SAPinsider

BENCHMARK REPORT

Cloud Security Trends

For SAP Customers

Robert Holland

November 2022

REPORT SPONSORS

Microsoft Azure

pathlock

rubrik

SUSE

TABLE OF CONTENTS

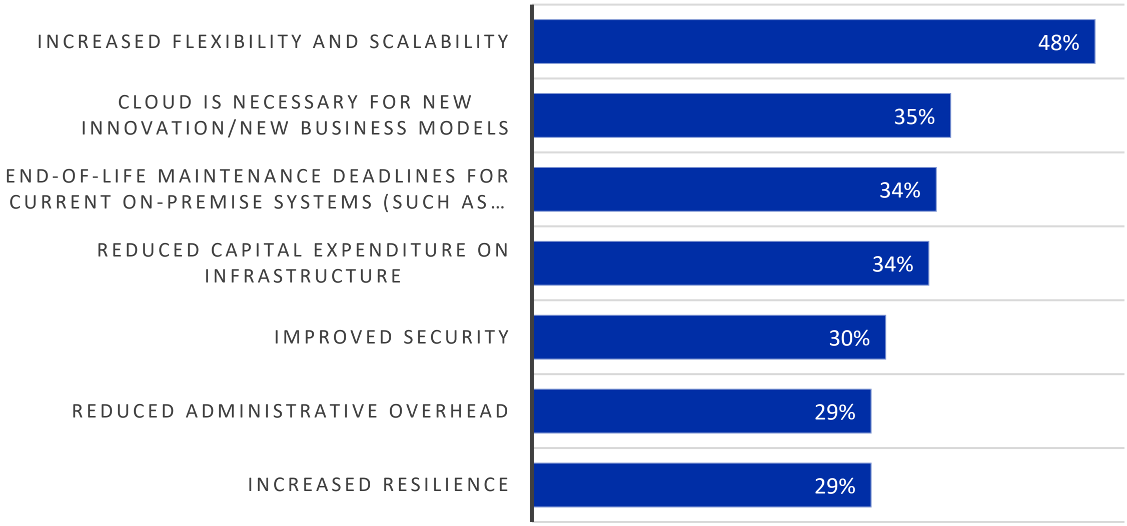
Executive Summary

The movement of enterprise workloads to the cloud continues to accelerate. Cloud environments, in one form or another, have been at the top of infrastructure choices for organizations over the last three years. This year, private cloud and public cloud environments were the top two infrastructure choices for organizations who are updating their SAP landscapes. And this does not consider how the many non-SAP solutions in use in today's business landscape are also moving to the cloud.

With so many applications moving to cloud environments, securing them is more important than ever. This is especially true with cybercrime on the rise globally, and the increased attack surface created by moving enterprise workloads to the cloud, makes it even more difficult for organizations to defend against cyber-attacks. The increase in cyber-attacks was demonstrated by the fact that 61% of respondents reported attacks made against at least one of their cloud providers. Having a security plan in place, for both cloud-based systems and the integration and data transfer points between those systems, is an imperative.

To learn more about the plans SAPinsiders have for securing their cloud environments, SAPinsider surveyed 162 members of our community between August and November 2022. The top business motivation for moving workloads to the cloud was that of increased flexibility and scalability, with nearly one in two respondents stating it as their primary motivator (**Figure 1**). This was followed by the cloud being necessary for innovation, end of maintenance deadlines for current on-premise systems, and a need for reduced capital expenditure on infrastructure.

Figure 1: Business motivations for adopting cloud-based applications



Source: SAPinsider, November 2022

INSIDER PERSPECTIVE

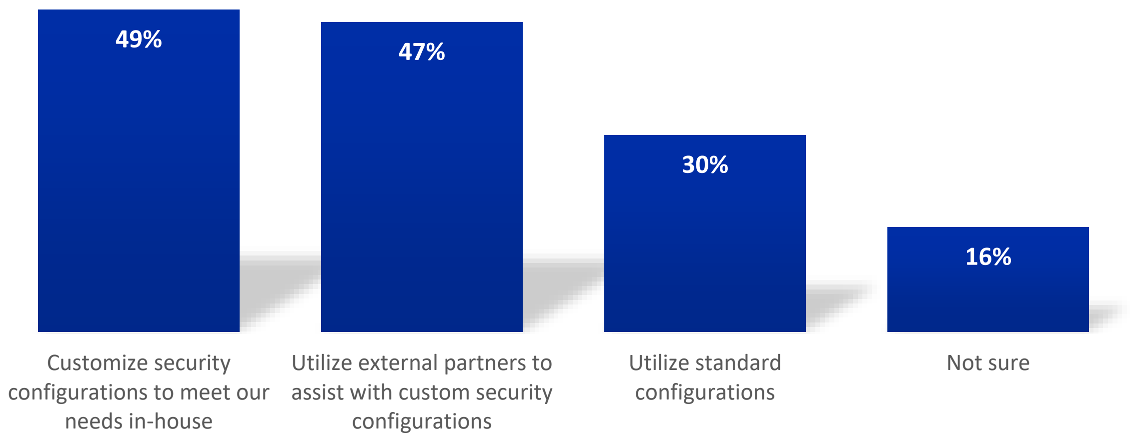
> "Cloud security is more important than ever before because organizations have to adapt and evolve with a changing landscape and still remain vigilant about confidential data. But the challenge is that changes are coming too fast for businesses to consume and manage. This makes it even more difficult to effectively secure systems."
>
> **~ Project Manager**
> **Software Company**

These motivatiors are similar to the finding's in SAPinsider's recent Enterprise Cloud Deployment report and what we have been tracking over the last four years. However, unlike the cloud deployment report where improved security was the second most important factor behind moving SAP workloads to the cloud, less than a third of respondents in this survey reported that improved security was a motivating factor for adopting cloud-based applications. This suggests that, while more security is a reason to move SAP workloads to the cloud, the focus is still primarily on flexibility, cost, and building a platform for innovation using cloud-based applications.

It is positive is that nearly eight in ten (79%) respondents reported that moving infrastructure and solutions to the cloud was an opportunity for their organizations to re-evaluate their security plans, policies, and solutions. This is important because moving workloads to the cloud both extends the security perimeter for organizations as well as increasing the potential attack surface. Re-evaluating existing security plans, reviewing policies, and determining if the right solutions are in place is essential for organizations and should be done regularly. This is especially true when there are significant landscape changes.

In terms of the process used for securing cloud systems and infrastructure, approximately half (49%) of the survey respondents said that they customized security configurations to meet their needs in-house, while almost as many (47%) utilized external partners to assist with custom security configurations (**Figure 2**). Customizing security configurations is important for organizations looking to tailor security settings based on their unique landscape while having in-house knowledge to complete these configurations is equally important. However, 35% of those customizing security configurations in-house are also utilizing external partners to assist with some configurations, and 37% using external partners also customize some configurations in-house.

Figure 2: Process for securing cloud systems and infrastructure



Source: SAPinsider, November 2022

While organizations are customizing security configurations that align with their landscapes, respondents have certain security expectations from their cloud service providers. Nearly two thirds (62%) said that they expect their cloud service providers to offer automatic security updates, and more than half expect vulnerability transparency (53%) and downtime thresholds (51%). These expectations, however, must be tempered with what can actually be provided. For example, while it is reasonable to expect that a company like SAP will offer automatic security updates on a software-as-a-service (SaaS) solution like SAP S/4HANA Cloud, automatic updates may not be available in infrastructure-as-a-service (IaaS) or other cloud environments. Respondent organizations must ensure that their security expectations from cloud service providers align with the services they are using.

In securing SAP and cloud landscapes, one of the challenges that organizations may face is the number of security vendors they engage with. Nearly half (46%) of respondents reported using 4-6 vendors, while 25% used 7-10, and 5% had more than ten. The number of vendors organizations are using is not surprising considering some solutions only address specific needs or provide specific functionality. However, 50% of respondents stated that they are looking to consolidate the number of vendors they work with because they needed simplified security management. Other reasons for looking to consolidate security vendors included improved security posture, reduced costs, and reduced complexity.

This year's survey revealed several other trends related to cloud security:

- More than two thirds (67%) of respondents have a patch management process in place for cloud infrastructure and cloud platforms. This is important as patching cloud-based environments can be much different than traditional systems.

- Six in ten respondents (60%) stated that their cloud vendor selection process includes ensuring their cloud vendors follow SOC 1 and SOC 2 compliance standards.

- More than half the respondents (56%) stated that they were running between six and ten cloud solutions, while 9% were running eleven or more.

- On average, respondents rated their organization's ability to secure cloud applications as 7.4 out of 10.

Required Actions

Based on the survey responses, organizations should take the following actions regarding cloud security:

- **Leverage moving solutions and infrastructure to the cloud as an opportunity to thoroughly evaluate your security plans, policies, and solutions.** Moving solutions and infrastructure to the cloud involves significant changes to an enterprise landscape. While most respondent organizations in this research are already using this opportunity to re-evaluate their security plans, it is critical that any organization moving workloads to the cloud take the time to thoroughly evaluate their security landscape. Doing this can ensure that the solutions and systems you plan to run in the cloud fits into your existing security plans. New security solutions, or updated versions of existing solutions, may need to be deployed in order to ensure that cloud systems are secure. But this is also where re-evaluating security plans, policies, and solutions may allow organizations to consolidate some of the mix of security solutions they are running today.

- **Educate security teams about what your cloud service provider offers and what your internal teams must support.** Not every cloud environment is the same. Organizations implementing SaaS solutions like SAP S/4HANA Cloud or SAP Success Factors have different security needs than running an IaaS environment in the private or public cloud. Ensuring that you thoroughly understand what the cloud service provider will secure and what your security or SAP teams need to secure is a crucial step in making any cloud security plan successful. Dedicate time to educate teams on these areas to avoid potential vulnerabilities developing in your attack surface. This should also include ensuring that security teams have the knowledge to customize security configurations to meet your specific needs.

- **Put security plans in place at the start of your cloud journey and ensure that business, IT, and security teams are aligned on those plans.** Many organizations start their cloud journeys unintentionally when business teams start using cloud-based solutions to meet specific needs or challenges. While this may address a critical need, scenarios like this can lead to security vulnerabilities. The most important step to address these challenges is to ensure alignment between business, IT, and security teams. One of the biggest challenges today is ensuring that an organization's security objectives are aligned with business objectives, and building that alignment into cloud plans is key to your success. In addition to aligning IT and business teams, it is also important that you include security planning at the beginning of your cloud journey. Trying to retrofit a security after deployments have stated can significantly delay the project and result in overlooking potential vulnerabilities. It is only by having security included from the start that you can ensure the security of cloud-based systems.

Chapter One: Cloud Security Overview

Organizations are moving workloads to the cloud for multiple reasons. While this may not yet be the case for all core workloads, many of the solutions that are integrated with these systems are starting to move to the cloud. This includes HR, CRM, analytics, planning, supply chain, and many others. With the enterprise landscape spread over multiple different infrastructures, it is more critical for organizations to ensure are their systems are secured against the ever-increasing threat of a successful cyber-attack. Threat actors can exploit vulnerabilities as soon as they are discovered, and having an appropriate security strategy in place is key to protecting your environment.

Best Practices Model – DART

SAPinsider grounds all its research insights in our proprietary DART model. This research model provides practical insights that connect business **D**rivers and **A**ctions to supporting **R**equirements and **T**echnologies. Drivers represent internal and external pressures that shape organizational direction. Organizations take Actions to address those Drivers. They need certain people, processes, and capabilities as Requirements for those strategies to succeed. Finally, they need enabling Technologies to fulfill their Requirements.

In this report, the top drivers for cloud security strategies were the need to secure data as it moves and is integrated between systems and environments, pressure to keep systems secure from growing ransomware and malware attacks, and changing regulations around data privacy. To satisfy these drivers, respondents indicated that they are implementing hybrid and multi-cloud environments for redundancy, regularly implementing patches and updates on platform-as-a-service-hosted (PaaS-hosted) applications, integrating new cloud systems with existing security processes, and implementing a zero-trust security model.

To support their ERP and innovation strategies, survey respondents highlighted several requirements they needed including improved endpoint security, strengthened access governance, threat intelligence, fully patched and updated hosted systems, real-time monitoring and logging capabilities, and effective management of cloud-based security controls. Respondents also use or plan to use a wide range of tools and technologies to support these requirements.

Respondents' answers to the survey and interview questions revealed clear trends that are summarized in **Table 1** and will be examined throughout this report.

INSIDER PERSPECTIVE

> "A big threat that SAP systems face today is that they are no longer a single on-prem system but a hybrid ecosystem of solutions. With the complexity of systems and applications in this ecosystem working together, in combination with the hacker community being more aware of exploits, SAP systems are being more targeted than before. There are more and more targeted attacks on the core of the organization, and the chance of being attacked is greater than ever."
>
> **~ Security Architect**
> **System Integrator**

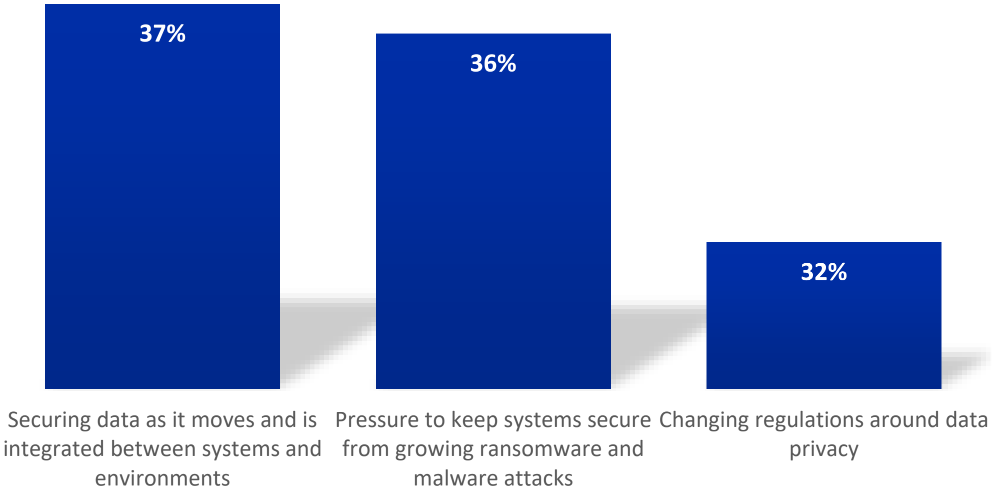
Table 1: DART model framework for enterprise cloud deployment

Drivers	Actions	Requirements	Technologies
• Securing data as it moves and is integrated between systems and environments (37%) • Pressure to keep systems secure from growing ransomware and malware attacks (36%) • Changing regulations around data privacy (32%)	• Hybrid and multi-cloud environments for redundancy (31%) • Regularly implementing patches and updates on PaaS-hosted apps (29%) • Integrating new cloud systems with existing security processes (28%) • Implementing a zero-trust security model (28%)	• Improved endpoint security (80%) • Strengthened access governance (77%) • Threat intelligence (75%) • Fully patched and updated hosted systems (73%) • Real-time monitoring and logging capabilities (73%) • Effective management of cloud-based security controls (73%)	• Access Control/Identity Management (24%) • Encrypted/secure connectivity (23%) • Vulnerability Management (21%) • Continuous Monitoring (20%) • Data Encryption (20%) • Security-driven networking (17%) • Dynamic authorization and least privilege (16%) • Zero-Trust Model (13%) • Code Vulnerability Analysis (12%) • Threat Intelligence Feeds (11%) • Behavioral analytics (10%)

What Drives Cloud Security Strategy?

The most important factor for cloud security strategy was that of securing data as it moves between integrated systems and environments (**Figure 3**). Selected by 37% of respondents, this is a very important part of today's security challenge and is often overlooked by organizations that may place a greater emphasis on securing the systems and not the integration points between them. The fact that this was chosen as the most important factor in driving cloud security strategy when asked to select the top two factors driving security strategy, suggests that organizations are recognizing the importance of this potential weakness in their attack surface, and are adapting their cloud security strategies to address this vulnerability before it can be exploited.

Figure 3: Top drivers for ERP and innovation



Source: SAPinsider, November 2022

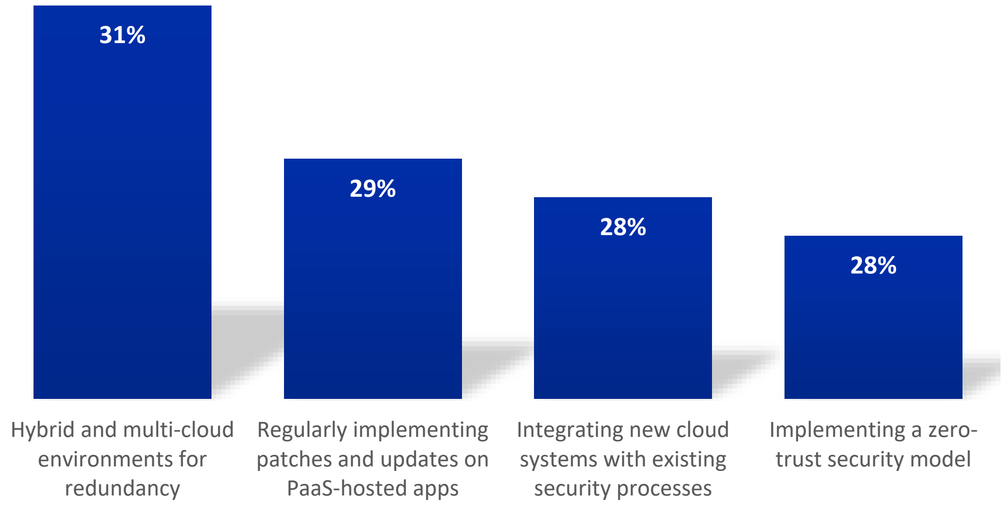
Pressure to keep systems secure from growing ransomware and malware attacks was the most important factor in driving strategy and plans for cybersecurity for SAP systems in the research we published earlier this year and is the second biggest factor behind cloud security strategy in this report. With new reports of ransomware or malware attacks in the media every day, even though these may not directly impact SAP systems, it is no surprise that this is one of the biggest drivers behind cloud security strategy for respondent organizations. However, organizations should also be aware that even though these types of attacks often receive the most attention they are not necessarily the biggest threats to SAP systems.

The last major factor driving cloud security strategy is changing regulations around data privacy. This is a particularly challenging area for organizations operating in EMEA where data privacy and data residency requirements can vary from country to country, and where even the ownership status of a cloud service provider can have in impact on what data can be stored on that provider as is the case in France. These regulations, even though they may not make up the majority of an organization's cloud security strategy, are an important part of the consideration process when formulating a cloud security strategy.

How Do SAPinsiders Address Their Drivers?

To address these drivers, organizations are taking several actions. The most important of these is having hybrid and multi-cloud environments for redundancy (**Figure 4**). This is important for overall resiliency in cloud applications, although it does not explicitly support any of the factors impacting cloud security strategy. However, having redundant systems can be very important in the event of a ransomware of malware attack so that an organization can recover quickly if their primary system is compromised. The fact that organizations are looking at hybrid and multi-cloud environments to provide this redundancy suggests that they are continuing to maintain some systems on-premise as well as running them either on at least two or more public clouds. This provides greater resilience in the event of a ransomware or other cyber-attack.

Figure 4: Top actions taken to address the top drivers



Source: SAPinsider, November 2022

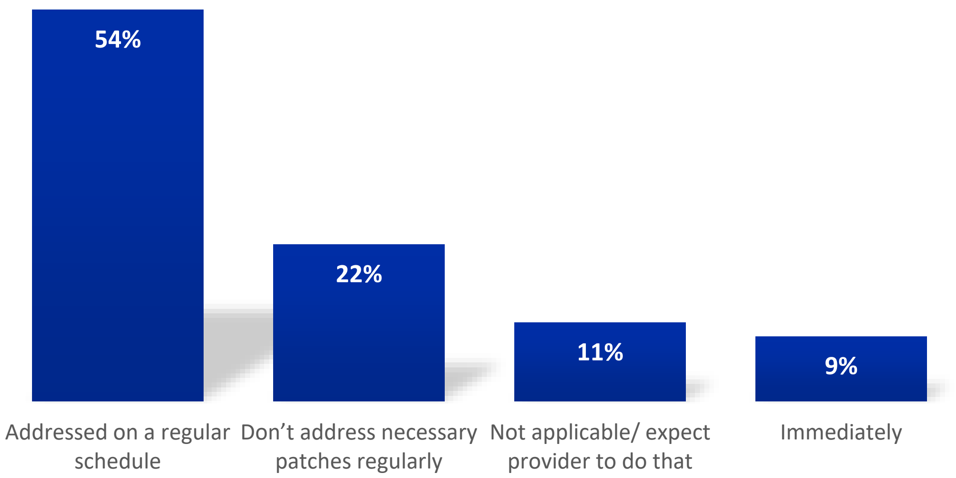
INSIDER PERSPECTIVE

> "Complexity is a driver for security challenges. ERP environments are already complex, and this complexity increases when you start integrating different technologies and concepts. Moving to the cloud introduces an additional layer of risk that needs to be factored into security plans. You need security architects, a threat model, and to understand where the risks are. The important thing is that organizations are seeing the move to the cloud as a compelling event to look at security."
>
> **~ CTO**
> **Technology Company**

Beyond having redundant environments, organizations are regularly implementing patches and updates on their PaaS based applications. While operating system and platform-related patches are typically applied by the vendor, organizations using PaaS applications need to manage the deployment of patches to the software they have installed. This is different than a SaaS environment, for example, where the vendor manages both software and infrastructure patching.

But having a patching strategy for any cloud-based systems or solutions is very important. Many SAP teams struggle to keep up with patches, which is why implementing and following a strategy can significantly help reduce the risk of cyber-attacks. Given how important regular patching is to reducing vulnerabilities, we asked respondents about their strategies for patching their cloud infrastructure and platforms (**Figure 5**). More than half (54%) stated that they addressed patches on a regular schedule, while 9% responded that they implemented new patches immediately. What was concerning was that almost a quarter (22%) don't address necessary patches regularly, while 11% expected their providers to implement patches. This may be a reasonable expectation for a SaaS solution, but organizations running IaaS environments must understand that they are responsible for software and operating system patches in those environments as the service provider only patches infrastructure.

Figure 5: Patching strategy for cloud infrastructure and platforms



Source: SAPinsider, November 2022

Integrating new cloud systems with existing security processes (28%) is the third most important action being taken by respondents. Having this integration ensures that the newly deployed cloud environments are protected from the start, which will help in protecting systems from ransomware and malware attacks and in securing data as it moves between environments. But organizations must ensure that as they integrate their cloud systems with existing security processes that data exchange is protect as well as the solutions themselves.

The last action being taken by organizations is of implementing a zero-trust security model. Zero-trust security models requires every device and user, whether inside or outside an organization's network, to verify and authenticate their connection. Zero-trust models can provide added security against ransomware and cybersecurity threats because they assign the least required access needed to perform specific tasks. They also help with protecting data as it moves between systems and environments by ensuring that every device connected to the network is authenticated, limiting the presence of untrusted devices.

Key Takeaways

When it comes to connecting cloud security strategy to business drivers and the requirements you must meet, the following takeaways are clear:

- **Ensure that you are securing data as it moves between systems as well as the data that is within cloud-based systems**. Most SAP security has historically focused on securing data in systems using a combination of access control and process control. While organizations have adapted to today's security challenges and are ensuring that their security strategy does more than than just ensuring that users only have access to the data for which they are authorized, securing data as it moves between systems is often overlooked. As you develop your cloud security strategy, ensure that it secures data as it moves and is integrated between systems and environments because this is a point where data can be compromised.

- **Keep your teams up to date about data privacy regulations and how they impact infrastructure choices.** Data residency is the most commonly considered guideline when it comes to how regulations for data privacy impact the way data can flow across borders. But while organizations may be aware of where their data must be stored geographically, data sovereignty can impact whether there is a governmental right of access to data stored within their borders, and data localization ensures that data created within certain borders remain within those borders. Keeping up with these data regulations, and which providers can be used for certain data types, can be challenging and expensive from an infrastructure perspective. Ensure that security and compliance teams are continually updated on changing data privacy regulations and how that might potentially impact cloud environments and cloud security strategy.

- **Create and implement a regular patching schedule for both on-premise and cloud-based systems and environments.** One of the biggest challenges identified by respondents to our March report on cybersecurity threats to SAP systems was keeping up with patches and updates. When deploying cloud-based systems this can become increasingly complex with some patches being managed by cloud service providers while others need to be maintained by the organization owning those systems. And when an organization is running a combination of different cloud environments it can be easy to overlook deploying patches for systems deployed in IaaS or PaaS environments because the responsibility for deploying those patches varies. Creating and implementing a regular patching schedule, as well as understanding criteria for reacting to critical updates, is key to ensuring the security of cloud-based solutions.

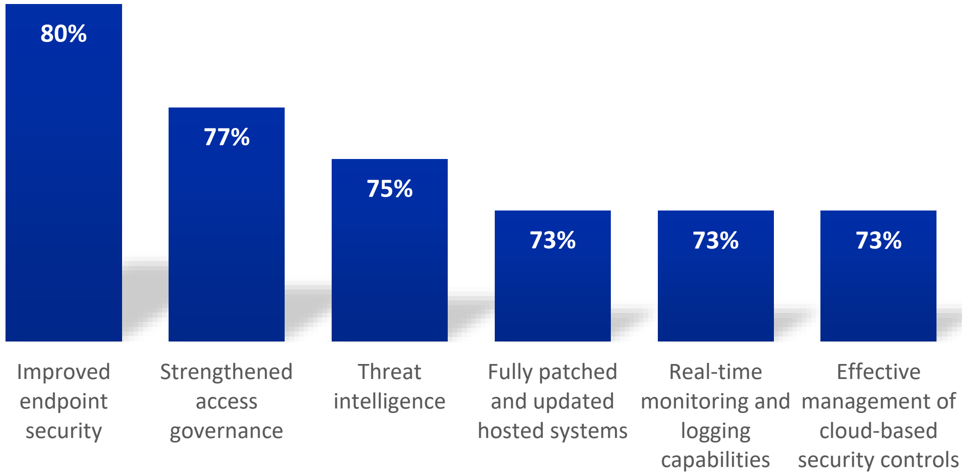
Chapter Two: How Do SAPinsiders Approach Their Cloud Security Strategy?

We have seen that respondents are driven by a need to secure data both within their systems and as it moves between environments as well as the pressure to keep systems secure from ransomware and malware attacks. In response to these challenges, they are patching regularly, integrating their cloud systems with existing security processes and solutions, implementing new security frameworks such as a zero-trust model to reduce their potential attack surface. We will now explore the requirements that they must meet as they take these actions and the technologies that they are using to make their cloud security strategy a reality.

Top Cloud Security Requirements

When asked to rank the importance of different requirements to their cloud security strategies, respondents were consistent in the way they responded. No requirement had more than 15% of our respondents say that it was not important or only slightly important, and only two requirements had less than 25% of our respondents not select them as being very important. This led to a set of closely ranked requirements as seen in **Figure 6**. But this also means that all these requirements are important for a successful cloud security strategy.

Figure 6: Top requirements for ERP and innovation



Source: SAPinsider, November 2022

INSIDER PERSPECTIVE

Cloud security is important because there are more dangers out there than in the past. Just as we would not leave our office doors unlocked, we need to ensure that our online projects are locked and secure. But even keeping up with patches is a significant project. The most important thing for me is to see what is working for others and separating the hype can often be my most important skill set.

“

~ Architect
Regional Manufacturer

Endpoint security is about ensuring that end-user devices such as desktops, laptops, and mobile devices are secure. Given that users increasingly want access to data irrespective of their location, it is no surprise that improved endpoint security is the top requirement of any cloud security strategy. This can often be a part of a zero-trust model but will also help reduce ransomware and malware attack vectors.

Strengthened access governance helps support changing regulations around data privacy as it ensures that users only have access to the data that they are supposed to see. But access governance goes beyond access control to verify who has data to what, when they have access to that data, and how they access it. This can be part of the zero-trust model where every device and user must verify access when connecting to the network. Appropriate access governance also ensures that data privacy regulations are being met.

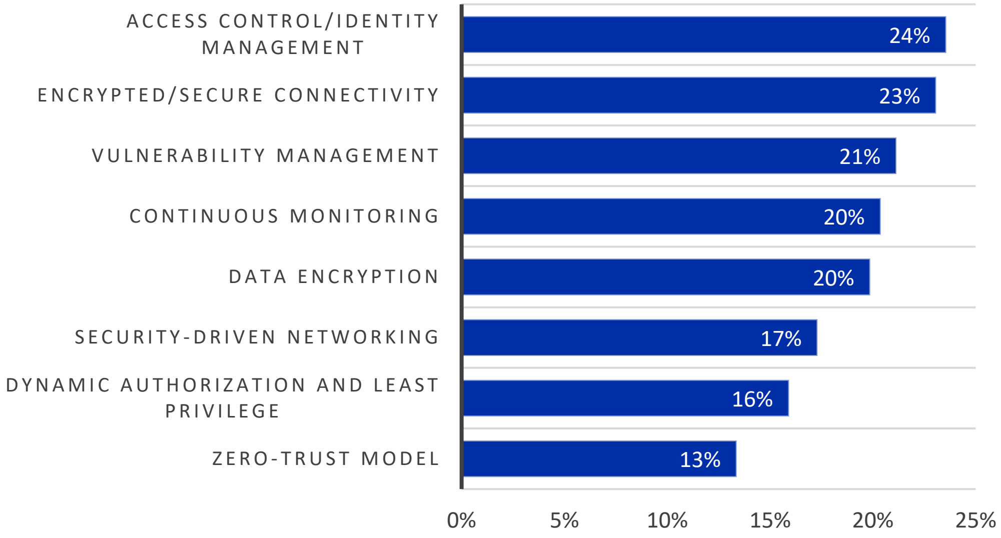
Increased adoption of threat intelligence was something we observed in our March report. Threat intelligence allows organizations to access data that has been collected, processed, and analyzed to understand potential targets and attack behaviors. By monitoring threat intelligence feeds organizations can learn about potential vulnerabilities and address them in real-time before they can be exploited. This helps reduce the risk of ransomware and malware attacks, and makes systems more secure in general.

Fully patched and updated systems were described at length in the previous chapter but having requirements for patching in place is part of a complete cloud security strategy. Other parts of this complete security strategy include real-time monitoring and logging capabilities, and effective management of cloud-based security controls. These three requirements are important for keeping systems patched, integrating new systems with existing security processes, keeping systems secure from cyber-attacks, and securing data as it moves between environments. All these requirements should be included in a broader cloud security strategy.

Which Technologies do Respondents Use for Cloud Security?

Historically the primary security model used for SAP systems was focused on ensuring that users only had access to the appropriate data. This evolved into SAP Access Control which, in combination with identity management, is used in the majority of SAP ERP systems today. Similar technologies are applicable to cloud-based SAP solutions, so there is no surprise that access control is the most used technology by respondents today (**Figure 7**).

Figure 7: Tools and technologies currently in use for cloud security



Source: SAPinsider, November 2022

Beyond access control the next most used technology is secure and encrypted connectivity. This is especially important for protecting data moving between systems, when securing the connection between users and systems, and can be a part of improving endpoint security. Many organizations also have dedicated secure connections between on-premise systems and their cloud environments, that increases the security of those connections.

Vulnerability management is less a technology and more a methodology that involves continuously monitoring and assessing potential risks before they can become vulnerabilities. While some organizations were leveraging vulnerability management in their broader SAP cybersecurity plans, it is encouraging to see an increasing number of respondents leveraging vulnerability management when it comes to their cloud security strategies.

Continuous monitoring can be a part of vulnerability management but is also a separate technology that allows organizations to maintain ongoing awareness of information security, vulnerabilities, and threats. For SAP systems it can also be used to look for any anomalous activity in the system which could be anything from an unexpected login to an unusual posting within a system.

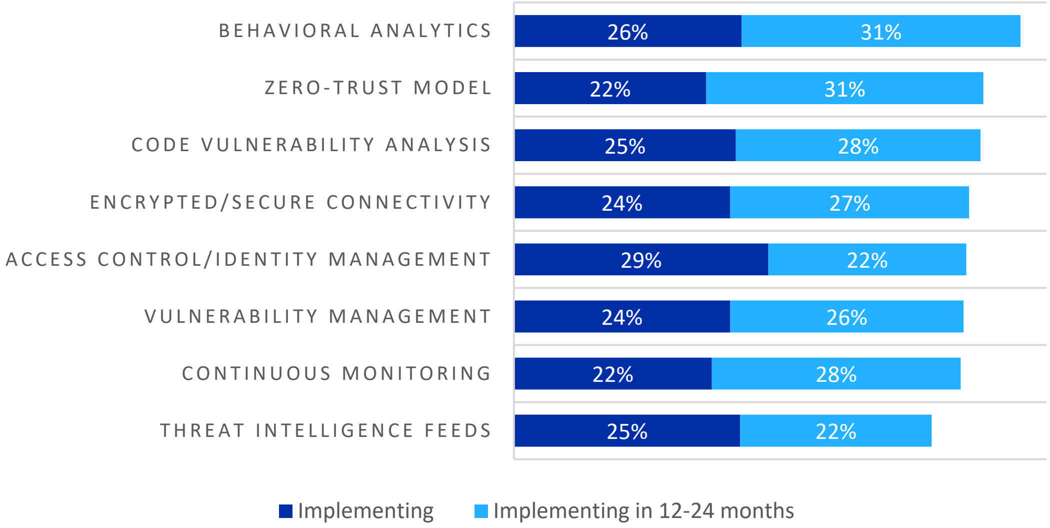
Other currently used technologies include data encryption, security-driven networking, dynamic authorization and least privilege which centralizes authorization policies and assigns the lowest privilege to any connection that is not authorized, and a zero-trust model.

INSIDER PERSPECTIVE

> "Zero-trust is a technology that companies are starting to adopt. But they are also focusing on hardening systems as well as threat monitoring and continuous vulnerability management. But even once set up, security plans must be updated and changed. If organizations miss these updates their systems may become more vulnerable to attack. Vulnerability management helps with this, but also important is data masking and data scrambling. This should especially be used in non-productive environments."
>
> **~ Security Architect**
> **System Integrator**

When we examine technologies being implemented, more than half (57%) of the respondents plan on implementing behavioral analytics over the next two years (**Figure 8**). A form of continuous monitoring, behavioral analytics leverages machine learning to collect and analyze data from actions performed by users. This can help organizations understand normal baseline behaviors for networks, users, and solutions to help identify aberrant behaviors. It also allows organizations to potentially detect when an individual's credentials have been compromised.

Figure 8: Cloud security tools and technologies being implemented



Source: SAPinsider, November 2022

We previously discussed the benefits of zero-trust models, but only a small number of respondent organizations reported that they were using them today. This number is likely to grow with 53% of respondents stating that their organizations plan to deploy zero-trust models as part of their cloud security strategy over the next two years.

Code vulnerability analysis is very important for most organizations running SAP systems due to the volume of custom code that exists in those systems. SAP's own solution identifies and helps address security vulnerabilities in ABAP code, but in a broader sense having tools that can help scan code developed for cloud applications or in applications that are moving to the cloud is hugely important to ensure that no exploitable code is included in applications.

Other technologies being implemented include access control and identity management, vulnerability management, continuous monitoring, and threat intelligence feeds. While threat intelligence was a requirement for organizations implementing a cloud security strategy, threat intelligence feeds help organizations to act on threat intelligence. Threat intelligence feeds provide actionable intelligence through warnings of newly disclosed weaknesses and planned attacks that a broader threat intelligence initiative may find difficult to reveal due to the volumes of data involved. Having threat intelligence feeds implemented is extremely important for reacting to and addressing newly discovered risks before they become vulnerabilities.

Technologies that respondents identified as being evaluated for use in their landscape include threat intelligence feeds (29%), dynamic authorization and least privilege (27%), security-driven networking (27%), code vulnerability analysis (26%), data encryption (26%), and zero-trust models (23%).

Key Takeaways

When it comes to equipping organizations with the capabilities and technologies required for an SAP landscape, consider the following:

- **Determine how you can improve security around endpoints and where users access your systems.** A part of this process should be focused on continuing education of end-users about threats like social engineering and how to ensure that they do not inadvertently compromise their credentials. Other steps may include hardening and improving authorization or evaluating zero-trust security models to ensure unauthorized devices are not able to access a network or system. More traditional authorization methods like two-factor authentication and multi-factor authentication should be part of this discussion as they can be used for accessing endpoints and when logging into a system or solution.

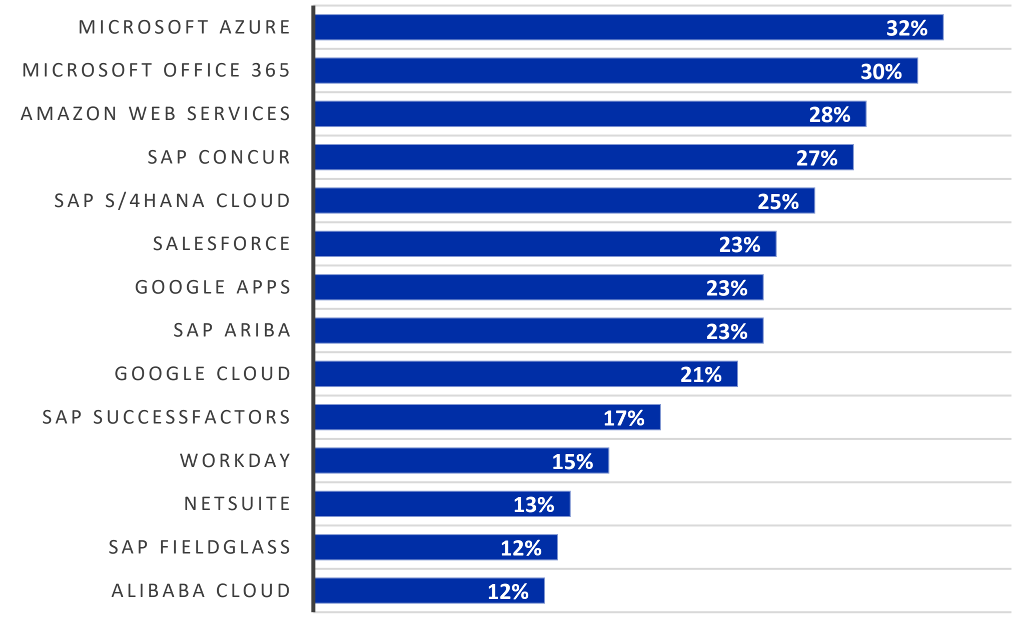
- Explore adopting threat intelligence in your cloud security strategy so that you can quickly react to newly discovered weaknesses. Threat intelligence, and threat intelligence feeds as a technology, are crucial for learning about newly discovered weaknesses and ensuring that they can be addressed before they become vulnerabilities. Threat intelligence feeds should be a part of your cloud security strategy as they help distill the volume of data that can be generated in broader threat intelligence into actionable tasks that security teams can immediately initiate. This can be crucial when a newly discovered common vulnerability and exposure (CVE) is discovered that impacts cloud infrastructure or cloud-based systems.

- **Evaluate behavioral analytics and the benefits that they can bring to your cloud security strategy**. Understanding what is normal in your environment and when something is anomalous can be a complex task when that environment consists of multiple of systems in different landscapes with dozens of connection points and thousands of users. Leveraging the capabilities of machine learning to help build a picture of normal system behavior will make discovering something unusual much easier should that occur. With cyber-attacks showing no sign of decreasing and a majority of organizations globally having experienced some form of cyber-attack over the past year, it is only a matter of time until you will need a technology like behavioral analytics to help reveal when a breach has occurred.

Chapter Three: Required Actions

Enterprise workloads are moving to the cloud and SAP workloads are very much part of that move. However, when creating a cloud security strategy, organizations must consider more than just their SAP workloads. Few organizations today are running only SAP solutions in their landscape. We can see just how widespread their solution base is in **Figure 9**.

Figure 9: Cloud solutions that are part of a cloud security strategy



Source: SAPinsider, November 2022

Organizations must not only consider their cloud service providers when determining their security strategy, they must also consider connected productivity solutions such as Microsoft Office 365. This is especially true with the Microsoft Teams integrations that now exist with SAP S/4HANA, SAP SuccessFactors, and SAP Customer Experience. A significant proportion of respondents are also running third-party solutions which must also be included in any cloud security plans.

As organizations formulate their cloud security plans, there are a number of points they must consider. Are their existing security solutions meeting their needs? Can new cloud deployments be covered by those solutions? Are new security capabilities required? Will those solutions secure data as it moves between systems and environments? Will they help meet new and changing data privacy regulations?

INSIDER PERSPECTIVE

> "
>
> For many organizations there is confusion in cloud service models and the security requirements needed for those models. SaaS is different from IaaS and PaaS. This is complicated by it being rare to go cloud first and use only cloud services and do everything using software-as-a-service models. This makes the environment a mixture of deployment models and solutions and makes it more complex to secure.
>
> "
>
> **~ CTO**
> **Technology Company**

All these are important points for organizations because the future of the enterprise is in the cloud. Even if some systems may remain on-premise for some years to come, key enterprise workloads are already there. So it is vital that any security strategy includes where the organizations' systems will be running in the future.

Steps to Success

Our research reveals that SAP customers should take the following key steps to ensure their cloud security strategy has a foundation for success:

- **Use the deployment of cloud-based solutions as an opportunity to evaluate and update security strategies.** Cyberattacks and the technologies they leverage are constantly evolving. New vulnerabilities are regularly discovered or revealed, and business are constantly playing catch up to address those vulnerabilities. When an organization starts deploying cloud-based applications the potential attack surface is increased. This makes it even more important to have an effective and up to date security strategy. Almost eight in 10 respondents are using the move to the cloud as an opportunity to evaluate and update security plans, policies, and solutions. You should do the same.

- **Build security into any new application deployment from the start of the process**. The best time to determine security plans for new applications or environments is before they are used. It is much easier to adjust plans for a new solution to ensure that it fits into existing security strategy at the start of the process than to have to retrofit them later. Just as it is important to use a move to the cloud as an opportunity to evaluate and update existing security plans, it is also important to put security front and center in the business case for any new solution. Securing data and systems has never been more important and making security central to any plans is essential for success.

- **Include data movement and integration points in cloud security strategies in addition to SAP and non-SAP solutions.** SAP teams may put the applications that they manage first, but these solutions do not exist in a vacuum. Most SAP systems are connected to multiple other systems in the enterprise. Any effective security strategy must include not just SAP systems but the other solutions they are integrated with. The strategy must also go beyond the solutions themselves to include the movement of data between solutions and landscapes and the integration points between them. Failure to secure data movement and integration points can lead to vulnerabilities at those points and the potential for data loss or exfiltration. This is why it is essential to include data movement and integration in your security strategy.

- **Evaluate and deploy technologies that will help expand the capabilities of cloud security strategies.** Many new technologies will help enhance an organization's security stance. Those being evaluated or implemented by respondents include behavioral analytics, a zero-trust model, threat intelligence feeds, dynamic authorization and least privilege, and security-driven networking. All of these technologies can significantly enhance the security capabilities of any organization. However, they must be worked into existing budgets, vendor relationships, and security strategies. Your organization may restrict their focus to making the most of existing solutions, but you should continue to evaluate and explore technologies that will reduce vulnerabilities as well as an organization's attack surface.

Methodology

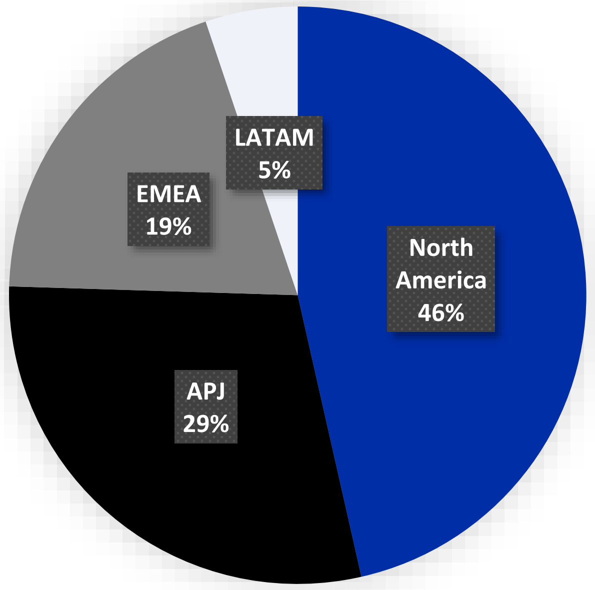
Between August and November 2022, SAPinsider surveyed business and technology professionals about their plans for securing their cloud solutions. Our survey was administered to 162 members of the SAPinsider community and generated responses from a wide range of geographies, industries, and companies. Respondents completed an online survey and provided feedback in customer interviews that contained topics such as:

- What are your top business motivations for adopting cloud-based applications?
- What expectations do you set for your cloud providers around security?
- Has your organization been subject to an attack on one of your cloud providers?
- Do you have a patch management process in place for cloud infrastructure and cloud platforms?
- Which cloud offerings are part of your security strategy?

The demographics of the respondents included the following:

- **Job function:** Functional areas reported by respondents include: IT Management (32%); IT Operations (17%); SAP Team (13%); Finance or Accounting (9%); Security (7%); Systems Implementation & Integration (7%); GRC (5%); and application Development (5%).
- **Market sector:** The survey respondents came from every major economic sector, including: Industrial (24%); Software & Technology (19%); Hospitality, Transportation, and Travel (15%); Financial Services & Insurance (12%); Media & Entertainment (10%); Healthcare & Life Sciences (9%); Public Sector (7%); and Retail, Distribution, and CPG (3%).
- **Organization size:** Survey respondents came from organizations of all sizes, including those with annual revenue: less than $10 million (5%); between $10 million and $49 million (14%); between $50 million and $499 million (25%); between $500 million and $2 billion (28%); between $2 billion and $10 billion (14%); and greater than $10 billion (10%).
- **Geography:** Of our survey respondents, 46% were from North America; 29% were from Asia-Pacific, Japan, and Australia (APJ); 19% were from Europe, the Middle East, and Africa (EMEA); and 5% were from Latin America (LATAM).

PARTICIPANT PROFILE



Appendix A:
The DART^{TM} 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 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

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/

pathlock

Pathlock brings simplicity to customers who are facing the security, risk, and compliance complexities of a digitally transformed organization. Pathlock provides a single platform to unify access governance, automate audit and compliance processes, and fortify application security. With integration to 140+ applications and counting, Pathlock customers 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.

Learn more at https://www.pathlock.com/

rubrik

Rubrik is a cybersecurity company. We are the pioneer in Zero Trust Data Security™. Companies around the world rely on Rubrik for business resilience against cyber attacks, malicious insiders, and operational disruptions. Rubrik Security Cloud, powered by machine intelligence, enables our customers to secure data across their enterprise, cloud, and SaaS applications. We automatically protect data from cyber attacks, continuously monitor data risks, and quickly recover data and applications.

For more information please visit www.rubrik.com and follow @rubrikInc on Twitter and Rubrik, Inc. on LinkedIn.

SUSE

SUSE is a global leader in innovative, reliable and enterprise-grade open source solutions, relied upon by more than 60% of the Fortune 500 to power their mission-critical workloads. We specialize in Enterprise Linux, Kubernetes Management, and Edge solutions, and collaborate with partners and communities to empower our customers to innovate everywhere – from the data center, to the cloud, to the edge and beyond. 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 www.suse.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.