SailPoint

SOLUTION BRIEF

Going Beyond Access Management with Identity Governance

Digital transformation has significantly increased the complexity and scale of managing users and resources within organizations. Enterprise environments are now more open and interconnected than ever, which creates additional levels of complexity and risk. Additionally, business users have driven a dramatic increase in the number of applications and the amount of data organizations need to manage.

Anytime, anywhere access has quickly become less of a luxury and more of an essential necessity. For businesses to compete and move forward, they need to provide an increasing variety of users with access to a constantly expanding amount of digital assets in order for those users to work effectively within the organization.

In today's business world, employees working 24/7 around the world need access in order to be productive. But manual IT processes simply can't keep up with access demands. Therefore, many enterprises have turned to access management to increase productivity and allow efficient access to applications and systems, with single sign-on (SSO) often procured as the first step to solve workforce enablement issues.

However, while access management provides a great deal of convenience and enhanced productivity with authenticated access, it is imperative for organizations to address the other side of the identity coin, which is identity governance. Put simply, identity governance allows organizations to control and govern each user's access after they have gained initial access, so the right resources are accessed at the right times, and for the right reasons. Without identity governance, organizations run the risk of over provisioning access to users; leaving themselves exposed to one of the biggest causes of data breaches – excess permissions, compromised accounts and insider threats.

Security continues to be a high priority for CIOs, with 86% expecting a spending increase.

Barclays, *Technology 2H19 CIO Survey*

77% of organizations do not have full visibility on user access.

SailPoint, *2018 Identity Score Report*

Go Beyond Access Management

Organizations that have already implemented an access management solution must now step further and implement an identity governance framework that will allow them to establish strong access controls and policies. Such a framework adds improved efficiency to their IT staff while addressing security, risk and compliance at its core. The end result? Business users can always have the appropriate level of access to the right applications and sensitive data for their particular job function and all at the right time. That is something access management cannot do alone.

Identity governance provides the visibility and control for organizations to be able to:

See Everything: You cannot protect what you cannot see. Gain insight into 'who is able to access what and how' – across all applications, systems, file shares, and cloud infrastructure, no matter where they are located or what devices they may use.

Govern Everything: Establish access models and policies that help enforce user access real-time. AI and machine learning keep up with the changes within in your organization and provide the information needed to keep models and policies always up-to-date. In addition, intelligent preventive and detective controls help ensure access is within policy at all times.

Empower Everyone: Ensure all users – including employees, partners, suppliers, contractors and even non human access such as RPAs – have the right access at the right time, from any device. 24x7 self-service enables workers to request and receive access to applications and reset passwords, all according to policy and without having to make a single call to the IT helpdesk.

Build a Secure Framework with Identity Governance

IT professionals need to manage and secure increasingly complex hybrid IT environments within extended enterprises. The best solution is a strong identity strategy that securely and effectively authenticates, provisions and governs access to all applications and data across the enterprise. Pairing identity governance with an existing access management solution means organizations increase speed and convenience while delivering control and security.

Identity governance determines what level of access is allowed based on user attributes. This can include their physical location, job role or function, device being used, and more. An example of how this applies is considering a sales person within an organization. They will receive access to the commissioning tool, but should only be allowed to see their commission but not calculate or approve their own commission. That same employee would also be allowed to access their HR system to view their own salary and benefits information, but not process their commissions to payroll. This is know as Separation of Duties (SoD) - a key component of ensuring compliance is maintained with an organization.

The combination of access management and identity governance also establishes end-to-end identity management to securely and effectively authenticate, provision and govern access to all applications and data across the enterprise. A single view of a user's accounts, entitlements and associated risk across all applications transforms technical identity data from multiple systems into easily-understood and business-relevant information. This enables an enterprise to quickly identify risks, spot compliance issues and make the right decisions to strengthen controls.

Identity governance complements and builds upon traditional perimeter- and endpoint-centric security solutions. By defining and governing the access rights of each user within each application, identity goverance helps minimize risk associated with user privileges, including entitlement creep, orphaned or dormant accounts and separation-of-duty policies.

Identity governance also provides role and risk models to automate processes such as:

- provisioning of accounts at onboarding time
- password resets and access requests, eliminating the need for help desk tickets or calls
- identifing risky user access using AI-driven insights and recommendations
- provisioning and de-provisioning of access when a worker's job function changes
- eliminating access violations or over-entitled users
- business manager certification of user entitlements
- account revocation at termination; and compliance and audit reporting

Move Forward Confidently with Identity Governance

For organizations that started their identity journey with access management, convenience now needs to be balanced with control. By integrating identity governance with your existing access management solution, enterprises can automate the governance controls needed to mitigate the risk of a security breach and enforce compliance policies.

SailPoint's identity governance platform enables organizations to gain the confidence of knowing they can provide easy access for users via SSO without sacrificing the visibility and control needed to secure their organization. The end result is an identity aware organization that is more flexible, efficient, secure
and compliant.

SAILPOINT: RETHINK IDENTITY

sailpoint.com

SailPoint, the leader in identity management, delivers an innovative approach to securing access across the enterprise with the SailPoint Predictive Identity™ platform. With SailPoint, enterprises can ensure that everyone and everything has the exact access they need, exactly when they need it, intuitively and automatically. Powered by patented Artificial Intelligence (AI) and Machine Learning (ML) technologies, the SailPoint Predictive Identity™ platform is designed to securely accelerate the business while delivering adaptive security, continuous compliance and improved business efficiency. As an identity pioneer and market leader serving some of the world's most prominent global companies, SailPoint consistently pushes the industry to rethink identity to the benefit of their customers' dynamic business needs.

Stay up-to-date on SailPoint by following us on **Twitter** and **LinkedIn** and by subscribing to the **SailPoint blog**.

© 2020 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.