SAPinsider
A Wellesley Information
Services Company

SAPinsider Benchmark Report

Impact of Cloud and SAP HANA on Enterprise Security Strategy

Robert Holland

March 2020

Research Partner

SAP®

Report Sponsors

Google Cloud NetApp™ Red Hat

Research Partner

The best-run businesses make the world run better. With courage, perseverance, and breakthrough technology, SAP customers tackle some of the world's biggest challenges. Find out how they work with SAP to make a lasting difference – and learn about the technology solutions that fuel their innovation.

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

Table of Contents

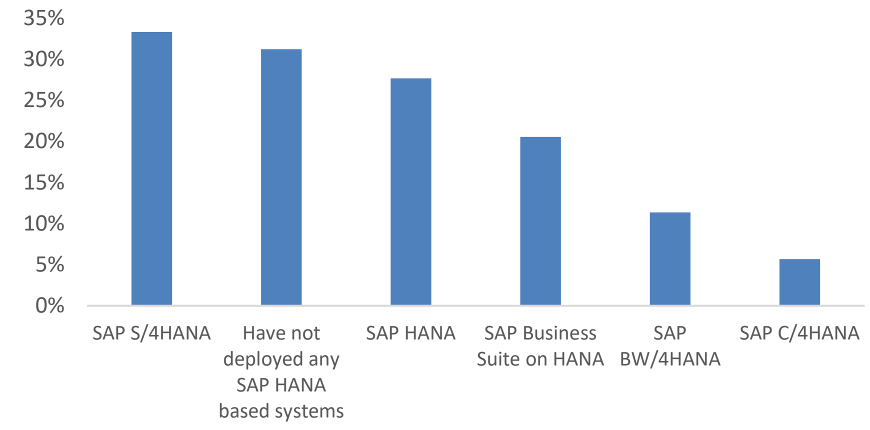
IMPACT OF THE CLOUD AND SAP HANA ON ENTERPRISE SECURITY STRATEGY

Executive Summary

SAP's transition to an enterprise cloud company has changed the way SAP customers consider and implement their enterprise security strategy. The inclusion of SAP HANA-based systems adds further complexity to these considerations, particularly when these systems are running in hybrid or cloud-based environments. Organizations now need to find a way forward that doesn't rely on existing physical and network security, and instead expands the security perimeter to include not only local systems, but also those that are running in cloud-based environments.

In Q1 of 2020, SAPinsider surveyed 152 members of our community to understand their current enterprise security strategy, and how their move to cloud-based applications and environments, combined with their deployment of SAP HANA-based systems, is impacting their plans. Continuing the adoption trends that we've seen in recent reports focused on SAP S/4HANA in the cloud and SAP S/4HANA migration, a majority (54%) of respondents are running a SAP HANA-based ERP with 33% using SAP S/4HANA, and 21% using SAP Business Suite powered by SAP HANA (see **Figure 1**).

Figure 1: SAP HANA-based systems in use



Source: SAPinsider, March 2020

PERSPECTIVE

> “We are constantly striving to simplify our customer’s journey when moving to the cloud. Consistency is required when moving from on-premise to a cloud environment and careful planning is needed. Customers should always plan to make the move to a cloud environment whether it’s imminent or not. Customers understand that integration is the key and SAP provides the tools to make that happen seamlessly.”

~ Anne Marie Colombo,

Cybersecurity Solution Advisor, SAP

The survey revealed several other trends regarding respondents' adoption of the cloud and SAP HANA-based applications.

- Of those who are running SAP HANA-based systems, 63% are doing so entirely on-premise.
- Over a quarter (28%) are using hybrid environments, where some components are deployed on-premise and others are in the cloud. An additional 15% of respondents are running their SAP HANA systems in the private cloud, while 14% are using the public cloud.
- Just over half of survey respondents (56%) are using cloud-native applications like SAP S/4HANA Cloud, SAP Cloud Platform, SAP SuccessFactors, and SAP Concur. Of those using cloud-native applications, 53% are using SAP-hosted environments, 30% are using private cloud environments, and 17% are using the public cloud.
- Of those who are using the public cloud (regardless of for which solution) the top provider was Microsoft Azure (48%). This was followed by Amazon Web Services (42%) and Google Cloud Platform (21%).

Required Actions

Based on the responses that we received in the survey, organizations that are determining and implementing their enterprise security strategy must:

- **Take a more holistic approach to enterprise security strategy that involves corporate culture.** With changes to deployment models and environments, a successful enterprise security strategy must encompass all aspects of security—from physical security to system and data access—as 35% of respondents indicated

SAPinsider
PERSPECTIVE

> When the client embarks on a cloud journey, security is foundational. The security aspects need to be addressed up front before you even move the SAP workload. Before they move to any cloud provider need to make sure they have the security strategy in place and approved.

~ Technology Executive, Global Services Organization

when they said a holistic approach was driving their security strategy. The strategy must also be fully integrated into day-to-day business activities and practices so that everyone in an organization understands why it is important and follows the appropriate procedures.

- **Build an integrated strategy that is aligned with controls and business processes and integrates existing systems.** An effective enterprise security strategy must integrate new and existing system deployments, as well as consider the access controls and business processes that are being used in those systems—a strategy being implemented by 48% of respondents. Without this integration, your strategy will struggle to engage users who rely on these systems as part of their day-to-day activities.
- **Ensure that education is a key part of the strategy.** When it comes to implementing an enterprise security strategy, the biggest challenge reported by respondents (58%) was a lack of resources/expertise. Ramping up internal education programs and training on security/cybersecurity awareness is key to making any security strategy successful.
- **Plan for a strategy that will include the cloud, even if it is not currently a key deployment environment.** While the majority (63%) of customers running SAP HANA-based systems are running those systems on-premise, 56% of respondents indicated that they are running at least one cloud-native solution. While all customers may not be running a cloud-based solution today, there is a high likelihood that they will be doing so in the future and should include these scenarios in planning for their enterprise security strategy.

SAPEXPERTS
PERSPECTIVE

> “While today, the majority of SAP HANA-based systems are still on premise, there is a continuously growing footprint of hybrid/cloud deployments. This, together with the fact that the boundaries that used to exist with pure on-premise systems are no longer there, forces organizations to rethink their enterprise security strategy, especially as they drive cloud migration projects.”
>
> **~ Juan Perez-Etchegoyen, Chief Technology Officer, Onapsis**

Chapter One: Enterprise Security Strategy Overview

With on-premise deployment models of the past, organizations could essentially rely on the security provided by their network configuration combined with applications that governed access control to their systems to ensure that systems and data were largely secure. However, as more systems have been deployed in the cloud, it is no longer possible to rely on network security because that does not extend to systems located in the cloud, or interactions with them across the internet. This is particularly true when implementing systems in an infrastructure as a service (IaaS) environment where the cloud vendor is not responsible for application security or controlling system access. Organizations must develop an effective enterprise security strategy if they want to not only address these immediate needs, but also head off future security concerns and challenges raised by additional system deployments.

Best Practices Model – DART

SAPinsider grounds all our 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 demand for a more holistic enterprise security strategy/approach coupled with the need to align security policies and controls with business processes emerged as the key business drivers. To satisfy these drivers respondents indicated that they are taking actions to make security an integral part of corporate culture and build an integrated security strategy that allows them to deploy SAP instances quickly and securely. They're also focused on creating a strategy that integrates existing systems and supports regular audits and security assessments.

In order to succeed in this approach, respondents know that they need to implement real-time monitoring and logging capabilities, use risk mitigation and remediation tools, ensure they are compliant with GDPR and other data handling requirements, and seek consistent cybersecurity tools across environments, as well as change management controls. Respondents use or plan to use a wide range of SAP and partner tools and platforms to fulfill these requirements.

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

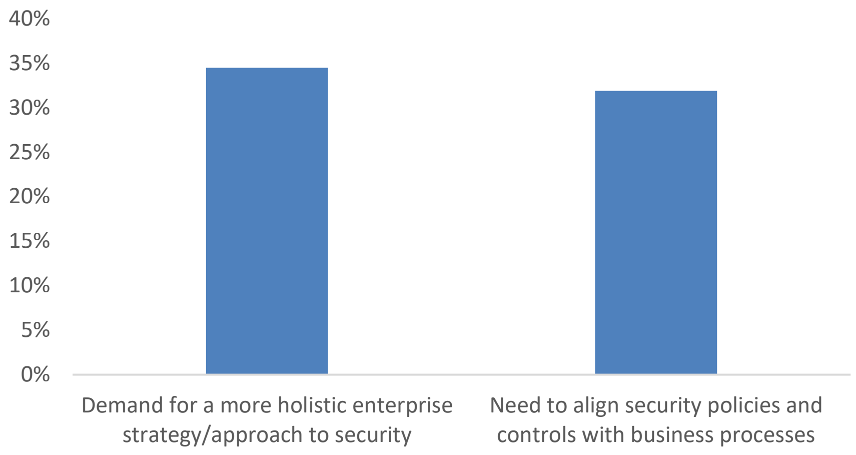
Table 1: DART model framework for enterprise security strategy

Drivers	Actions	Requirements	Technologies
• Demand for a more holistic enterprise strategy/approach to security (34%) • Need to align security policies and controls with business processes (32%)	• Make security an integral part of corporate culture (50%) • Build an integrated security strategy (47%) • Quickly and securely deploy SAP instances (39%) • Create security strategy to integrate existing systems (38%) • Conduct audits and security assessments (37%)	• Real-time monitoring and logging capabilities (56%) • Risk mitigation and remediation tools (53%) • Compliance with GDPR and other data handling requirements (50%) • Consistent cybersecurity tools to protect cloud-based systems across environments (49%) • Change management controls (46%)	• Single sign on (46%) • Data encryption (35%) • Identity management (35%) • Secure user provisioning and deprovisioning (33%) • Continuous monitoring (32%) • Business process controls (31%) • Access governance solutions (26%)

What are the Business Drivers for Enterprise Security Strategy?

Over one third (34%) of survey respondents indicated that their primary driver for an enterprise security strategy was the demand for a more holistic enterprise strategy/approach to security, and 32% said that the need to align security policies and controls with business processes drove their approach (see **Figure 2**). The accelerating adoption of cloud-based systems (our research published in July 2019 on enterprise cloud migration showed that 92% of SAP customers had deployed some sort of cloud solution) combined with SAP's project "Embrace" (which provides a streamlined path to implementing SAP S/4HANA and SAP Cloud Platform solutions in the public cloud) means that organizations need a comprehensive strategy for enterprise security to accommodate both on-premise and remotely located systems and meet the need to rapidly deploy and test new cloud-based solutions.

Figure 2: Top drivers for enterprise security strategy



Source: SAPinsider, March 2020

Part of taking a comprehensive approach is ensuring that security policies and controls are aligned with business processes. Our February 2020 research on SAP S/4HANA migration showed that many organizations are using their move to SAP S/4HANA to improve business operations and re-engineer processes, and any enterprise security policy needs to be in alignment with these updates. Whether an organization is running SAP S/4HANA or utilizing the capabilities of SAP HANA to drive better analytics or business intelligence (BI) performance, security policies and controls must align with the business processes to prevent delays of daily work.

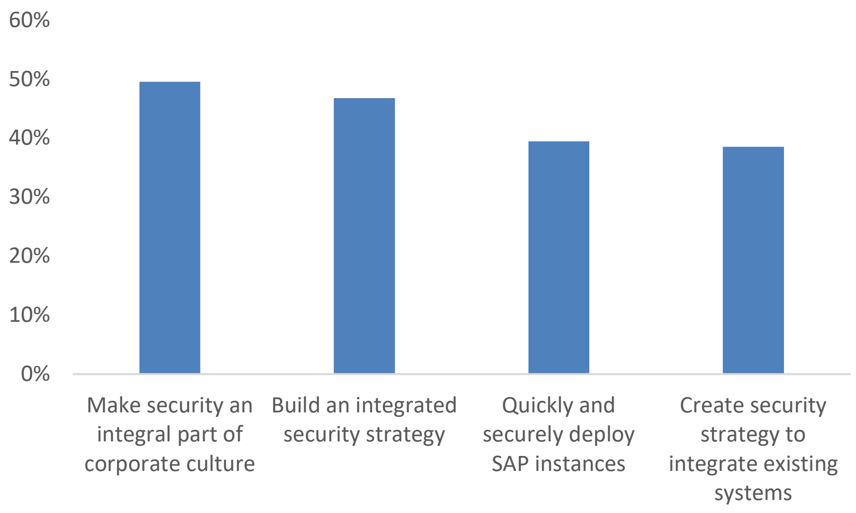
SAP PERSPECTIVE

> "Customers host their systems and applications across various deployment options and have a heightened interest for an enterprise-wide security strategy. With the increasing number of applications running in different environments and, in particular, as customers migrate into the cloud, this becomes even more important. To meet these expectations, we work continuously to strengthen and improve security features in SAP S/4HANA Cloud. These include compliance controls, global data center strategy, data protection, and privacy standards built to support secure cloud deployments and cloud infrastructure."
>
> **~ Michael Herrmann ,**
>
> **SAP S/4HANA Cloud Delivery, Security Officer, SAP**

How Do Customers Meet Their Business Drivers?

Half (50%) of respondents indicated that making security an integral part of corporate culture was the number one action they were taking in relation to their enterprise security strategy (as seen in **Figure 3**). This directly supports the driver to have a more holistic approach to security by integrating security awareness into employees' thought process.

Figure 3: Top strategies prioritized to address the top drivers of change



Source: SAPinsider, March 2020

Additionally, 47% of organizations chose building an integrated security strategy – one that provides unified configurations, rules, policies, and practices for every solution that they run – as a top strategy. Doing so allows organizations to ensure that their strategy is fully aligned with the day-to-day business needs of the organization, and directly supports the driver to align security policies and controls with business processes.

Supporting a similar strategy to that which was seen in our December 2019 research on SAP S/4HANA in the cloud, 39% of respondents said that a top strategy for their enterprise security was the ability to quickly and securely deploy SAP

SAPinsider
PERSPECTIVE

> “There is a lot of emphasis in terms of environments that are secure. On-prem you can get away without paying a lot of attention, but there are a lot of new things for the cloud. However, many tools and approaches are now becoming standard and making it easier to follow implementation approaches. 3-4 years ago everyone was very concerned about security, but now there are standards that are widely adopted.”

~ Technology Executive, Global Services Organization

instances. While the rapid deployment of SAP instances indicates that organizations are looking to be agile in how they deploy and use SAP systems, doing this securely is only possible if they have a holistic enterprise security strategy, and one that is aligned with business processes and is integrated with existing systems.

The final top strategy, selected by 38.5% of respondents, was that of creating a security strategy that integrates existing systems. While creating an enterprise security strategy that only applies to new systems and configurations may support changes moving forward, it will not address potential gaps and vulnerabilities with existing systems. This further supports respondents' previously mentioned need for a holistic security strategy.

Key Takeaways

Based on our research with respect to enterprise security strategy, the following takeaways are clear:

- **Take a comprehensive approach when implementing an enterprise security strategy.** In the past security would be implemented as needed on systems that required specific access or process controls. That sort of piecemeal approach is no longer effective as more systems are being implemented more quickly – an action 39% of respondents indicated they are taking. A holistic approach that includes plans for how security will be implemented on new and existing systems is critical for effective overall enterprise security.

- **Ensure that the strategy is aligned with business processes.** Almost half (48%) of respondents indicated that one of the challenges they faced with an enterprise security strategy was disruption to operations. In order to avoid this level of disruption, it is critical that the security strategy be aligned with business processes within the organization. Without this alignment the strategy is also far less likely to be truly adopted within any organization.

- **Make the security strategy an integral part of corporate culture.** For any enterprise security strategy to permeate an organization, it must be part of the corporate culture. Half (50%) of respondents indicated that they are taking this approach, and for good reason. If you want your teams to behave in a secure manner and be thinking about the security ramifications of what they are doing, it must be second nature to them.

- **Build an integrated security strategy.** In addition to taking a comprehensive approach to enterprise security, it is also critical that the security strategy be integrated with existing systems so that it unifies configurations, rules, policies, and practices across the organization. Just as a security strategy should be comprehensive, including both existing and planned system implementations–an integral part of any enterprise–it also needs to be integrated to ensure it is successful.

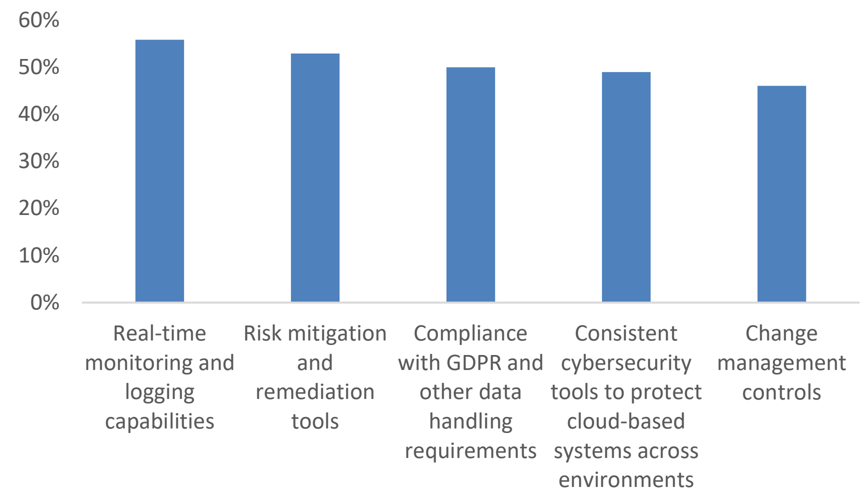
Chapter Two: How Do SAP Customers Approach Enterprise Security Strategy?

Creating an effective enterprise security strategy can be complex as it involves both IT groups and business teams to combine different systems and data in order to align design and business case decisions. This section explores how respondents prioritized the different requirements and capabilities that their organizations needed for a successful enterprise security strategy, and the tools they used to support those requirements.

Top Requirements for Enterprise Security Strategy

Respondents to the survey selected real-time monitoring and logging capabilities as their most important requirement, with 56% indicating that this was very or extremely important to their organization (see **Figure 4**).

Figure 4: Top requirements for enterprise security strategy



Source: SAPinsider, March 2020

SAPEXPERTS PERSPECTIVE

> Real-time monitoring and logging stands out as the most important requirement for the security strategy, which definitely aligns with the expectations we see from SAP customers. As organizations start adopting a sound enterprise security strategy for their business applications, they need visibility and control around the operations of their SAP HANA-based applications.
>
> **~ Juan Perez-Etchegoyen, Chief Technology Officer, Onapsis**

IMPACT OF THE CLOUD AND SAP HANA ON ENTERPRISE SECURITY STRATEGY

Real-time monitoring and logging is a critical requirement for any enterprise security strategy as it provides organizations with the ability to monitor system access and usage, implement automated routines based on various logged events, and enables rapid reaction to momentary events. It is also a necessary tool in determining whether organizations are appropriately aligning security policies and controls with business practices and supports the action of building an integrated security strategy.

Respondents (53%) chose risk mitigation and remediation tools as the second most important requirement because it is critical that they have procedures and tools in place to lower the potential risk in systems that may already be deployed within their security perimeter. The necessity of this requirement becomes clear when we remember that many of the respondents are creating a security strategy that integrates existing systems, most of which may not yet have been updated into a new enterprise security strategy, or may still need updates or upgrades to reach a compliant state from a security perspective. Also, these risk mitigation and remediation tools can work with the real-time monitoring tools to trigger different actions based on various logged events.

Other top requirements included compliance with GDPR and other data handling requirements (50%), consistent cybersecurity tools to protect cloud-based systems across environments (49%), and change management controls (46%). With the changes in data privacy requirements in Europe, the Middle East, and Africa (EMEA), and other countries, data handling requirements are now a major part of any enterprise security strategy. Because employees must inherently know how they should handle different types of data in order to comply with requirements, it makes sense that respondents chose making security an integral part of corporate culture as a necessary action to achieve alignment between security policies and controls and business practices.

Based on respondents' indication earlier in the report that the number one challenge with implementing an enterprise security strategy was a lack of resources and/or expertise (58%), it should come as no surprise that many plan to work with partners and System Integrators (SIs) to bridge this gap. Correspondingly, respondents' number one interaction with partners and SIs was around technical expertise (58%), and 49% said they plan to use SIs for knowledge transfer to help build that base of knowledge within the organization. Additional areas of engagement with SIs were with security tools and technologies (53%) and assistance in business case and strategy development (52%).

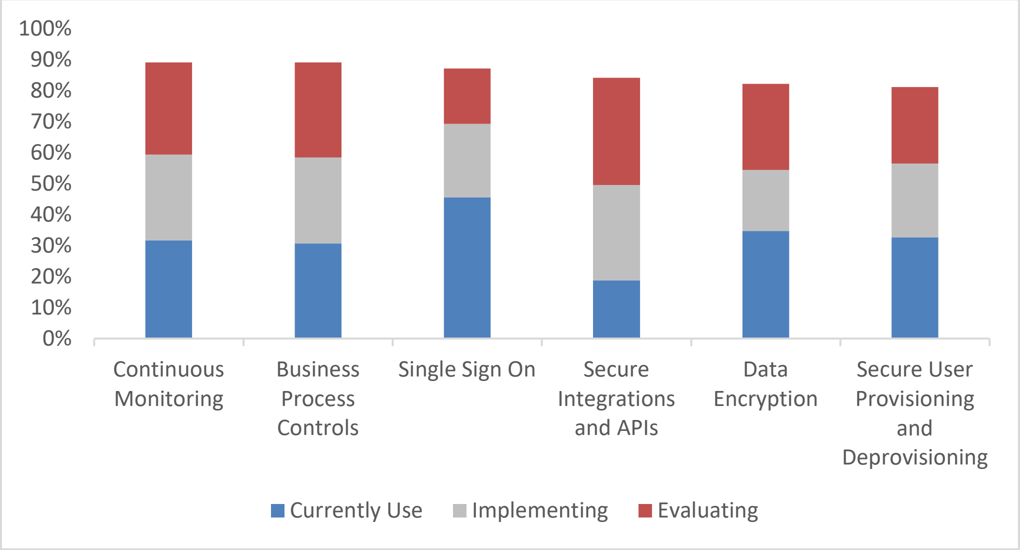
SAPinsider PERSPECTIVE

> “Moving to the cloud requires a new way of doing things, different skillsets. It’s easy to provision hardware and servers for a PoC or demo, but the biggest challenge is trying to use it for production level applications. That’s where the expertise is needed that customers are struggling to find.”
>
> **~ Technology Executive, Global Services Organization**

Which Tools Do Respondents Use to Support Their Enterprise Security Strategy?

When it comes to the tools that respondents are using to support their enterprise security strategy, 46% said they are using single sign on (SSO) (see **Figure 5**). This allows users to access multiple systems on different environments without needing to sign in each time.

Figure 5: Popular technologies for enterprise security



Source: SAPinsider, March 2020

Although SSO is the tool used most by survey respondents, continuous monitoring was either in use or planned to be used by 90% of respondents, the same percentage as those who are using or plan to use business process controls. The use of continuous monitoring directly supports the requirement for real-time monitoring and logging capabilities and provides a way for organizations to see, at any time, how their systems are being used, as well as any potential security events that may be occurring on those systems. The use of business process controls supports not only the driver to align security policies and controls with business processes, but also the requirement for change management controls, and consistent cybersecurity tools across environments when they are implemented in an appropriate manner.

SAP customers also plan to use secure integrations and APIs (85%), data encryption (83%), and secure user provisioning and deprovisioning (82%). Secure integrations and APIs allow organizations to more effectively and securely integrate different applications and systems. This supports respondents' actions to create an integrated security strategy and ties to the requirement for risk mitigation, as ensuring that any system access happens through secure connections reduces the inherent risk of data transfer and access. Data encryption is also critical to any enterprise security strategy because it fulfills the requirement for compliance with GDPR and other data handling requirements, and should be used to encrypt all data exchanges between cloud-based systems and distributed clients in order to fulfill that requirement.

Key Takeaways

When it comes to equipping organizations with the capabilities and technologies required for an effective enterprise security strategy:

- **Implement real-time monitoring and logging.** Whether you are using the monitoring and alerting infrastructure within SAP Solution Manager, using a security information and event management (SIEM) tool like SAP Enterprise Threat Detection, or third-party monitoring and logging tools, actively monitoring your system landscape for threats is critical to heading off potential security intrusions and aligns with the action of building an integrated security strategy.

- **Leverage tools and technologies to mitigate risk and provide remediation capabilities.** Tools that provide continuous monitoring, like SAP Enterprise Threat Detection, are the starting point of enterprise security. However, they must be combined with tools that control access to systems and processes, provide secure login and authentication, securely integrate different systems and locations, and provide data encryption between systems within the enterprise, the cloud, and a distributed user base in order to fulfill the important requirements of real-time monitoring and logging capabilities and GDPR compliance and data handling.

- **Make sure that the security strategy accounts for and complies with data handling requirements.** Compliance with regulations like GDPR was a requirement that 50% of respondents indicated as very or extremely important to their organization, and this will continue to increase as more governments enact similar data privacy standards. While it can be addressed on a case-by-case basis, it is more effective if the overall enterprise security strategy includes plans for these data handling requirements.

- **Use tools that can provide consistent capabilities across environments.** Security tools can be system or environment specific, which complicates not only implementation, but also education, as users will need to be trained on each specific tool, which then impacts acceptance and usage. Tools that are consistent across environments, which 49% of respondents indicated were very or extremely important to them, will provide benefits beyond just being able to manage multiple systems and configurations. They will also reduce the number of systems that users and administrators need to be educated in by streamlining acceptance and usage.

Chapter Three: Required Actions

The previous chapters clearly show how SAP customers currently align business drivers and actions with supporting requirements and technologies.

In this survey, 54% of respondents indicated that they are running an ERP system based on SAP HANA – either SAP S/4HANA (33%) or SAP Business Suite on HANA (21%). Roughly a quarter (28%) said they are running SAP HANA to support other SAP products, and 17% said they are using SAP BW/4HANA or SAP C/4HANA. Although 63% of these SAP HANA systems are running in on-premise environments, over a third are running in cloud-based or hybrid environments.

A similar proportion of respondents (56%) indicated that they are running cloud-native applications such as SAP SuccessFactors, SAP Concur, or SAP Ariba. Slightly more than half (52%) of these respondents are using SAP hosted environments, 30% are running in the private cloud, and 18% are running these cloud-native solutions in the public cloud. These cloud-native applications, and the SAP HANA-based solutions running both on-premise and in the cloud, have upended the security of many customers' technology landscapes (47% of respondents indicated that they faced the challenge of security disrupting operations) and have forced organizations to develop new security strategies that address these immediate needs and provide a plan for the future.

Around a third of respondents are facing the demand for a more holistic enterprise strategy/approach to security (34%) and are looking to align security policies and controls with business practices (32%) in order to address the challenges and new requirements that these environments have introduced. Customers are already starting to take actions to support these drivers, including making security an integral part of corporate culture (50%) and building an integrated security strategy (47%) that can integrate existing systems (38%).

SAPEXPERTS PERSPECTIVE

> “Implementation of security controls for business applications must consider all aspects of where organizations implement their business applications: cloud and hybrid environments end to end. This is especially important as we consider the drivers for SAP HANA adoption which include SAP S/4HANA, SAP HANA standalone, and SAP Business Suite on HANA from a product perspective, and a strong on-premise footprint but with significant hybrid and cloud-based environments from a deployment perspective.”

~ Juan Perez-Etchegoyen, Chief Technology Officer, Onapsis

Steps to Success

Our research reveals that SAP customers should apply the following key steps to execute their enterprise security strategy.

- **Take the opportunity to build a more holistic approach to enterprise security strategy.** Any enterprise security strategy that is effective must encompass both systems still running on-premise, as well as those being implemented in the cloud. If the strategy doesn't include existing systems they will be left exposed to potential attacks by anyone who is able to breach a physical network, as has happened at many organizations over the last few years. It is also critical that any new implementations, whether on-premise or in the cloud, be a major part of any strategy – especially if using infrastructure-as-a-service environments where it is incumbent upon the user to provide appropriate security controls.

- **Align security policies and controls with business processes in order to ensure that compliance can be managed more effectively and be connected to a centralized security process.** 32% of respondents indicated that their top driver for enterprise security strategy was the need to align security policies and controls with business processes, and 47% said that they were building an integrated security strategy that addresses these needs. This explains why 90% of respondents indicated that they either use or are planning to use business process controls as part of their enterprise security strategy. This integration is critical to minimize disruption to operations, a challenge faced by 48% of respondents, and facilitates compliance with government regulations and data handling requirements.

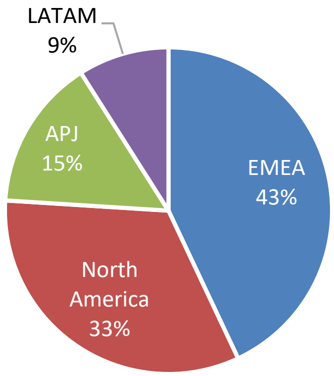
- **Focus on education and making the security policy part of the corporate culture.** Training across the organization is key to making security an integral part of corporate culture, chosen by 50% of respondents as the top action they are taking, and for building an integrated security strategy, which 47% of respondents indicated was critical. Lack of resources and expertise was a challenge for 58% of respondents, and 43% said that they judged the success of their enterprise security strategy through security awareness training results. After implementing a comprehensive security strategy, 46% of respondents said that they saw an improvement in those same training results. Education and learning are key to security being understood and used daily across the organization.

- **Build an integrated strategy that will encourage alignment between business process controls and knowledge and will also help reduce total cost of ownership (TCO), as well as the number of systems with known vulnerabilities.** An integrated security strategy provides a unified solution for every system in the enterprise landscape. Having this integrated security strategy not only supports the action being taken by 47% of respondents, but is also linked to the strategy of integrating existing systems required by 39% of respondents. And while cost management and containment is a challenge faced by 47% of respondents, an integrated strategy has lowered TCO for 31% of respondents. Lastly, an integrated strategy can assist with the reduction in systems with known vulnerabilities, something 55% of respondents indicated they saw improvement in after implementing a more comprehensive enterprise security strategy.

Methodology

In Q1 of 2020, SAPinsider examined the experiences of businesses and technology professionals related to their enterprise security strategy. Our survey was administered to over 150 SAP customers 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 for your organization's approach to enterprise security strategy?
- Which of the following technologies is your company currently using or planning to use to support your needed capabilities?
- What metrics do you use to judge the effectiveness of your enterprise security strategy?
- What challenges have you faced, or do you expect to face, when adopting an enterprise security strategy?



The demographics of the respondents included the following:

- **Job function:** Functional areas reported by respondents include: Information Technology (62%), Business Development (9%), GRC (7%), Supply Chain (4%), and Finance (3%)
- **Market sector:** The survey respondents came from every major economic sector, including: Software & Technology (32%), Industrial (28%), Financial Services & Insurance (13%), Public Services & Health Care (12%), and Retail & Distribution (10%)
- **Geography:** Of our survey respondents, 43% were from Europe, the Middle East, and Africa, 33% were from North America, 15% were from Asia-Pacific, Japan, and Australia, and 9% were from Latin America.

Appendix A: The DART^{TM} Methodology

SAPinsider has rewritten the rules of research to provide demonstrable 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 actionable insights including:

- **Drivers:** These are macro level events that are impacting 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 drivers impact on the business. These are the integration of people, process and technology. These should be business first but fully leverage technology enabled solutions to be relevant for our focus.

- **Requirements:** These are business and process level requirements to support the strategies. These tend to be end-to-end for a business process.

- **Technology:** There are technology and systems related requirements that enable the business requirements and support the overall strategies that the company is taking, they must consider the current technology architecture and provide for the adoption of new and innovative technology enabled capabilities.

For more information, visit SAPinsiderOnline.com.

Report Sponsors

Google Cloud brings customers industry leading AL/ML, trusted security, an open approach, and an innovation culture. Customers can migrate their data, workloads, and applications to a flexible, modern cloud to operate more effectively, modernize for core business growth, and innovate to drive new business models and revenue streams. Learn more about our solutions for SAP customers here: cloud.google.com/SAP

NetApp is the leader in cloud data services, empowering global organizations to change their world with data. Together with our partners, we are the only ones who can help you build your unique data fabric. Simplify hybrid multicloud and securely deliver the right data, services and applications to the right people at the right time. Learn more at www.netapp.com.

Since the companies' first collaborative efforts more than 20 years ago, Red Hat and SAP have continued to work together to champion innovation in the enterprise datacenter—first with Red Hat Enterprise Linux for SAP Applications (NetWeaver) and later with Red Hat Enterprise Linux for SAP HANA. Over 2400 global customers trust Red Hat solutions for SAP at more than 290 of the Fortune 500 companies. Red Hat offers SAP clients a comprehensive, fully open platform for embracing SAP's strategy of intelligent enterprises. www.redhat.com

SAPinsider
A Wellesley Information Services Company

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.