SailPoint

eBook

# A how-to guide: Identity security & mitigating risk

## Strong security risk posture requires an identity-first approach

# Preface

Cybercriminals today have more opportunities than ever to infiltrate your business. We've seen an explosion both in cyber threats—including software supply chain attacks, ransomware, advanced persistent threats—and ever-changing international, federal, state, local, and industry-specific regulations intended to help mitigate these risks.

It's a given that data breaches pose a serious risk to the enterprise, with consequences ranging from significant financial loss to reputational damage and downtime. If you have recently suffered a breach, you know first-hand it takes just one compromised identity to potentially cost an enterprise **tens (to even hundreds) of millions of dollars in lost revenue and regulatory fines.**

One thing is clear, as work environments get more complex and continue shifting to the cloud, attackers are increasingly targeting identity as a vector. **With 90% of organizations experiencing an identity-related incident in the last year**[1], identity security is the critical line of defense to mitigate potentially existential threats to your business.

Let's navigate through the crucial role of identity security in mitigating risks, highlighting its significance in reinforcing an organization's defenses against the ever-growing spectrum of cyber threats. Discover how to get started on this journey.

[1] 2023 Trends in Securing Digital Identities, IDSA.

# Automate access controls to reduce risk

In the current digital landscape, organizations are increasingly recognizing the importance of robust identity security measures as a critical component of their overall cyber risk mitigation strategy. Without a unified identity security program and governance measures in place, enterprise security falters.

Central to these efforts is the automation of access controls, which plays a pivotal role in reducing the likelihood of unauthorized access by former employees, third-party non-employees, and cybercriminals, thereby significantly lowering the risk of potential security breaches.

Key access control strategies include:

- **Automating identity access processes:** Streamlining the provisioning and deprovisioning of access rights prevents over-provisioning and eliminates backdoor access, minimizing the chances of unauthorized entry into the system.
- **Enforcing least privilege:** Employing roles and policy logic to ensure that access is granted based on the principle of least privilege provides individuals with only the access necessary to perform their job functions — nothing more, nothing less.
- **Proactive detection and remediation:** Leveraging technology to swiftly identify and correct instances of excess or inappropriate access ensures that access rights remain aligned with organizational policies and user requirements.
- **Resolving policy violations:** Addressing and rectifying policy violations, including separation-of-duty (SoD) conflicts, helps maintain a secure and compliant operational environment.
- **Increasing visibility and control:** Enhancing the ability to monitor and manage access rights for all identities provides organizations with the tools needed to identify potential vulnerabilities before they can be exploited.
- **Continuous monitoring:** With dynamic and constantly evolving cyber risks, implementing the practice of continuous monitoring enables organizations to quickly adapt to new threats and vulnerabilities as they arise.

Adopting these strategies enables organizations to build a stronger, more resilient defense ensuring that digital assets and operations are protected in an increasingly interconnected world.

# 5 steps to mitigating identity risk

Taking a siloed, manual approach to managing and governing access is the greatest threat to your company's hybrid, multiple-application business systems. This is why organizations must put proper access controls in place to protect against a cyber-attack – but where do you begin?

First and foremost, truly shoring up identity security risk requires a fundamentally different way of thinking about cyber security. By leveraging advanced AI-driven identity security, organizations can effectively identify and manage access risks with these five steps:

1. **Stay ahead of risk** by identifying SoD violations and sensitive access risks across ERP systems. Look for on-going risks by user, role, and business processes. Automated and AI-informed identity security solutions give you the visibility and actionable information you need to gain deep visibility and analysis of a user's access history.

2. **Leverage AI (Artificial Intelligence)** to help you detect and prevent toxic access combinations that could lead to fraud or data theft. AI makes it easy to identify risks at scale and monitor behaviors, helping you to build a more resilient organization.

3. **AI can also help you identify and prevent access risk before provisioning** and have the intelligence needed to run "What If" scenarios. Put in place a process to elevate or grant emergency access with automated controls and streamlined reviews.

4. **Automate workstreams** for administrators and reviewers to ensure simplified, accurate periodic access review cycles. Keep your entire team — IT, audit, compliance, security business owners, and board members — continuously informed of threats with reports.

5. Longer term, **make cyber risk mitigation a part of security design**, implementations, and remediation activities.

> **"Identity is critical for Philips to become a digital company and is a center of security. It helps us to grow, to manage the access-related risks and enable the business to delight our customers.**
>
> **Michiel Stoop**
> Business Process Owner and Domain lead for Logical Access Control, Philips

# How SailPoint can help

SailPoint harnesses the power of AI and machine learning to revolutionize identity security, offering a forward-thinking solution to mitigate cyber risk. AI plays a significant role in strengthening security by helping to detect and remediate vulnerabilities – while also improving operational efficiencies. It enables organizations to easily spot risky users and access outliers, helping you be more secure, more resilient, future proof. With SailPoint, you gain a proactive partner with the expertise you need to secure digital identities across large, complex IT environments.

**The advantages of SailPoint's targeted strategy for risk mitigation include:**

- **Detecting and managing access risks:** Pinpoints and manages potential security vulnerabilities early on
- **Preventing fraud and data breaches:** Uses AI to anticipate and block dangerous access combinations
- **Streamlining risk prevention:** Automates the identification and prevention of access risks before they occur
- **Enhancing operational security:** Automates critical security processes, ensuring consistent protection
- **Strengthening compliance posture:** Assists in maintaining compliance, minimizing legal and financial repercussions

To fully understand how SailPoint can secure and streamline your cyber risk mitigation processes, schedule a consultation with a member of the SailPoint team. Experience the difference that unified, AI-driven identity security can make for your organization.

Visit **sailpoint.com/solutions/mitigate-cyber-risk/** to learn more.

SailPoint

**About SailPoint**

SailPoint equips the modern enterprise to effortlessly manage and secure access to applications and data through the lens of identity - at speed and scale. As the category creator, 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 the world's most complex, sophisticated enterprises create a secure technology ecosystem that fuels business transformation.