SAPinsider

BENCHMARK REPORT

by Robert Holland October 2023

SAP CYBERSECURITY PRIORITIES

SPONSORED BY

FORTINET Microsoft Azure pathlock splunk> SUSE

Insider Perspective

"A cybersecurity breach can disrupt business operations, leading to downtime and financial losses for our organization. Protecting SAP systems allows us to ensure business continuity and prevents disruptions in critical processes."

– ARCHITECT, RETAIL CORPORATION

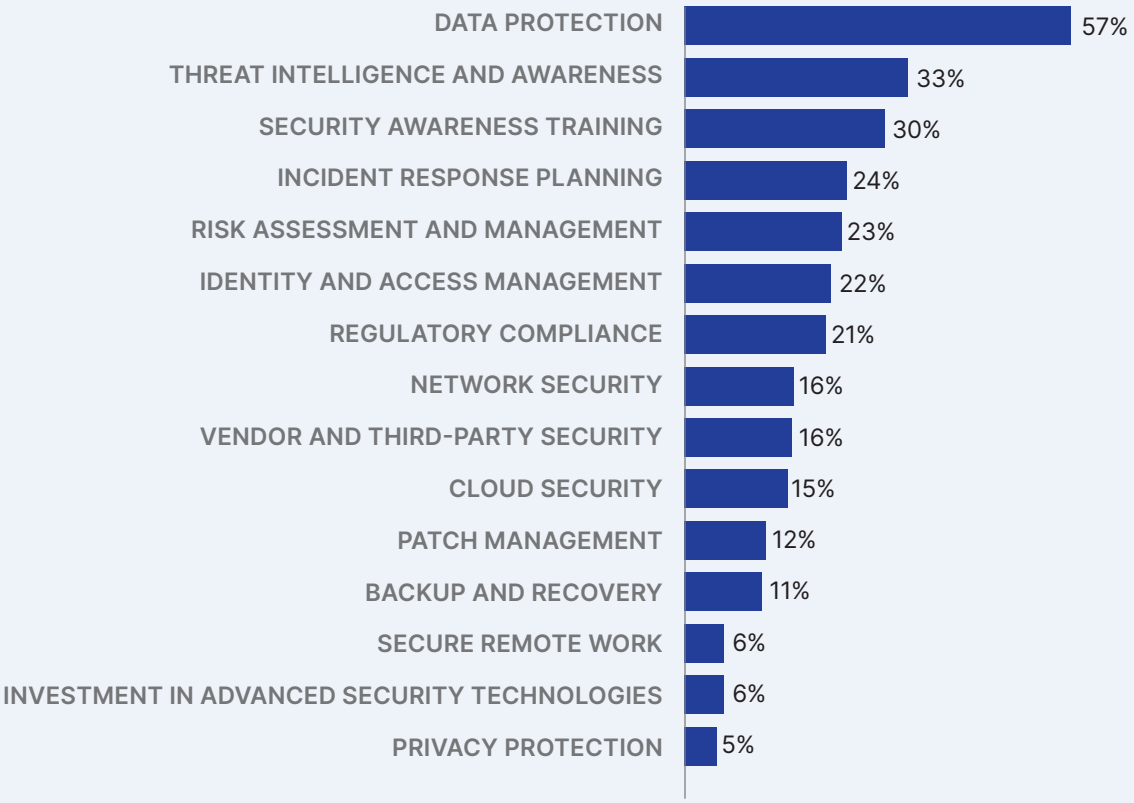
CYBERATTACKS AND CYBERCRIME continue to grow across the globe. The latest statistics show growth in both the frequency and cost of attacks, and as many as two thirds of organizations may have experienced a cyberattack during the past year. With cybersecurity on the minds of many businesses, it is important to examine what organizations are prioritizing when it comes to their SAP systems. Earlier this year, SAPinsider research revealed that ransomware attacks, unpatched systems, and compromised credentials were the top three cybersecurity threats to SAP systems. This report will focus on what organizations are prioritizing to secure their SAP systems and how they are ensuring their teams are ready to meet these threats.

SAPinsider surveyed 144 members of its community between July and October 2023 to generate insights on what organizations prioritize when it comes to their SAP systems. The survey questioned the respondents on the factors most responsible for driving their organization's strategy and plans around cybersecurity priorities. Aligning with the fact that, earlier this year, protecting the data in SAP systems was the biggest factor behind cybersecurity strategies for those systems, the top cybersecurity priority for respondents in this research was that of data protection **(Figure 1).**

The data stored in an SAP system typically represents the most valuable data an organization has. Suppliers, partners, customers, financials, transactions, banking connections, and more are part of that data set. Given the value of this data, it is no surprise that organizations want to make sure that it is well protected. This is why data protection is so much more important to respondents than areas like risk management and assessment or identity and access management – even though these are also important.

Notably, the size of the respondent organization had no impact on how important it was to prioritize data protection. Larger

Figure 1: **Top Cybersecurity Priorities for SAP Systems**



organizations, those with annual revenues in excess of $2 billion, were just as focused on data protection as smaller organizations (revenue below $2 billion). And in each case, the next most important priority was at least 10 percentage points lower than protecting data. For example, 58% of respondents from large organizations said that data protection was their top cybersecurity priority, and this was followed by identity and access management (37%). In smaller organizations, data protection (54%) was followed by risk assessment and management (43%).

This focus on data protection is completely aligned with the factors most responsible for driving cybersecurity priorities. Just as 57% of respondents say that data protection is their top cybersecurity priority, 53% of respondents reported that the biggest factor driving cybersecurity priorities is the need to keep sensitive and confidential data in SAP systems protected from potential threats **(Figure 2).** The size of the drop to the next most important factor behind cybersecurity priorities, the need to support the adoption of new technologies and processes as part of digital transformation at 22%, demonstrates just how important data protection is for SAP customers.

In response to this need to protect data in SAP systems, the primary strategy companies prioritize is to invest in regular employee training to raise awareness of cyberthreats **(Figure 3).** Cybersecurity awareness training is a very important part of ensuring that employees are aware of potential attack vectors and current threats as employees are frequently the first line of defense against external threats.

Figure 2: Factors Responsible for Driving Cybersecurity Priorities

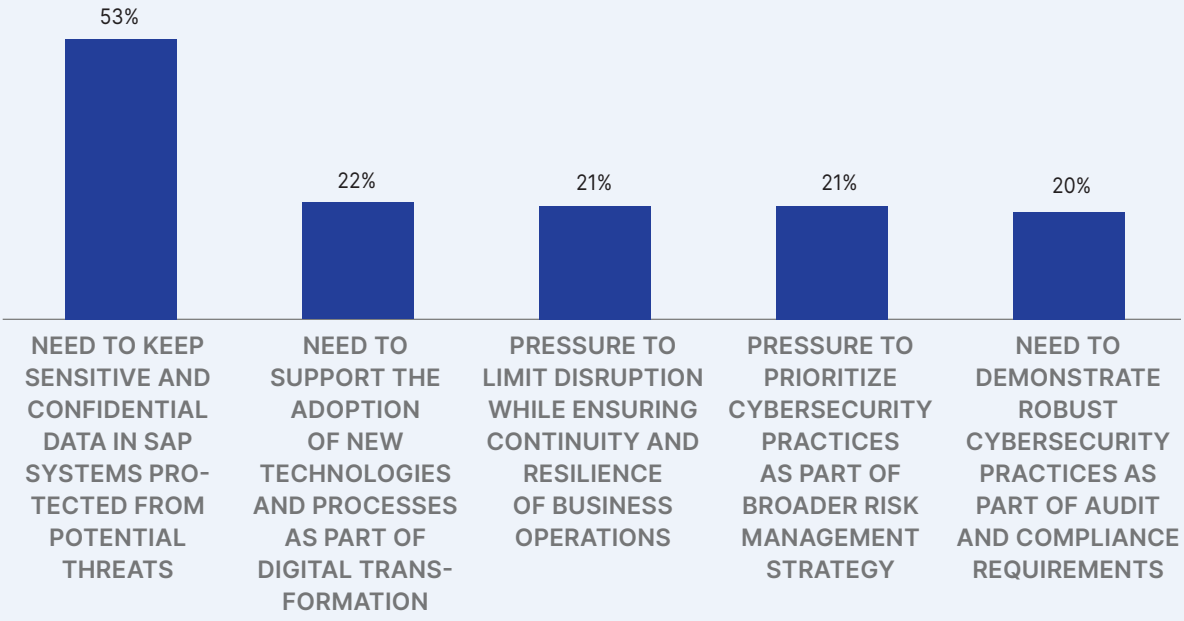
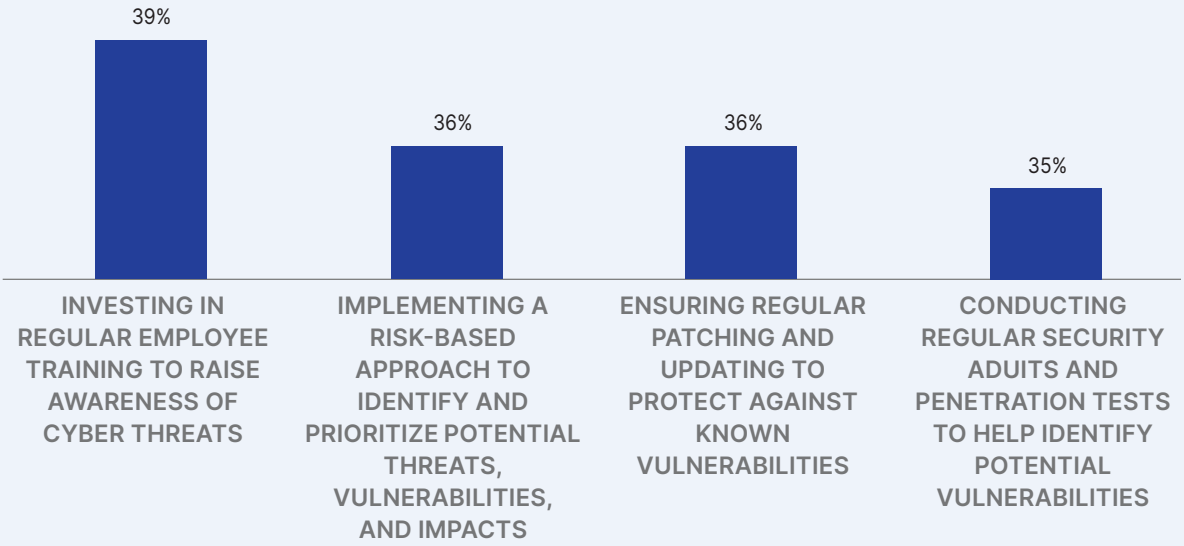


Figure 3: Cybersecurity Strategies Being Prioritized to Better Secure SAP Landscapes



However, it is important to ensure that employees understand the value of this training and that it be readily understood, relatable, and diverse enough that it does not become tedious.

Beyond investing in cybersecurity awareness training, there are three strategies that a very similar proportion of respondents prioritize. The first is implementing a risk-based approach to identify and prioritize potential threats, vulnerabilities, and impacts. Using this approach, in which vulnerabilities that are discovered are prioritized based on the risk they pose, allows organizations to tailor the approach that they are taking to addressing potential risks. It also provides a foundation for organizations to implement a tailored approach to addressing the risks that pose the highest risk to their landscapes.

Equally as important of a strategy is ensuring regular patching and updating to protect against known vulnerabilities. SAPinsider's report earlier in 2023 on Cybersecurity Threats and Challenges to SAP Systems showed that unpatched systems were one of the biggest challenges respondents faced in securing their SAP systems. This is why regularly implementing patches and updates was the most important strategy organizations followed to address their cybersecurity needs. In this report, ensuring regular patching and updating protects the organization against known vulnerabilities is a reinforcement of that need. However, since most organizations should already have a patching strategy in place, it is not being as highly prioritized as raising cybersecurity awareness.

The last strategy being prioritized by respondents is that of conducting regular security audits and penetration tests to help identify potential vulnerabilities. Regular security audits help organizations identify vulnerabilities, ensure compliance, understand and categorize potential risks, and safeguard sensitive data. Penetration tests can help refine response procedures to potential threats, provide real-world training scenarios for teams, validate the security measures of vendors and third parties, and ensure that security measures are evolving with the changing

Insider Perspective

"Our SAP systems store sensitive business and customer data. We are prioritizing cybersecurity measures for these systems to help in protecting this data from unauthorized access, theft, or manipulation."

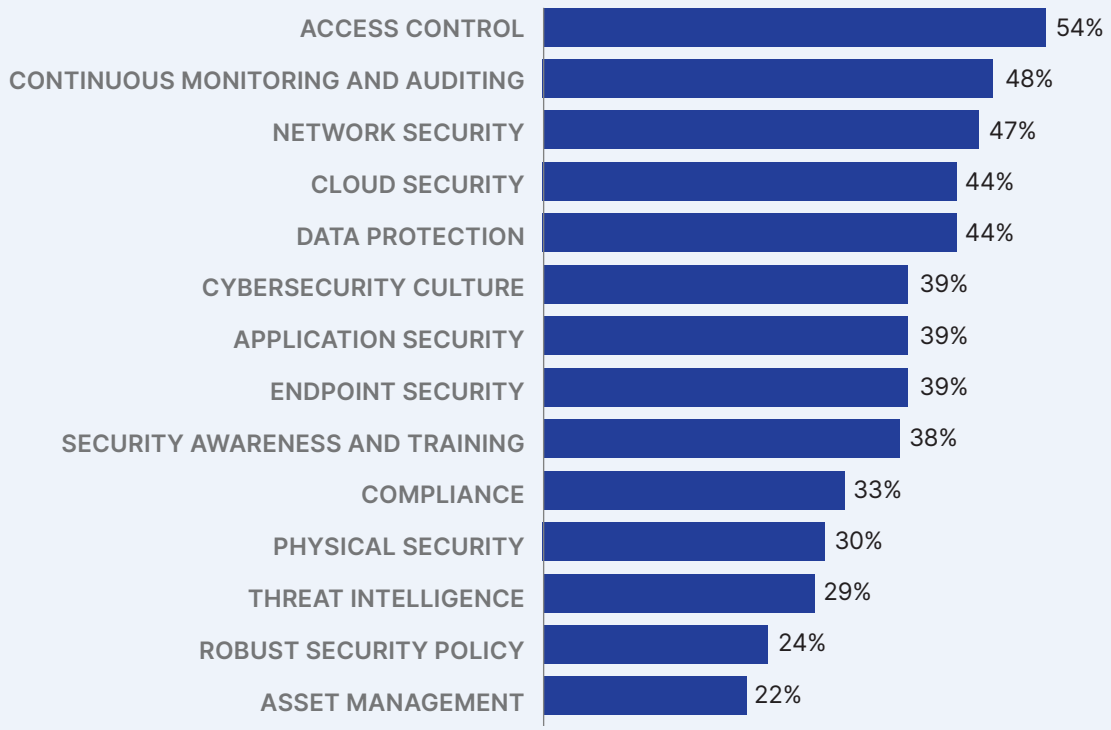
– PROJECT MANAGER, REGIONAL MANUFACTURER

threat landscape. Used in conjunction with each other, these two best practices can help ensure that risks are detected and addressed before they become vulnerabilities.

Protecting data in SAP systems is the highest cybersecurity priority for organizations, and to achieve this goal respondents report that they are focusing on a number of elements **(Figure 4).** The most important of these is access control, which is a traditional means of securing SAP systems. Access control is about ensuring that users are granted access only to the data that they should be able to see. But not far behind is continuous monitoring and auditing, supporting the strategy of regular audits and pen tests, and network security which can help stop unauthorized access before it even reaches SAP or non-SAP systems.

While respondents from both large and small organizations indicated that they were prioritizing access control as a key element to securing their SAP systems, the next most important element for large organizations were that of cloud security (51%) and continuous monitoring and logging (51%). Just behind these were network security, endpoint security, and cybersecurity culture which were all selected by 49% of respondents. For small organizations, continuous monitoring and logging (46%) was just as important as access control, and these were followed by network security (43%), data protection (43%), and cloud security (41%). These differences in emphasis are because larger organizations are more likely to be moving enterprise workloads to the cloud and so are emphasizing cybersecurity elements that will support that move.

Figure 4: Elements Being Prioritized to Create a Secure Environment for SAP Systems



Insider Perspective

"Our SAP systems are a crucial part of our business. In addition to cybersecurity measures being implemented at the system level, we are also prioritizing cybersecurity at the network level to minimize attacks on external systems. Since we are running SAP S/4HANA externally to the organization, having network-based cybersecurity is very important to achieving this goal."

– SAP FINANCE MANAGER, GLOBAL MANUFACTURER

This year's survey also revealed the following trends:

- Nearly three quarters (74%) of respondents indicated that, as they implement cybersecurity awareness training, this is being done for both users and security teams. Less than one in five (19%) said that their training was for security teams only, and just 4% said that the training was for users only.
- Awareness training (68%) is the security education that is most likely to be prioritized, followed by policy and procedure training (54%), phishing simulation training (53%), and compliance training (50%).
- Despite the macroeconomic climate, a third (33%) of respondents stated that they see a greater demand for security due to increased threat activity, and 29% report that they are seeing no impact on their cybersecurity budgets. However, 32% report that they are evaluating alternatives to existing providers to reduce costs, and 24% report that security teams have been forced to reduce staff or are scaling back planned investments. Perhaps not surprisingly, it is larger organizations that are experiencing the least impact while smaller organizations are much more likely (37%) to be evaluating alternatives to reduce costs.

REQUIRED ACTIONS

Based on the survey responses, organizations should make the following plans when it comes to cybersecurity priorities for their SAP environments:

- **Focus on protecting the data in SAP environments.** When ranking the cybersecurity threats to SAP systems earlier this year, ransomware and malware attacks were at the top of the list. However, in this research, credentials compromise was at the top of the list of cybersecurity threats. This is because a threat actor gaining access to the data in an SAP system is potentially much more damaging than the system going offline due to a ransomware attack. Someone with access to the system, and the data it contains, can do anything from review employee or customer personal identifiable information (PII) to initiate bank transfers for millions of dollars. And these threat actors are not necessarily external. This is why protecting data in SAP systems is so important for all SAP customers.
- **Initiate plans for cybersecurity training and education if these are not already in place.** Organizations can put tools and technology in place to prevent unauthorized devices from connecting to networks and ensure that users only see allowed data, but employees are the first line of defense when it comes to cybersecurity. Both employees and IT teams must be aware of current threats, understand how policies and procedures impact their roles, and receive training on how topics like phishing attacks, compliance, and privacy will impact their roles.

- **Appraise existing cybersecurity capabilities to ensure that they meet the needs of changing requirements and landscapes.** As organizations undergo infrastructure transformation, digital transformation, and move more enterprise workloads to the cloud, cybersecurity will become increasingly important. These cybersecurity capabilities will need to support and protect transformation processes, limit disruption and improve resilience, and help meet audit and compliance requirements. While these changes will not all come at once, organizations must prioritize their cybersecurity needs ahead of time. Only by doing this can they be certain that they have effectively evaluated security needs and built them into changes from the beginning.
- **Do not neglect patching as the starting point for keeping systems secure.** Most organizations have a patching strategy in place, but previous SAPinsider research has shown that some organizations may not have a patching schedule or only apply critical patches as part of their scheduled patching process. While patching can be difficult to manage in SAP environments, usually because of the need to limit downtime, putting an effective and timely patching process in place should be the starting point for any cybersecurity strategy. Then organizations can confirm that SAP systems are secure against known issues.

DART
MODEL FRAMEWORK

SAP CYBERSECURITY PRIORITIES

DRIVERS

- Need to keep sensitive and confidential data in SAP systems protected from potential threats (53%)
- Need to support the adoption of new technologies and processes as part of digital transformation (22%)
- Pressure to limit disruption while ensuring continuity and resilience of business operations (21%)
- Pressure to prioritize cybersecurity practices as part of broader risk management strategy (21%)
- Need to demonstrate robust cybersecurity practices as part of audit and compliance requirements (20%)

ACTIONS

- Investing in regular employee training to raise awareness of cyber threats (39%)
- Implementing a risk-based approach to identify and prioritize potential threats, vulnerabilities, and impacts (36%)
- Ensuring regular patching and updating to protect against known vulnerabilities (36%)
- Conducting regular security audits and penetration tests to help identify potential vulnerabilities(35%)

REQUIREMENTS

- Regular training and measurement of cybersecurity training (82%)
- Identification of cybersecurity incidents and responses and escalation procedures (79%)
- Identification of business-critical assets and systems (77%)
- Regular monitoring of patches and updates (77%)
- Adoption and ongoing monitoring of cybersecurity framework (77%)
- Understanding of privacy requirements and regulations (76%)

TECHNOLOGIES

- Continuous Monitoring (54%)
- Encrypted/Secure Connectivity (47%)
- Data Encryption (45%)
- Vulnerability Management (42%)
- Security-Driven Networking (40%)
- Zero-Trust Models (26%)
- Code Vulnerability Analysis (26%)
- Platform centralizing cybersecurity technologies (26%)
- Threat Intelligence Feeds (25%)
- Embedded Hardware Authentication (24%)
- Application-Aware Network Security (22%)
- Automated Testing for Compliance (21%)
- Behavioral Analytics (20%)
- Automated Code Vulnerability Testing Tools (18%)
- UI Masking (18%)

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

Report Sponsors

Fortinet (NASDAQ: FTNT) makes possible a digital world that we can always trust through its mission to protect people, devices, and data everywhere. This is why the world's largest enterprises, service providers, and government organizations choose Fortinet to securely accelerate their digital journey. The Fortinet Security Fabric platform delivers broad, integrated, and automated protections across the entire digital attack surface, securing critical devices, data, applications, and connections from the data center to the cloud to the home office. Ranking #1 in the most security appliances shipped worldwide, more than 565,000 customers trust Fortinet to protect their businesses. And the Fortinet NSE Training Institute, an initiative of Fortinet's Training Advancement Agenda (TAA), provides one of the largest and broadest training programs in the industry to make cyber training and new career opportunities available to everyone.

Learn more at https://www.fortinet.com, the Fortinet Blog, or FortiGuard Labs.

Microsoft enables digital transformation for the era of an intelligent cloud and an intelligent edge. It partners closely with SAP to help joint customers accelerate their cloud journey on Azure. Microsoft's cloud platform is optimized for enterprises to run mission-critical SAP applications with unmatched security and reliability, and is the market leader with the most compliance and industry certifications. Customers trust the Microsoft Cloud to leverage data analytics and gain intelligent insights to democratize decision-making, accelerate innovation, and build an intelligent enterprise.

For more information, visit https://azure.microsoft.com

Pathlock brings simplicity to customers who are facing the security, risk, and compliance complexities of a digitally transformed organization. New applications, new threats, and new compliance requirements have outpaced disparate, legacy solutions. With the industry's broadest support for business applications, Pathlock provides a single platform to unify access governance, automate audit and compliance processes, and fortify application security. With Pathlock, some of the largest and most complex organizations in the world can confidently handle the security and compliance requirements in their core ERP and beyond.

Whether it's minimizing risk exposure and improving threat detection, handling SoD with ease, or unlocking IAM process efficiencies — Pathlock provides the fastest path towards strengthening your ERP security & compliance posture.

For more information, visit https://www.pathlock.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

SUSE is a global leader in innovative, reliable, and secure enterprise-grade open source solutions, relied upon by more than 60% of the Fortune 500 to power their mission-critical workloads. For over 20 years, SAP and SUSE have delivered innovative business-critical solutions on open-source platforms, enabling organizations to improve operations, anticipate requirements, and become industry leaders. Today, the vast majority of SAP customers run their SAP and SAP S/4HANA environments on SUSE. SUSE is an SAP platinum partner offering the following Endorsed App to SAP software: SUSE Linux Enterprise Server for SAP applications.

For more information, visit http://www.suse.com or http://www.suse.com/unlock-excellence

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.