Be Secure. Be Compliant. Why Access Management Alone is Not Enough
The rapid transformation to the digital world has required major changes to how organizations manage their workforce and how they deliver and govern access to critical applications and data. That workforce is no longer just human users – employees, contractors, and vendors – but also bots or service accounts, each needing their own set of access requirements, restrictions, and locations. Additionally, data and applications spread across cloud, on-premises and hybrid infrastructures are being accessed from anywhere, on a variety of devices.

Today, many organizations are relying on identity tools designed to quickly authenticate and federate access to workers. While these tools often offer basic lifecycle management capabilities to enable workers with 24/7 access, they lack the needed security access controls and policies required to effectively know who can access what and more importantly deliver access based on who should access what. Unknowingly, these organizations are perpetuating their risk exposure by doling out access without governance oversight and enforcement.

These access risks can only be addressed by identity security that puts proper access controls in place to mitigate the risk of toxic access combinations, updates worker access as their job role/status changes, and continuously monitors for access risk.

## Prevent Access Management Blind Spots and Over Provisioning

By implementing an end-to-end identity program that integrates access management capabilities, such as SSO and MFA, with the lifecycle management and governance of identity security, organizations can secure their environment while also benefitting from the efficiency of an integrated strategy.

Liken this to the analogy of an office building and its security setup. To enter the building, you’re required to present ID that proves you are who you say you are in order to be allowed in — this is access management authentication. But letting you in should also mean controlling where you can go and what you can access (which floors, which rooms, which systems), since employees, guests, contractors, and vendors all need...
different levels of access. This is what identity security does: Putting policies in place to properly manage ALL user access, ensuring every worker has the precise amount needed to do their job. No more, no less. Without it, organizations have a false sense of security and may find themselves exposed.

A lifecycle management tool not equipped with identity security controls can quickly lead to over-provisioning (giving access to those who shouldn’t have it) as well as compliance issues (failing to secure and protect critical data). But the biggest danger is what can result if accounts are compromised or are the target of insider or external threats: catastrophic data breaches and costly compliance violations.

"With 84% of organizations experiencing an identity-related breach in the last year, it is vital to ensure access to all your corporate resources is secured, monitored, and governed."

With SailPoint Identity Security, organizations can enable complete end-to-end identity management by unifying access management with AI-driven identity security to effectively discover, manage and secure access to all applications and data across the hybrid IT environment.

The result is an identity-aware organization that is more efficient, secure, and compliant.

An identity-aware infrastructure is essential for today’s enterprise that must proactively address security risks and compliance needs while still effectively meeting the strategic goals of the business.

By leveraging the SailPoint Identity Platform, organizations benefit from complete visibility and intelligence that enables them to automate and accelerate the management of all user identities, entitlements, systems, data, and cloud services – including the ability to manage and secure cloud IaaS environments like AWS and Azure.

Discover the Core of Identity Security

Identity security helps protect businesses from the inherent risk that comes with providing technology access across today’s varied and remote workforce.

At the core of SailPoint Identity Security is AI and machine learning, a foundation that delivers the unmatched intelligence, frictionless automation, and comprehensive integration needed to easily manage access across the largest, most complex cloud enterprises worldwide. Some of the key benefits of SailPoint Identity Security include the ability to:

• Collect the right data on each identity (human and machine) to better assess what they already have access to, how access is being used, and what they should have access to.

• Gain a 360-degree view across all identities and their access, leveraging this intelligence to detect and address access anomalies and reduce access risk.

• Replace manual processes with AI-driven workflows to automatically provision, adjust, and terminate access as workers join, change roles, or leave the organization.

• Use AI and machine learning to monitor your organization as it evolves – enabling you to autonomously adapt access models and policies, such as separation-of-duty (SoD), so your security stays up-to-date and compliant.

• Simplify the administration of your identity program by automating important identity decisions like access requests, role modeling and access certifications.

• Integrate seamlessly with existing business and security systems to infuse identity context into the workflow of the business, creating a frictionless, user-centric experience.

• Understand, report on and dynamically manage critical identity security policies across your ever-evolving enterprise environment.

• Centrally manage and control access to all data, applications, systems and cloud infrastructure—for all identity types.

Build Your Identity Security Strategy

Organizations must consider the big picture and take a more strategic approach to managing their identities and building cyber resilience. An identity program includes much more than just access – which is the tip of the iceberg. What lies beneath is identity context that is gained by an identity security program. This rich context is used to enable smarter identity management by sharing with other critical IT and security resources in the IT ecosystem. When a smart identity approach is used, organizations quickly see it is so much more than application governance and provisioning, lifecycle management,
About SailPoint
SailPoint is the leading provider of identity security for the modern enterprise. Enterprise security starts and ends with identities and their access, yet the ability to manage and secure identities today has moved well beyond human capacity. Using a foundation of artificial intelligence and machine learning, the SailPoint Identity Security Platform delivers the right level of access to the right identities and resources at the right time—matching the scale, velocity, and environmental needs of today’s cloud-oriented enterprise. Our intelligent, autonomous, and integrated solutions put identity security at the core of digital business operations, enabling even the most complex organizations across the globe to build a security foundation capable of defending against today’s most pressing threats.

©2022 SailPoint Technologies, Inc. All rights reserved. SailPoint, the SailPoint logo and all techniques are trademarks or registered trademarks of SailPoint Technologies, Inc. in the U.S. and/or other countries. All other products or services are trademarks of their respective companies.

sailpoint.com