SailPoint

White Paper

Journey to the cloud: Best practices for managing SAP access

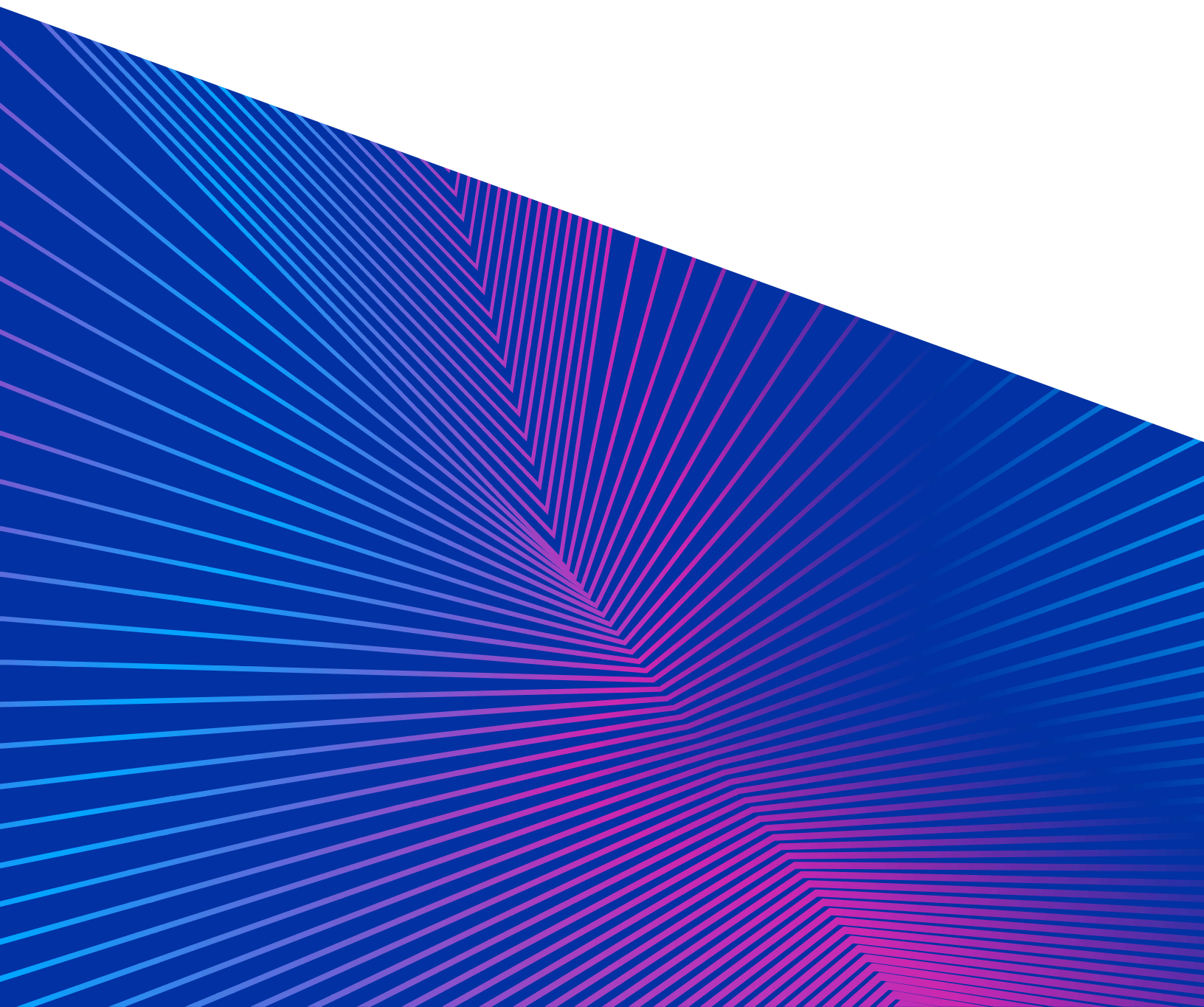


Table of contents

Navigating SAP changes

The development, implementation, and maintenance of SAP applications ranks as one of the most critical and ongoing IT investments for today's enterprises. Significant SAP business strategy changes and an expanded focus on cloud-based infrastructure, applications, and services are fueling a convergence of business scenarios that underscore the need to secure access to SAP ecosystems.

These changes have become a defining moment for all SAP customers as enterprises are adjusting IT strategies and searching for solutions that will help them secure their most critical resources as they adapt to and satisfy transformation initiatives.

The SAP ecosystem is overwhelming and diverse with a multitude of cloud, hybrid and custom applications and services, plus new infrastructure like SAP Business Technology Platform (SAP BTP), S/4HANA Private Cloud (RISE offering), SAP Cloud Integration Services (CIS) and SAP Identity Access Governance (SAP IAG) alongside existing on-premises infrastructure, applications and systems.

There's also the challenge of managing and securing application access for a rapidly changing and expanding user base. Today's reality is that no user works in just one application to do their job – not to mention that the definition of a "user" is constantly changing. For that reason, it makes more sense to think of users as identities.

An identity could be an employee, a temporary or contingent worker, other business users like partners or service providers, or even machine identities. And, these identities might be working on-premises, or within cloud-based or hybrid infrastructure, services and application scenarios.

Visibility across so many infrastructure layers is key to both zero trust and smooth transformation, as is implementing a comprehensive and centralized identity security program across SAP environments from which organizations can easily manage access.

This whitepaper dives deeper into these issues to help you understand not only the overall organizational and business issues of SAP convergence and the challenges of secure access, but also what efficient and secure identity governance looks like in the real world. We'll also identify the best practices and identity security solutions that will help smooth and secure your journey to the cloud, including:

- Importance of securing SAP on-premises, cloud and hybrid environments
- How to manage access to critical SAP line-of-business applications
- Achieving identity security continuity while transitioning to SAP cloud
- Support for separation of duties (SoD) and governance needs
- Maintaining compliance and audit requirements amid transformation

Understanding SAP convergence

Significant SAP business changes are driving the need for secure access to the SAP ecosystem. First, the company's cloud-first strategy and the replacement of on-premises SAP Enterprise Central Component (SAP ECC) to cloud-based S/4HANA is prioritizing the development, delivery, and enhancement of SAP products and services using cloud-based platforms instead of traditional on-premises solutions.

This approach supports migration and modernization efforts for complex ERP systems to ensure agility and scalability in business operations. While there is no constant but change, especially when it comes to complex IT environments, the dilemma of securing business-critical applications and protecting considerable internal SAP investments amid such significant transition presents new challenges for SAP customers.

Second, the SAP landscape is complex with dozens of on-premises, cloud, hybrid and custom-built applications that have complex dataflows both within and outside of the SAP landscape (such as for non-SAP applications). Unauthorized SAP system and application access is a challenge without centralized policies, and organizations are faced with how to secure access and mitigate the risks associated with transition as they move to S/4HANA and adopt more cloud-based solutions.

According to the **2024 Pulse of the SAP Customer study** from ASUG, the world's largest independent SAP user group, while members increasingly see themselves in the cloud with about 62 percent planning to run S/4HANA, those currently running on-premises SAP instances cite costs or resources, security, and compliance as the top hurdles preventing their migration efforts.

And, as SAP expands its focus on delivering innovations for its cloud customers, enterprises are looking for solutions that can effectively meet them where they are, at any transformation stage. This includes adopting multiple cloud and hybrid solutions to help them make the transition—including SAP S/4HANA Cloud, RISE with SAP, SAP Analytics Cloud, SAP HANA Enterprise Cloud, and SAP BTP. However, this also expands the list of services that enterprises must secure.

Finally, enterprises also need to control access and implement end-to-end security measures for applications outside their SAP environments. As the legacy SAP Identity Management (SAP IdM) solution, SAP GRC, and ECC applications move toward end-of-life, organizations are searching for alternative identity security solutions that can not only secure their IT landscapes and align with stringent regulation, compliance and policy requirements, but that can also secure their SAP environments and make a secure transition from SAP ECC to S/4HANA.

Difficulty in securing access across SAP systems

There's no question that the SAP ecosystem is wildly diverse with a staggering number of cloud, hybrid and custom applications and services; existing on-premises infrastructure, applications and systems; and new infrastructure platforms like SAP BTP and SAP IAG.

This landscape's depth and breadth alone makes it challenging for organizations to get overall visibility into application, system and infrastructure access, but there are other concerns that further impact that difficulty.

Complex application environments

The SAP application environment—with its disparate technical architectures, multiple API end points, and security models—is equally complex, which makes it difficult to implement comprehensive, more automated identity governance.

Specific access challenges include:

- **Siloed application governance:** Distinct application security models make it challenging to govern risk related to identity across the organization.
- **Massive data volumes:** Searching and navigating SAP objects and resources to accurately define and assign roles for access can be overwhelming.

- **Disparate user lifecycle management:** No single interface to see and manage access throughout a user's lifecycle.
- **Fragmented API interfaces** for gathering user access, entitlement, and attribute information

Centralizing security policies

Understanding and setting up centralized security policies across new and legacy SAP applications to secure the entire ecosystem is a mammoth and challenging task, as is managing access rights and controls across SAP on-premises, cloud and hybrid applications. Any mismanagement of user permissions can lead to unauthorized access, posing significant security risks.

Securing identities

Maintaining accurate user access is also challenging amidst frequent organizational changes like onboarding, role transitions, and terminations. Manual provisioning is risky and time-consuming for multiple SAP applications; there's a need for automation and efficiency. Without automated lifecycle management, ensuring that user entitlements are promptly updated can be labor-intensive and error prone.

Resolving SoD conflicts, maintaining compliance

Identity security administrators must also monitor for separation of duties (SoD) conflicts and access certifications. Both pose high risks if unresolved and can result in internal fraud and regulatory non-compliance issues.

Governance across the enterprise

Integrating SAP systems with existing identity governance frameworks is a daunting task, often requiring specialized knowledge and significant resource allocation to ensure seamless interoperability and comprehensive oversight. "Traditional" identity security administrators and specialized SAP administrators must align on identity security and zero trust initiatives to properly manage access across the business.

Governance for non-SAP applications

Every organization that uses SAP to run their business also needs to govern access to non-SAP applications that are equally critical to their business, such as ServiceNow, Oracle, Salesforce, Workday, and others.

The modern enterprise requires coordinated, consistent, end-to-end identity governance across an organization's entire IT landscape to properly secure access, mitigate risks, and ensure compliance with regulatory and compliance requirements. This becomes even more important as organizations are reinventing their business and IT landscapes to align with SAP's cloud-focused strategy.

Importance of secure access to SAP on-premises, cloud and hybrid landscapes

Identity security that supports transformation should cover SAP cloud, on-premises, and hybrid applications and infrastructure, and that starts with visibility to an organization's ecosystem.

Without clear visibility of the granular access for each user across all the SAP applications and access paths, securing and auditing the entire SAP ecosystem is a challenging task. Here are a few key areas to consider:

- **Roles and provisioning:** Provisioning access rights and defining roles needs to be done consistently across all applications—on-premises, cloud, and hybrid—so organizations can stay productive.
- **Security Policies:** Organizations should have defined security policies and procedures that accommodate access right changes throughout the user lifecycle as access rights change.
- **Regulatory compliance:** No matter where in the world they are, in the world, every organization needs to comply with ever-increasing and changing regulatory requirements and ensure timely access certifications and SoD needs. This also includes proper reporting and audit trails.
- **Holistic identity security:** Securing your organization's entire technology landscape in important for complete security—from SAP on-premises, cloud, and hybrid applications and services to non-SAP applications.

Managing Roles and Provisioning

In provisioning access, you want to assign the right level of access to the right people (both employees and contractors) to do their jobs without delays that frustrate users and waste valuable time, especially in the case of expensive contractors.

But how do you achieve the enterprise-level visibility needed to do this within the complex security structure of SAP ecosystems? If organizations can't see the complete story of a user's access—both SAP and non-SAP applications—they can neither provision nor govern access efficiently.

Organizations are also challenged with seeing and managing user access rights across diverse applications in the SAP ecosystem—controlling the disparate identity governance systems of each application individually can get overwhelming. The review process for SAP is also different from that of other applications.

Finally, multiple teams addressing multiple requests can delay receiving access and create the potential for multiple points of failure. It can be difficult to track progress in provisioning access or identify the correct individuals to follow up with in the event of an issue. And manual provisioning processes put organizations at a disadvantage to show alignment with compliance regulations (SOX 404 ITGCs, GDPR, etc.).

Implementing Security Policies

As users take on new roles, move or leave the business altogether, the access rights originally provisioned must change, aligning to the security policies of an organization. In the ideal world, access rights change requests would follow easy, well-defined, centralized access security policies and procedures.

If the processes you use are cumbersome or time-consuming, the temptation is to circumvent security procedures. But this goes beyond planned changes—such as when an employee exits, or a contractor completes a project. The reality is that unexpected change requests happen all the time and that could open the door to granting access quickly without following proper procedures.

The bottom line is that manual processes make it difficult to easily, efficiently, and comprehensively secure changes to access. Unfortunately, how well (or poorly) organizations manage change also affects their ability to comply with regulations.

Meeting Regulatory Compliance

Securing identity and access permissions across the organization is fundamental to complying with virtually any regulation. But just as manual provisioning and implementing security policies can be labor-intensive and prone to errors, the same goes for manual compliance reporting. It's yet another result of consequence unclear visibility into user access and entitlements across the SAP ecosystem. Let's talk about these issues in detail:

Separation of Duties (SoD)

Implementing internal SoD controls is a fundamental risk management principle that requires the division of tasks and responsibilities among different individuals to minimize the risk of error or fraud. The idea is that no single individual should have control over all aspects of a financial transaction or operational process to prevent conflicts of interest and ensure accountability.

Access Certifications

In most organizations, certification and review processes are manual and time-consuming. In fact, certifications are often rubber-stamped without a detailed review and, in some cases, don't happen at all. Certifications alone don't tell organizations much about the risk associated with users getting access to specific roles and the ability to perform certain transactions. And in the case of a specific transaction, what role should be requested to gain access to it? What other transactions are granted with it?

Reporting and Audit Trails

Organizations should also be able to generate comprehensive and accurate reports in a timely fashion. However, there are multiple tables in (potentially) multiple systems that need to be extracted and joined to paint the full picture, depending on the intended goal of a report, so even this can get complicated.

Comprehensive identity security across the enterprise

Every organization uses multiple applications for human resources management, onboarding, training, vendor management, account & finances, infrastructure management, reporting, IT helpdesk, and much more that go beyond core SAP environments.

Think Microsoft Entra, Workday, ServiceNow, Salesforce and others that are critical to everyday business operations and productivity—all of which require comprehensive access management. Any of these application endpoints can be targeted for access to critical customer, finance, or other proprietary data.

SailPoint supports more than 1,100 enterprise applications and 20,000 custom applications. Our technology allows customers to extend, connect, and integrate core identity security capabilities with the critical business applications they use every day, all under a single identity umbrella, which is essential in jumpstarting identity security time-to-value.

This also extends to SailPoint's strategic technology collaboration with SAP. **SailPoint Identity Security for SAP** includes flexible and comprehensive solutions that align with industry best practices and SAP technical requirements to help enterprises control and manage access to SAP cloud, hybrid and on-premises applications and infrastructure. These solutions also offer options for efficient SoD and access certification capabilities via SAP GRC Access Controls, GRC-IAG bridge, and SailPoint Access Risk Management.

Available for SailPoint Identity Security Cloud and IdentityIQ, these powerful enterprise identity security solutions securely support SAP transformation initiatives from on-premises SAP ECC to cloud-based S/4HANA, as well as those transitioning from SAP's IdM solution.

SailPoint Identity Security Cloud is a unified, AI-powered approach with a scalable SaaS architecture that is designed to meet identity security needs for every type of identity at every phase of the identity security lifecycle. Identity Security Cloud is a market-tested solution for SAP IdM customers as they prepare for the end of maintenance in 2027.

Journey to the cloud: Focus on best practices, alignment with SAP architecture

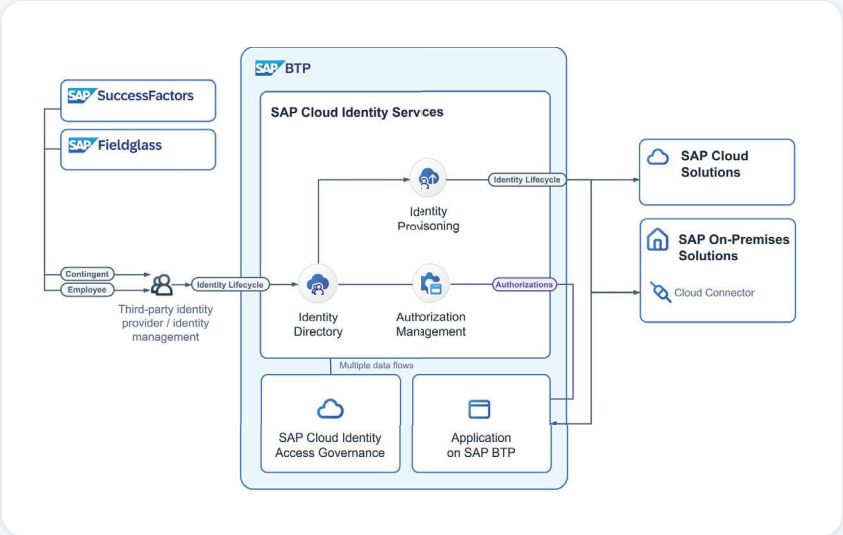
SailPoint's approach to identity security for SAP applications aligns with SAP's strategic vision, reference architecture, product offerings, integration landscape, methodologies, and roadmap.

Our integration with SAP's Identity Provisioning Service (IPS) gives customers the ability to quickly extend identity security to the most widely used SAP cloud applications. This core identity security functionality includes access requests, access approvals, lifecycle management, internal certifications, and insights to provide deep governance for critical SAP applications, whether on-premises or cloud.

According to SAP's System Integration Guide, SAP CIS is a group of services within SAP BTP that operate as an interface to integrate identity and access management between systems. The goal is to provide a seamless user access management experience across systems while also ensuring secure access.

The SAP Identity Directory serves as the central repository for storing user and group information within SAP CIS. As the authoritative source for SAP ecosystem users, it holds crucial data accessible through both APIs and the Identity Authentication service UI.

SailPoint is committed to the continued expansion and integration with SAP applications and systems for efficient management of users and entitlements. This extends to SAP cloud applications, on-premises systems and other non-SAP applications in the customer's ecosystem to deliver a unified perspective and governance of their entire organizational landscape.



Source: **SAP CIO Guide: Identity Lifecycle in SAP Landscapes, p. 30**

Identity security for the SAP enterprise and beyond

SailPoint Identity Security for SAP solutions give enterprises the ability to control and manage access to SAP cloud and on-premises applications—plus offer SoD and access certification capabilities—to support transformation at any stage. These solutions can help enterprises solve complex governance issues for equally complex SAP environments, including:

- **Identity security coverage for new SAP cloud infrastructure services to help spur quick adoption:** Integrations for SAP's new cloud infrastructure, including the SAP BTP and SAP Identity Directory/IAS for centralized user administration and provisioning to 40+ SAP applications through SAP CIS, in alignment with SAP's reference architecture.
- **Ability to manage access to SAP cloud line of business applications and services:** Integration with most business-critical SAP cloud line of business applications like SuccessFactors, SAP HR, Concur, Ariba, Fieldglass, and more using SAP IPS for quick and extensible integrations that can be tailored to suit business needs.
- **Integrations that help achieve identity security continuity for customers transitioning to SAP cloud:** Comprehensive identity security coverage for on-premises SAP Business Suite applications and for S/4HANA cloud, plus support for ECC applications moving to SAP RISE and integrations with SAP GRC and SAP IAG to perform SoD checks.

- **Secure coverage for SAP on-premises and hybrid landscapes:** Includes deep governance capabilities for SAP on-premises applications like ECC, S/4HANA, and SAP GRC for risk analysis, provisioning, access certifications, and SoD checks that span hybrid SAP landscapes, giving enterprises centralized identity security and end-to-end transparency into access.
- **Solutions that satisfy SoD needs:** Enterprises that need to implement centralized security policies and check risks, policy violations, and access certifications across their applications have multiple options, including SailPoint Access Risk Management (ARM); SAP GRC integration; and the SAP GRC-IAG (Identity Access Governance) bridge integration for those using SAP GRC and SAP IAG for provisioning and SoD analysis of on-premises and cloud SAP applications in a hybrid ecosystem.
- **Identity security for the enterprise:** Thousands of **existing SailPoint connectivity solutions** extend coverage beyond the SAP ecosystem to secure other business-critical applications and deliver comprehensive identity security coverage across the enterprise.

Conclusion

Targeted identity security for SAP landscapes

Managing SAP environments is a complex undertaking without the right systems in place to do so. A targeted approach to SAP identity security can help organizations achieve comprehensive visibility across both SAP and non-SAP environments and the kind of centralized control that's critical to zero trust initiatives.

It's important to take a strategic approach and consider holistic technology solutions that can integrate within existing on-premises, cloud and hybrid SAP environments, as well as with non-SAP applications so that enterprises can:

- **Control access across SAP:** Manage SAP on-premises, cloud and hybrid applications, infrastructure and services
- **Maintain compliance:** Define and enforce policies to ensure the right users have the right access
- **Secure non-SAP applications:** Bring SAP and non-SAP applications and data under a unified identity security solution that includes access requests, certification reviews, and automated lifecycle management.

Using well-established industry standards and SAP best practices, SailPoint delivers an integrated, holistic approach in partnership with SAP to build effective integrations for IT environments and help organizations secure access to key SAP applications.

How SailPoint can help

SailPoint can help organizations manage access to important SAP applications, improve security postures, satisfy compliance requirements, deliver a clear view of access across the organization, and achieve identity security continuity for those transitioning to the cloud.

Learn more about how SailPoint integrates with SAP applications.
Find out more about SailPoint Identity Security Cloud and IdentityIQ.

About SailPoint

SailPoint equips the modern enterprise to seamlessly manage and secure access to applications and data through the lens of identity – at speed and scale. As a category leader, we continuously reinvent identity security as the foundation of the secure enterprise. SailPoint delivers a unified, intelligent, extensible platform built to defend against today's dynamic, identity-centric cyber threats while enhancing productivity and efficiency. SailPoint helps many of the world's most complex, sophisticated enterprises create a secure technology ecosystem that fuels business transformation.