TURNKEY

SailPoint ONAPSIS

KEY INSIGHTS GUIDE

SECURING YOUR PERIMETER: WHAT PERIMETER?

www.turnkeyconsulting.com

CONTENTS

3 **PREFACE: WHAT PERIMETER?**
Adopting zero-trust for SAP

4 **CHAPTER 1: SAP SECURITY - WHAT DOES THE THREAT LOOK LIKE IN 2024**
Onapsis assesses the current level of threat to SAP systems

8 **CHAPTER 2: NEVER TRUST, ALWAYS VERIFY**
SailPoint explores the challenge of an unclear perimeter, and the components of an identity-centric security model

12 **CHAPTER 3: HOW TO ENABLE A MORE INTEGRATED APPROACH**
Turnkey explain how to address your security blindspots, and provide 7 ways to achieve a more integrated approach to security

PREFACE
WHAT PERIMETER? ADOPTING ZERO-TRUST FOR SAP

Turnkey, SailPoint, and Onapsis have collaborated on this guide and represent the three core pillars of SAP security: application (Onapsis), identity and access management (SailPoint), and effective consulting, implementation and integrations to help manage risk (Turnkey).

Legislative changes, such as the US National Cybersecurity Strategy, are placing a greater emphasis on the need for businesses to secure their systems and data. These businesses are also adopting new technologies within their core ERP systems, like SAP, as part of their digital transformation journeys. Cloud-hosting solutions, such as SAP's RISE, or other hyperscalers will help ensure these estates are secure.

The traditional view of network perimeters has changed - as have our systems, endpoints, users, and data that sit within those perimeters. Our approach to securing our data and systems needs to also adapt, especially when considered in the context of increased threats from malicious actors.

Adoption of zero-trust approaches to securing the enterprise needs to be applied to the SAP estate, taking into account all the elements involved. Being able to trace data to assets, whether they are on-premise or in the cloud, validates that those assets are secured. It also verifies the authenticity of the users accessing. Systems and data must both work together in order to minimise the risk of compromise to the SAP estate. In this guide, we will look at how integrating vulnerability management with effective access governance is a key piece of the puzzle when it comes to securing these business-critical systems.

If you would like to discuss any of the topics in more detail, you can get in touch with us at www.turnkeyconsulting.com/contact-us

→

Ed Davis
Managing Director
Turnkey APAC

CHAPTER 1:
SAP SECURITY - WHAT DOES THE THREAT LOOK LIKE IN 2024

→

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 from 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 mean 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 ManpowerGroup, 2022 saw talent shortages reach a 16-year high, with 3 in 4 employers reporting that it's difficult to find the talent they need[2], and this shortage has persisted. 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.

Companies have accelerated the digitisation of their customer and supply-chain interactions and their internal operations by three to four years.

Managed Service Providers under cyberattack in 2022:

MSPs have been hit with a successful cyberattack

MSPs saw increased attacks targeting customers

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. A 2022 study found that 90% of MSPs have been hit with a successful cyberattack in the past 18 months, and 82% said attacks targeting their customers has increased[4].

Whilst it's widely acknowledged that phishing attacks are on the rise, vulnerability attacks also pose a potentially unappreciated risk. These vulnerability exploits are difficult to spot without the help of Application Vulnerability Management services like Onapsis' 'Assess'.

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, and 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 to 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 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.

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.

[1] McKinsey Digital and Strategy & Corporate Finance Practices How
[2] https://go.manpowergroup.com/hubfs/Talent%20Shortage%20 2022/MPG-Talent-Shortage-Infographic-2022.pdf
[3] https://www.forbes.com/sites/forbestechcouncil/2021/04/13/analyzing-the-software-engineer-shortage/?sh=74b30951321c
[4] https://www.mspinsights.com/doc/of-msps-surveyed-have-had-cyber-attacks-penetrate-their-defenses-0001
[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: NEVER TRUST, ALWAYS VERIFY

→

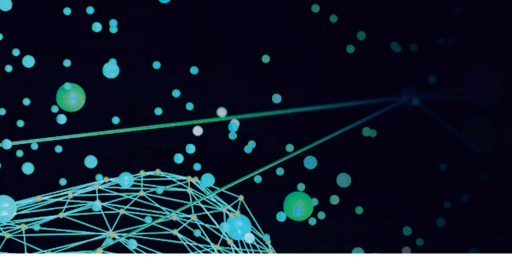
SailPoint enables user access and protects your business. Everywhere.

Security has been moving away from traditional perimeter-based approaches for several years with concepts such as zero-trust. This has only accelerated following the pandemic, which spurred a much greater need for users to access data and systems from anywhere.

Traditional network-based and boundary-based security allows us to make assumptions around access. If you know that the only place to access an application is from within a closed-off network with static entry points, then a low level of authentication may be adequate; moving that control point to a VPN changes the perimeter but doesn't fundamentally alter the way the applications work. Management of that, however, adds overhead and makes it difficult to expose applications and data to external users whether internal but remote (or on BYO/mobile devices), partners, or customers.

Furthermore, the widespread adoption of cloud computing means that many applications are no longer within the traditional perimeter. This, combined with greater mobile usage means that, for some organisations, most business operations are conducted outside of the corporate network.

These trends have resulted in organisations shifting the traditional security perimeters to focus on their users - including employees, contractors, partners, vendors, suppliers, and non-human bots. The trends apply across all forms of applications, from SAP and other ERP systems to small business line applications.



The principles of cloud computing and SaaS are here to stay for most organisations.

This is the basis of identity security: enabling the right access for the right users at the right time. This is also foundational to a successful Zero Trust security strategy.

Zero Trust Security is based on the notion of "never trust, always verify" and "assume the breach." What this means in practice is that no one should automatically be trusted to access resources, whether inside or outside of an organisation. Essentially, every user is considered suspect until proven safe. When all network traffic by default is untrusted, the only viable security strategy is one with identity at the centre.

According to a recent IDSA report, nearly all (97%) IT security experts agree identity is a foundational component of a Zero Trust security model[1].

Key principles of implementing an identity-centric security model include:

- **Never trust, always verify**: Enable accurate access decisions to be driven with contextual, up-to-date identity data. This starts with building a holistic view of users, their access, and context – you can't verify what you don't have visibility of.
- **Deliver just enough, timely access**: Enforce least privilege using roles and complex policy logic and provide for changes rapidly using automation, including removing unused access.
- **Continuously monitor, analyse, and adapt**: Keep security up-to-date and dynamically respond as changes happen and threats are detected. This will extend beyond the identity platform itself and leverage shared signals and data from associated systems covering security and access.

So, why are we doing this?

With workers no longer found purely within the confines of an office, they form easier targets than traditional attacks through the network. Whether it's social engineering, phishing, or just negligence (everyone has heard a story about laptops left in public, or passwords on post-its).

It only takes one point of exposure to be compromised, and compromise in one system can quickly lead to another, particularly if passwords are shared across systems. With each point of exposure, there's a person – an identity associated. That identity will have access across multiple systems – the larger the number of systems and the greater levels of access across those, the worse any potential breach may be.

With this, we can see that the concepts of just enough, least privilege access become paramount. Understanding and controlling which users have access to which data helps us to (in some cases) prevent and (in others) mitigate those breaches. Following the principle of assuming a breach, it makes sense to limit what access a user needs.

[1] 2021 Trends in Securing Digital Identities.

Limiting access isn't just about removing, it's also about making sure that people (or other users) have what they need when they want it – this means that if we remove unnecessary privileges for users, we provide a way for them to get the access they need. For example, the ability to perform a highly privileged action regularly, such as producing end-of-quarter financial reports, need not be permanently assigned to a user if there's a simple way to request, approve and provision that access when it's needed. Unfortunately, many companies are still reliant on manual processes for changing access, which makes this strategy unsustainable without automation built into those identity-centric processes.

By implementing an integrated, automated, and enterprise-wide IAM solution that doesn't exclude SAP and your cloud applications, not only will you protect 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.

When all network traffic by default is untrusted, the only viable security strategy is one with identity at the centre.

97%

of IT security experts agree identity is a foundational component of Zero Trust.

CHAPTER 3: HOW TO ENABLE A MORE INTEGRATED APPROACH

→

Turnkey are committed to making the world a safer place to do business.

TURNKEY

As you've seen in the previous chapters, implementing zero-trust approaches to SAP applications is a key element of securing your business-critical information and the processes that information supports.

How much of your business is conducted on SAP?

It is important to consider how your SAP environment is treated in the wider context of the enterprise IT estate, where additional controls may be applied but not cover the SAP systems, databases, and endpoints in the same way. Part of this challenge is a disconnect between information security functions and application owners, where there is a need to bridge the gap between these two areas.

It is not uncommon for the SAP estate to be handled a little differently from other applications and infrastructure. This can often be because SAP can behave a little differently from some other systems which would be in the scope of information security, but that perceived difference can result in blind spots of security coverage.

For example, from a CISO's perspective, SAP may only represent around 10% of the total IT landscape which must be secured, and so will be treated as though it only requires 10% of their attention. If we take an enterprise risk view, however, that 10% footprint may equate to 90% of the attack surface which Advanced Persistent Threats (APTs) may be targeting. Consider how much customer data, supply chain risk, or core business processes may depend on your ERPs, Extended Warehouse Management (EWM), or management information systems. Then the risk profile of your estate can be understood (and prioritised) very differently. Similarly, SAP application owners, while understanding the risk, may have less knowledge of the need to integrate controls with enterprise solutions. Terms such as DLP, XDR, SIEM, and SOC operations may not be foremost in mind for an SAP specialist and so may not garner the attention needed to achieve true security for the whole estate.

For example, databases are not necessarily part of the controls attestations an application owner may have full visibility of, but migrating to HANA, and the exposure of data views to new frontends, forces a change in the way we secure these critical systems. Securing privileged access to the database is more critical than ever, as is the need for data segregation within the logical structures of the database itself. Have you included your databases in your Privileged Access Management (PAM) processes?

Consider: Do you know who accesses the database, how they do so, and what mechanisms are in place to control those? If not, how can you have confidence that your data is secure?

PAM controls applied to the entire estate should be applied to all elements of the SAP landscape, ensuring that you can provide controlled access to operating systems, servers, databases, applications, and endpoints. Especially where those endpoints are migrating away from traditional desktop-based usage of systems and onto mobile devices and into more fluid ways of working.

Securing privileged access to the database is more critical than ever, as is the need for data segregation within the logical structures of the database itself.

7 steps to enable a more integrated approach

The key to achieving effective security and management of risk is being able to know, in real time, whether your systems are secured against threats. If an application has a new vulnerability, how quickly can you identify that, and respond? Have you got the processes in place to act on the information which tools like Onapsis and SailPoint are giving you about the health of your estates and identities?

1. Link your control demonstration to risk

For a given risk, you can identify where SAP may be contributing and measure how effectively you are controlling this. Is data loss prevention your primary concern, or are you worried about interruptions to the supply chain? This will help you prioritise solutions and measure how effectively you are meeting the control objectives.

2. Map your estate

Once you know the risks to your estate, ensure you know the full extent of the estate itself – do you know what systems are within the SAP estate, do you know their patch level, operating system, privileged accounts, and how current the information is? Without knowing where you may be vulnerable, you cannot determine where to spend your efforts to improve. Has the estate changed with the adoption of new technologies, or migration to cloud services? Are your endpoints known?

3. Know your Data

Some information is more attractive to malicious actors or more of a risk to your organisation. By mapping the risk to the data and the data to the estate, you know where to focus your efforts and what solutions should be in place to fill any gaps in controls.

4. Manage your vulnerabilities

Ensure SAP is included in vulnerability scans, pentests, and patching programmes, both for the application and the estate. This is especially important on systems you have identified as critical in points 2 & 3.

5. Integrate your SAP systems with enterprise IDAM & PAM

Through automation of Joiner, Mover, Leaver (JML) processing and a consistent approach to identity, you can ensure that you know who is accessing your data, from where, and how. This allows you to take a zero-trust approach to key processes, putting in place policy-based access controls alongside the more traditional role-based access controls.

6. Integrate with SOC/SIEM operations

Find out what your infosec operations are and whether they're applied to the SAP estate – is telemetry included from Extended Detection and Response (XDR) for the SAP servers? Can you enrich data for Indicators of Compromise (IOCs) with SAP information so an attack could be identified and shut down before it causes issues for business-critical systems or data?

7. Train your users

Users of SAP systems hold the keys to important information and processes. Consider them as privileged users within your estate, even if they're not system administrators. Is a baseline level of security awareness (like an annual course) really enough for this user base? By training SAP users with regard to cybersecurity and information classification to a higher baseline, you can reduce the vulnerabilities to your data and systems. Integrate the completion of this training with your IDAM programme to ensure access is only granted to users who have qualified to be able to deal with your sensitive information.

ABOUT TURNKEY

Turnkey Consulting is helping to secure enterprises and drive performance through its specialised expertise across Integrated Risk Management, Identity and Access Management, and Cyber and Application Security. We elevate risk and security professionals by creating digital enterprise resilience through business strategy and consulting, technology implementation and managed services.

CONTACT

If you have any questions about Zero Trust for SAP, or any of Turnkey's services, we'd love to hear from you.

Contact us

✉ info@turnkeyconsulting.com

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

TURNKEY SailPoint ONAPSIS