TURNKEY

SailPoint ONAPSIS

THE PRACTICAL GUIDE TO SAP SECURITY: TEN STEPS TO A MORE SECURE ESTATE

A JOINT GUIDE FROM THE MEMBERS OF THE SECURITY HUB: TURNKEY, SAILPOINT, AND ONAPSIS

UKISUG CONNECT

www.turnkeyconsulting.com/UKISUG

CONTENTS

PREFACE

For UKISUG Connect 2021, Turnkey, SailPoint and Onapsis have joined forces to form the Security Hub. This group represents three core pillars of SAP security: application security (Onapsis), Identity and Access Management (SailPoint), and effective consulting and implementation (Turnkey).

Over the last few years, the challenge of SAP security has increased considerably. Digital transformation and rapidly changing working habits have made SAP security increasingly complex, while the threat from cybercrime has risen, both in terms of scale and sophistication. For SAP customers, this means they need to take a truly end-to-end approach to security, one which recognises the scale of the task at hand.

Collectively, the Security Hub possesses a wealth of expertise, covering every facet of SAP security. In this guide, we've sought to bring all of that expertise together, and give you some practical advice for creating a more secure and compliant SAP estate. We'll cover the current threat landscape, the barriers to effective SAP IAM, and how you can build security into your S/4 HANA migration.

We'll also provide a very practical roadmap to a more secure SAP estate, detailing ten key steps to improved security and compliance.

If you're attending UKISUG Connect 2021 and would like to discuss any of the topics in more detail, join us at the Security Hub on stand G15, or get in touch at www.turnkeyconsulting.com/UKISUG.

→

Tom Venables,
Cyber & Application Security Practice Director, Turnkey.

INTRODUCTION: SAP SECURITY TODAY - WHAT IS THE THREAT?

→

Onapsis protects the mission-critical applications that run the global economy, from the core to the cloud.

ONAPSIS

Traditionally, best practices were to keep business-critical SAP systems on-premises and to install layers of security around them, creating a theoretical and impenetrable fortress of castle walls and moats.

However, the shift of the traditional on-premises perimeter to a distributed hybrid cloud model, and the recent need for every organisation to transform how it does business digitally has changed this paradigm. SAP is no longer in a lockbox, and threat actors have taken notice, targeting SAP with fast, sophisticated, and increasingly successful attacks. Organisations need to be aware and equipped to face the increased threats facing their most critical systems.

Accelerated digital transformation is emphasising speed over security

Digital transformation projects were underway well before 2020, but the global impact of the COVID-19 pandemic accelerated the digitisation of business across all fronts. From customer demands for increased digital interactions to completely remote workforces, the COVID-19 pandemic has given digital transformation a new sense of urgency as well as a mandate to prioritise digital readiness above all else.

This shift has left organisations vulnerable to new risks - both because of a larger number of externally-facing critical systems and far fewer resources to implement security best practices. According to a global survey of executives, companies have accelerated the digitisation of their customer and supply-chain interactions and their internal operations by three to four years. The share of digital or digitally-enabled products in their portfolios has accelerated by seven years.[1]

Digitised operations and products means business-critical applications and their data now reside in cloud-based, often public-facing systems and not within on-premises infrastructure. This has greatly increased the risk of exploitation. Organisations trying to keep up with the fast pace of acceleration may also be overlooking risks that potentially leave them susceptible to exploits, including the due diligence of security best practices.

Increased outsourcing and reliance on third parties introduces unknown risk

Hiring IT staff, especially application developers and managers who have experience with business-critical platforms like SAP, is a challenging task. According to United States labor statistics by the end of 2020 the global talent shortage amounted to 40 million skilled workers worldwide[2] and this shortage is expected to persist. Enterprises continue to hire contractors and system integrators in order to try to fill this gap. According to a Harvey Nash/KPMG CIO survey, 41% of organisations have plans to increase their spending on software outsourcing[3].

Bringing in third-party specialists who have advanced knowledge of SAP security best practices is likely to be a part of most security projects. However, turning to generalists to help meet project deadlines can result in increased risk. Organisations need a way to validate the work of these third parties to make sure they are setting up SAP environments correctly and writing high-quality and secure code. In-house application leaders need visibility and automation capabilities for assessing the code, transports, configurations, and patching efforts from third parties, so they can ensure corporate standards are met, security checks aren't interfering with their team's ability to meet project timelines, and security issues aren't being introduced to their most critical systems.

64%

of organisations have reported a breach of their critical SAP systems within the last 24 months.

Attacks on SAP are increasing and threat actors are smarter and faster than ever

The shift to cloud models, accelerated pace of digital transformation, and increased reliance on third parties discussed earlier have left business-critical SAP applications more vulnerable than ever - and threat actors have taken notice. Malicious cyber activity targeting SAP has increased over the last several years and those efforts appear to be paying off for the cyberattackers, with 64% of organisations reporting a breach of their critical SAP systems within the last 24 months[4].

Threat actors not only have the sophisticated domain knowledge to target SAP through a variety of attack vectors, but they are doing so at a faster pace than ever before. Onapsis research has found that there can be as little as 24 hours between the disclosure of a vulnerability and observable scanning by attackers looking for vulnerable systems, and just 72 hours before a functional exploit is available[5].

Beyond malicious activity targeting unpatched SAP applications, Onapsis researchers also observed evidence of attacks against known weaknesses in application-specific security configurations, including brute-forcing of high-privilege SAP user accounts. Additionally, attempts at chaining vulnerabilities to achieve privilege escalation for OS-level access were observed, expanding potential impact beyond SAP systems and applications[6].

Why this matters: The business and regulatory compliance impact of a successful SAP attack

The business impact of a successful SAP breach could be profound. In many scenarios, the attacker would be able to access the vulnerable SAP system with maximum privileges (Administrator/SAP_ALL), bypassing all access and authorisation controls (such as segregation of duties, identity management and GRC solutions). This means that the attacker could gain full control of the affected SAP system, its underlying business data and processes.

Having administrative access to the system would allow the attacker to manage (read/modify/delete) every record, file and report in the system. Successful exploitation of a vulnerable SAP system would allow an attacker to perform several malicious activities, including:

- Steal personally identifiable information (PII) from employees, customers and suppliers
- Read, modify or delete financial records
- Change banking details (account number, IBAN number, etc.)
- Administer purchasing processes
- Disrupt critical business operations, such as supply chain management, by corrupting data, shutting processes down completely or deploying ransomware
- Perform unrestricted actions through operating system command execution
- Delete or modify traces, logs and other files
- Exfiltrate critical intellectual property

For many organisations, business-critical SAP applications are under the purview of specific industry and governmental regulations, financial and other compliance requirements.

Any enforced controls that are bypassed via exploitation of threats discussed in this report might cause regulatory and compliance deficiencies over critical areas such as:

- Data privacy (e.g. GDPR, CCPA) due to unauthorised access of protected data, regardless of exfiltration
- Financial reporting (e.g. Sarbanes-Oxley) due to unauthorised changes to financial data or bypassing of internal controls causing inaccurate financial reporting
- Industry-specific regulations such as NERC CIP or PCI-DSS due to impact to regulated data

Having known vulnerabilities and misconfigurations in SAP systems that can allow unauthenticated access and/or the creation of high-privileged user accounts would be a deficiency in IT controls. For organisations that must meet regulatory compliance mandates, this would trigger an audit failure and violate compliance. This could lead to disclosure of the violation, expensive third-party audits and penalties that might include fines and legal action.

---

[1] McKinsey Digital and Strategy & Corporate Finance Practices How COVID-19 has pushed companies over the technology tipping point—and transformed business forever October 2020
[2] https://www.forbes.com/sites/forbestechcouncil/2021/06/08/is-there-a-developer-shortage-yes-but-the-problem-is-more-complicated-than-it-looks/?sh=383c6ef83b8e
[3] https://www.forbes.com/sites/forbestechcouncil/2021/04/13/analyzing-the-software-engineer-shortage/?sh=74b30951321c
[4] IDC Report, ERP Security: The Reality of Business Critical Application Protection
[5] Onapsis Threat Intelligence Report Active Cyberattacks on Mission-Critical SAP Applications
[6] Onapsis Threat Intelligence Report Active Cyberattacks on Mission-Critical SAP Applications

CHAPTER 2:
THE IMPACT OF ACCESS

→

SailPoint enables user access and protects your business. Everywhere.

SailPoint

The increasingly hybrid and distributed estate Onapsis have referred to not only increases the likelihood of cyberattacks, but also the difficulty of defending against them.

Identity and Access Management is a key tool in this fight, but with increased complexity, implementing effective IAM across the estate is becoming more and more challenging. Organisations need to ensure that the right people have the right access, at the right time, across both on-premise and cloud applications. If this cannot be achieved, both the risk of cyberattacks, and the damage inflicted by them, can increase significantly.

As Onapsis has pointed out in the first part of this guide, if an attacker was able to gain access to a user account that had unnecessarily broad privileges, then they could do much more damage than would be possible if access was appropriately controlled.

Facing such complexity, organisations need automated, job-based IAM processes which are fully integrated with HR data, in order to ensure appropriate access is provisioned across all of their business applications.

Without this automation, businesses will likely be burdened with heavily manual and disjointed IAM processes, and be exposed to much greater risk from cyber attacks as a result. SAP customers often find themselves in this position, because rolling out these solutions can come with considerable challenges when SAP is included.

Challenges of including SAP in IAM rollout

These challenges often make the inclusion of SAP into Identity and Access Management programmes so complex that many organisations do their best to avoid it.

Our recent survey of over 800 SAP customers worldwide has found that this is leading to IAM within SAP being managed in a heavily siloed fashion[1]. In fact, we found that more than 50% of SAP customers manage access to SAP separately from their other enterprise applications. With this siloed approach, consistent and automated IAM processes are made much more difficult, and a single, aggregated view of access risk cannot be achieved - making the effective mitigation of that risk harder than it should be.

The reasons cited for leaving SAP out of IAM programmes are many, but most commonly, they are:

- **Skills and tools shortages**: it's unlikely that the average IAM project team has sufficient expertise in SAP to handle it properly within the rollout. Bringing in the specialist tools and skills required is possible, but adds extra cost and complication that many organisations may feel they can do without
- **Staff availability**: SAP environments can change so fast that they can easily swallow up much of the SAP project delivery team's time: so much so that they can't commit the appropriate human resource to an IAM project. The simplest solution to this problem is just to leave SAP out altogether
- **Mothballing**: IAM rollouts are often presented to senior management as multi-phased projects, with SAP to be worked on some way down the line. As plans change and other areas need attention, SAP is often quietly dropped from the rollout and its addition never materialises
- **Avoiding complexity**: some IAM solution architects may intentionally leave out SAP. That's because they feel it's just too complicated to address its unique challenges around roles and granular access, vital for ensuring compliant segregation of duties. It also takes a lot of hard work to develop access that's clean from a SOX or JSOX perspective, with strong expertise needed to establish the low-level controls required

Protecting your SAP environment from access risk

The way to solve these challenges is to ensure that, come what may, SAP is included in your IAM rollout. As the previous section demonstrated, breaking down these barriers is far from simple, but the rewards on offer make the process more than worthwhile.

By implementing an integrated, automated, and enterprise-wide IAM solution that doesn't exclude SAP, not only are you protecting your organisation from cyber attack, you will also:

- **Improve user experience**: through automated access provisioning, employees will receive all the access they need to do their job as soon as possible
- **Increase operational efficiency**: removing delays around access provisioning means employees will be as efficient as they can be, throughout the joiner/mover/leaver processes
- **Reduce costs and demonstrate tangible ROI**: automation reduces the burden of heavily manual processes, reducing costs and improving the ROI of your IAM projects

[1] 2021 SAP Identity & Access Management Survey Report

CHAPTER 3: BUILDING SECURITY INTO YOUR S/4 HANA MIGRATION

→

The World's Risk, Identity, & Security Experts

TURNKEY

The previous chapters have covered the threat facing SAP systems, and the importance of including SAP in IAM programmes.

However, for many SAP customers, who are either contemplating their migration to S/4 HANA, or have already started, there are a whole host of other security considerations that they need to be aware of.

The good news is that SAP has recognised just how complicated the S/4 HANA migration can be, and so has extended its end-of-support deadline for ECC from 2025 to 2027. As of 2019, 91% of SAP customers had either started their migration or begun planning it, which means many are still at an early enough stage of the process to factor in any security considerations they might have missed [1].

Taking action now to cover off any security concerns with S/4 HANA is vital, in order to avoid the need to apply them retrospectively, as was frequently the case with ECC. Several legacy issues with ECC security suffered by organisations were due to certain measures being overlooked during initial implementation. Given that S/4 HANA migration will be complex enough, ensuring security is well-implemented now will avoid additional remediation costs further down the line, as well as the disruption to resources a post-implementation remediation project will inevitably bring.

SAP S/4 HANA Security considerations

Although SAP S/4 HANA has been created to give end-users simplicity, the same cannot be said for those implementing or managing security within the platform. Implementing S/4 HANA will demand major security involvement, mainly because some of the processes delivered to users have changed, so ensure you bear in mind the following:

What you need to consider with SAP S/4 HANA Security

- **Database security**: As the HANA database is an inherent part of the solution, the same level of security needs to be applied to the database, as the application itself
- **SAP Fiori access**: Fiori enables access from many different access points, which increases the surface area for potential external threats
- **Roles and authorisations**: S/4 HANA will contain more information and data, and so it's at greater risk should it be breached. Not giving access will no longer work as a risk reduction method, so applying roles and authorisations to correctly balance user access is a must
- **Catalogs and content**: S/4 HANA's relatively broad template roles come with inherent risks around compliance and Segregation of Duties within their standard catalogs and content, so these should not be deployed as standard
- **Process re-engineering**: S/4 HANA projects will likely result in major changes to business processes, meaning job functions, permissions and roles will probably need to be redefined
- **S_TCODE**: this will no longer be the go-to point for getting the best view of access risk, because standard transactions will no longer be the primary method for users to perform functions

91%

of SAP customers have either started their migration to S/4 HANA, or are planning to do so.

[1] Latest IDC Survey: Customers Are on the Move to SAP S/4HANA

How to build security into your S/4 HANA migration

Thankfully, professionals across GRC, access control, auditing and wider IT teams are showing strong awareness of just what a challenge security poses for S/4 HANA migrations. These five steps can help ensure that security is made, and remains, a top priority throughout the migration process:

- **Benchmark data**: analyse existing usage data from SAP ECC ahead of any brownfield migration, so that projected usage within S/4 HANA can be mapped out. This should apply to any business processes that aren't being redesigned
- **Align usage data**: for the business processes being retained, usage data should be aligned so that it can inform designs of other processes in the future. This can be complicated because of S/4 HANA's transaction code changes, but it's a worthwhile exercise
- **Assess standard roles**: whether a greenfield or brownfield implementation, assessing the 170 standard roles within S/4 HANA is an absolute must. ECC 6 had 4000, so the much smaller range within S/4 HANA means that they aren't segregated enough to minimise risk. These roles must be split out to meet your access needs and to avoid major risks being introduced
- **Risk mitigation**: it's more than likely that risks within these roles can't be eliminated completely as the roles can't be defined to a sufficiently granular level without making usual operations impractical. Identification and mitigation of those risks with controls is the best alternative
- **Considering SAP Fiori**: as Fiori is SAP's new primary user interface, how the security element of S/4 HANA migration fits in with it is critical. User interface security has to be taken into account when designing roles for the back-end, and not default to the SAP standard business roles, which generally aren't good enough for the job

CONCLUSION: 10 STEPS TO A MORE SECURE ESTATE

In this section, we've collated the top ten tips from each of the members of the Security Hub. Implementing each one of them will move you one step further to a more secure and compliant SAP estate.

1. Implement a vulnerability management program for SAP

Threat actors can exploit vulnerabilities from system configurations, user settings, custom code, and missing patches to gain access to your critical SAP systems. Finding and remediating these vulnerabilities before they can be exploited is essential to protecting your SAP environment.

2. Build application security testing into development processes

Incorporating security checks into your SAP development and change management processes allows you to find issues in the shortest possible time. Fixing issues before they hit production is typically easier and less expensive, and helps avoid negative impact to system security, compliance, performance, or availability.

3. Continuously monitor for internal and external threats

SAP is an attractive target for malicious actors, both inside and outside the organisation. Keeping an eye out for unauthorised changes, misuse, or attack indicators is crucial to identifying this type of malicious behavior early so actions can be taken to prevent serious consequences.

4. Ensure you have clear visibility of access risks

Implement business-friendly reporting to gain full visibility of your access risks, while enabling your business to make data-driven decisions on areas for remediation.

5.
Implement an Integrated Identity Platform

Any SAP IAM implementation needs a seamless, integrated platform with a simple user interface and common governance operations. All underpinned with flexible support to craft granular SOD policy violation rules that meet evolving business needs and provide improved security and compliance.

6.
Create easy to use access governance processes

JML, recertifications, firefighter – Business users will be key participants of the governance process, so this needs to be easy to set up, maintain and govern.

7.
Go beyond the application

It's common for SAP customers to focus the attention of their security programmes on the application. However, all of the data at the application layer is also available via the infrastructure on which the application sits. To provide the highest level of security, make sure you apply consistent levels of protection to both the application and the infrastructure layers.

8.
Consider the impact of "UK SOX"

The security of your SAP system is likely to come under much more scrutiny as a result of the impending "UK SOX" requirements. While the details aren't yet fully clear, ensure you keep your finger on the pulse, so you're ready to respond as soon as possible.

9.
Build security into your S/4 HANA project from day one

SAP customers which neglect security at the early stages of their S/4 HANA project are likely to face expensive remediation projects later down the line. Save yourself the expense and disruption this will inevitably cause by building security into your migration from day one.

10.
Visit the Security Hub at UKISUG Connect 2021

For those considering how to improve their SAP security posture, make sure to visit the Security Hub on stand G15 at UKISUG Connect 2021. By doing so, you'll get access to lots more SAP Security insights, that will help you move one step closer to a more secure and compliant SAP estate.

Why Turnkey and Onapsis

In partnership with Onapsis, Turnkey is helping clients to ensure their SAP systems are protected against vulnerabilities and prepared to integrate SAP with the wider enterprise cyber controls environment. Our skilled team of consultants can help you to prioritise findings and apply the right remediations to minimise the risk to your critical business systems and operations.

Leveraging the power of the Onapsis Security platform, Turnkey will help ensure that you have visibility of exposures, can remediate weak spots and provide continuous monitoring over your estate, whether those issues are within configuration, compliance or heavily customised code.

Why Turnkey and SailPoint

Turnkey is a leading SAP IAM consultancy, with years of experience both implementing and integrating SailPoint and SAP. Our deep understanding of the detailed processes within SAP and SailPoint make us perfectly positioned to help ensure your SailPoint implementation is a success.

By working with us, you'll benefit from our understanding of the layers of access within SAP and be able to surface cross-system risks which will impact both the SAP and non-SAP landscapes. You'll also be able to take advantage of our identity and access management expertise - as well as our S/4 HANA Access Risk Ruleset and established SAP Segregation of duties frameworks.

www.turnkeyconsulting.com
www.sailpoint.com
www.onapsis.com

TURNKEY SailPoint ONAPSIS

TURNKEY SailPoint ONAPSIS