JULY 2026

SAPinsider

Intelligence Benchmark SERIES

Benchmarking the Capabilities that Define SAP Leaders

Cybersecurity Threats and Challenges to SAP Systems 2026

By Robert Holland
Chief Research Officer

RESEARCH PARTNER
SAP

SPONSORED BY
ONAPSIS

Executive Summary

Cybersecurity threats have become more prevalent than ever. In fact, cybercrime now accounts for nearly a third of all offenses in some regions. Moreover, 2025 represented the greatest number of high impact or critical patches ever released by SAP as flaws were discovered in ageing solutions that are often now more exposed than ever in cloud-based environments. The increased use of AI both inside enterprise landscapes and by malicious actors only makes it more important to ensure that the valuable data in SAP systems is effectively secured.

To provide insights into how SAP customers are thinking about cybersecurity today, SAPinsider surveyed its community between April and June of 2026. This year, to provide increased insight into the cybersecurity maturity of organizations, respondents were asked three questions and were scored based on their responses. The assessment started by asking about overall cybersecurity maturity and posture with a specific focus on SAP. Respondents were asked to indicate whether their cybersecurity teams were proactive and well-funded with strong executive support and full visibility across infrastructure, applications, and data, if they had increased investment and maturity of people, process, and technology across multiple security domains, whether they put core protections in place but were primarily focused on regulatory compliance, or if their cybersecurity strategy was mostly reactive and secured critical systems only.

Respondents were also scored on how frequently their organization performed security validation for their SAP environment. Answer choices included:

- Having automated tools that monitor and validate security posture daily.
- Conducting deep-dive scans or audits on a monthly cycle.
- Quarterly validation or staying in alignment with SAP Security Note release cycles.
- Comprehensive annual assessments or third-party penetration tests once per year, only after major system upgrades, migrations, or deployments, or having no formal schedule at all.

Lastly, respondents were asked about the level of automation in their SAP cybersecurity operations. This with fully automated environments with security monitoring, threat detection, and compliance monitoring received the highest score on the assessment, while those with some automation that still requires manual attention for response and remediation, partial automation that still includes manual audits, or entirely manual security processes received proportionately lower scores.

Respondents with the highest scores were more likely to have an increased level of cybersecurity investment and maturity of people, processes, and technology across multiple security domains. These respondents were the most likely to be using continuous or real-time security monitoring that validates their security posture at least daily. And while some had fully automated security systems, it was most likely that these cybersecurity leaders had mostly automated monitoring but still required manual intervention during the response and remediation phases. These represented 30% of respondents.

Those with the least mature cybersecurity strategy, referred to as security beginners, were the most likely to have core protections in place but were primarily focused on regulatory compliance with limited advanced cybersecurity capabilities. These respondents (25%) were also most likely to be doing ad-hoc validation and using either manual or partially automated cybersecurity processes. The remaining 44% of respondents represent a majority group.

One of the most important questions asked to respondents was about evaluating the top cybersecurity threats in order of importance **(Figure 1)**. This year, rather than comparing the data to previous years, the list compared how those at different cybersecurity maturity levels were evaluating these threats. For example, social engineering attacks were rated the biggest threat by both cybersecurity leaders and the majority group. On the other hand, cybersecurity beginners were most concerned about credentials compromise. However, respondents of all maturities rated connections to other systems or applications and ransomware attacks as highly important. Only the majority group rated insecure application configurations as more important than those two potential threats.

INSIDER
INSIGHT

"As we have completed our digital transformation initiatives, our SAP systems have become more connected than ever. They are integrated with other enterprise systems, cloud platforms, as well as external partners and suppliers. This has expanded our attack surface and provided more entry points for potential intrusions. This is why we must protect against intrusions at every connection point because one breach can quickly spread across the network and compromise our entire ecosystem."

—SECURITY LEAD, TECHNOLOGY COMPANY

FIGURE 1

Top Cybersecurity Threats to SAP Systems

While still important, the threat of data exfiltration is now eighth on the list for security leaders. It is also no more important for other groups despite being the most important threat last year, suggesting a shift to 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. More than half (51%) the respondents to this year's survey reported that they regarded the business processes and data supported by their SAP applications as mission-critical with highly confidential data and that any disruptions would severely impact revenue, operations, or compliance obligations. Another 44% report that these systems and processes are highly important with sensitive data although, while problematic, disruptions would be manageable. This makes protecting these processes and data vital.

Still, the focus is on credentials and connectivity-related threats, which is reflected in the factors most responsible for driving cybersecurity strategy and plans **(Figure 2)**. Given that these types of attacks can develop from an initial incursion to a broad penetration in a matter of hours. it is no surprise that they are in the spotlight. However, 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%).

37%

of respondents report that protecting access to sensitive a nd confidential data is the biggest factor influencing their cybersecurity strategy and plans

FIGURE 2

Factors Driving Strategy and Plans for Cybersecurity for SAP

Despite the seeming contradiction, protecting the data in SAP systems has been the most important factor driving cybersecurity strategy for four of the last 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 that are stored in SAP systems.

The other factors impacting cybersecurity strategy for security leaders include the pressure to keep systems secure from ransomware and malware attacks (31%), , a need to stop cyber attacks from other systems impacting SAP environments (23%), pressure to keep critical systems and operations online (23%), and a need to secure systems that are transitioning to the cloud (23%). Except the the last factor, these are the same reasons that were driving cybersecurity strategy last year. The difference this year is that security leaders placed a much greater emphasis on protecting the data in their systems and protecting systems from ransomware and malware attacks, while last year both those factors received equal weightage from respondents.

For the majority group, the single most important factor is keeping systems secure from ransomware and malware attacks (50%). This is followed by protecting the data in their SAP systems (33%). Interestingly, the next most important factor driving cybersecurity strategy for this group was that of keeping critical systems and operations online (22%). No other factor received more than 17% of responses, demonstrating that these respondents are heavily focused on a smaller number of topics when creating their cybersecurity strategy rather than a larger number of factors receiving a similar weight as is the case for security leaders.

Cybersecurity beginners, on the other hand, are almost exclusively focused on keeping critical systems and operations online (70%) when defining their cybersecurity strategy. This reflects the lack of cybersecurity maturity in this group, not because this is an unimportant topic, but because they are focusing on this factor almost to the exclusion of concern against ransomware and malware attacks, securing systems moving to the cloud, and stopping cross-contamination between systems.

Interestingly, this is a significant change from last year where all three respondent groups were focused on protecting the data in their SAP systems and securing systems from ransomware and malware attacks. This suggests that those who are the most manual or reactive in cybersecurity maturity and who are only performing security validation on an ad-hoc basis may be overwhelmed in the need to keep systems online and available. This can be a challenge for any organization as they must weigh the needs of business users against keeping systems up to date and protected, but it is obviously a greater one than ever for security beginners.

INSIDER
INSIGHT

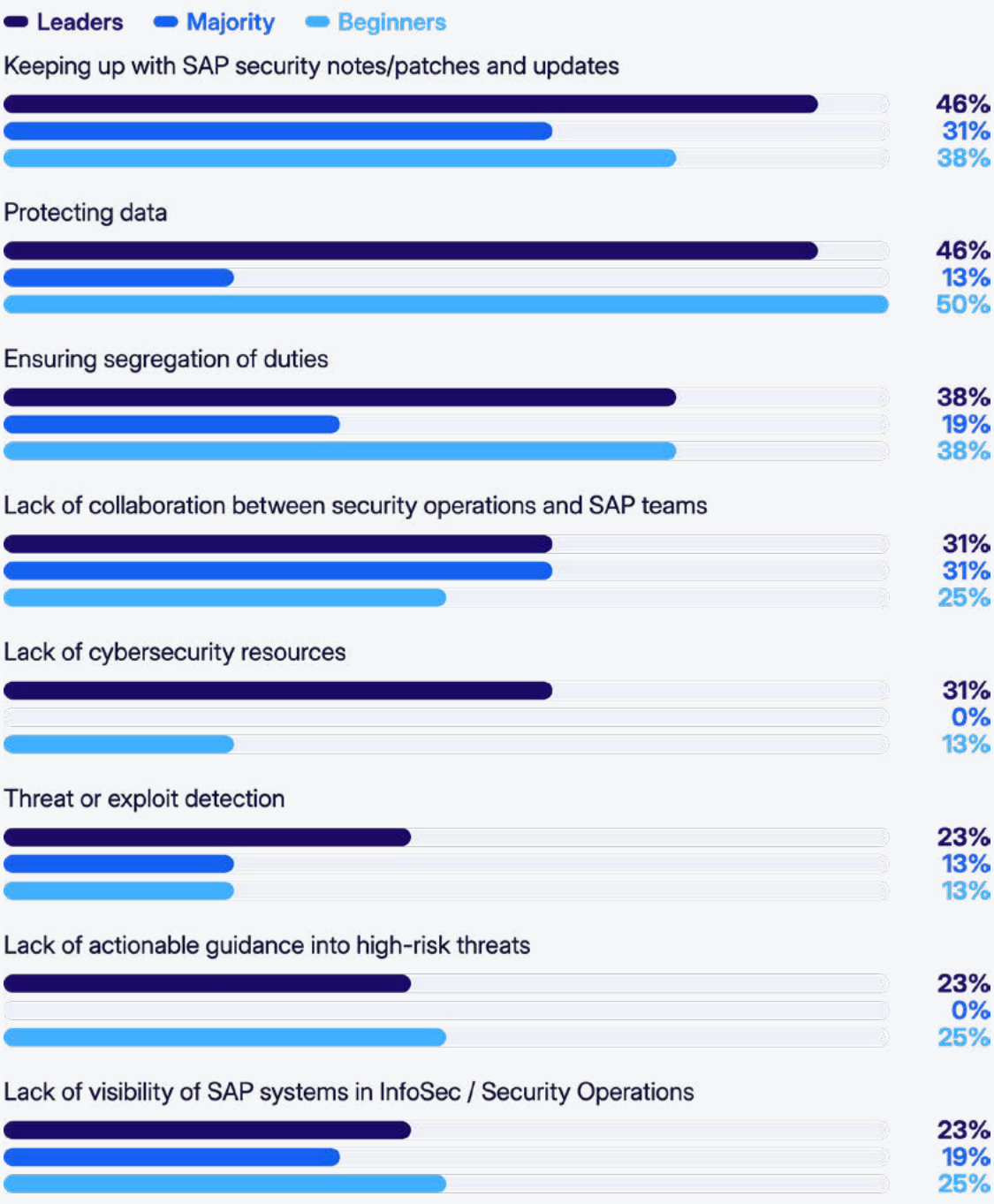
"Our SAP systems contain a wealth of valuable data including sensitive customer information, financial records, intellectual property, and trade secrets. This makes our SAP systems prime targets for data breaches and theft. The exposure of any sensitive data can result in legal consequences, financial liability, and damage to our reputation which must be avoided at all costs."

—ARCHITECT, GLOBAL MANUFACTURER

In addition to cybersecurity threats, respondents also reported the hurdles they faced in securing their SAP systems **(Figure 3)**. As has been the case for several years now, keeping up with SAP security notes, patches, and updates remains the biggest obstacle for security leaders, and the respondent majority, and the second most important factor for security beginners. 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 is easier to see why applying them in a timely manner continues to be an issue.

FIGURE 3

Challenges Faced in Securing SAP Systems



The biggest factor behind keeping up with patches for security leaders was difficulty in verifying whether SAP security notes or patches were being correctly applied (67%). For the respondent majority, the biggest issue with patching is having limited resources to apply those patches (80%), while security beginners struggled with both the volume of patches and notes (67%) and competing business priorities (67%). 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.

Other challenges faced by both security leaders and security beginners were protecting the data in SAP systems and ensuring segregation of duties (SoD). While traditional SAP security has always focused on role-based access control (RBAC), the change to a primarily remote workforce during the global pandemic often had a significant negative impact on SoD procedures. This was because, instead of workflows being passed between colleagues that may meet regularly to ensure processes were handed off cleanly from one group to another, roles and access were often changed to streamline timelines and remove the need for meetings that were no longer happening. Unless organizations have gone back and updated their access controls, it is not surprising that security teams are struggling with SoD challenges.

For the respondent majority, the biggest challenge faced in securing SAP systems was secure application development (44%). This was a much greater obstacle for the respondent majority than for any other group by a significant margin. In fact, no other maturity group had more than 25% of respondents see this as a challenge. The next most important issue for the respondent majority was the lack of collaboration between security operations and SAP teams (31%). That these two challenges were so important for this group perhaps reflects the fact that these respondents said that they have a lack of resources to deploy patches. This lack of resources is very likely becoming a barrier towards application development and team collaboration as teams simply don't have the headcount to check on these tasks.For the respondent majority, the largest planned investment area is in audit and monitoring tools for SAP systems. Given that this group is more reactive than security

INSIDER
INSIGHT

"It is very important, as we have started moving applications to the cloud, that they are properly secured by the partners that run our cloud systems. This has meant that we need to make sure that cybersecurity is taken seriously and the appropriate technologies and resources are in place to achieve this goal."

—SAP COE LEAD, GLOBAL RETAILER

38%

of respondents say that keeping up with patches and updates is the biggest challenge they face in securing their SAP systems.

Given the growth in cybersecurity threats over the past year, an important question involves where respondents plan on making cybersecurity investments. For security leaders, there is an obvious focus on patch and vulnerability management. This is much higher than the resources planned to be dedicated to this topic by 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 and no surprise that security leaders are investing in patch and vulnerability management.

FIGURE 4

Areas of planned SAP-specific cybersecurity investments.

leaders, it is no surprise that they are planning on investing in tools that will provide greater insight into their SAP environments. The next most important area of investment for this group is that of secure development practices (38%), which aligns exactly with their concern around secure application development. Only a third on the list for the majority is governing or monitoring AI capabilities.

Security beginners plan their greatest investment in data protection and privacy controls (63%). Since these respondents are almost exclusively reactive in their cybersecurity posture or are following largely manual processes, having additional data protection and privacy controls makes perfect sense. The next most important areas for security beginners are governance and monitoring of AI capabilities (50%) and cloud and hybrid security (50%). Security leaders are spending less on cloud security because they have likely already made investments in this space. However, the focus on AI monitoring shows that, even though they are lagging in many areas, security beginners realize that they cannot afford to fall behind when it comes to managing AI.

Yet, the current economic climate is causing challenges for all respondents. The most likely scenario for all groups is to be evaluating 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.

Despite the importance of cybersecurity in the SAP space, respondents face challenges. From protecting against new technologies and threats like AI to dealing with the age-old challenge of patching, securing SAP systems is not straightforward. This makes it more important than ever that SAPinsiders focus the resources they have to achieve the most they can. Only by doing this will the data and processes in their SAP systems be secure.

This year's survey also revealed other trends, including the following:

- Even though more than two in three (68%) respondents plan on moving to SAP Cloud ERP Private (often still referred to as RISE with SAP), less than half (42%) have more than a general understanding of their role under the Shared Responsibility Model. Those with a greater level of cybersecurity maturity are somewhat better off, but 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.

- This year 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.

- Most respondents (41%) report that their information security organization (CISO) owns and oversees their SAP security programs. The next most reported group is that of the office of the CIO (22%). Notably, both cybersecurity leaders (46%) and the respondent majority (50%) report that they have joint ownership of their cybersecurity programs between their CIO and CISO. Having 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 towards this level of collaboration.

Required Actions

Based on the survey responses, organizations should consider the following when creating their cybersecurity strategy and plans for their SAP systems.

Establish a fixed patching cadence with formal validation.

Keeping up with SAP security notes, patches, and updates remains the single biggest challenge in this year's survey. The reasons for this backlog relate to difficulty validating whether security patches have been properly applied, the volume of SAP security patches and notes, difficulty scheduling downtime, difficulty understanding which notes are the most critical, and limited resources for patching. Organizations should set a fixed patching cadence with pre-approved maintenance windows and a formal validation step, treating patch management as a scheduled operational discipline rather than a task that has to be fit around other priorities. But flexibility in patching should also be included in any plan should there be a need to apply a critical or urgent patch in a short timeframe.

Build and test a dedicated SAP incident response plan.

Even though a growing number of respondent organizations report having a dedicated incident response plan for SAP-related cybersecurity incidents, not more than a third report that this is something that is well-documented and tested. For the 49% that either have a plan they have not fully tested or are still in the process of developing a plan, putting a focus on completing and running it through a tabletop exercise this year instead of deferring for the future, may be absolutely vital to the protection of SAP environments.

Close the Shared Responsibility Model knowledge gap before RISE with SAP adoption.

Although more than two thirds of respondents are considering or already moving to SAP Cloud ERP Private, only 42% describe themselves as expert or knowledgeable about which security responsibilities sit with SAP and which remain with the customer. Moving to a cloud ERP model without clarity on this division leaves gaps that neither party covers. Security and infrastructure teams should map ownership boundaries for each control area before migration begins. For many, this could be a situation in which they are already behind, only emphasizing the importance of focusing on the Shared Responsibility Model.

DART
MODEL FRAMEWORK

CYBERSECURITY THREATS AND CHALLENGES TO SAP SYSTEMS 2026

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 Vulnerabililty Testing Tools (32%)
- Code Vulnerability Analysis (30%)
- Threat Intelligence Feeds (30%)
- Application-Aware Network Security (30%)
- Automated Testing for Compliance (27%)

APPENDIX | THE DART™ METHODOLOGY

SAPinsider has rewritten the rules of research to provide actionable deliverables from its fact-based approach. The DART methodology serves as the very foundation on which SAPinsider educates end users to act, creates market awareness, drives demand, empowers sales forces, and validates return on investments. It is no wonder that organizations worldwide turn to SAPinsider for research with results.

The DART methodology provides practical insights, including:

DRIVERS	These are macro-level events that are affecting an organization. They can be both external and internal, and they require the implementation of strategic plans, people, processes, and systems.
ACTIONS	These are strategies that companies can implement to address the effects of drivers on the business. These are the integration of people, processes, and technology. These should be business-based actions first, but they should fully leverage technology-enabled solutions to be relevant for our focus.
REQUIREMENTS	These are business and process-level requirements that support the strategies. These tend to be end-to-end for a business process.
TECHNOLOGY	These are technology and systems-related requirements that enable the business requirements and support the company's overall strategies. The requirements must consider the current technology architecture and provide for the adoption of new and innovative technology-enabled capabilities.

REPORT SPONSORS

Onapsis is the global leader in SAP cybersecurity and compliance, helping the world's leading organizations reduce business risk, protect revenue, and keep critical operations running as they accelerate their SAP Cloud and AI initiatives. Built for and by SAP defenders, the SAP-endorsed Onapsis Platform enables Cybersecurity and SAP teams to proactively prevent breaches, accelerate audits, and respond faster to threats across RISE with SAP, S/4HANA Cloud, and hybrid environments. Powered by intelligence from the Onapsis Research Labs, Onapsis delivers rapid time to value, measurable risk reduction, and the confidence enterprises need to innovate faster.

Connect with Onapsis on LinkedIn, X, or visit **onapsis.com**

RESEARCH PARTNER

SAP is creating opportunities through learning and development for all with free, self-guided, and premium learning resources, opportunities to engage in the SAP Community and to experience SAP solutions hands-on.

Learn more at **https://learning.sap.com**

SAPinsider

SAPinsider comprises the largest and fastest-growing SAP membership group worldwide. It provides SAP professionals with invaluable information, strategic guidance, and road-tested advice through events, magazine articles, blogs, podcasts, interactive Q&As, white papers, and webinars. SAPinsider is committed to delivering the latest and most useful content to help SAP users maximize their investment and leading the global discussion on optimizing technology.

For more information, visit **SAPinsider.org.**