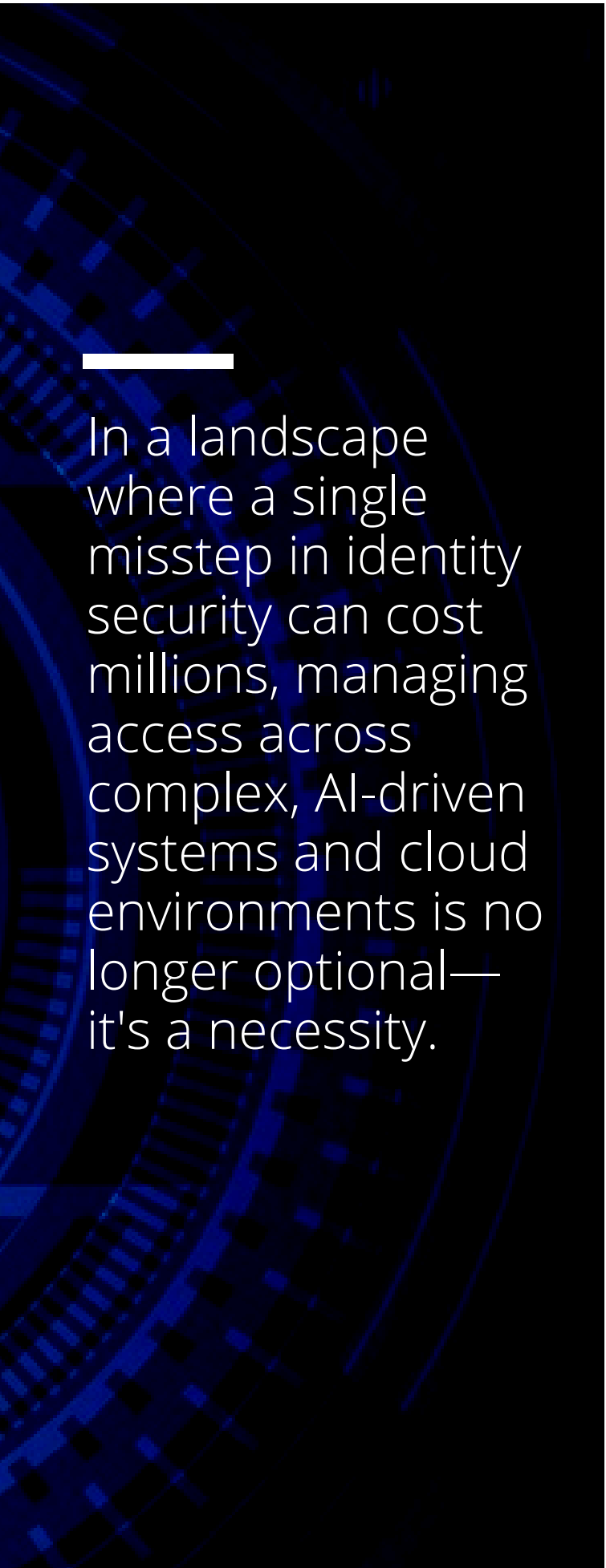




SHOULD YOU OPT FOR MANAGED SAILPOINT SERVICES?

2025



In a landscape where a single misstep in identity security can cost millions, managing access across complex, AI-driven systems and cloud environments is no longer optional—it's a necessity.

Executive Summary

As enterprises navigate through rapid digital transformation, identity security has emerged as a major challenge. Companies are increasingly adopting SailPoint's identity solutions to automate and secure the management of user identities, systems, entitlements, data, and cloud services. However, in an era dominated by new technologies such as Artificial Intelligence (AI) and a growing reliance on cloud environments, the complexity of managing identity security escalates.

Organizations face mounting pressure to provide the right access to the right resources, at the right time, while maintaining security and regulatory compliance. The growing number of endpoints, applications, and data sources further complicates the task of ensuring that the right users have access to the right resources without exposing the organization to unnecessary vulnerabilities. This rapid evolution demands more than just static identity policies; it requires adaptive, real-time identity governance solutions that can scale across increasingly sophisticated systems and environments.

While SailPoint offers an effective solution for identity management, many organizations struggle to optimize its functionalities, resulting in underutilized investments and a higher risk of breaches. Additionally, the adoption of AI presents new challenges related to securing complex, AI-driven systems, automation, and data privacy. This is where managed SailPoint services can step in, providing the expertise to maximize the value of SailPoint solutions while addressing both traditional security risks and new challenges posed by AI technologies.

How Managed SailPoint Services Could Help Ensure Identity Security?

Managed services for SailPoint go beyond basic security measures. They are crucial in helping organizations proactively address evolving security threats, mitigate risks associated with AI technologies, and navigate the complexities of hybrid IT environments. These services provide the expertise and support necessary to ensure seamless integration, optimize SailPoint's capabilities, and enhance overall identity security. By leveraging managed services, organizations can better safeguard sensitive data, enforce compliance, and drive operational efficiency, all while focusing on strategic growth and innovation.

Maximize ROI from SailPoint investment: Often enterprises are seen to either implement SailPoint in an ineffective manner or not optimize all its functionalities. A managed service provider helps in maximizing the ROI of the existing SailPoint tools by expanding the use case purview, efficient updation of the IAM platform and definitely avoiding shelfware. SailPoint investment is further enhanced as managed services help in minimizing compliance costs, taking care of skill gap challenges, cutting down maintenance costs, along with eliminating manual efforts to undertake identity solutions.

Avoid compliance issues: Stringent laws such as GDPR, California Data Protection Act or industry-specific regulations such as HIPAA, mandate enterprises to manage identities properly, while ensuring data privacy and security. Any gap in identity management could lead to breaches and thereby, financial and reputational loss for the company. Managed service provider could help in achieving compliance goals by not only overseeing user access to enterprise apps and resources, but also through integration of security solutions with critical business systems.



Keep Identity Platform Updated and Mitigate AI Integration Risks:

With the growing complexity of IT ecosystems, including cloud, hybrid, and AI-enabled platforms, managing up-to-date identity solutions becomes challenging. Managed SailPoint services ensure continuous updates to address emerging risks, including those related to AI. They provide robust monitoring and access controls to mitigate AI-related security concerns—such as data privacy and model vulnerabilities—while ensuring compliance with identity security policies and preventing disruptions in user access and system performance.

Get real-time security updates: With security becoming a core requirement for digital enterprise, it is imperative for the leadership to be aware of any vulnerability in the system, as compromised data or user could cause huge losses to the company. A third-party service provider could help the leadership get more visibility in their security posture by providing transparent and real-time security updates, which includes tracking any insider with malicious intent.

Undertake seamless cloud migration: In order to truly become a digital enterprise, accessibility to data at all time is the core requirement. Enterprises are thus, migrating to cloud environment, which is posing unique challenges as well. It is imperative to secure data on cloud platforms, while migrating SailPoint to the cloud. Employing experts to undertake such a task could not only help companies to avoid any security risks, but also ensure any future updation on cloud in a seamless manner.

BENEFITS OF MANAGED SAILPOINT SERVICES

Enterprises that are either struggling to hire professionals in-house or planning to outsource their security solutions to an expert team for managing their SailPoint solutions, could opt for managed services, and reap the following benefits:

1

MAXIMIZE ROI FROM SAILPOINT INVESTMENT:

Enhancing SailPoint investment by minimizing compliance costs, taking care of skill gap challenges, cutting down maintenance costs and eliminating manual efforts to undertake identity solutions.

2

AVOID COMPLIANCE ISSUES:

Achieving compliance goals by not only overseeing user access to enterprise apps and resources, but also through integration of security solutions with critical business systems.

3

UPDATE IDENTITY PLATFORM & MITIGATE AI RISKS:

Ensure seamless updates to identity platforms across cloud or hybrid environments, while addressing AI-related security risks effectively.

4

GET REAL-TIME SECURITY UPDATES:

Helping the leadership get more visibility in their security posture by providing transparent and real-time security updates, including tracking any insider with malicious intent.

5

UNDERTAKE SEAMLESS CLOUD MIGRATION:

Securing data on cloud platforms while migrating SailPoint to the cloud, enabling companies to avoid any security risks.

Along with implementing SailPoint's identity solutions to secure the data and users, it is also imperative for enterprises to gain control and visibility into their IAM platforms by managing and updating them on a regular basis. With the scope of identity and access management increasing daily, enterprises may as well benefit by hiring a managed SailPoint service provider to govern and secure the important corporate assets – data and users.



HOW TO CHOOSE THE RIGHT MANAGED SECURITY SERVICE PROVIDER

When selecting a managed service provider for SailPoint solutions, businesses need to perform due diligence to ensure that the provider can address both traditional and emerging security challenges. Consider the following:

Does the provider have a mature security program?

Verify if the managed service provider has implemented a mature security practice in its own organization or not. Often organizations overlook this important component, which may result in causing data breaches from vulnerable systems and networks from the vendor's end. Find out about the authentication and authorization tools being used by the provider and how they have been maintaining their systems.

Does the provider have sufficient understanding of your sector / business?

It is critical for the managed service provider to understand the sector that you operate in, along with knowledge of your business practices, as it helps them in mapping the risks associated with your particular business / sector. Further, sectoral knowledge ensures that the provider will be able to align regulatory compliances, as well as your business goals, with the identity security requirements. Understand if the provider has worked in similar sector or clients in the past, and ask for testimonials or recommendations.

Is the vendor willing to provide customized solutions? Every organization needs different solution as per their business requirements, and thus, a provider should be willing to offer highly-customized consulting-driven solution to the client. Find out if the provider is willing to connect and listen to your challenges and offering solutions based on your unique pain-points or is only interested in selling a subscription-based package.



Five points to consider before hiring a managed security service provider

As a managed service provider is responsible for securing the sensitive data of an organization, it is pertinent for businesses to be cognizant of selecting the right third-party provider. Here's a checklist to consider while hiring a managed service provider:



1 Does the provider have a mature security program?

Verify if the managed service provider has implemented a mature security practice in its own organization or not.

2

Does the provider have sufficient understanding of your sector / business?

Understand if the provider has worked in similar sector or clients in the past, and ask for testimonials or recommendations.



3

Is the vendor willing to provide customized solutions?

Find out if the provider is willing to connect and listen to your challenges and offering solutions based on your unique pain-points or is only interested in selling its services.



4

What benefits will you derive out of the collaboration?

List down all the benefits you may derive from such collaboration and ensure that they become a part of the service level agreement (SLA).



5

What will be the cost of the engagement?

Ensure the cost should include management, monitoring and reporting services, and listed in the SLA as well.



What benefits will you derive out of the collaboration?

When you outsource your security solutions, you need to partner with an organization that is willing to collaborate with you to help you grow without letting you being perturbed about security obstacles. List down all the benefits you may derive from the collaboration – such as protecting your data, systems, clients, and users – and ensure that they become a part of the service level agreement (SLA).

What will be the cost of the engagement?

It is essential to understand the costing and how it would impact your venture's monthly budget. You may need to ensure that the cost should include management, monitoring and reporting services, and listed in the SLA as well. The provider should ensure that any other costing, outside the scope of the SLA, should be first approved by your organization.

Undertaking a stringent due diligence process and evaluating providers at the initial stage of selection could help ventures to not only ensuring long-term security posture, but could also save cost.

How Avancer Helps?

At Avancer, we specialize in offering managed SailPoint services that go beyond basic implementation. Our team of experts helps businesses optimize their SailPoint solutions, ensure compliance, and mitigate emerging risks associated with AI and cloud migrations. We integrate DevSecOps practices to build security protocols throughout the stages of development and implementation, ensuring that SailPoint solutions evolve with your organization.

Some of our SailPoint managed solutions include:

Managing SailPoint in any IT environment: We understand that enterprises still have lots of their assets linked on-premises or have shifted some to the cloud. Our solutions are developed in such a way that we could manage SailPoint on the cloud or on-premises or in a hybrid environment in a seamless manner.

Providing consulting-based advisory: Our certified IAM experts not only supervise the identity platform and undertake regular updation, but they also provide recommendations in a proactive manner to help companies identify potentially risky user behavior, avoid possible threats and remain compliant.

Streamlining operations: Along with enabling companies to run their systems in an efficient manner, we focus on implementing best practices and standardized templates to help streamline various processes related to on-boarding applications or implementing newer solutions.

Undertaking rapid implementation and integration: We implement our tried-and-tested SailPoint implementation and integration process to help accelerate the timeline, without compromising the security posture. This enables the organization to undertake the process with minimal business disruption.

As a trusted SailPoint partner, we at Avancer focuses on maximizing a company's security program, along with optimizing the company's ROI for its investment in SailPoint technology.

AVANCER'S EXPERTISE IN IAM



CONSULT IT SECURITY ADVISORS AT AVANCER

Allow us to serve you, reach out to IT Security and IAM experts to strategize your IT Ecosystem

Avancer Corporation is a multi-system integrator focusing on Identity and Access Management (IAM) Technology. Founded in 2004, we have proven expertise in the field of Identity and Access Governance and IT Security. With a depth of experience in end-to-end IT Security Solutions, Avancer has evolved as a specialist in integrating enterprise IT security through a range of solutions, products and services focused in IAM Technology. For more information on how we can make a difference in your organization, drop us a request [here](#) or directly contact our IT Security Leaders

Contact Us

RAJESH MITTAL, CTO | ARUN MEHTA, CEO

Avancer Corporation

30 N Main Street

Suite 201 Cranbury

NJ 08512, USA

Tel: +1 (609) 632-1285

Email: info@avancercorp.com

Website: avancercorp.com

© 2025 Avancer Corporation.

All rights reserved. All copyright in this presentation and related works is solely and exclusively owned by Avancer Corporation. This report may not be reproduced, wholly or in part in any material form (including photocopying or storing it in any medium by electronic means and whether or not transiently or incidentally to some other use of this presentation), modified or in any manner communicated to any third party except with the written approval of Avancer Corporation. This report is for information purposes only. While due care has been taken during the compilation of this report to ensure that the information is accurate to the best of Avancer Corporation's knowledge and belief, the content is not to be construed in any manner whatsoever as a substitute for professional advice. Avancer Corporation shall not be liable for any direct or indirect damages that may arise due to any act or omission on the part of the user due to any reliance placed or guidance taken from any portion of this presentation. Secondary information has been taken for the analysis is from the public domain.