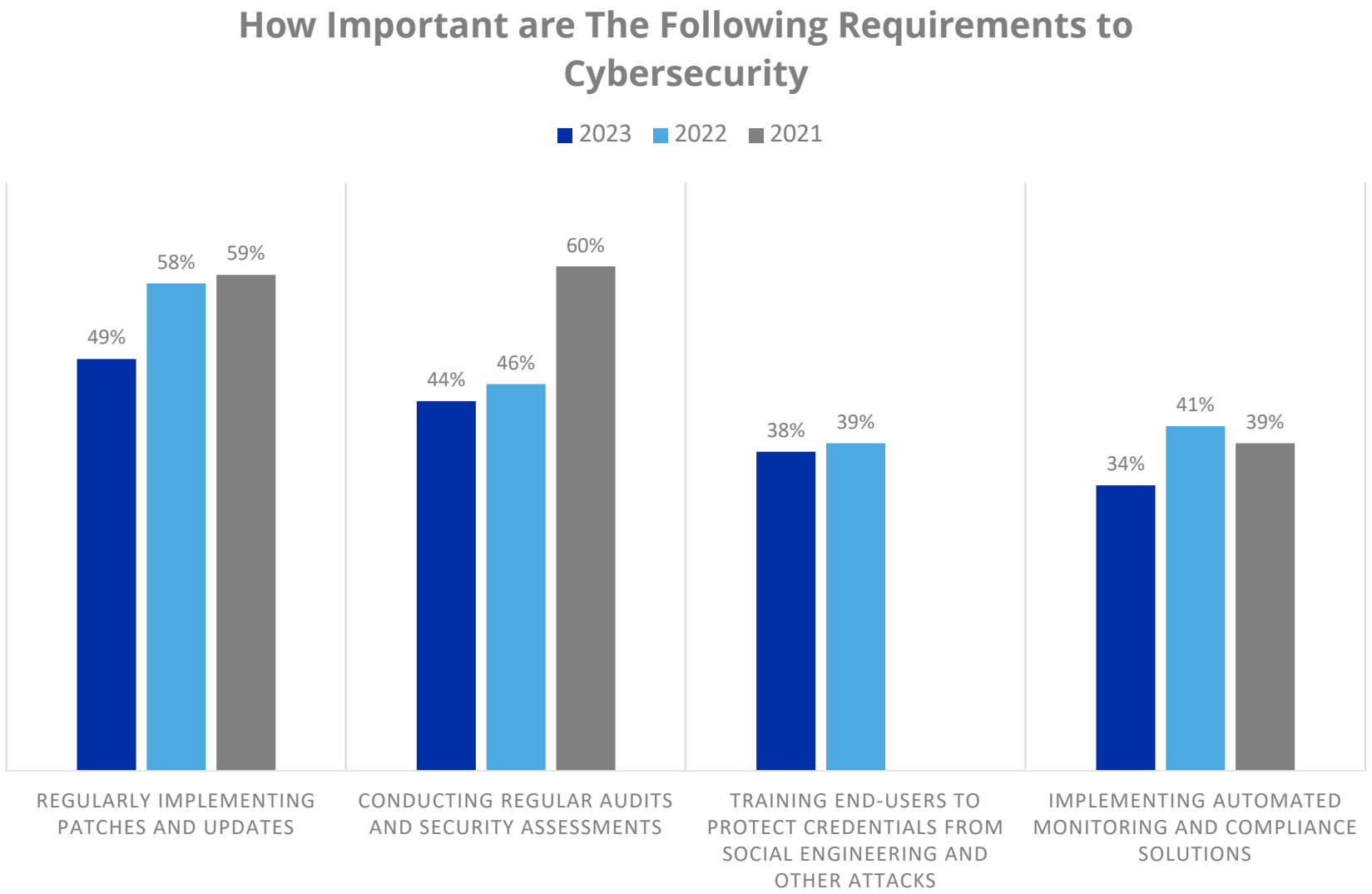


DETAILED FINDINGS

5

Having fully patched systems and being able to protect systems from newly discovered threats before patches are created, demonstrate the importance of patching when it comes to cybersecurity strategy for SAP systems. But ensuring users have safe password practices and data protection compliance are also crucial.

Review data protection, confidentiality, and security strategies, in addition to patching strategy, and look for opportunities for improvement.

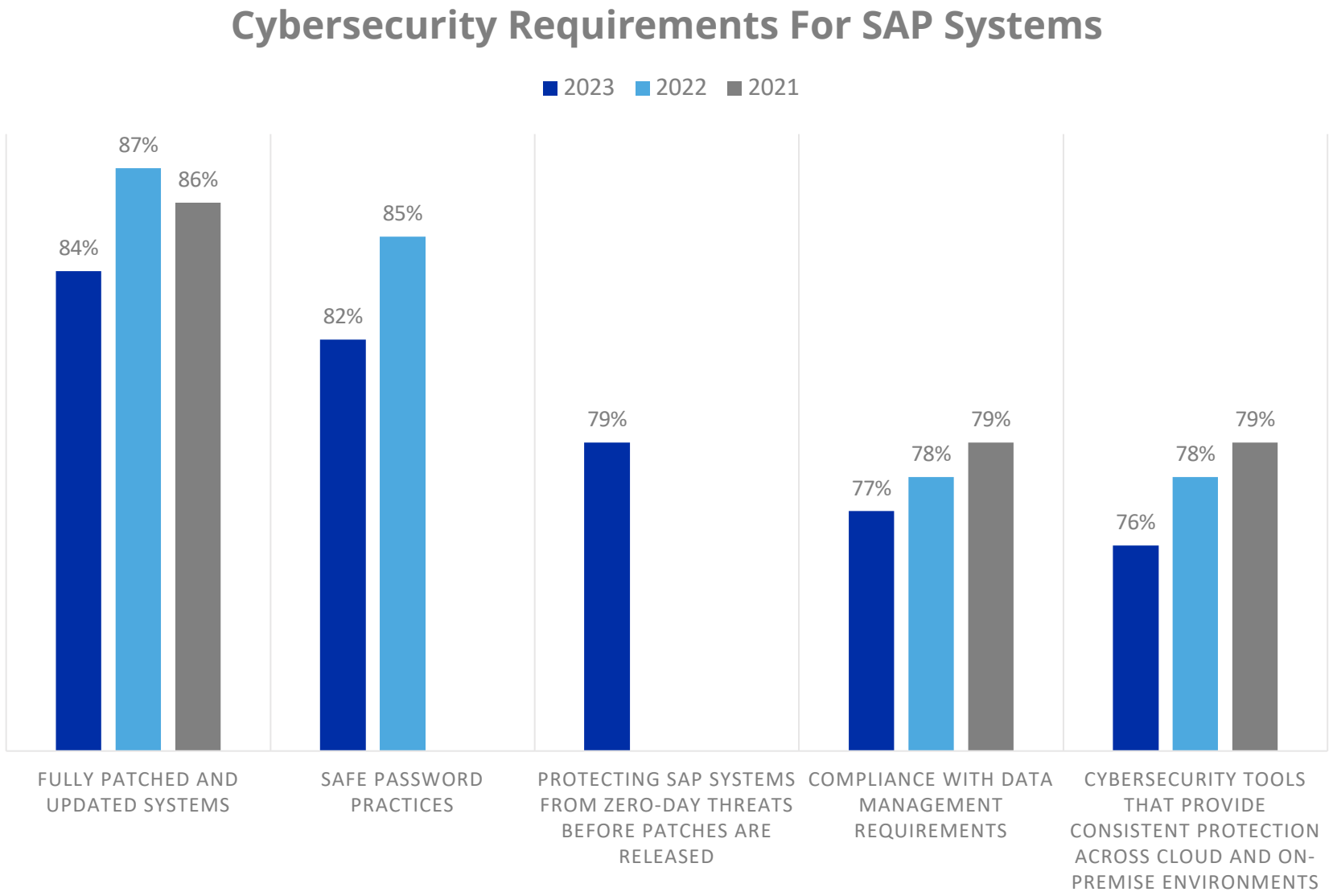


DETAILED FINDINGS

6

Having fully patched and updated systems continues to be the most important cybersecurity requirement for SAP systems for the third consecutive year, with safe password practices being almost as important.

Protecting SAP systems from zero-day threats before patches are released, a new option for 2023, immediately became the third most important requirement showing just how concerned respondents are about newly discovered vulnerabilities being exploited.



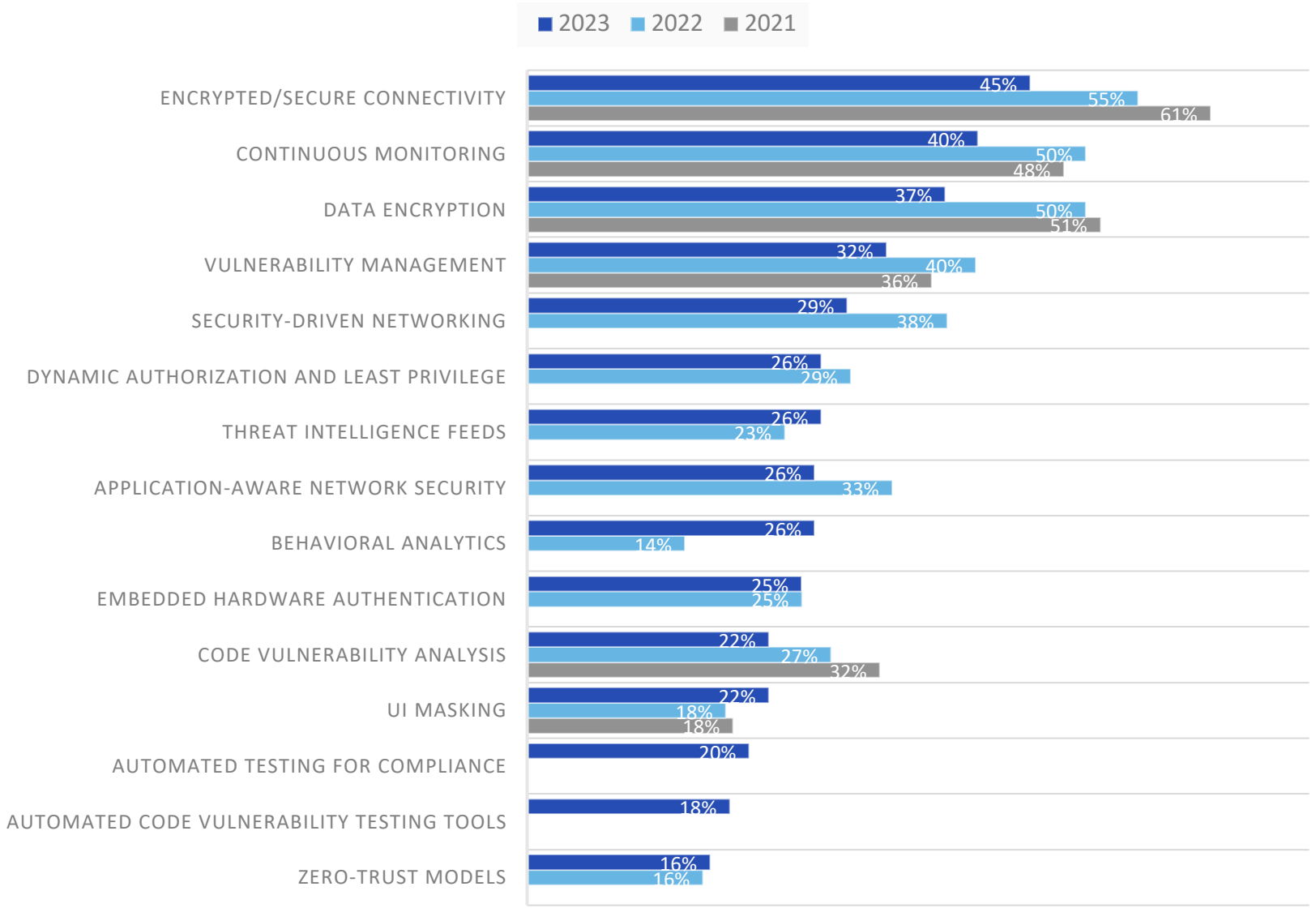
DETAILED FINDINGS

7

This year saw increased usage of technologies that provide information about new threats or help discover attacks that may already be in progress — threat intelligence feeds, behavioral analytics, and UI masking.

Explore these technologies in addition to those that automate tasks like threat detection, application lifecycle management, and patching as they can streamline addressing newly discovered patches and accelerate response to attacks in progress.

What Cybersecurity Technologies Are Currently in Use?

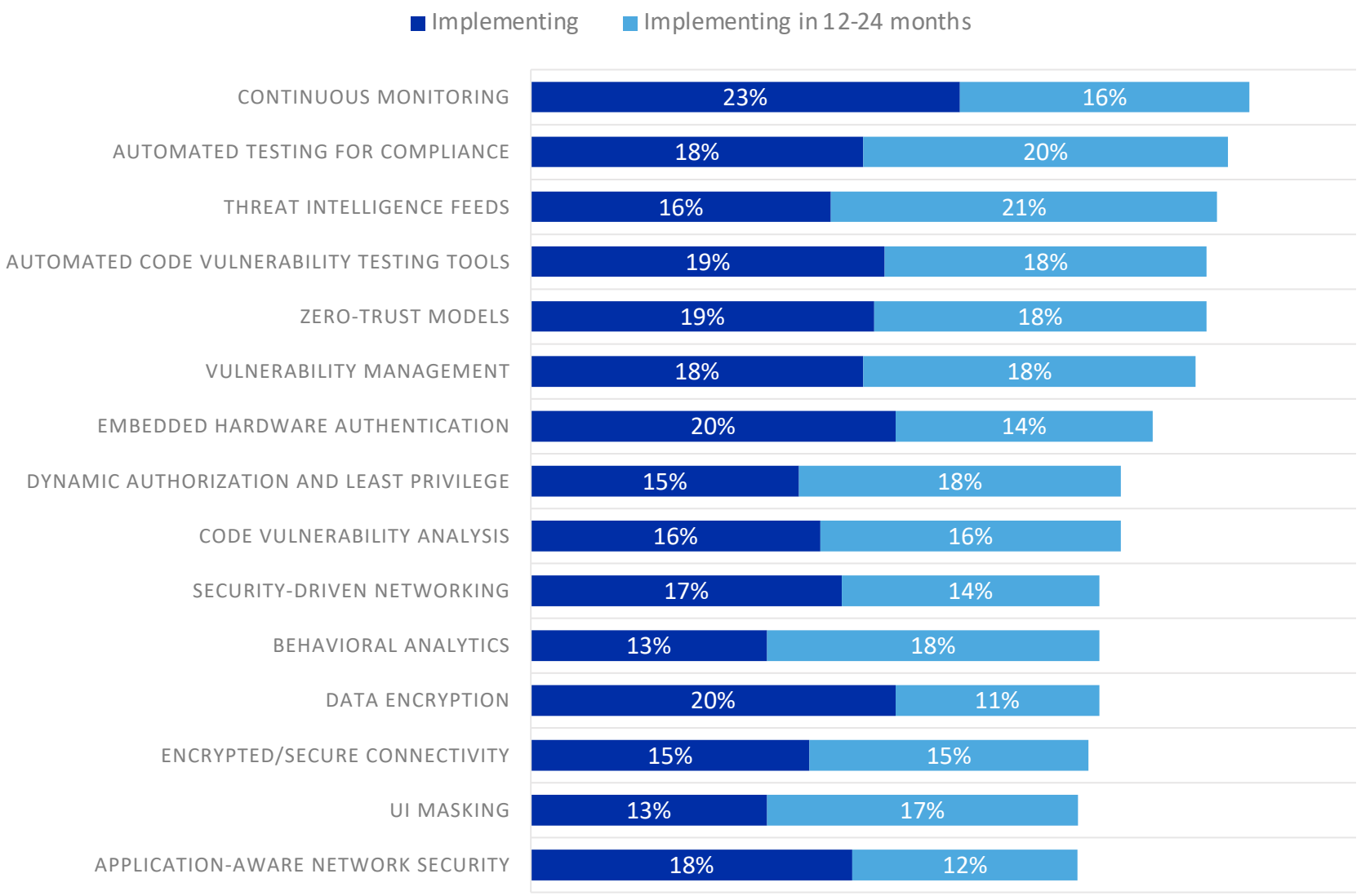


DETAILED FINDINGS

Technologies being implemented reinforce the ongoing shift in focus towards those that provide information about threats or reveal attacks in progress. There is also a move towards tools that help automate security tasks including compliance and vulnerability testing.

Inventory technologies currently available and work to ensure that it is being used to its fullest capacity. Then focus on technologies that can help free up resources for more critical tasks.

What Cybersecurity Technologies Are Being Implemented?

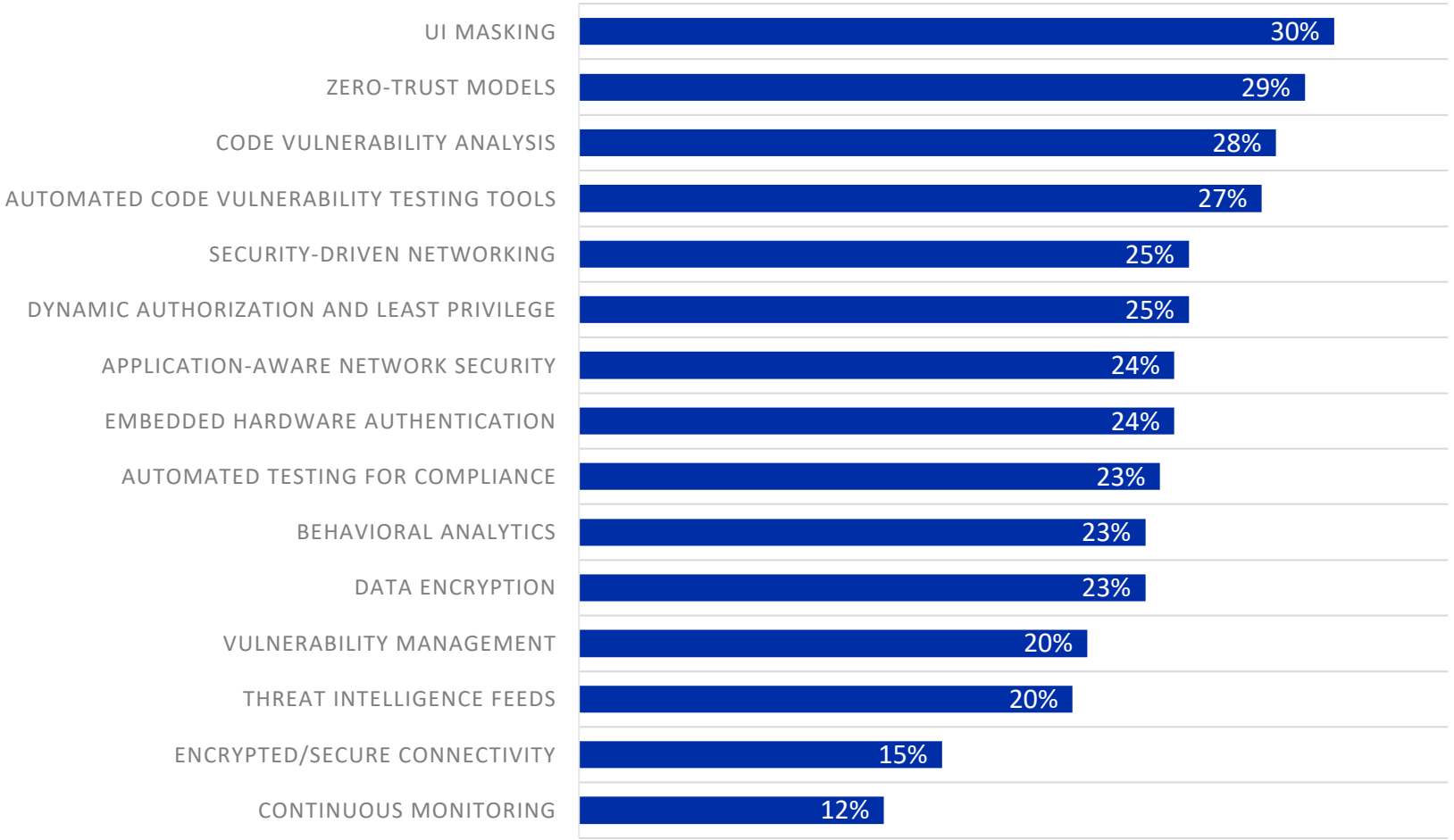


DETAILED FINDINGS

Respondents are shifting towards technologies that will help ensure data is only available to those that should see it. This includes technologies such as UI Masking, but also Zero Trust Models that ensure every device connected to a system or network must explicitly authenticate.

Ensure that future technology plans align with the shift towards accelerated risk management and the shift in SAP landscapes from on-premise to the cloud.

What Cybersecurity Technologies are Being Evaluated?

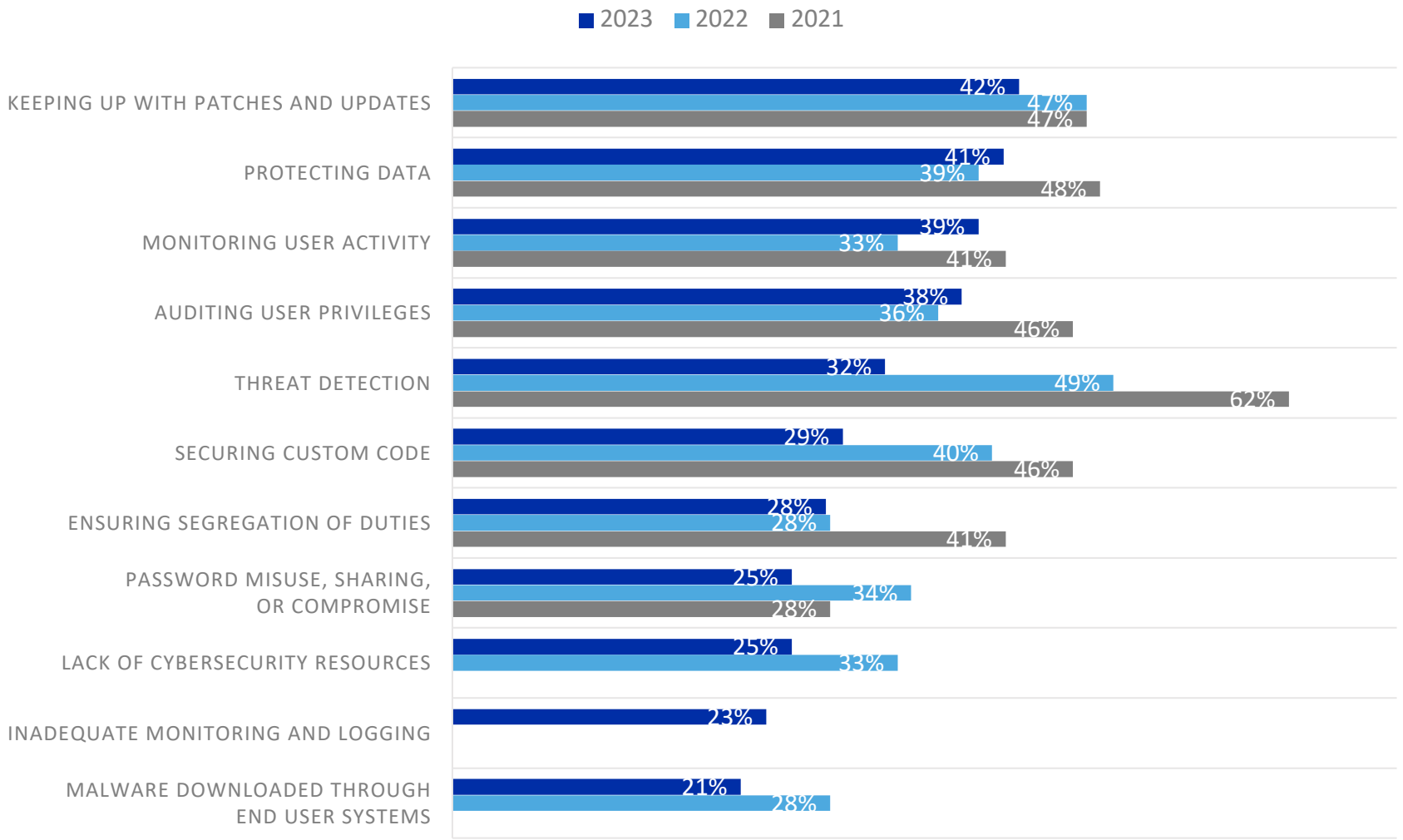


DETAILED FINDINGS

Protecting data in SAP systems was the top factor driving cybersecurity plans for SAP systems, and patching systems was the primary strategy being followed. But these are also the top two challenges being faced by respondents in securing their SAP systems due to the size and complexity of SAP environments.

Keeping systems patched is a key part of protecting data. Align these goals as part of a complete cybersecurity strategy.

What Challenges Exist in Securing SAP Systems?

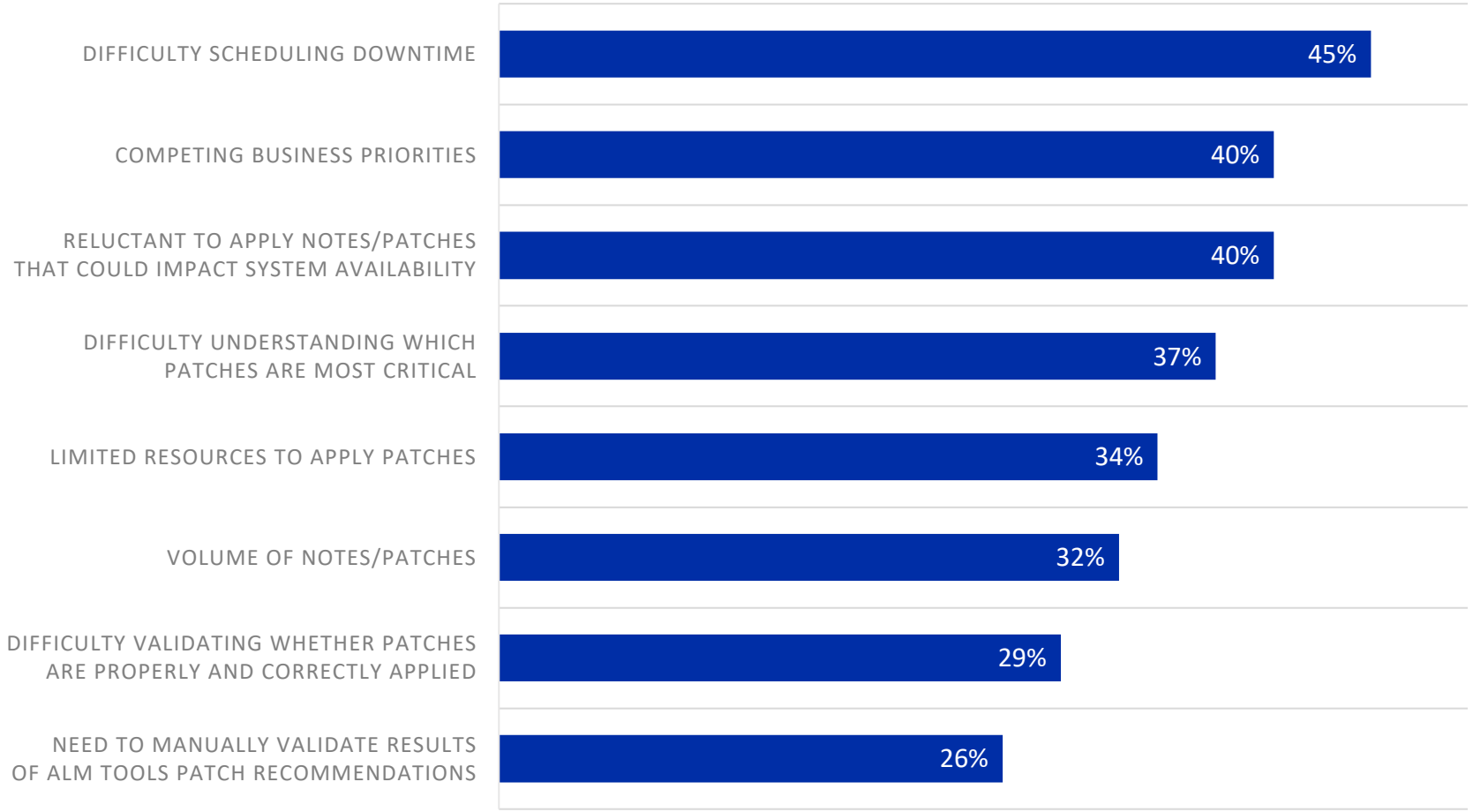


DETAILED FINDINGS

Patching is a complex process, especially for SAP systems. It starts at the hardware level and embedded software updates, progresses through the operating system, virtual machine hypervisor (if applicable), the database, and finally to the SAP solution.

While uptime and business priorities are regularly measured at many organizations, they must be balanced with ensuring that necessary patches are applied. It is vital that organizations have a strong patching strategy if systems are to be effectively protected.

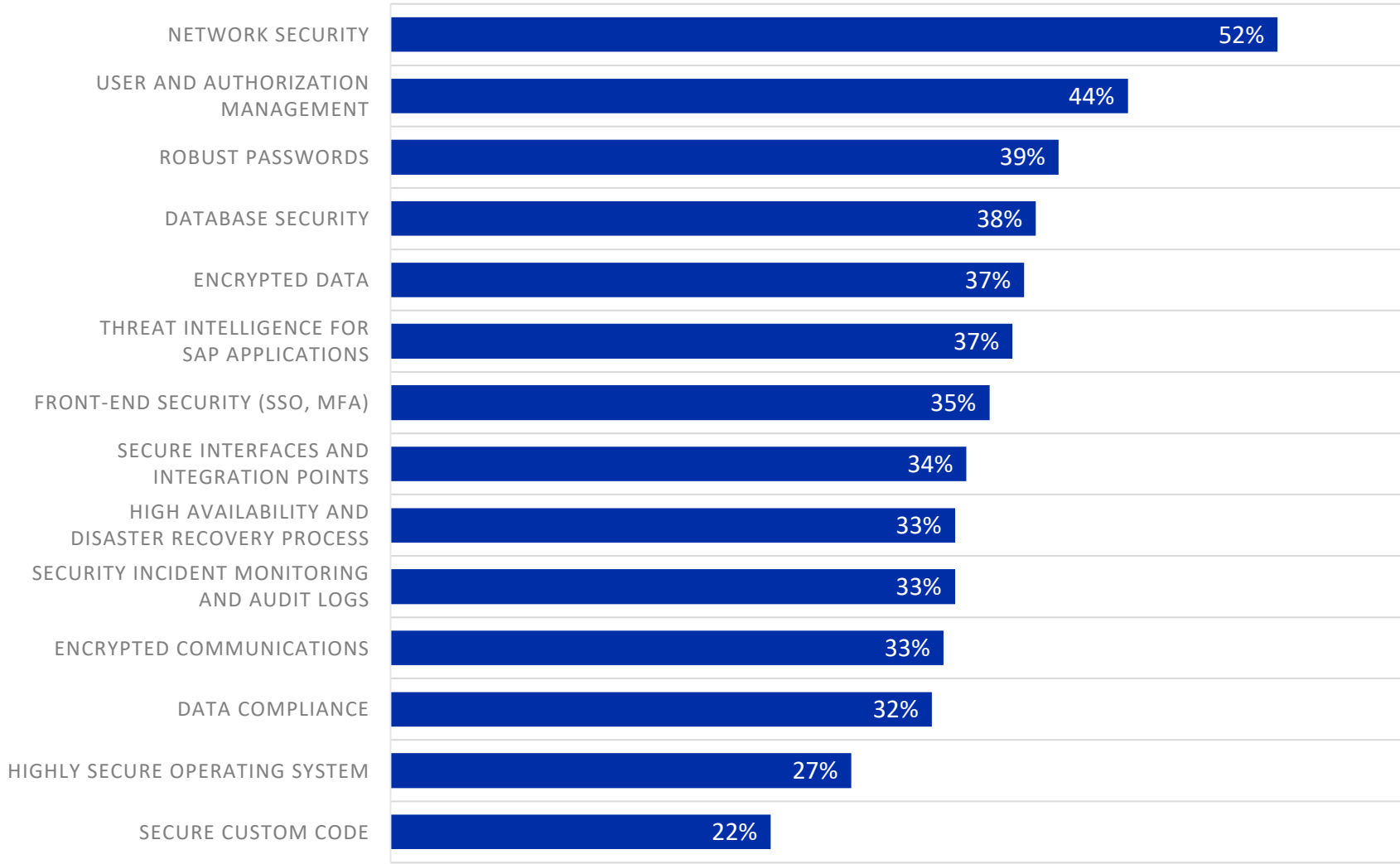
What Issues Lead to a Patching Backlog?



DETAILED FINDINGS

Network security is always the primary cybersecurity defense and keeping those defenses current technologically is a wise use of funds. Managing user access and passwords will protect credentials, limit unnecessary system access, and reduce the likelihood that a threat actor can use a pilfered identity to traverse a wide area of the system. Keeping database security up to date and encrypting data help protects that data from zero-day vulnerabilities, reducing the risk between the time the vulnerability is uncovered and the manufacture can issue the system patch.

What Elements Are Required to Make a Secure Environment?

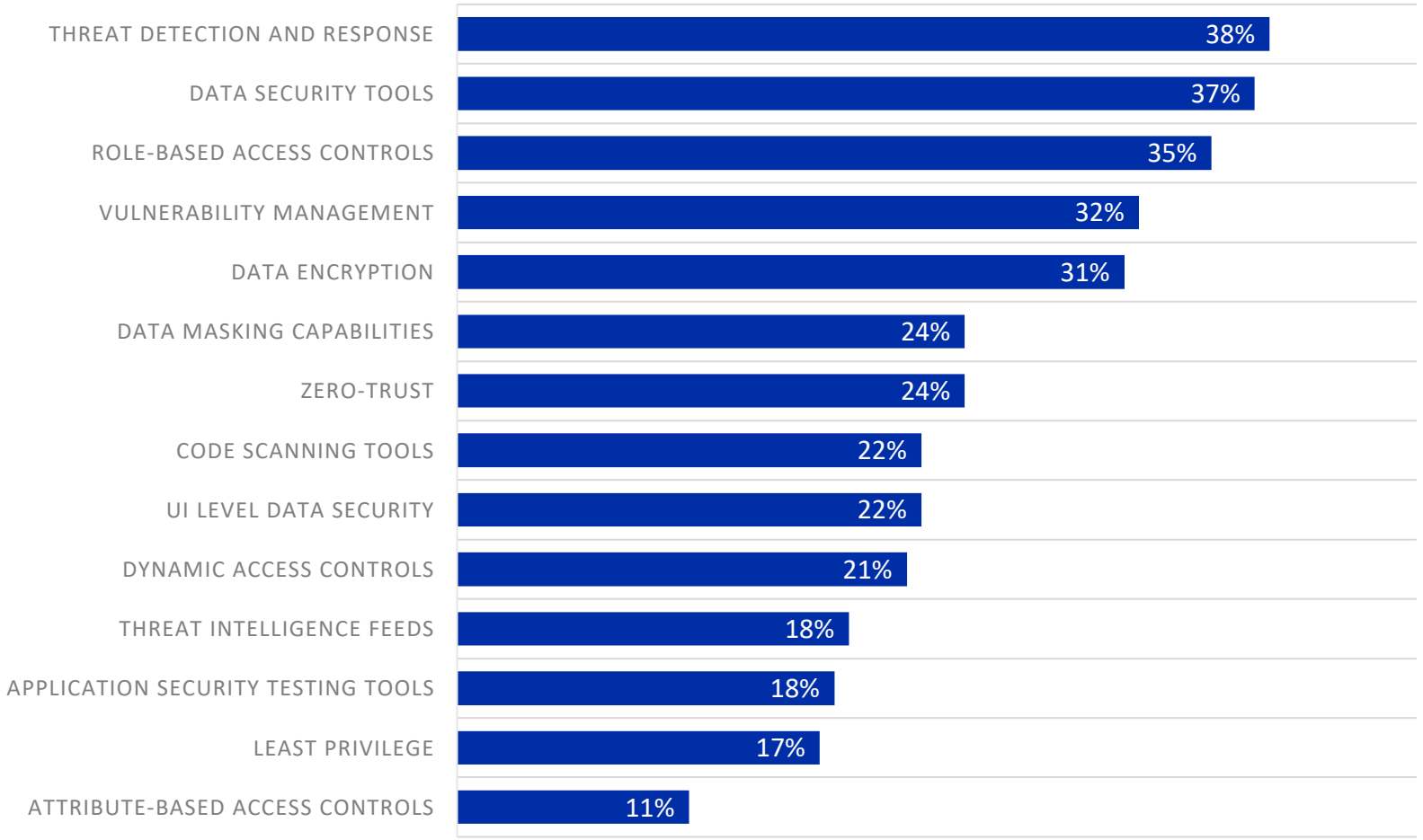


DETAILED FINDINGS

13

Security Information and Event Management (SIEM) tools are a key component in network security. Looking for ways to integrate SAP into a company's existing SIEM tool set can provide elevated protection for the SAP landscape. Integrating SAP logs into the SIEM provides threat detection at the SAP level by identifying unusual activity, major data movement, repetitive failed login attempts, or access during unusual times and days. This can expose compromised credentials, database penetration attempts, data exfiltration, and internal threats such as disgruntled employees and fraud.

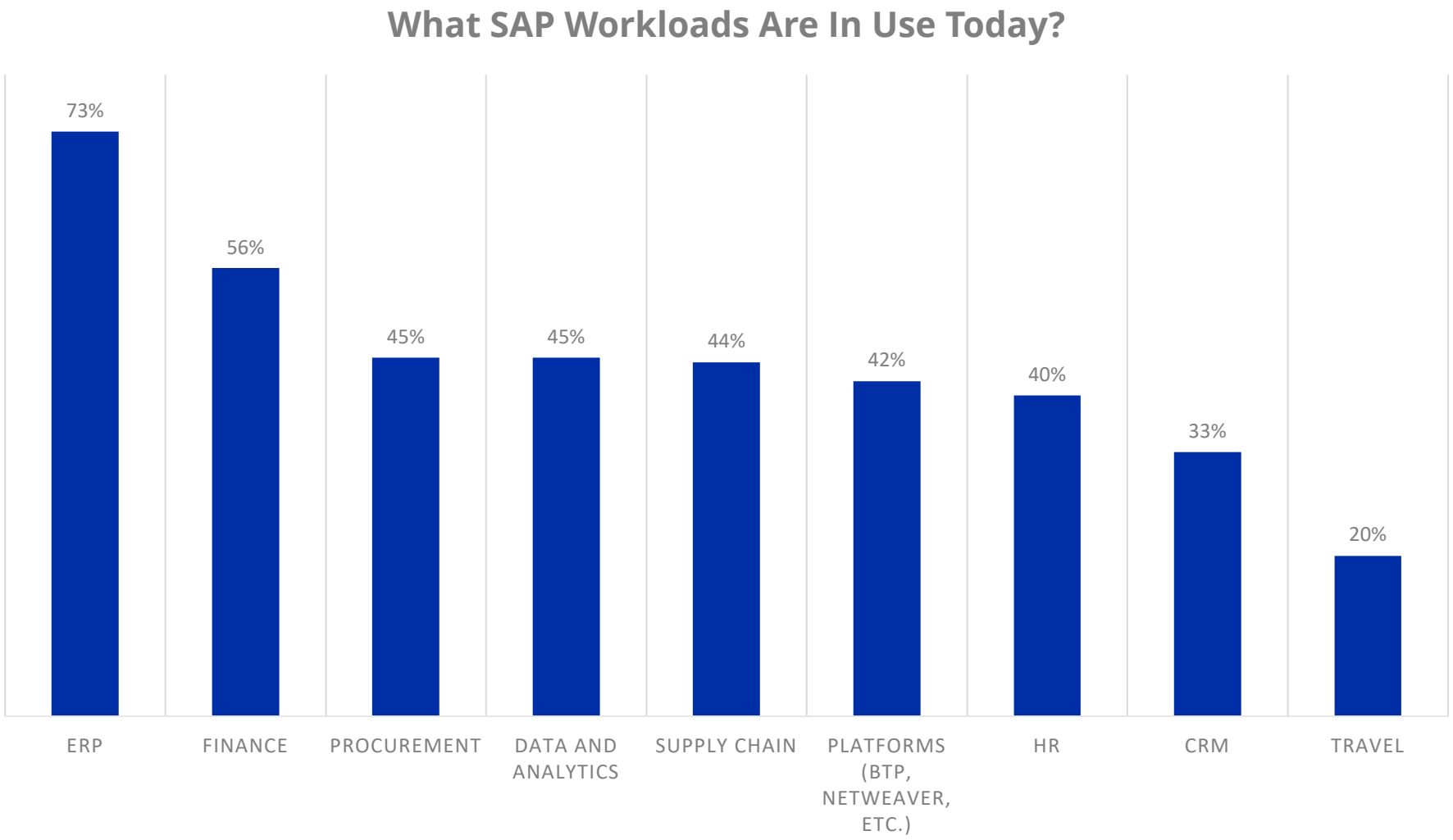
In Which Areas of Security is Investment Planned?



DETAILED FINDINGS

14

Respondents were asked which SAP workloads they were running to gain an understanding of where they were prioritizing cybersecurity efforts.

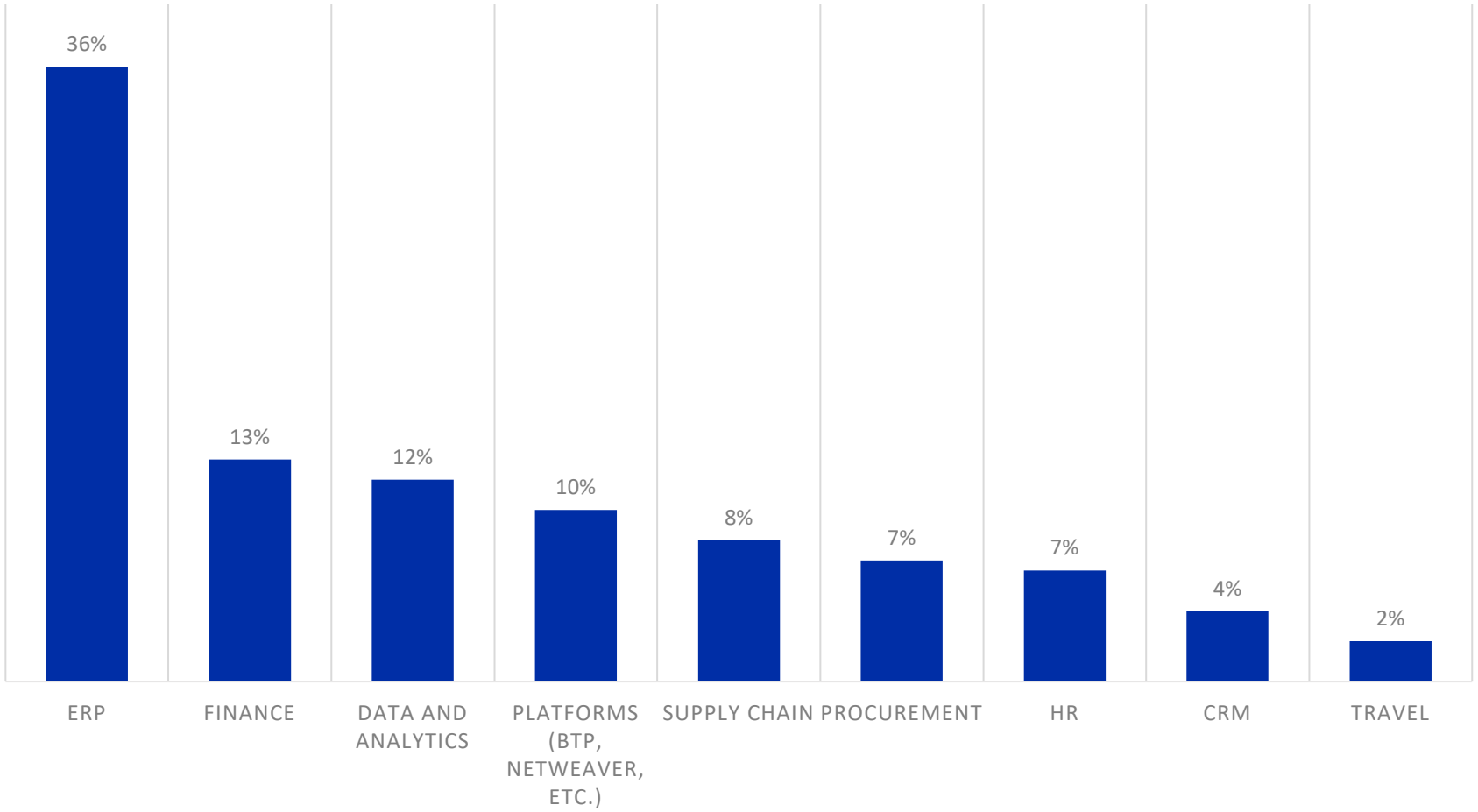


DETAILED FINDINGS

15

Having insight into the workloads in use, respondents were asked which they considered the most vulnerable. The fact that ERP systems were considered the most vulnerable aligns with the most important factor driving cybersecurity strategy in the SAP space — that of protecting access to sensitive and confidential data.

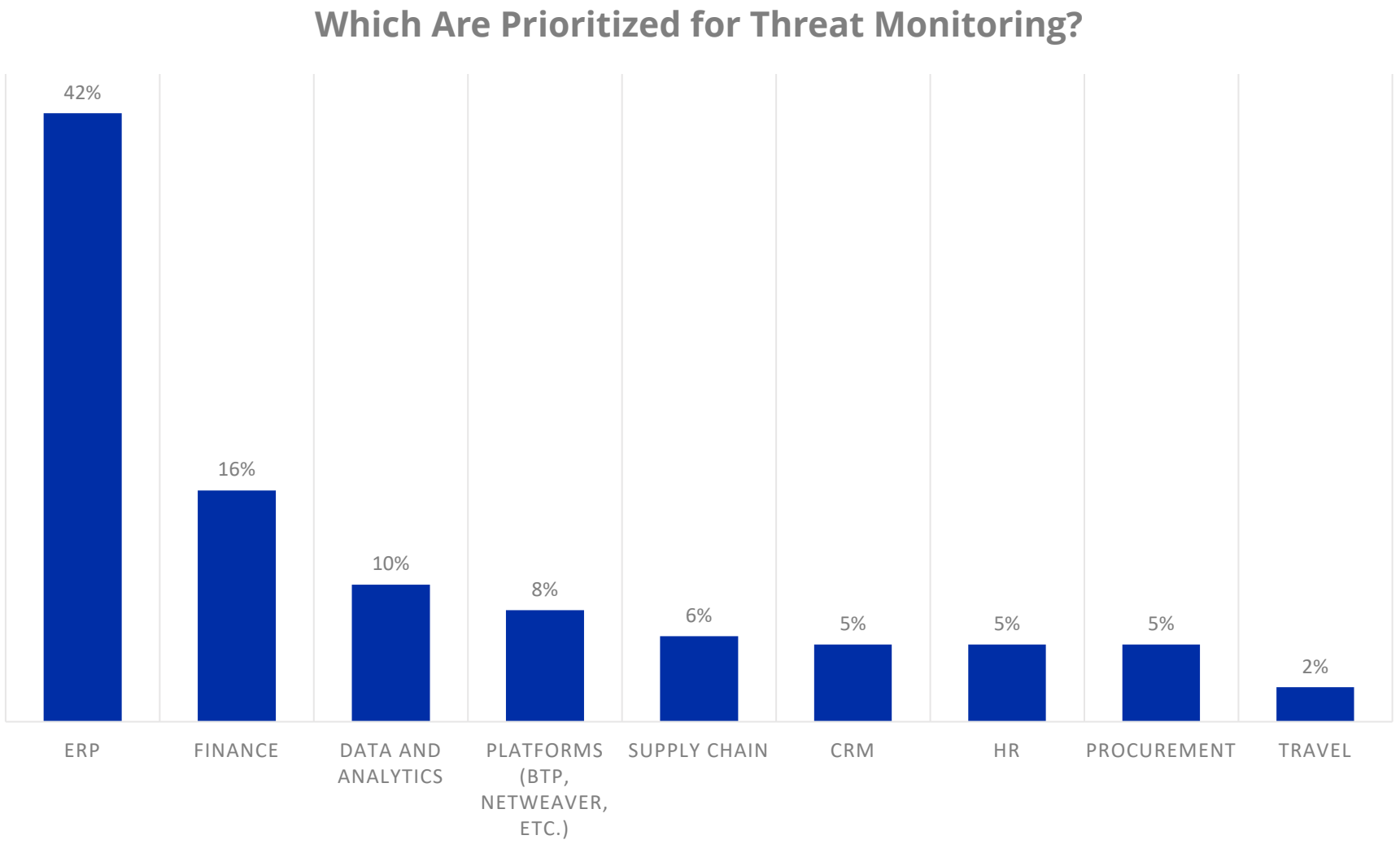
Which Workloads Are Most Vulnerable?



DETAILED FINDINGS

17

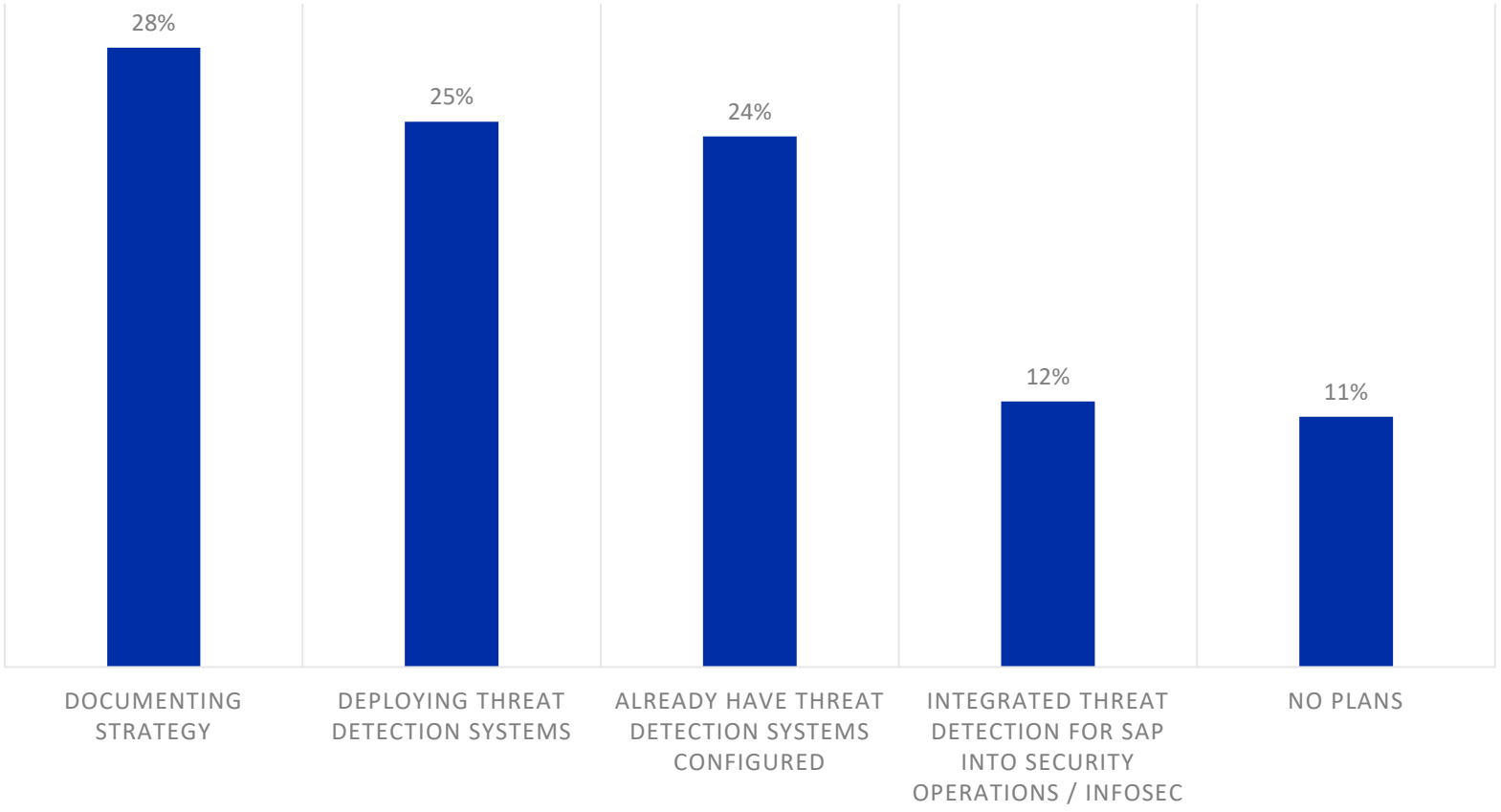
The emphasis on protecting sensitive data in ERP systems is even more pronounced when examining where organizations are prioritizing threat monitoring.



DETAILED FINDINGS

Most organizations are in the process of moving along the path of integrating their threat detection for SAP into their broader security operations environments, although the majority are only in the early stages of that process.

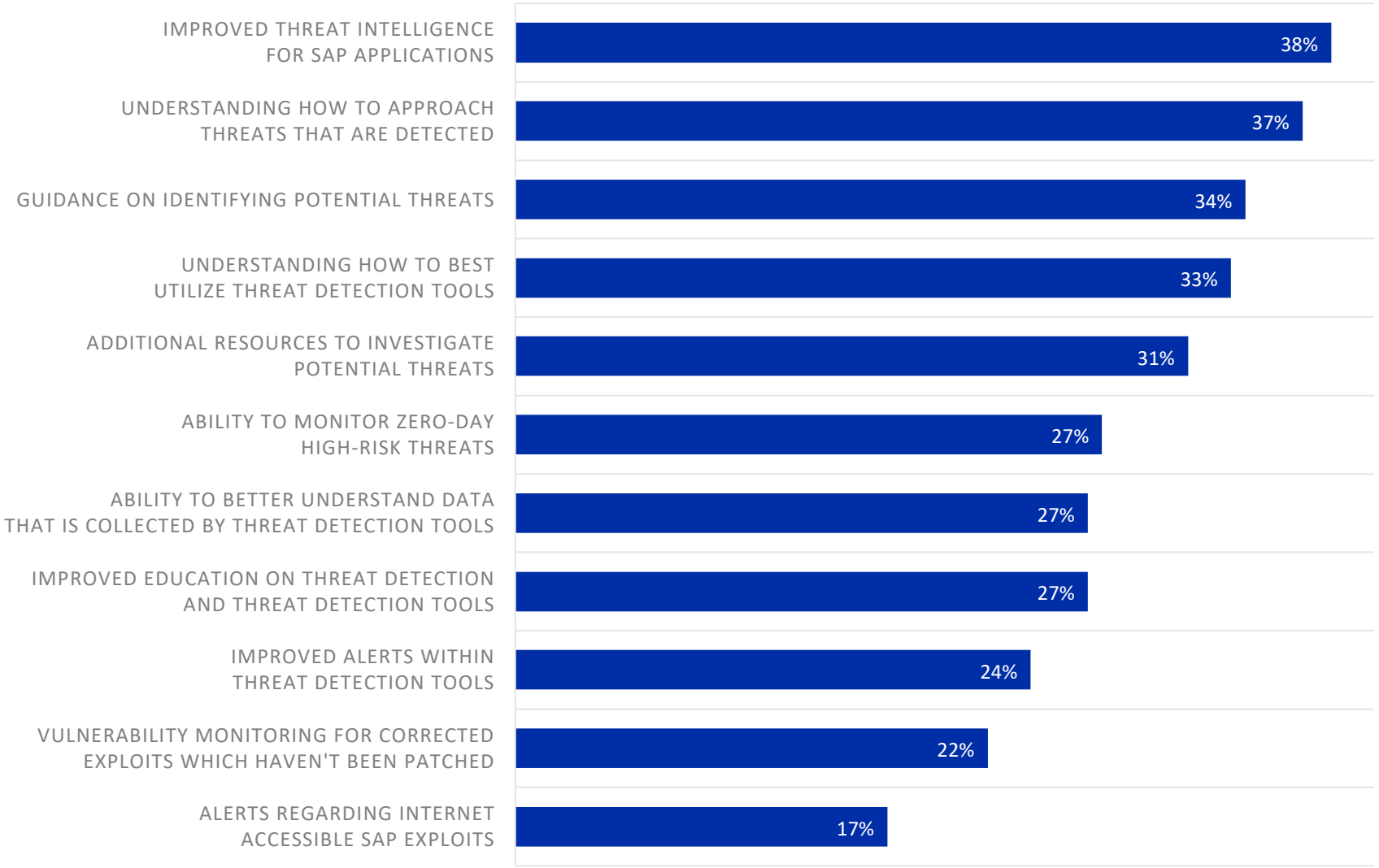
What Stage Has Been Reached With Threat Detection and Response?



DETAILED FINDINGS

Nearly two thirds (62%) of respondents indicated that their organization was experiencing challenges with threat detection across multiple layers of the stack, for example between cloud an on-premise environments. This explains why a major need for threat detection is improved threat intelligence in general.

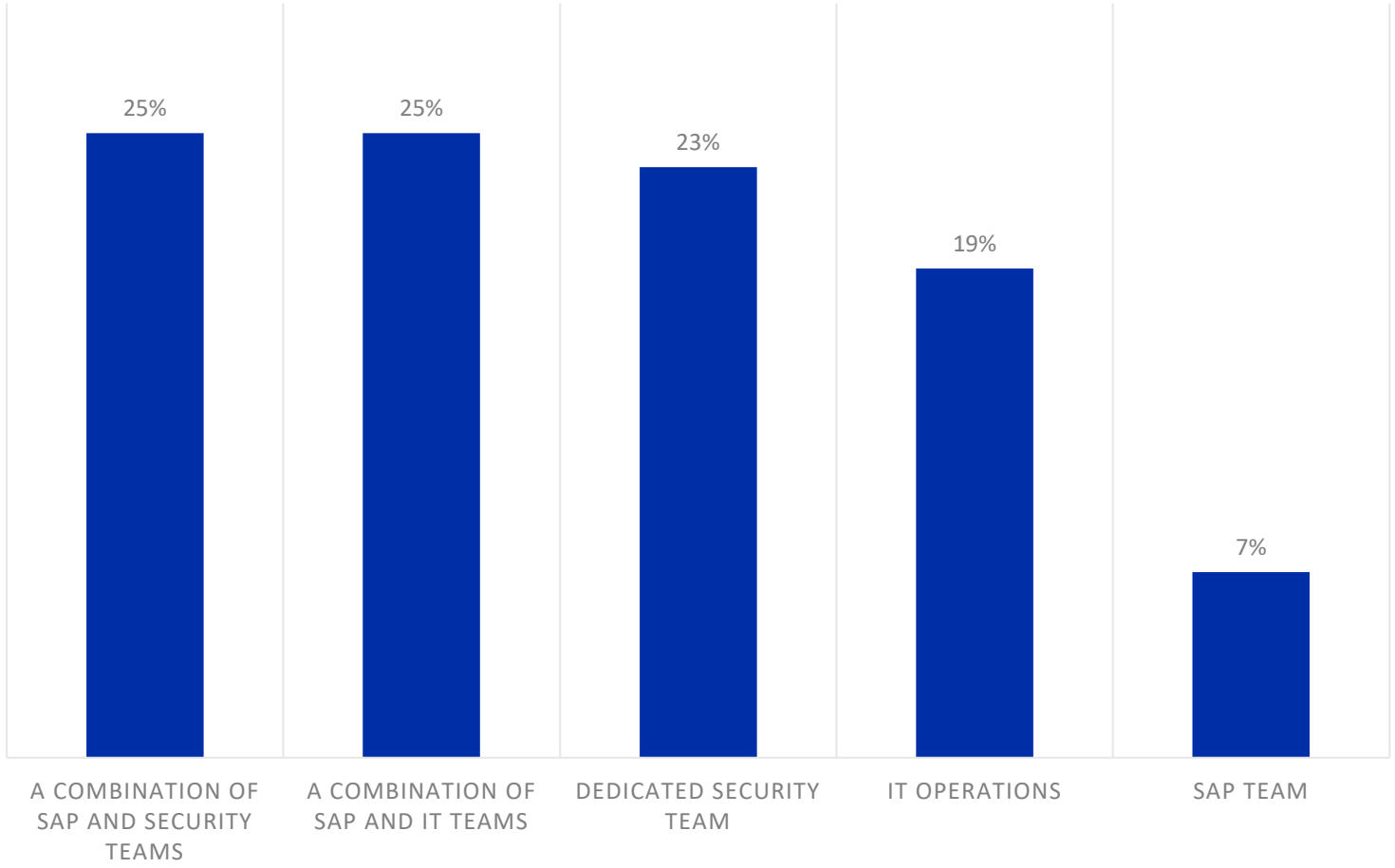
What Needs Exist Regarding Threat Detection?



DETAILED FINDINGS

Historically SAP teams managed the security of SAP systems because security was primarily focused on access and process control. However, even though few organizations now rely solely on SAP teams, for more than half the SAP team still an integral part of overall security management.

What Teams Are Tasked with Securing SAP Systems?



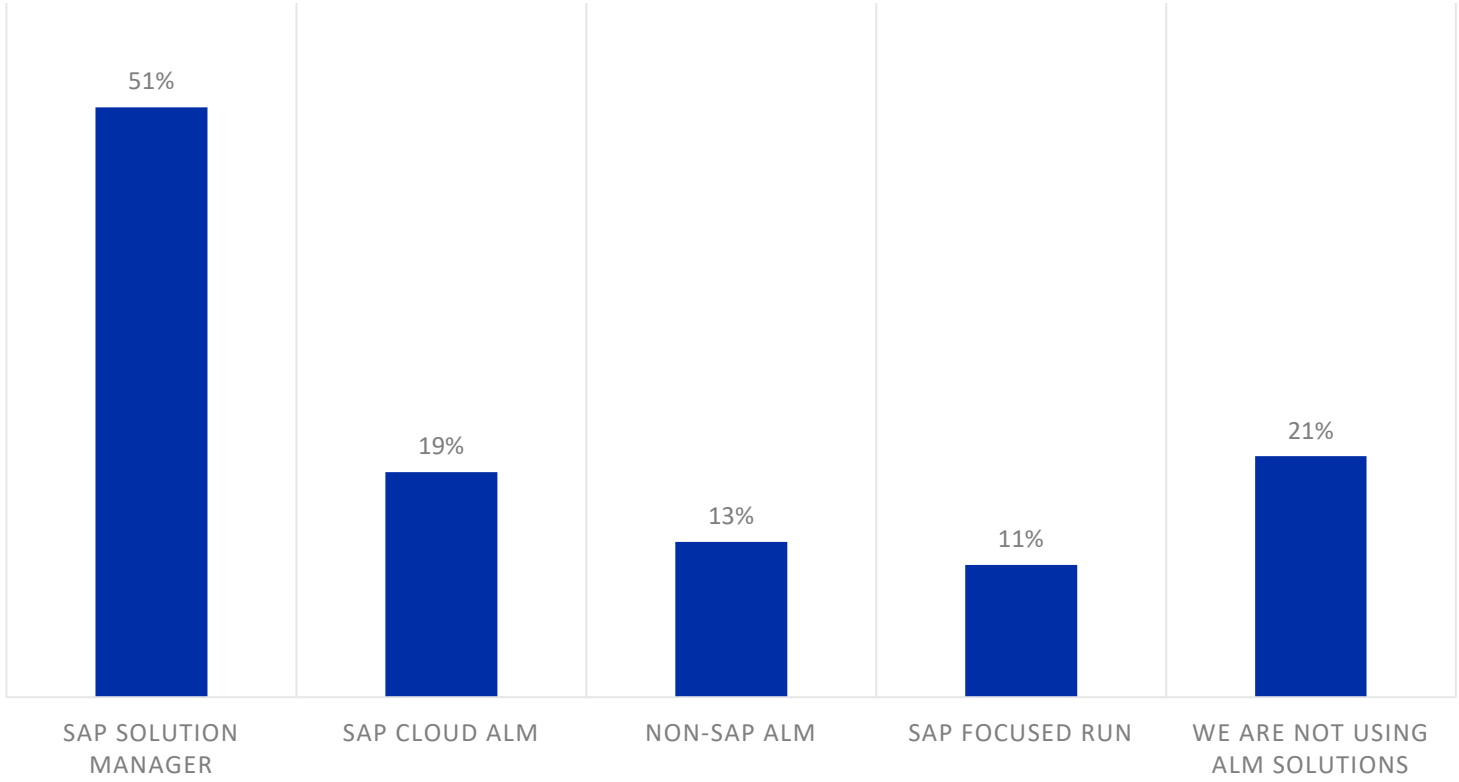
DETAILED FINDINGS

21

Customers that have had SAP environments for more than a few years are likely to be using SAP Solution Manager simply because this is the main tool used to deploy patches and maintain SAP NetWeaver-based environments.

Organizations moving to cloud-based environments need to consider SAP Cloud Application Lifecycle Management (ALM) because SAP Solution Manager does not fully support cloud solutions and environments.

Which Application Lifecycle Management Solutions Are in Use Today?

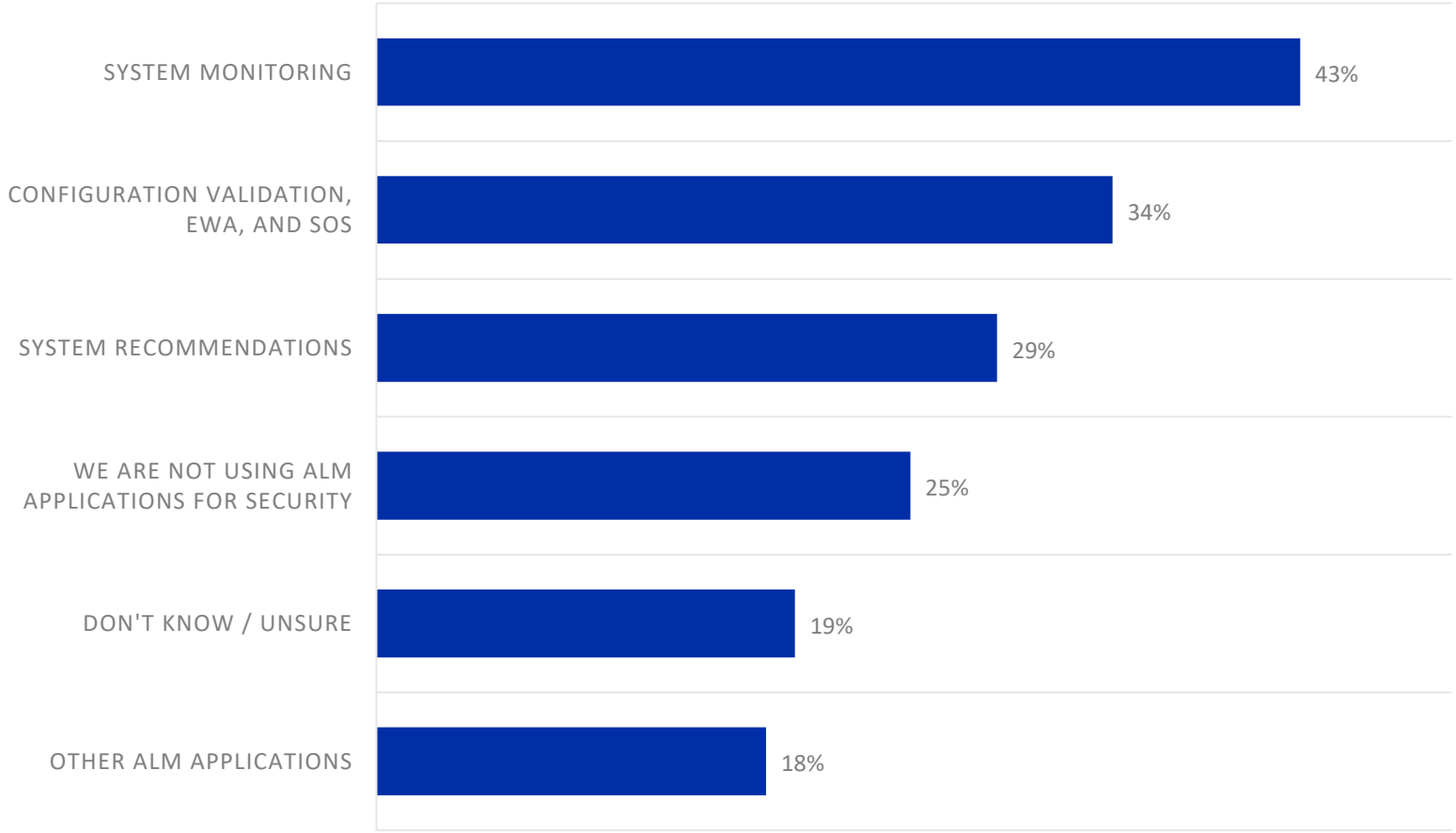


DETAILED FINDINGS

SAP has long encouraged organizations to leverage the features in SAP Solution Manager to monitor their systems, but while the plurality of respondents are using SAP ALM tools for system monitoring, that is still less than half of all respondents.

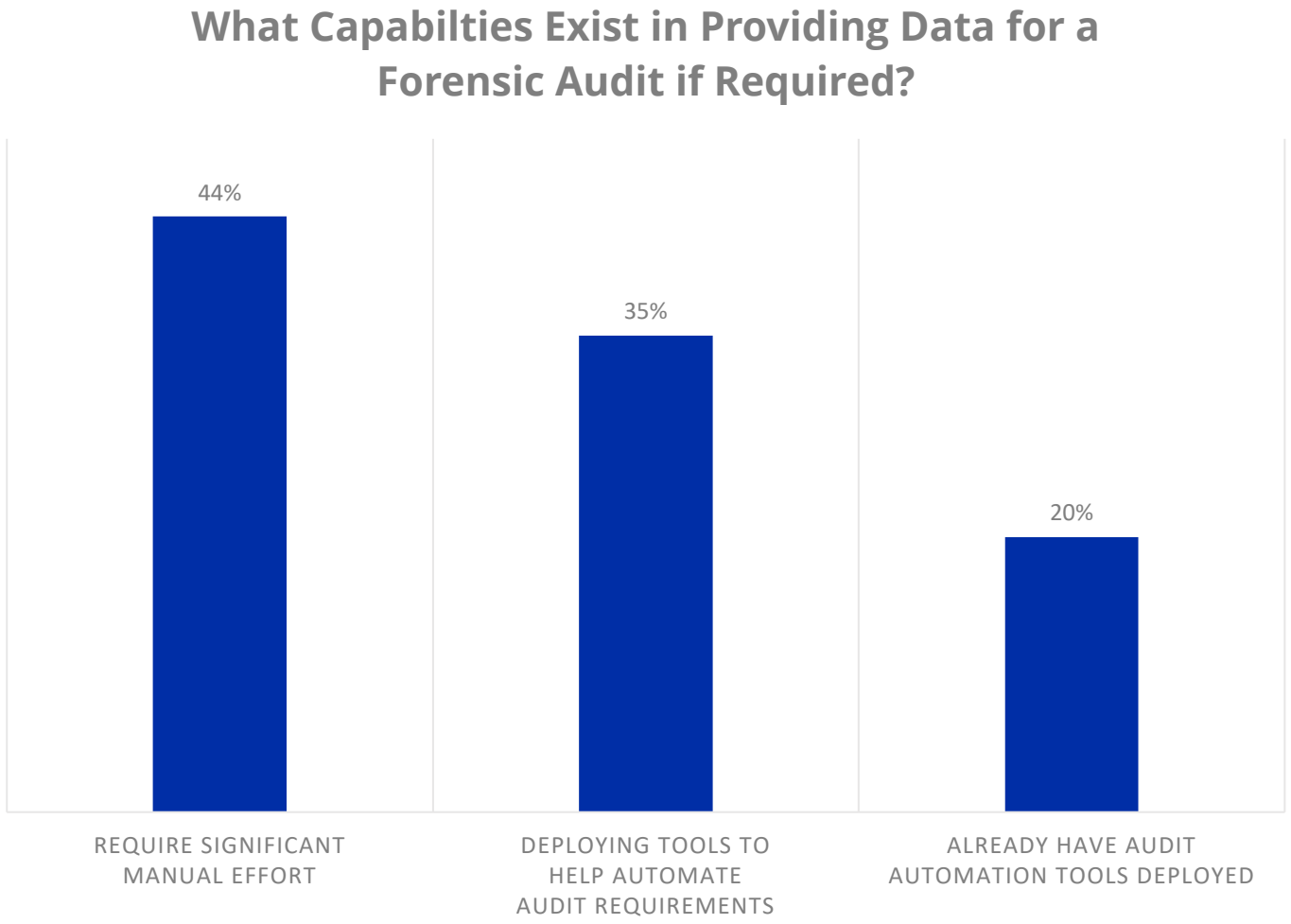
This also correlates with the fact that while 26% of respondents are logging complete user activity data activity for SAP systems, 66% are logging minimal data only and 9% are logging no user activity data at all.

How Are SAP ALM Solutions Leveraged for Security?



DETAILED FINDINGS

Forensic audits are often required to determine how and when a vulnerability may have been exploited, but only one in five respondents indicated that their organization already has audit automation tools deployed. This means 80% of respondent organizations still require significant manual effort for any sort of forensic audit, potentially resulting in significant time and cost investment when an audit is required.



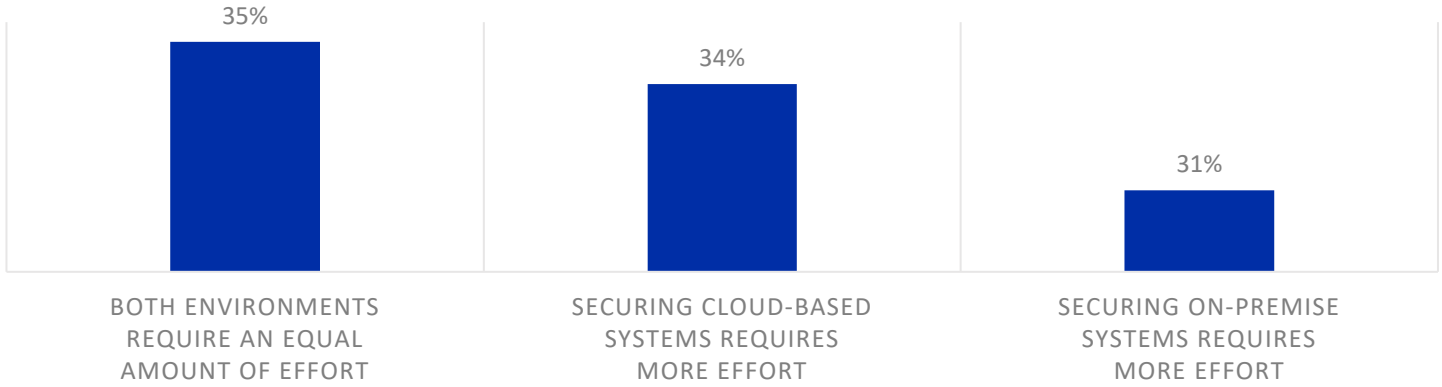
DETAILED FINDINGS

Respondents were largely equally split on whether securing cloud or on-premise environments required more effort, but nearly one in two planned on managing that security using internal teams.

Over a quarter expected that all security would be managed by their provider, which could be problematic unless they are using software-as-a-service solutions.

What Are The Security Expectations from Cloud and Service Providers?

How Much Effort is Required to Secure Systems?

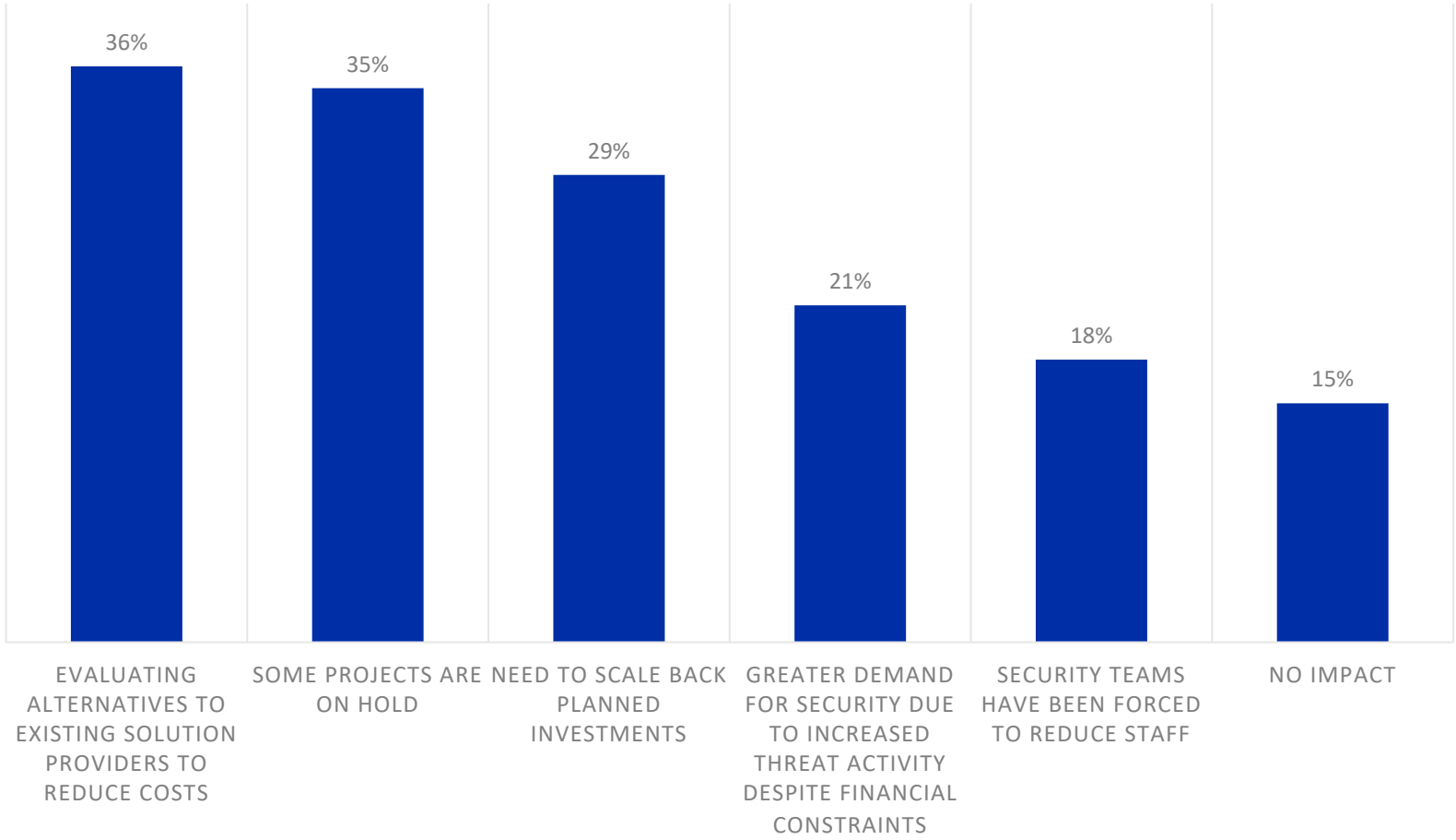


DETAILED FINDINGS

More impact than expected is being seen from the current economic climate on the security objectives of respondent organizations. Only 21% of organizations say that they are seeing a greater demand for security due to increased threat activity, with another 15% seeing no impact.

The most likely impact is that of some projects being put on hold or a desire to switch or consolidate solutions or providers in an effort to reduce costs.

How Are Security Objectives Being Impacted by the Economic Climate?

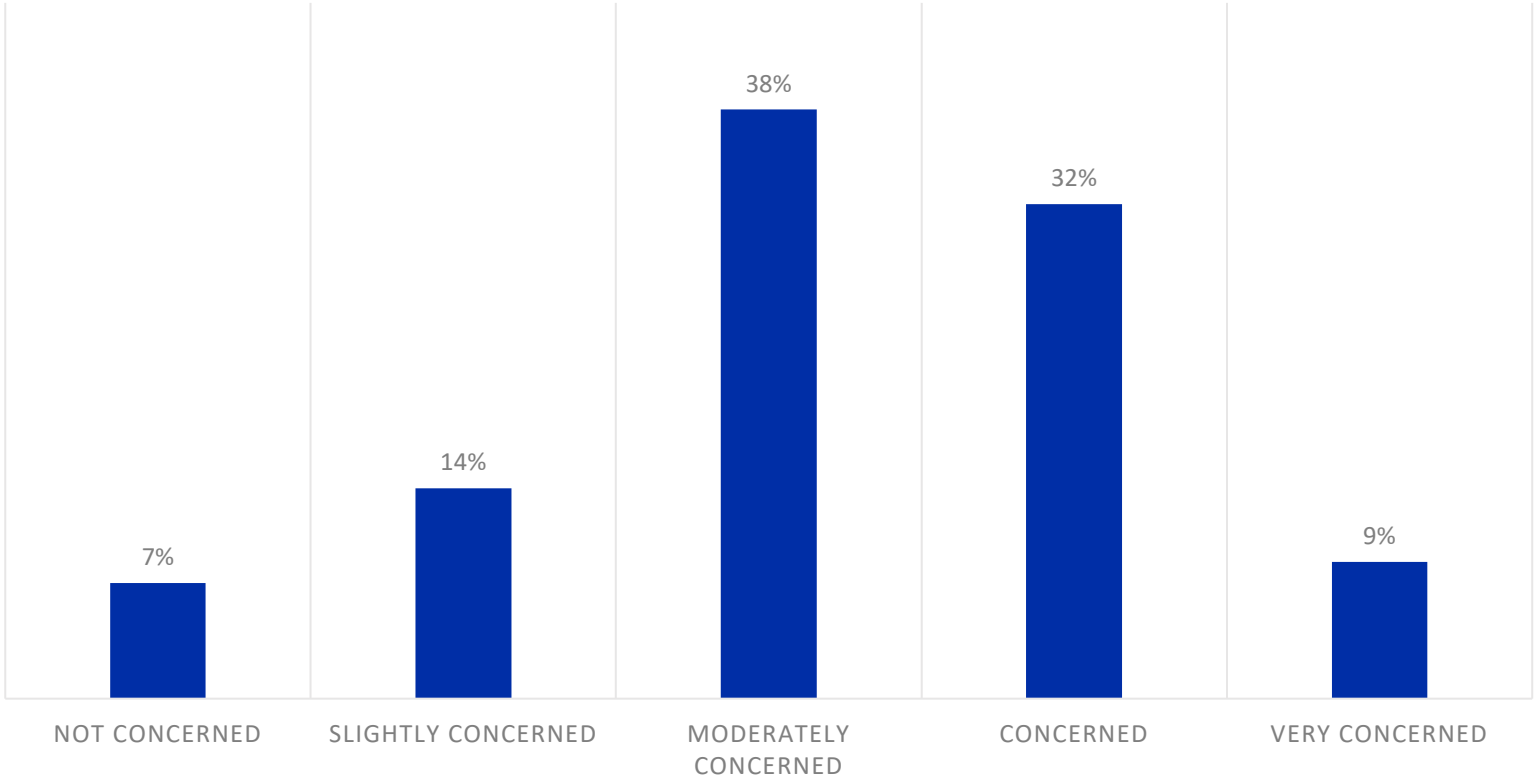


DETAILED FINDINGS

Four in ten (41%) of respondents indicated that they were concerned or very concerned about managing vulnerabilities in open source components provided by their software vendors.

An additional 38% indicated that they were moderately concerned about managing these vulnerabilities.

What Concerns Exist About Managing Vulnerabilities in Open Source Components?



DETAILED FINDINGS

27

The proportion of respondents experiencing the impact of different types of attacks on their SAP environments is largely consistent with 2022, although there is a slight increase in those experiencing the impact of a credentials compromise or social engineering attack. Given that accessing the data in SAP systems can be more valuable than impacting those systems with malware, it is not surprising that these types of attacks are slightly more commonly experienced.