SAPinsider

A Wellesley Information Services Company

SAPinsider Benchmark Report

Securing the SAP Landscape Against Cyber Threats

Robert Holland

April 2021

Report Sponsors

CyberSafe

onapsis

COMMVAULT

SAPinsider
A Wellesley Information Services Company

Table of Contents

Executive Summary 1
Required Actions 4
Chapter One: Securing the SAP Landscape Overview 6
Best Practices Model – DART 6
What Drives Security for the SAP Landscape? 7
How Do SAPinsiders Address Their Drivers? 9
Key Takeaways 10
Chapter Two: How Do SAPinsiders Approach Securing Their SAP Landscape? 13
Top Cybersecurity Requirements 13
Which Technologies Do Respondents Use to Secure Their SAP Systems? 14
Key Takeaways 17
Chapter Three: Required Actions 19
Steps to Success 20
Methodology 22
Appendix A: 23
The DART™ Methodology 23
Report Sponsors 24

Executive Summary

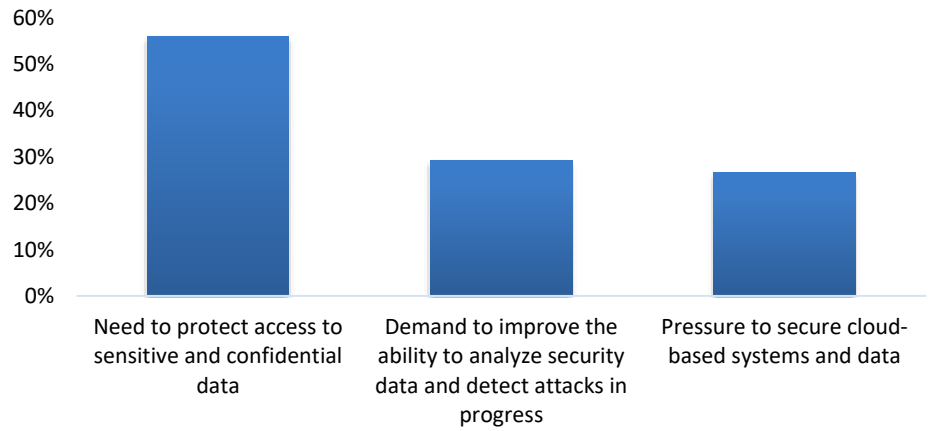
SAP systems and the critical data they contain are being targeted by cybersecurity attacks at an increasing rate. Multiple forces are driving this change. First, the data contained within SAP systems has become even more essential to the organization, and therefore more attractive to hackers, due to increased integration between systems, with applications like SAP SuccessFactors and SAP Ariba now connected with financial and ERP systems. Second, there is more information being found and shared about potential exploits and security flaws, making exploiting these flaws easier. Third, a largely remote workforce has placed systems at higher risk as user roles and access broaden to facilitate teams no longer under the same roof.

To understand what SAP customers are doing to secure the systems in their SAP landscape, SAPinsider surveyed 263 members of our community in March and April of 2021. The goal of the survey was to understand the most important factors driving security choices, and what strategies are being taken to address these factors. By far the greatest need for survey respondents (56%) was that of protecting access to sensitive and confidential data (**Figure 1**).

SAPinsider PERSPECTIVE

> Today, our company's critical assets and processes are supported by SAP (Finance, Manufacturing, Supply Chain, Sales, HR, etc.). For that reason, securing our SAP systems is critical for us.
>
> ~ Cybersecurity Manager
> Healthcare Company

Figure 1: Top drivers for securing SAP systems

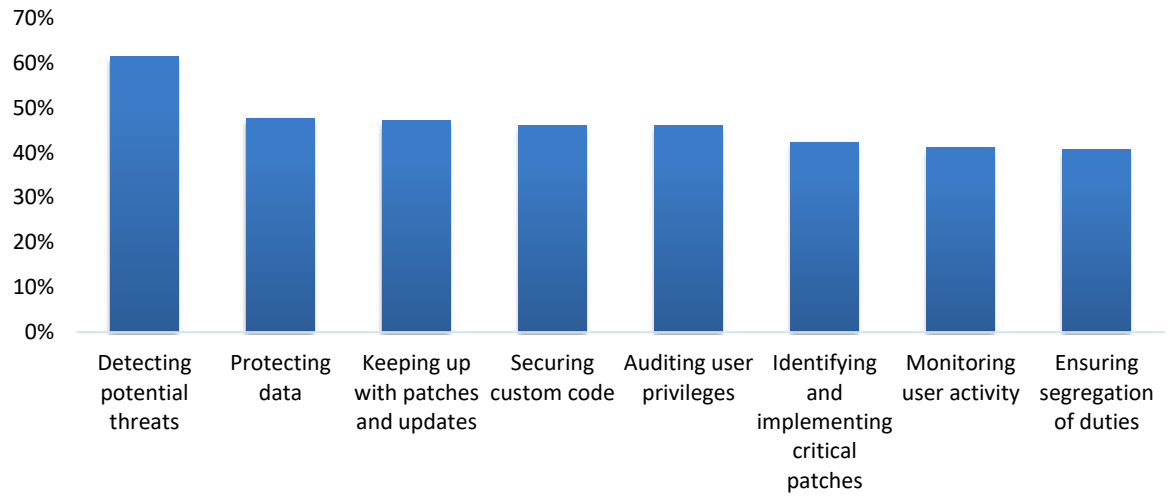


Source: SAPinsider, April 2021

This need is driving security considerations for the SAP landscape more than ever. With organizations using the move to SAP S/4HANA to create a single source of business and financial truth, this makes for a much more attractive target that, if breached, can expose a vast amount of sensitive information.

Detecting potential threats was identified by survey respondents (62%) as the biggest challenge that they face when it comes to protecting their data. This ranked as a significantly greater challenge than others identified, like protecting data (48%), keeping up with patches (47%), securing custom code (46%), and auditing user privileges (46%) as seen in **Figure 2**. Detecting potential threats may be considered most challenging because these threats are not necessarily dependent on security being breached or a firewall being compromised — which is likely to be flagged immediately — but rather commonly occur via social engineering or credential misuse.

Figure 2: What challenges are you currently facing with securing your SAP systems and landscape?



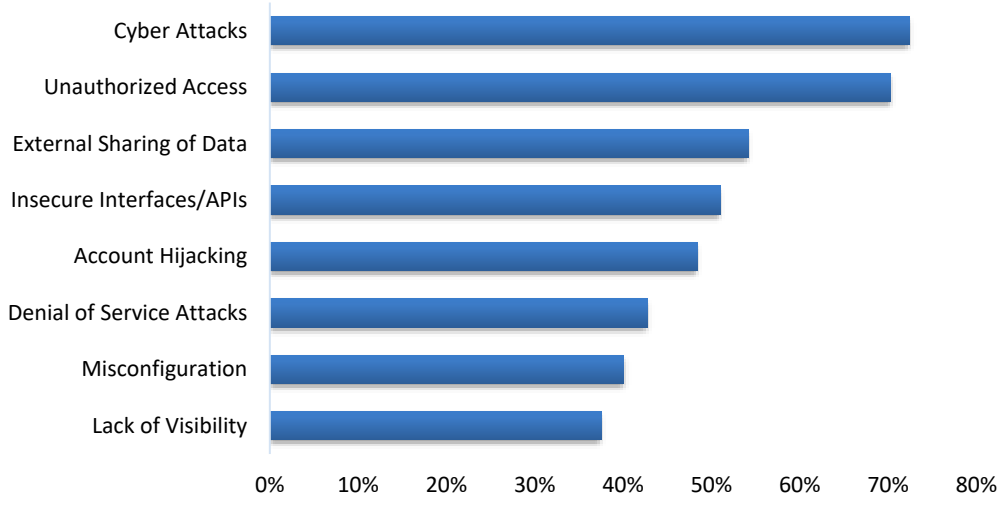
Source: SAPinsider, April 2021

Consider for example that an unauthorized user obtains the credentials of a registered user via social engineering or a password being shared. Logins using those authorized credentials

may not be detected for days or weeks, as the login may not appear to be anything other than a standard use of the system. This can be especially true if the user continues to perform his or her daily activities which may make it harder to separate normal usage from abnormal. It is only when using and examining tools like audit logs that it may be possible to determine that the compromised account is performing actions or accessing data that it should not be.

Respondents that are using cloud-based systems have concerns of their own, including potential cyberattacks and unauthorized access to those systems (see **Figure 3**). Not only can securing these cloud-based systems require different tools or technologies, an organization's responsibility for, and insight into, security can vary significantly depending on what type of cloud environment they are using.

Figure 3: What security concerns do you have with cloud deployments?



Source: SAPinsider, April 2021

SAPinsider PERSPECTIVE

"Social engineering is a threat we take seriously. Every 2-3 months the security team makes available threat training that is well-targeted and contains guided examples. End-users must click though and are tested on what is suspicious. This training is mandatory, and the results are checked. Someone follows up if they are not completed."

~ Basis Lead
Global Industrial Company

This year's survey revealed several other trends regarding respondents' plans for securing their SAP landscape:

- Over two thirds of survey respondents (67%) said that they are relying on a combination of SAP and non-SAP tools to ensure that their SAP systems are secure and to resolve challenges around protecting data, detecting potential threats, and avoiding cyber-attacks and unauthorized access.
- Over a quarter of respondents (27%) said that their company has experienced credentials being obtained through either social engineering (phishing attacks) or a form of password misuse, showing that systems are vulnerable even when they are fully patched and up to date.
- Although those running cloud-based systems are most concerned about cyber-attacks and unauthorized access, 66% of survey respondents said that they believed their cloud service provider was sufficiently securing their systems and data. This did not necessarily reduce their concerns about the potential threats to those systems.

Required Actions

Based on the survey responses, organizations should make the following plans around their SAP S/4HANA transitions:

- **Evaluate the security solutions and practices you have in place for your SAP systems. Do they address your biggest challenges?** The biggest driver around protecting SAP systems is the need to protect sensitive and confidential data. And the biggest challenge is detecting potential threats. If your security solutions and practices do not help you meet these challenges, then they are not effectively protecting your data.
- **Develop a proactive methodology for detecting threats to those systems and ensure it provides the monitoring you need.** Determining when unauthorized access is occurring within a

system can be a huge challenge for organizations, especially when that access may be occurring using legitimate credentials. You must understand how potential threats to your systems are being detected. Do you use the audit log? Is UI logging appropriate? How are you analyzing those logs? Are tools like SAP Enterprise Threat Detection something you should explore? With cybersecurity failure having both a significant impact on organizations as well as having a high likelihood, it is critical that you understand how you will detect these threats.

- **Implement a strategy for securing your cloud deployments before starting an implementation — and go beyond what is included by your cloud provider.** Start with the basics and make sure that you understand exactly what your cloud service provider will secure and what you need to secure. Once you know what you need to do, see whether your existing tools provide what you need. Technologies like encrypted connectivity, single sign on (SSO), and multi-factor authentication should be where you begin. These will help secure data moving back and forth to these systems as well as help prevent unauthorized access.
- **Ensure you have a plan for responding to potential credentials breaches.** With over a quarter of the survey respondents indicating that their organization had experienced a credentials breach, every organization must have plans in place for how they will react to that situation. Days or weeks can sometimes pass before these breaches are detected, providing ample time for an attacker to make changes that could hinder resolving the situation. Know what you will do and how you will respond ahead of time.

Chapter One: Securing the SAP Landscape Overview

In April 2020, SAPinsider published research that looked at the impact cloud environments were having on enterprise security strategy. The biggest drivers for that strategy included a demand for a more holistic approach to security, and the need to align security policies and controls with business practices. While those remain drivers for many organizations today, the shift to a mostly virtual work environment and the accelerated adoption of cloud-based technologies have added a focus on protecting the data that is in their systems and that is more likely to be running in a cloud-based 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 need to protect access to sensitive and confidential data, a demand to improve the ability to analyze security data and detect attacks in progress, and pressure to secure cloud-based systems and data emerged as the top drivers. To satisfy these drivers, respondents indicated that they are conducting audits and security assessments, regularly implementing patches and updates, integrating existing systems with new security processes, and training end-users to protect credentials.

SAPinsider PERSPECTIVE

> Confidentiality and protection of the information in SAP systems is very important because they process sensitive information. They need to be protected from improper or unauthorized access.
>
> ~ SAP Basis Engineer
> Energy Company

In order to secure their SAP landscapes against cyber threats, there are several requirements that our survey respondents indicated they need, including fully patched and secure systems, compliance with data management requirements, cybersecurity tools that provide consistent protection across cloud and on-premise environments, and real-time monitoring and logging capabilities. Respondents also use or plan to use a wide range of SAP and SAP partner tools and technologies to support these requirements for securing their SAP systems.

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

Table 1: DART model framework for security strategy

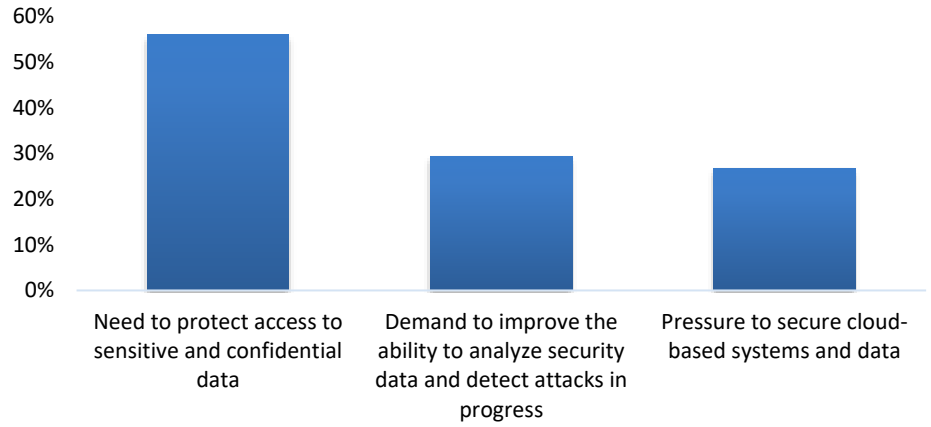
Drivers	Actions	Requirements	Technologies
• Need to protect access to sensitive and confidential data (56%) • Demand to improve the ability to analyze security data and detect attacks in progress (29%) • Pressure to secure cloud-based systems and data (27%)	• Conducting audits and security assessments (60%) • Regularly implementing patches and updates (59%) • Integrating existing systems with new security processes (42%) • Training end-users to protect credentials (39%)	• Fully patched and updated systems (86%) • Compliance with data management requirements (79%) • Cybersecurity tools that provide consistent protection across cloud and on-premise environments (78%) • Real-time monitoring and logging capabilities (78%)	• Encrypted/secure connectivity (78%) • Single Sign On (77%) • Two/Multi-Factor Authentication (74%) • Secure User Provisioning (68%) • Continuous Monitoring (68%) • Data Encryption (68%) • Access Governance Solutions (60%) • Business Process Controls (59%) • Vulnerability Management (54%) • Integrated Cybersecurity Apps or Platforms (52%) • Code Vulnerability Analysis Tools (47%) • UI Masking (33%)

What Drives Security for the SAP Landscape?

The need to protect access to sensitive and confidential data was identified as the main factor behind securing their SAP systems by

more than half the respondents (56%). The demand to improve the ability to analyze security data and detect attacks in progress was identified by 29% of respondents as a top driver for their security strategy, and the pressure to secure cloud-based systems and data was identified as a top driver by 27% of respondents (see **Figure 4**).

Figure 4: Top drivers for securing SAP systems



Source: SAPinsider, April 2021

The need to protect access to sensitive and confidential data demonstrates how important the data in SAP systems has become. With organizations accelerating the integration of SAP systems like SAP Success Factors, SAP Concur, and SAP Ariba with their enterprise ERP, this has created an environment where having access to just one system can provide access to data from multiple HR, finance, and invoicing systems. And with many organizations looking at their move to SAP S/4HANA as an opportunity to consolidate data from multiple financial systems into a single source of truth, this also presents a more inviting target for anyone who can gain access. With so much financial and HR data available in SAP systems, keeping that data secure is critical for SAP customers.

Correlating directly with the fact that the biggest challenge identified by nearly two thirds (62%) of survey respondents was that of detecting potential threats, slightly less than a third (29%) said that their security strategy is being driven by the demand to

SAPinsider PERSPECTIVE

> Setting up regular and mandatory enablement sessions in conjunction with constant awareness communications are the most important steps for training end-users to protect their credentials.
>
> ~ Director
> Implementation Partner

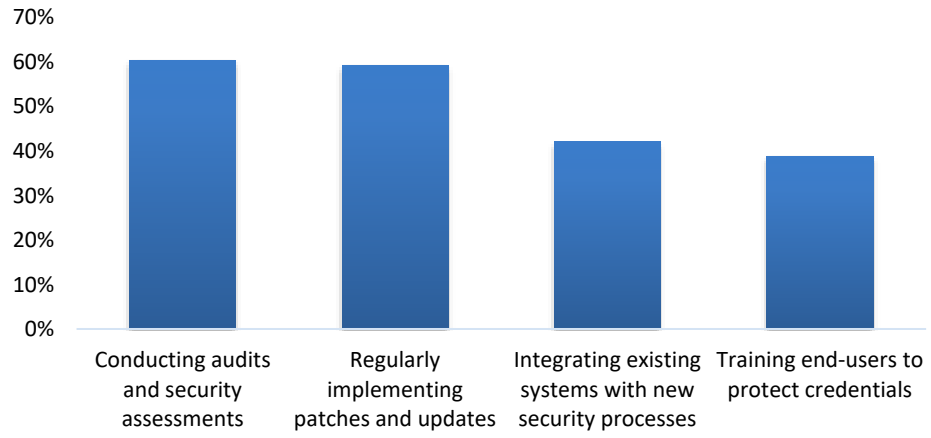
improve the ability to analyze security data and detect attacks in progress. If user credentials are compromised, having tools that can analyze security data and determine whether abnormal behavior is occurring, effectively detecting an attack in progress, is critical to the security of SAP systems.

Nearly all respondents to an SAPinsider survey conducted in Q4, 2020 — 99% — say that they are running at least some systems in the cloud, and 95% plan on running at least some SAP S/4HANA instances in cloud-based environments. With more and more enterprise systems moving to the cloud, securing these cloud-based environments has become just as important as the traditional security of on-premise systems.

How Do SAPinsiders Address Their Drivers?

Over half of survey respondents (60%) said that they are pursuing the strategy of conducting audits and security assessments (as seen in **Figure 5**). This strategy supports two top drivers: the need to protect access to sensitive and confidential data, and the need to provide a means of detecting attacks that may be in progress by reviewing which users have access to which systems and assessing whether that access is appropriate.

Figure 5: Top strategies taken to address the top drivers



Source: SAPinsider, April 2021

SAPinsider PERSPECTIVE

> We subscribe to the SAP alerts around patches and look for anything coming in with a CVE rating. Those that have scores above 9 we are looking to implement within a matter of days. Staying on top of patches has meant that there is nothing that's come up that we've been so far behind that we haven't been able to apply the patch.
>
> ~ Basis Lead
> Global Industrial Corporation

Almost as many respondents (59%) indicate that they are regularly implementing patches and updates. Keeping systems patched and up to date helps ensure that issues that have been identified and addressed by SAP will no longer impact the systems within an organization and supports the driver of protecting access to sensitive and confidential data. However, SAPinsiders should understand that applying patches and updates only covers those issues which have already been addressed, so staying on top of system monitoring and conducting audits remains important.

A smaller number of respondents (42%) said that they are taking action to integrate existing systems with new security processes. This will allow them to add additional layers of protection to their most sensitive systems but will also enable them to improve their ability to monitor those systems and detect potential attacks in progress.

The final top strategy is that of training end users to protect credentials. Selected by 39% of respondents as a strategy that they are taking to help keep systems secure, this is an important way of educating users particularly about the way social engineering can be used to gain access to credentials. This is an important strategy that can be used in conjunction with regularly implementing patches and conducting audits to support all the top drivers.

Key Takeaways

Based on our research with respect to securing SAP landscapes, the following takeaways are clear:

- **Make protecting your data the starting point for the plans to secure your landscape.** All respondents interviewed for this report indicated that securing the data in their SAP systems is critical to their businesses. Some talked about the potential for financial and reputational losses, while others said that it is this data on which their daily decisions are made, and a loss of access would stop them from being able to function. Regardless of the reasons behind your decision, making sure

that the data in your systems is protected must be the starting point of your cybersecurity strategy.

- **Stay up to date with patches and updates and follow guides for hardening your systems.** As stated by one survey respondent, "patching is key." Allowing patches to go unaddressed complicates the patching process as several older patches may need to be applied when a critical patch is released. Also focus on hardening systems according to the security guides SAP publishes for platforms like SAP NetWeaver, and solutions like SAP S/4HANA and SAP Cloud Connector. This approach should be combined with patching to ensure that you reduce the vulnerability of your systems as much as possible.

- **Ensure that you are performing regular auditing and monitoring.** While patching regularly is critical to keeping your systems as secure as possible, so is regular auditing and monitoring. Most listed companies must perform regular strict audits on systems, but SAPinsiders should ensure that they are conducting audits outside of mandatory events. Often it is only by performing these audits that unusual activity is detected in a system that might reveal a potential breach or misuse from inside the organization.

- **Train users to ensure that your security strategy becomes part of the corporate culture.** No matter how much patching is done on a system, if users do not act securely then there is a risk that any security in place can be bypassed by simply obtaining credentials. Users need to be trained specifically about how to protect their credentials, as well as how to behave securely in their interactions with other team members and with partners. Corporations operating in Europe have already rolled out training to educate users on topics like General Data Protecting Regulation (GDPR) and why protecting customer data is important, but the same must be done around other security topics to ensure security does not remain an afterthought.

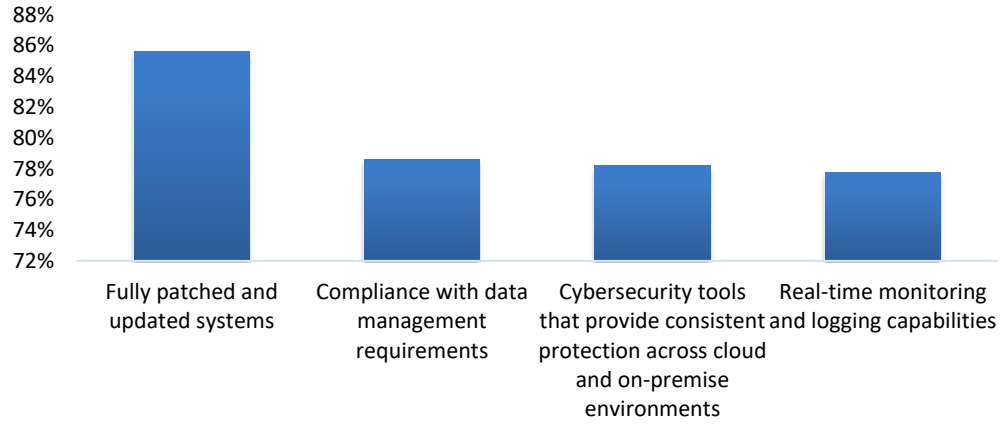
Chapter Two: How Do SAPinsiders Approach Securing Their SAP Landscape?

We have seen that the biggest factors now driving strategy around securing SAP systems is that of the need to protect access to the data that is in those systems, including a growing pressure to secure cloud-based systems. Combined with this need to secure systems is a demand to improve the ability to detect attacks that may be in progress. We will now examine what requirements respondents are facing, and the technologies they are using as part of their strategy for securing their SAP landscapes.

Top Cybersecurity Requirements

Ensuring that systems are patched and updated was identified by 86% of respondents as their most important requirement for securing their SAP landscape. Keeping systems up to date is the best way for many organizations to prevent attacks that leverage known exploits, and directly supports the strategy of regularly implementing patches and updates. However, organizations often struggle with keeping systems up to date because it is the same team that implements patches and performs maintenance. They must also balance this requirement with that of limiting downtime.

Figure 6: Top requirements for cybersecurity strategy



Source: SAPinsider, April 2021

SAPinsider PERSPECTIVE

"Apart from securing the IT & SAP infrastructure with the usual security topics, access to our SAP systems is a major area for our security risk response. But to fully secure our SAP systems there are many more measures such as securing software development, monitoring emergency users, encryption of networks and data, as well classification of critical data that must be considered."

~ Director IT Services

Being compliant with data management requirements was the second most important requirement identified by 79% of survey respondents. While many organizations may already ensure that data moving across networks and to and from systems is secure, particularly for cloud-based systems, this requirement can also apply to ensuring that governmental regulations like GDPR and the California Consumer Privacy Act (CCPA) are being adhered to. With multiple countries now introducing regulations like GDPR, it is extremely important for organizations to comply with data management requirements for their systems.

Respondents also see a need for cybersecurity tools that provide consistent protection across cloud and on-premise environments (78%). With more and more SAPinsiders deploying cloud-based environments, having tools that will function for both their on-premise applications as well as their cloud applications is critical – not just from a protection standpoint but also from a training and usage standpoint. Having these consistent tools supports the ability to integrate existing systems with new security processes, as well as conduct security audits and assessments.

The other top requirement is that of real-time monitoring and logging capabilities (78%). Real-time monitoring and logging can assist with conducting security audits and assessments, as well as with the ability to analyze security data and detect attacks in progress. With organizations looking for ways to gain insight into what is happening with their systems so that they can more rapidly detect intrusions, especially with many of those intrusions going undetected for extended periods of time, using real-time monitoring and logging in conjunction with log analysis tools and performing regular audits and assessments will help organizations with protecting the data in their SAP systems.

Which Technologies Do Respondents Use to Secure Their SAP Systems?

Survey respondents indicated that encrypted/secure connectivity (78%), single sign-on (SSO) (77%), and two/multi-factor

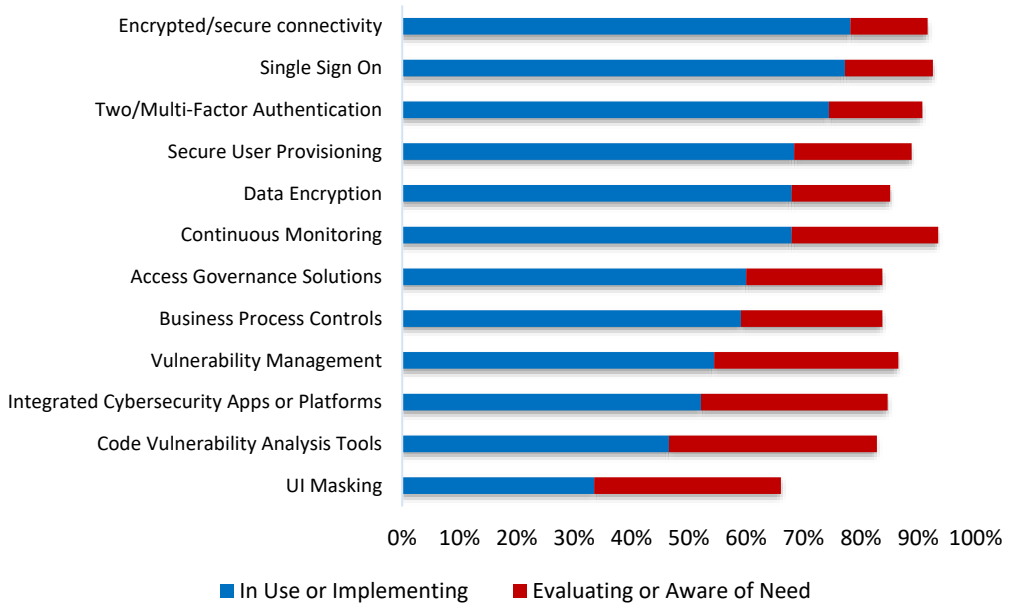
authentication (MFA) (74%) are the tools that are used the most or being implemented most frequently today (**Figure 7**). These tools represent the starting point for organizations putting technology in place to secure their SAP systems, with three quarters of survey respondents saying they are already using them or in the process of implementing.

SAPinsider PERSPECTIVE

"The technologies that are the starting point for securing our SAP systems are HTTPs protocols and multi-factor authentication."

~ Director Implementation Partner

Figure 7: Cybersecurity tools and technologies



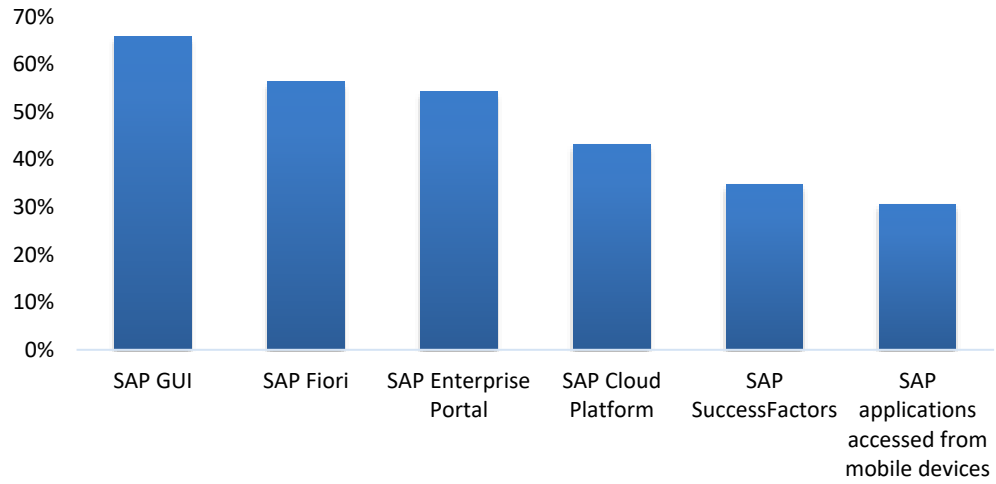
Source: SAPinsider, April 2021

Encrypted or secure connectivity provides a way for organizations to ensure that data is moving securely between systems, particularly between systems that are running on-premise and those that have been deployed in the cloud. It can also be used with a virtual private network (VPN) to encrypt traffic between remote clients and SAP systems, and should be one of the first technologies that is put in place in the SAP landscape.

While approximately two thirds of respondents (68%) reported that the SSO technology they are using for their SAP applications is SAP SSO, 32% said that they were using an alternative SSO product or protocol to connect to their SAP systems. The most common SAP

application with which they were using SSO is SAP GUI (66%), followed by SAP Fiori (56%) and SAP Enterprise Portal (54%), as seen in **Figure 8**.

Figure 8: SAP applications for which SSO is used



Source: SAPinsider, April 2021

A similar number of respondents to those using SSO (59%) said that they are using MFA for both SAP and non-SAP applications. However, nearly a third (31%) said that they are only using MFA for non-SAP applications. Most frequently used with VPN logins (71%), MFA is also being used in conjunction with network or domain logins by 48% of respondents, and with mobile devices by 45% of respondents.

The next most frequently used technologies were secure user provisioning (68%), data encryption (68%), and continuous monitoring (68%). Each was in use by between 48% and 53% of respondents and being implemented by 15 to 20%. Secure user provisioning helps automate and streamline user provisioning in a way that ensures users are quickly able to get the access they need while keeping systems protected from inappropriate access, while data encryption ensures that data stores cannot be accessed by anyone without the encryption key. Continuous monitoring is a very

important part of identifying attacks in progress and allowing security teams to address them.

Access governance solutions are in use or being implemented by 60% of survey respondents. Similarly, Business process control solutions are in use or being implemented by 59% of respondents. These tools, typically part of a broader Governance, Risk, and Compliance (GRC) solution, help organizations remain compliant with data management requirements as well as conduct audits and security assessments.

Some of the most advanced technologies that can be used to secure SAP landscapes are vulnerability management (54%), integrated cybersecurity applications and platforms (47%), and code vulnerability analysis tools (47%). While at least a third of survey respondents are aware of the need for these solutions, only those that are leaders in securing their SAP landscapes currently have them in use. Vulnerability management helps these leaders provide a process around testing, categorizing, prioritizing, and resolving vulnerabilities in enterprise systems, providing a more proactive methodology for addressing gaps before they can be exploited. As these respondents move beyond a reactive approach to cybersecurity, integrated cybersecurity applications and platforms accelerate that approach by helping them more readily monitor the status of multiple systems. Those running customized code and applications should consider putting in place code vulnerability analysis tools earlier in the process.

Key Takeaways

When it comes to equipping organizations with the capabilities and technologies required to effectively secure their SAP landscapes, consider the following:

- **Adopt encrypted connectivity, SSO, and MFA.** Wherever your SAP systems are running, putting these technologies in place will immediately help address the drivers of protecting access to sensitive and confidential data and securing cloud-based systems and data. According to survey respondents, these are

the technologies that the majority have in place as the starting point for securing their systems, and should be where you start your plans for securing your SAP landscapes.

- **Prioritize secure user provisioning, data encryption, and continuous monitoring.** Once you have put in place basic connectivity, SSO, and MFA technologies, the next technologies to adopt should be secure provisioning, data encryption, and continuous monitoring. Already in use by approximately half of survey respondents and being implemented by nearly 20%, they provide additional capabilities towards securing your SAP landscape and should be the next step in creating a comprehensive security strategy for your SAP systems.
- **Implement access governance and process control to support compliance and data management.** Particularly relevant for ensuring that users only have access to the data and applications/transactions that they should be able to see, as well as streamlining enterprise compliance efforts, these technologies also support the need to conduct audits and security assessments and the need to remain compliant with data management requirements. In use or being implemented by 60% of respondents, these technologies may be more in use by organizations that have large user bases and need to keep roles consistent across multiple instances and environments. But they also form a big part of managing Segregation of Duties (SoD) which is part of any audit and review process.
- **Develop a plan for vulnerability management, integrated cybersecurity apps, and code vulnerability analysis tools.** Less than a third of respondents said they are currently running these technologies, but they represent the most comprehensive capabilities for securing your SAP landscape. Even though you may only be in the process of putting into place technologies like SSO or MFA, you should start formulating a plan for how and when you will implement these capabilities.

SAPinsider
A Wellesley Information Services Company

Chapter Three: Required Actions

Enterprise systems — particularly SAP ERP systems — are increasingly the target of cyberattacks, and both SAP and its partners regularly find and address vulnerabilities. However, staying on top of patches and updates only goes so far when it comes to protecting the sensitive and confidential data that resides within these systems, especially when juggling the downtime that can be required to implement patches. If SAPinsiders want to protect their data, secure cloud-based systems, and improve their ability to detect attacks in progress, they need to put comprehensive plans in place for how they will achieve this.

With more than a quarter of survey respondents indicating that their organization has suffered from credentials being obtained either through social engineering or some form of password misuse, systems being breached is not uncommon. Unauthorized users who gain access to credentials often have access to systems for weeks or months before being detected, putting pressure on organizations to plan for how they will respond should a breach occur. Technologies like MFA can make it more difficult for unauthorized users to log into systems with stolen credentials, and continuous monitoring can help with detecting these attacks should they occur, but organizations should plan for more proactive responses.

SAP is working to consolidate its GRC and cybersecurity tools into one broad portfolio of solutions, but two thirds of respondents said that they currently rely on a combination of SAP and non-SAP tools to secure their SAP systems. For most this may simply mean that they are using a non-SAP MFA tool within their network, or are using third-party tools to provide security at the transport or network layers. However, those who are using both SAP and non-SAP tools are also less likely to believe that their cloud service provider is sufficiently securing their data (43%) than the survey as a whole (34%), which shows that they may be using this combination of tools as they are more concerned about security overall. Whatever approach they take, SAPinsiders should ensure

SAPinsider
PERSPECTIVE

“Our SAP systems are used for core business procedures and functions. Without them, we would not have the data we need for management decisions, nor would we be able to manufacture and collaborate with customers and suppliers.”

~ Director
IT Services

that they are understand the capabilities of the tools that they have and that they are effectively using them.

Steps to Success

Our research reveals that SAP customers should apply the following key steps to secure their SAP landscape against cyber threats:

- **Conduct audits, stay up to date with patches, and train your end users.** To effectively protect the data that is in your SAP systems you need to have an effective strategy in place. SAPinsiders must not take for granted the importance and effectiveness of performing traditional maintenance, such as regular audits and security assessments and implementing patches and updates. Just as important is training end users to protect their credentials. No matter how much you audit and patch, if a breach occurs because of a phishing attack or a mishandling of credentials, much of the technology you have in place can be bypassed.
- **Ensure that you have covered the basics by having secure connectivity, SSO, and MFA in place. Add continuous monitoring, data encryption, and secure user provisioning.** To secure your SAP landscape you must put the basic technologies in place and have plans for when and how you will move to additional levels of security. Over three quarters of survey respondents are currently using or implementing secure connectivity, SSO, and MFA, showing that these are the first steps to securing your landscape. More than two thirds of respondents have implemented continuous monitoring, data encryption, and secure user provisioning. If you are not using at least some of these technologies, you should put plans in place for when you will do so.

- **Integrate your existing systems with new processes that you deploy and ensure that your cybersecurity tools are consistent across cloud and on-premise environments.** As you formulate new security processes and roll out new tools and technologies within your landscape, make sure that they are integrated with your existing systems. This will ensure that your new processes and existing systems are protected. To make this integration easier, make sure that you deploy tools that provide consistent protection whether you are looking at on-premise or cloud-based systems. Having this consistency will eliminate the need for your security teams to use multiple tools for different systems and will make it easier to protect your systems in a holistic manner.
- **Develop plans for a more proactive approach to securing your systems and move beyond being reactive.** Leveraging methodologies like vulnerability management — where you identify potential security gaps and address them before they can be exploited — and technologies like integrated cybersecurity platforms provide a more forward-looking approach to securing your SAP landscape. Applying patches and updates will keep your systems secure, but these only address issues that have already been found and corrected. Real-time monitoring and logging capabilities will help detect attacks in progress, but if credentials can be obtained then these are already reactive. Create plans that will help you take a more proactive stance towards security, because this is the way in which you will best protect your data.

Methodology

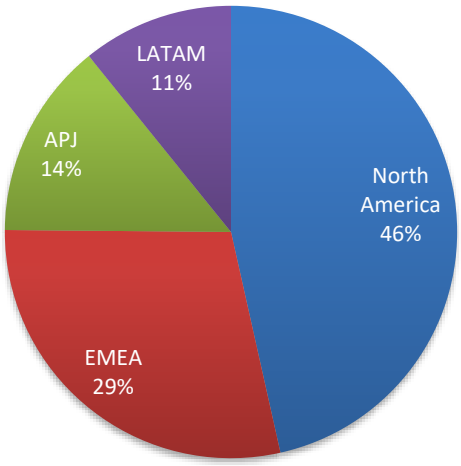
In March and April 2021, SAPinsider examined the experiences of business and technology professionals about how they are securing their SAP landscapes. Our survey was administered to 263 members of the SAPinsider Community and generated responses from across a wide range of geographies, industries, and company sizes. Respondents completed an online survey and provided feedback in customer interviews that questioned them on topics such as:

- What are the top drivers of your organization's current cybersecurity efforts?
- Are you relying entirely on SAP tools for the security of your SAP systems?
- What challenges are you currently facing with securing your SAP systems and landscapes?

The demographics of the respondents included the following:

- **Job function:** Functional areas reported by respondents include: Information Technology (74%), GRC, Risk, and Compliance (7%), Business Development (3%), and Product Development and Product Management (3%).
- **Market sector:** The survey respondents came from every major economic sector, including: Software and Technology (39%); Industrial (30%); Public Services & Health Care (10%); Financial Services & Insurance (8%); Hospitality, Transportation, and Travel (6%); Retail & Distribution (5%); and Media & Entertainment (1%)
- **Geography:** Of our survey respondents, 46% were from North America; 29% were from Europe, the Middle East, and Africa; 14% were from Asia-Pacific, Japan, and Australia; and 11% were from Latin America.

PARTICIPANTS PROFILE



Appendix A:

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's 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

We are a global security software vendor, providing mature, proven, standards-based solutions that enable true enterprise-class security for mission critical business applications – on the intranet or in the cloud. Our TrustBroker products leverage two decades of Kerberos expertise and existing infrastructures, such as Microsoft Active Directory – for authentication and key management, to lower costs and deliver exceptional return on investment. TrustBroker integrates seamlessly with solutions from leading vendors, including SAP and Sybase, to reliably deliver strong authentication, single sign-on and end-to-end protection of application data in transit. For more information, visit https://cybersafe.com

Onapsis is more than your typical application cybersecurity company. We're different because our solutions help eliminate the costs and risks preventing you from building better, smarter and more dynamic applications, faster and more securely. We protect you at the core of your business, keeping the business-critical applications you depend on daily secure, compliant and available. Because we're application-focused, we're also deeply invested in enabling your future—helping you build in the cyber resilience you need to pursue digital transformation. For more information, visit https://onapsis.com

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 SAPinsiderOnline.com.