SAPinsider

BENCHMARK REPORT

by Robert Holland May 2023

CYBERSECURITY THREATS TO SAP SYSTEMS

SPONSORED BY

LAYER SEVEN SECURITY · Microsoft Azure · ONAPSIS · pathlock · SUSE

Insider Perspective

> "With the rise of digital transformation initiatives, SAP systems are now more interconnected than ever. They are integrated with other enterprise systems, cloud platforms, and even external partners and suppliers. This interconnectedness expands the attack surface, providing more entry points for potential intrusions. That means a breach in one system can quickly spread across the network, affecting multiple interconnected systems and compromising the entire ecosystem."
>
> — ENGINEER, GLOBAL SOLUTION PROVIDER

IN 2023, the focus of cybersecurity strategies for SAP systems shifted away from ransomware and malware attacks to addressing unpatched systems, concentrating on addressing system vulnerabilities over attack vectors. Exploring the details behind these changes, SAPinsider revealed some interesting year-over-year trends during its third year of research on cybersecurity threats. Increasing regulatory compliance requirements, hybridization of environments, and economic pressures all played a role in influencing this shift in thinking.

SAPinsider surveyed 206 members of its community between January and April 2023 to generate the insights necessary for this research. The survey asked the respondents to rank the top cybersecurity threats to their SAP systems, ranging from most to least important **(Figure 1).** Ransomware attacks, unpatched systems, and credentials compromise were ranked as the most important threats to systems, similar to last year.

These three threats are interconnected when it comes to root cause analysis. Credentials compromise is the gateway for threat actors to infiltrate systems and plant ransomware or malware. Failure to regularly apply patches exposes vulnerabilities that allow hackers to exfiltrate data, plant malicious code, or traverse across the network.

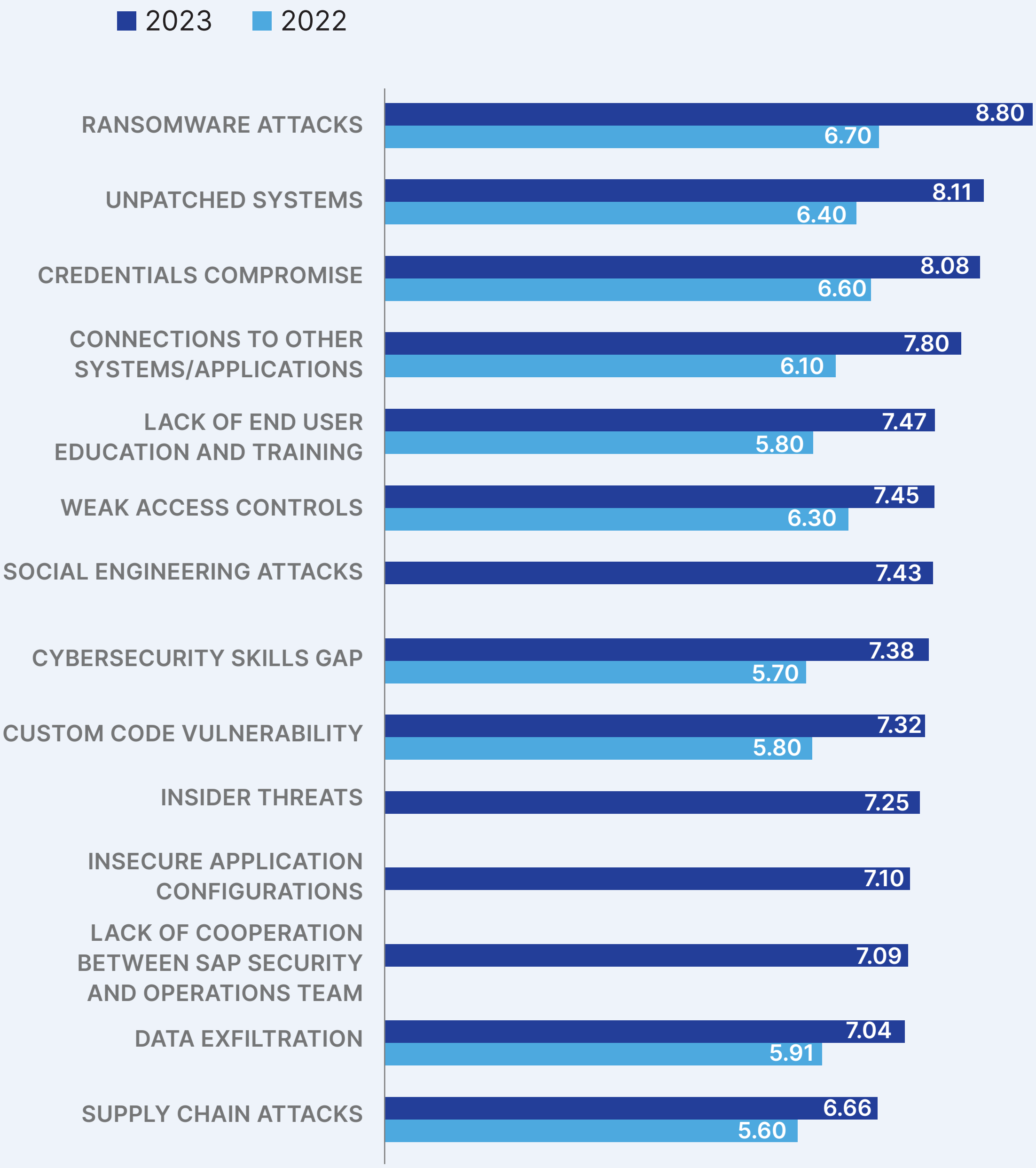
The top five factors impacting cybersecurity strategy in 2023 are protection for secure and confidential data (37%), system availability (33%), prevention of ransomware and malware attacks (29%), data protection compliance (23%), and cyber risk from connections to other systems (18%). These indicate the increasing importance of data integrity and availability that is driving security concerns in the SAP landscape **(See DARTdiagram on page 9).**

Protecting secure and confidential data is a complex subject that includes intrusion detection and prevention, application lifecycle management, patching and vulnerability remediation, secure data access management, secure coding practices, encryption, user access management, data input validation, data obfuscation, disaster recovery and business continuity planning, along with many regional-, industry-, and business-specific concerns.

Growth in the integration and hybridization of systems has fueled requirements for increased availability. However, cloud systems and applications connections that tie into vendor or customer experience, demands of a global economy, and the wide global reach of business-critical activities have created challenges for system maintenance.

This demand for increased availability, the second-most important factor impacting cybersecurity plans, complicates plans for software updating and patching. Urgent system updates for ransomware, malware, zero-day vulnerabilities, security updates, data integrity issue resolution, and other critical patches cannot be performed frequently, or as necessary, when there is a requirement for 100% availability.

Figure 1: Top Cybersecurity Threats to SAP Systems



Creative solutions with hot failover sites and clustering can aid this, but cost can be a limiting factor when considering such options.

Data protection compliance, the fourth-biggest factor impacting cybersecurity strategy, is driven by global-, regional-, and industry-specific regulations. As more of these regulatory requirements are created, the complexity of proving compliance increases. Annual audits or post-incident data forensic investigations also take significant time and effort from security and audit teams and add to the complexity of compliance challenges.

As cloud integration and migration continue to grow, the risks brought in by external connections have also grown. This year's survey included an answer choice of "risk from connections to other systems," and it was interesting to see it in the top five factors driving cybersecurity strategies. The continued growth of cloud migration, integration, data augmentation, virtualization, mobile device access, and Internet of Things (IoT) has made securing these connections a critical path for cybersecurity. Vulnerabilities because of unsecured systems and connections can be a direct channel to SAP for ransomware, malware, and other attacks.

When looking at the strategies used to address cyber risk against the top drivers for cybersecurity strategy and plans, a conflict is observed between regular patching and updating and keeping systems available. Keeping systems patched and updated is a challenge across the board when it comes to identifying the necessary updates, implementing the updates on non-production systems, testing, and ultimately getting downtime to implement the changes in the production systems.

Although the importance of conducting regular audits and security assessments decreased slightly, it is still a key strategy for managing security risk. Audits and assessments are often the only method for identifying unusual activity, over-provisioned users, and inappropriately used credentials.

Insider Perspective

"Moving into the world of cloud hosting of applications, we need to ensure our applications are being secured by our partners who run our cloud systems. This involves making sure that cybersecurity is being taken seriously and the appropriate controls and actions are being put in place. We cannot afford a data breach, or a loss of service, due to the potential adverse reputational impact."

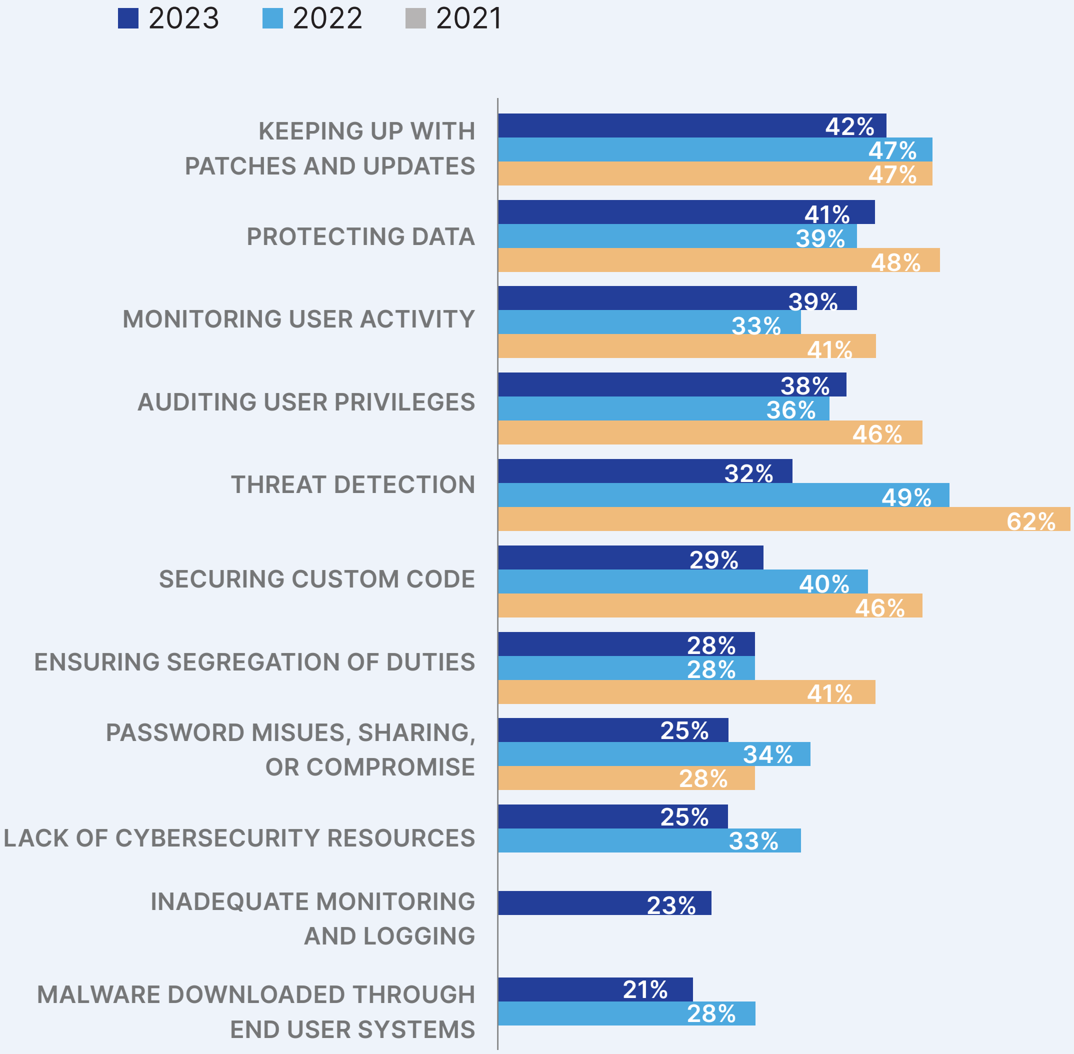
— SAP COE LEAD,
GLOBAL RETAILER

Training end-users to protect credentials from social engineering and other attacks continues to be in the top four risk management strategies. Security awareness training has become an annual mandate for many companies, with refresher courses each year.

Implementing automated monitoring and compliance solutions remains on the strategies list, dipping a little from last year. Automated monitoring and compliance solutions protect SAP System access, and detect and prevent ransomware, malware, and other vulnerabilities. These can also automate manual tasks performed by the SAP security and configuration management teams.

Beyond the cybersecurity threats, respondents were questioned on the challenges they faced when securing SAP systems **(Figure 2).** While threat detection was a top challenge over the last few years, it ranked number five in 2023. Keeping up with patches and updates has been in the top three challenges for the last three years, but this year, it is number one, sharing a slim margin with protecting data.

Figure 2: **Challenges Faced with Securing SAP Systems**



When correlating the top security threats with the challenges respondents had with securing those systems, system data security, confidentiality, and availability are often in direct conflict with the need to have downtime to patch systems.

But, why is patching so hard? Survey respondents were asked about the issues that contributed to a patching backlog. The results noted included difficulty scheduling downtime (45%), competing business priorities (40%), reluctance to apply notes/patches that could impact system availability (40%), difficulty understanding which patches are most critical (37%), limited resources to apply patches (34%), the volume of notes/patches (32%), difficulty validating whether patches are properly and correctly applied (29%), and the need to manually validate results of ALM tools patch recommendations (26%).

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. Each update requires an individual review ensuring its applicability, and a test plan that ascertains it remediates the problem it is meant to solve, and also that it does not introduce any new problems.

Once testing strategies are designed and the test plan is built, the application of these patches starts at the development system level and moves up through the entire landscape. Some patches are as simple as importing the code change, but others may require manual updates to the system configuration. Knowledge and skill are required to evaluate and implement the changes, which can potentially involve hundreds of systems and virtual machines. After testing is complete and a decision to move forward with applying patches to production environments is made, downtime needs to be scheduled. However, the need to protect data, secure custom code, and the lack of cybersecurity resources impact keeping up with patches and updates.

Overall, the trends over the last three years detail a shift from watching and waiting to respond to a potential attack to a focus on vulnerability management, data protection, user access management, and security education.

We also asked respondents in which areas of security is their organization investing or planning to invest **(Figure 3).** The top five planned investments were in the areas of threat detection and response, data security tools, role-based access controls, vulnerability management, and data encryption.

An interesting correlation between the elements required to provide a secure environment for SAP systems and areas for future security investment is the link between network security and threat detection and response. 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

Insider Perspective

"SAP systems contain a wealth of valuable data, including sensitive customer information, financial records, intellectual property, and trade secrets. These assets make SAP systems prime targets for data breaches and theft. The exposure of such sensitive data can result in legal and regulatory consequences, financial liabilities, and damage to an organization's reputation."

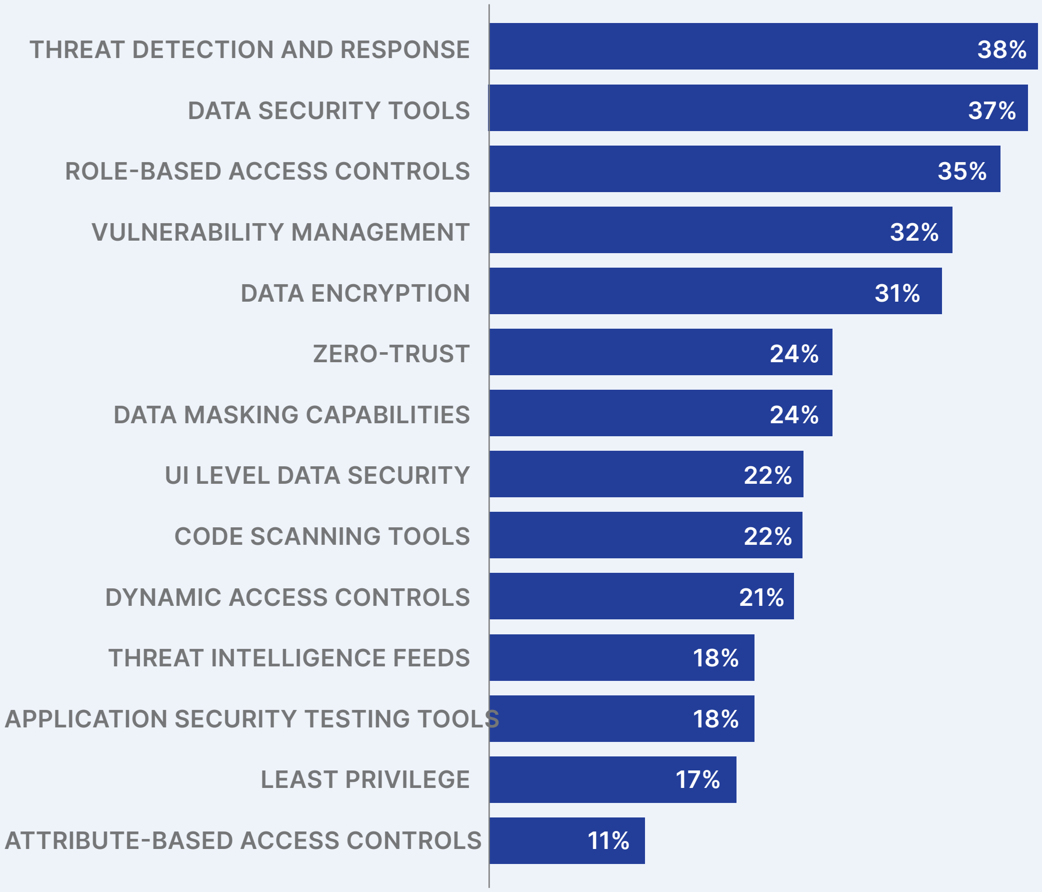
— PRODUCT DEVELOPMENT MANAGER, SOFTWARE COMPANY

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.

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

- Thirty-one percent of respondents said that their organization had experienced a credentials compromise or password misuse that had impacted their SAP systems; 29% have suffered a cybersecurity attack that has impacted their SAP environment; and 27% have suffered a malware attack that has impacted their SAP environment.
- The current economic climate is impacting cybersecurity efforts in many companies. Thirty-six percent of companies are evaluating lower cost solutions to reduce costs, 35% have put cybersecurity projects on hold, and 29% are scaling back planned investments.
- Cloud technology is useful for reducing architecture cost, but the ability to secure and monitor the integrated landscape effort has stayed the same or increased. Forty-nine percent of companies expect to manage security for their cloud environments using their internal teams, 35% feel that both on-premise and cloud systems require the same amount of effort to secure, and 62% of organizations are experiencing challenges with threat detection across multiple layers of the stack (e.g., cloud and on-premise or network and application layers).

Figure 3: Areas for Future Security Investment



REQUIRED ACTIONS

Based on the survey responses, organizations should make the following plans around their cybersecurity strategies:

- **Take a holistic view of your cybersecurity strategies to make sure they address the current threat vectors and challenges.** Moving from being focused on a couple of specific types of threats, like ransomware and malware, leaves your systems open to a multitude of other vulnerabilities. Focus your cybersecurity strategies on vulnerability management as a primary goal and threat detection as a secondary goal. This strategy needs to include patching, securing connections to other systems, cybersecurity education for end users, secure software development practices, and configuration management.
- **Create a patch management plan for your SAP systems and build in time for implementation.** Patching is a critical part of a cybersecurity vulnerability management program. Pushing this off because of system availability requirements or competing business priorities leaves your systems vulnerable to threat actors of all varieties. Consider implementing or expanding your Application Lifecycle Management system (SAP Solution Manager, SAP Cloud ALM, SAP Focused Run, or other non-SAP offerings) to help automate the patch management process.
- **Review your data protection, confidentiality, and security strategies and look for opportunities to improve.** Look at what technologies, policies, and practices you have in place for data protection. This would include data input validation, user access reviews (should a user have access to see or change this data), data at rest protections, backup and restore processes, and configuration management around software development and transport management processes. There are a lot of internal things that can be done to protect the confidentiality and integrity of your data without a major investment.
- **Implement a strategy to respond to breaches and attacks.** Whether your organization is concerned about user actions, system failures, or if your industry makes you a target for potential cyber-terrorist attacks, having a plan in place that can be quickly enacted following a breach or attack is essential. With the prevalence of cyberattacks across all industries and regions, no organization is immune from attack. The data within SAP systems is critical for ongoing operations, and this makes them a key target for attackers. Ensure that you have a strategy in place for how you will respond to cybersecurity breaches and attacks.

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%)

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

LAYER SEVEN SECURITY

Layer Seven Security secure SAP systems from cyber attack. The company's Cybersecurity Extension for SAP is a software addon for SAP ALM that delivers advanced vulnerability management, threat detection and custom code security for SAP solutions.

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

Microsoft Azure

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

ONAPSIS

Onapsis protects the business applications that run the global economy. The Onapsis Platform uniquely delivers vulnerability management, threat detection and response, change assurance, and continuous compliance for business-critical applications from leading vendors such as SAP, Oracle, and others. The Onapsis Platform is powered by the Onapsis Research Labs, the team responsible for the discovery and mitigation of more than 1,000 zero-day vulnerabilities in business-critical applications.

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

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

SUSE

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.