SAPinsider

RESEARCH
REPORT

JUNE 2024

Cybersecurity Threats and Challenges to SAP Systems

By Robert Holland

Executive Summary

INSIDER PERSPECTIVE

"The SAP space is far more interconnected than it was ten to fifteen years ago. Multiple cloud-based solutions, APIs, and partner tools updating SAP increase the chances of a cybersecurity threats. SAP solutions' reliance on third-party software, plugins, and integrations also introduces additional security risks. If these components are not maintained, they can become potential vulnerabilities that can be exploited to access the SAP environment."

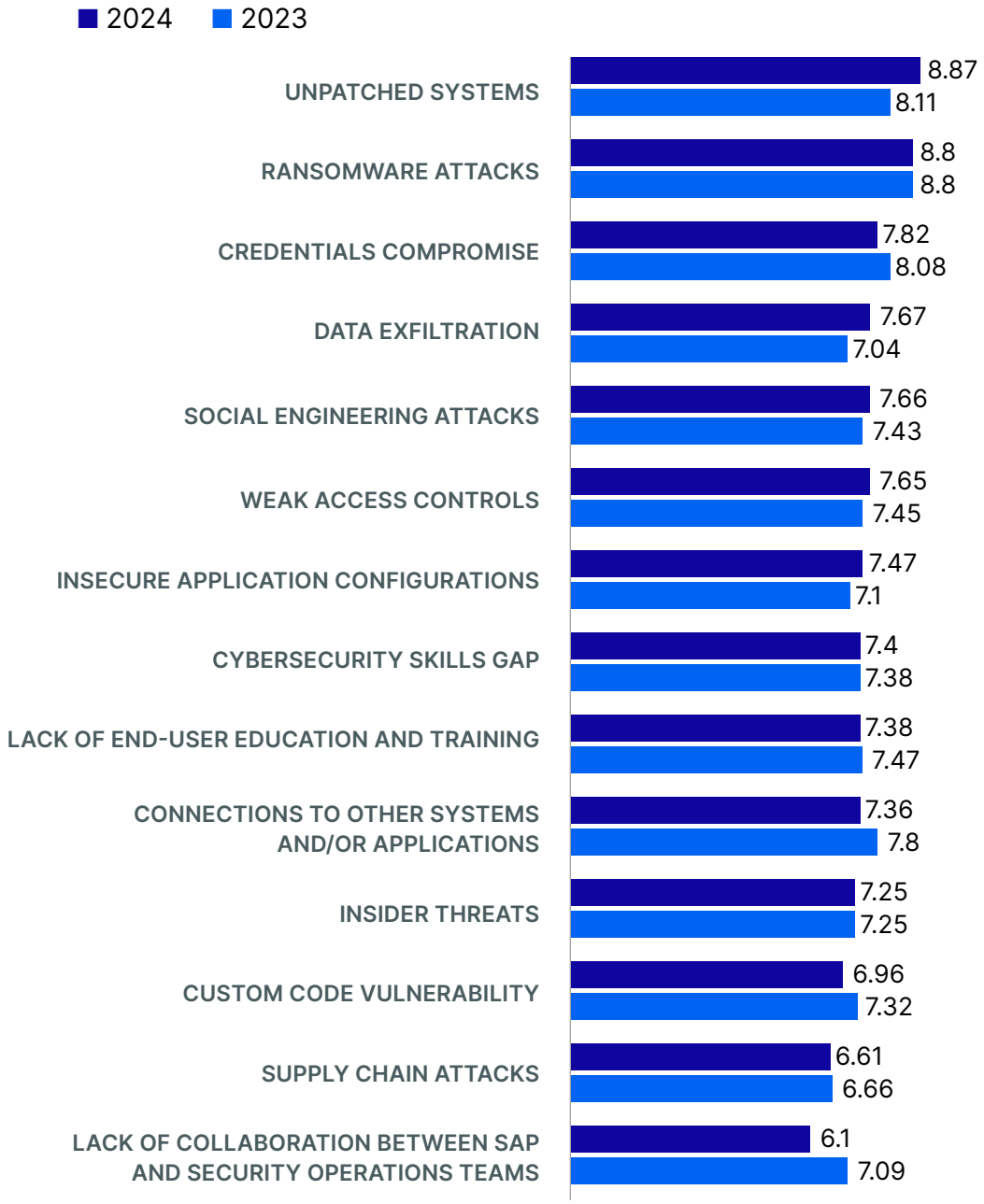
SENIOR ARCHITECT, GLOBAL MANUFACTURER

THE THREAT LANDSCAPE for SAP systems continues to expand. Ransomware and malware attacks are increasing in frequency and, even if not directly targeting SAP systems, often affect connected systems or environments. For SAP customers, a more more concerning issue is the increase in social engineering or credential compromise attacks, which, if successful, can expose valuable data within SAP systems. Consequently, SAPinsiders have identified addressing system vulnerabilities as one of their most critical needs.

To provide insights into today's cybersecurity concerns and strategies, SAPinsider surveyed 173 members of its community between February and June 2024. The survey asked respondents to rank the top cybersecurity threats to their SAP systems in order of importance, from most to least important **(Figure 1).** Unpatched systems, ransomware attacks, and credentials compromise were ranked as the most important threats, similar to the data from the last two years. The most significant change this year is that unpatched systems moved to the top of the list of security threats.

Failure to regularly apply patches exposes systems to vulnerabilities and allow threat actors to exploit them using code found online, exfiltrate data, plant malicious code, or potentially directly access systems. Online forums hosting discussions on exploiting a vulnerability withing hours of SAP patch releases highlights the critical urgency of implementing patches. But this

Figure 1: Top Cybersecurity Threats to SAP Systems



must be balanced with minimizing downtime and ensuring systems accessibility for business users.

Ransomware attack, credentials compromise, and social engineering attacks are often interconnected and highlight the root cause of many cyber-attacks. While credentials compromise can be a method for threat actors to infiltrate systems and deploy ransomware or malware, social engineering is often used to expose credentials and manipulates employees into divulging usernames and passwords. Organizations need to ensure that employees are

regularly educated on potential threats as sophisticated attacks increase.

Comparing the responses from organizations of various sizes provide additional insight into the challenges. For example, while respondents from organizations with revenues over $2 billion annually were more concerned about unpatched systems (9.43), data exfiltration (8.43), and weak access controls (8.34), respondents from organizations with revenues under $2 billion were more concerned about ransomware attacks (9.40), unpatched systems (8.82), and credentials compromise (8.44). (Numbers represent the ranking and can be compared to the chart in Figure 1.) Given the complexity and number of systems in larger enterprise landscapes, and the difficulty in scheduling downtime, patching is a significant challenge for larger organizations.

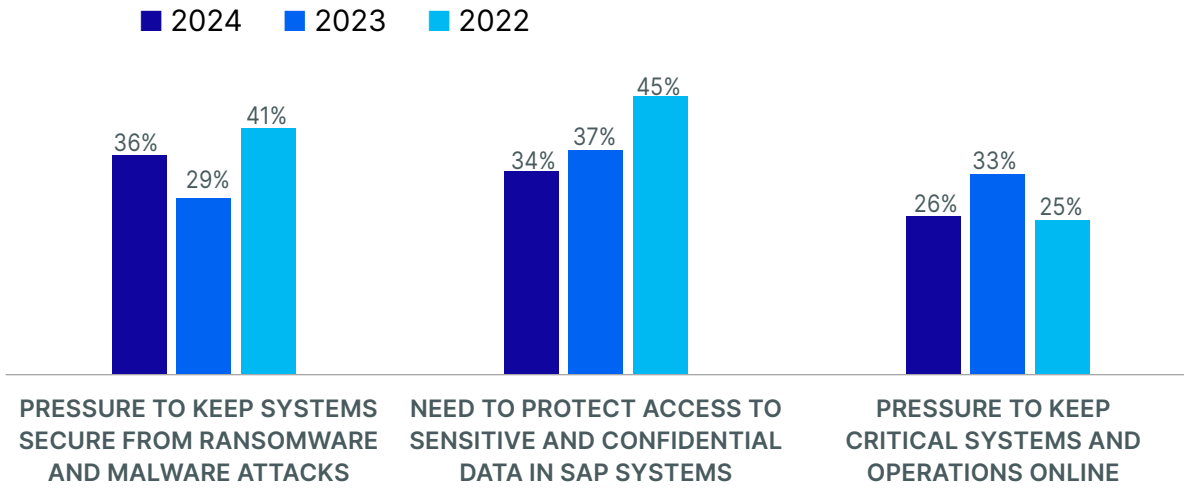
These cybersecurity threats directly correlate with the factors that are most responsible for driving cybersecurity strategy and plans **(Figure 2).** The pressure to keep systems secure from ransomware and malware attacks (36%) is at the top of the list this year, followed by the need to protect access to sensitive and confidential data in SAP systems (34%), and pressure to keep critical systems and operations online (26%). A combination of these factors underscore the importance of data integrity and availability for SAP solutions.

Keeping systems secure from ransomware and malware attacks is one of the main goals of security teams today. However, this can be especially complex for SAP solutions since their security is not always managed by dedicated security teams, although this is changing. This is why organizations must ensure collaboration across SAP, security, and IT teams as lack of alignment can result in coverage gaps. The need for collaboration is particularly true for organizations moving to the cloud as cloud landscapes can introduce significant security complexity around data integration and connection points.

Protecting data in SAP systems has been one of the major factors driving cybersecurity strategy for SAP, evidenced by ongoing research by SAPinsider in this space. While this slipped to second place this year, protecting data connects to other cybersecurity topics. These include detecting and preventing intrusions, user access controls, process controls, data masking, and encryption, and also covers areas like coding practices, disaster recovery and continuity planning, and regional and industry specific concerns.

Keeping SAP systems online has been a priority for organizations and the growing

Figure 2: Factors Driving Strategy and Plans for Cybersecurity for SAP Systems



INSIDER PERSPECTIVE

"We rely heavily on our SAP systems to manage critical business processes. This includes finance, human resources, supply chain, and CRM. Because these systems contain sensitive data, they have become attractive targets for those looking to gain unauthorized data access. This has made focusing on security for our SAP systems so much more important than in the past."

SAP ARCHITECT, MANUFACTURING COMPANY

complexity of SAP landscapes, including the deployment and integration of cloud-based solutions, has made increased availability even more important. However, this has also made it difficult to perform urgent updates to address concerns such as ransomware, malware, security updates, zero-day or one-day vulnerabilities, or resolve data integrity issues.

Corresponding with cybersecurity challenges, significant differences were also seen in the factors driving cybersecurity strategy for organizations of different sizes. Larger organizations were most concerned about the need to protect data in their SAP systems (41%). This was significantly more important for these organizations than keeping systems secure from ransomware and malware attacks (32%) and keeping systems and operations online (27%). On the other hand, smaller organizations were most focused on protecting against ransomware and malware attacks (35%) and keeping systems online (26%). They also reported that the need for better data protection compliance (25%) had a larger impact on their cybersecurity strategy than protecting data in their systems (22%).

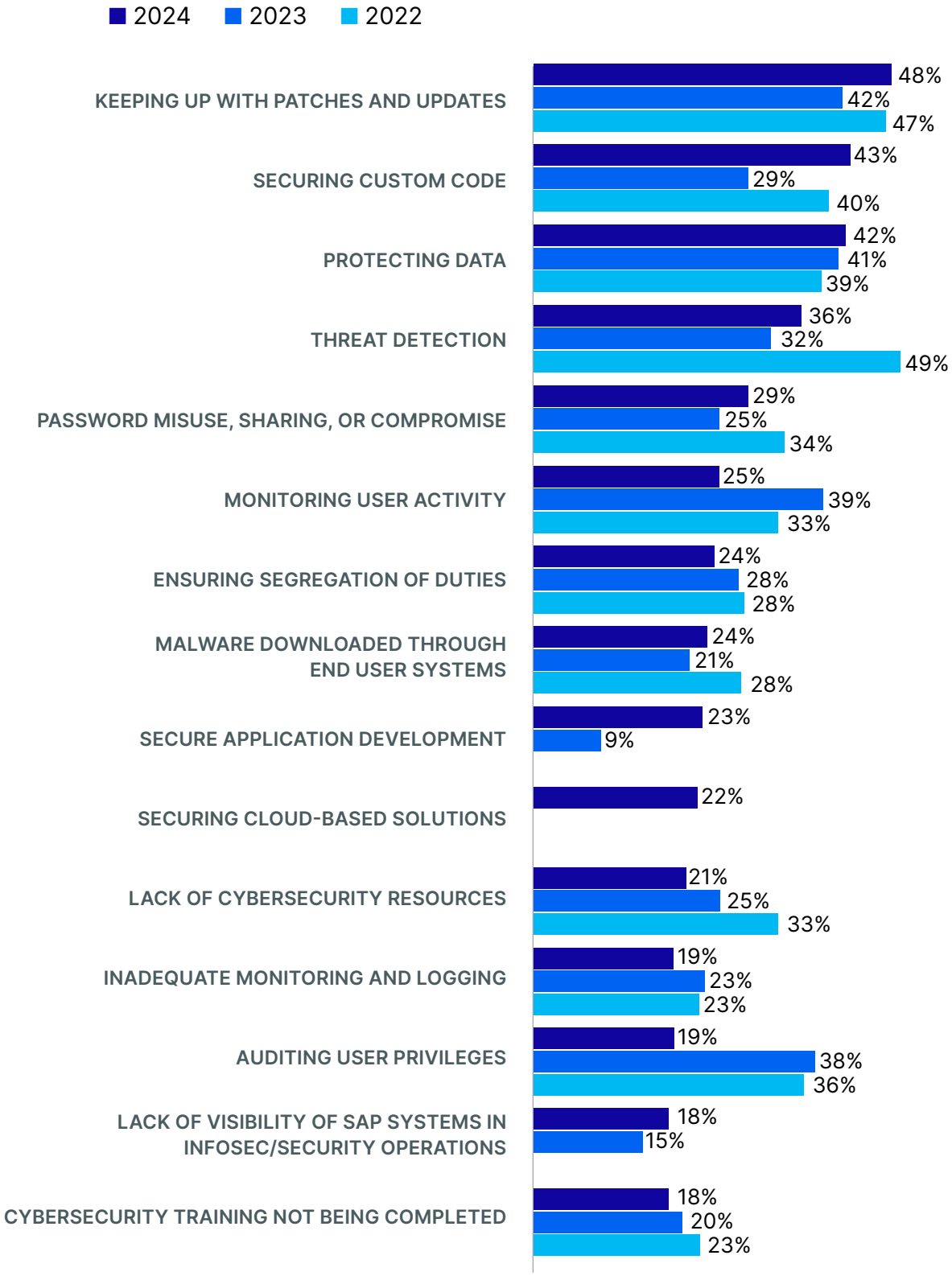
In addition to cybersecurity threats, respondents also reported the challenges they faced in securing their SAP systems **(Figure 3).** Similar to 2023, the biggest challenge this year was in keeping up with patches and updates (48%). As discussed earlier, the complexity of SAP landscape can make it challenging to schedule downtime for patch application. This is because larger organizations are much more likely to have challenges with keeping up with patching (55%) than smaller organizations (41%).

Respondents reporting challenges in keeping up with patches and updates were asked a follow-up question about the issues causing this. Unsurprisingly, the two biggest factors impacting patching were difficulty scheduling downtime (53%) and competing business priorities (47%). Limited resources to apply patches (37%) was also a significant factor, though this was a bigger challenge for smaller organizations (46%) compared to larger organizations (33%). However, for larger organizations the biggest concern was competing business priorities (71%) which caused difficulties with scheduling downtime (58%).

Reemerging as a top challenge for organizations this year is securing custom code (43%). Ranked slightly higher than protecting data (42%), respondents are obviously concerned about potential vulnerabilities in the mass of custom code that is often a part of large SAP implementations. Interestingly, respondents from smaller organizations see a bigger challenge in securing their SAP systems (46%) than larger organizations (43%) possibly due to having fewer security resources.

Cloud security has emerged as a new area to this year's research. With more enterprise workloads moving to the cloud, organizations must ensure that they are effectively securing their cloud systems. However, this can be a complex scenario

Figure 3: Challenges Faced in Securing SAP Systems



since 46% of all respondents reported using two to three cloud providers with another 19% reporting using four to six. Demonstrating the additional complexity of their environments, 41% of respondents from larger organizations reported that they are using at least four cloud providers. Given the importance, respondents were also asked about their concerns regarding the use of cloud-based solutions, particularly SAP solutions **(Figure 4).**

While the top concern was about cloud providers meeting SLAs (32%), other important concerns included insufficient visibility into data residency (32%), unauthorized access to data by other cloud tenants (31%) or from external sources (31%), or a skill gap for cloud capabilities (29%). Though many of these challenges can be addressed by working closely with cloud providers, others require educating internal teams to have the knowledge for securely configuring cloud-based systems.

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

- Only a small number of respondents (8%) reported their SAP teams being exclusively responsible for managing their SAP systems' security. A plurality of respondents reported the security for their SAP systems being managed by the SAP team working together with either a dedicated security team (31%) or IT teams (31%).
- Although the global macroeconomic climate is less unstable than last year, respondents still reported impacts on their security objectives. A third (34%) are evaluating alternatives to existing providers to reduce costs, while 33% reported holding off projects, and one in

Figure 4: Concerns With Using Cloud-Based Solutions

four (26%) scaling back planned investments. While these numbers are slightly lower than last year, they still represent significant impact.

- Despite the impact of the economic climate, respondents reported their organizations planned to invest in the following areas of security: cloud security (49%); threat detection and response (44%), vulnerability management (39%), data security tools (34%), and zero-trust (31%).

Required Actions

Based on the survey responses, organizations should consider the following when making their plans for data, integration, and platforms:

- **Stay current on patches for systems and solutions and conduct regular audits.** System and security patching has historically taken a back seat to other development and operational requirements in SAP. There is often a lack of clarity about what patching entails from both an analyst and a system perspective. However, many resources are available that can assist in establishing a program for evaluating and implementing system and security patches. Prioritize setting up an SAP system and security patching policy and build a program to address these key vulnerabilities and managing risk.
- **Assess current and emerging technologies to balance cybersecurity investments for current systems and those for use in the future.** Perform an inventory of all technology currently being used to assess what functionalities are available, what is obsolete, or if a newer version has capabilities that are not included in any security plan. Set aside time for your SAP team to research and verify whether tools on hand could potentially be utilized to advance your cybersecurity objectives. Stay abreast of technologies in the market to solve current security issues and make security a budgetary priority before threat actors force that response.
- **Prioritize cybersecurity for SAP and integrate it into the overall cybersecurity program.** A cybersecurity program is a holistic, all-systems program that assesses every application and device, incorporating the unique needs and requirements of each, and also focuses on risk management. If the network security program treats SAP like any another application on the network, it is a large vulnerability. Have IT and dedicated security teams shadow one another for a few days so they can learn from each other. Let the network security teams see what the SAP team does to configure the system. Then, let the SAP team see how the network security team configures and monitors the network. Cross-training teams will ensure that each understands the importance of the role the other performs and will help better integrate each team into a broader cybersecurity program.

INSIDER PERSPECTIVE

"The concepts around securing our SAP systems have matured. In the past, it was seen as a process that had to be undertaken with, hopefully, a minimum amount of effort. Today, it is fully embedded in our delivery lifecycle and the IT security teams are engaged from day one."

SAP COE LEAD, GLOBAL RETAILER

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%)

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%)

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 helps organizations protect and optimize their SAP investments. The largest companies in the world leverage the Onapsis Platform to secure and enhance their digital transformation projects, eliminate SAP blindspots, automate compliance processes, and strengthen DevSecOps for custom application development. Trusted by 30% of the Global Forbes 100, Onapsis offers simple, complete, and SAP-endorsed security for even the most complex landscapes.

For more information, visit: https://onapsis.com/

Rubrik is on a mission to secure the world's data. With Zero Trust Data Security™, we help organizations achieve business resilience against cyberattacks, malicious insiders, and operational disruptions. Rubrik Security Cloud, powered by machine learning, secures data across enterprise, cloud, and SaaS applications. We help organizations uphold data integrity, deliver data availability that withstands adverse conditions, continuously monitor data risks and threats, and restore businesses with their data when infrastructure is attacked.

For more information, visit https://www.rubrik.com

Splunk helps make organizations more digitally resilient. Leading organizations use our unified security and observability platform to keep their digital systems secure and reliable. Organizations trust Splunk to prevent infrastructure, application and security incidents from becoming major issues, recover faster from shocks to digital systems and adapt quickly to new opportunities. Splunk helps SecOps, ITOps and Engineering teams deliver these outcomes with comprehensive visibility, rapid detection and investigation, and optimized response, all at the scale necessary for the world's largest organizations.

For more information, visit splunk.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.