SailPoint

SOLUTION BRIEF

Addressing the Identity Lifecycle Management Gap

Governing user access to applications and systems across an entire enterprise is a critical component to any security strategy. But oftentimes, it presents one of the greatest challenges security professionals face. As employees, contractors or temporary staff join the company, change jobs or assignments, or eventually leave the company, organizations must constantly update access policies to ensure users only have access to what they need, while removing access they don't need. Of utmost importance is ensuring user productivity and preventing unauthorized users from accessing business-critical systems.

Unfortunately, many organizations today address this challenge with manual processes executed by different people and for different systems. Manual processes, however, are not effective at addressing the issues for a number of reasons:

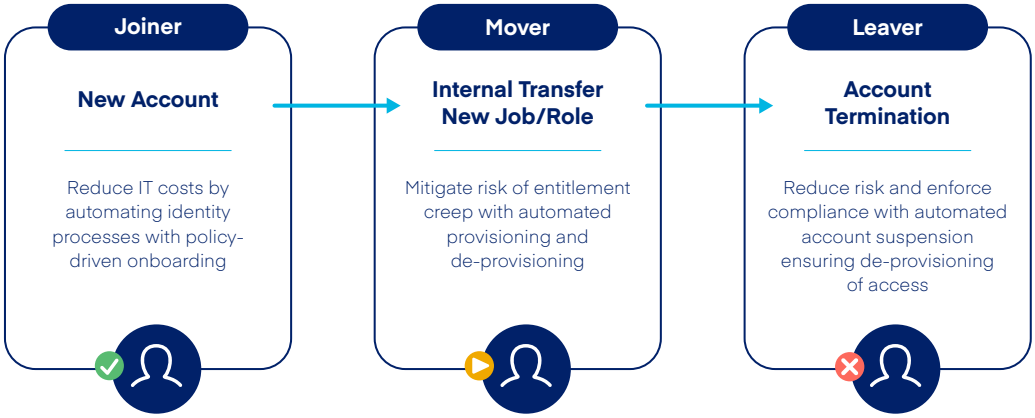
1. Users must wait to get the access they need to do their job.
2. They are more prone to errors.
3. Policies do not cover all access needed and are often applied haphazardly.
4. They are much more costly than automated processes.

The modern era requires that enterprises automate manual IT processes to both increase productivity and reduce costs. Organizations cannot afford to rely on anything less than proven and trusted products when it comes to the critical tasks of managing access and data.

The SailPoint IdentityIQ platform is a next-generation, market-leading solution built on over 10 years' worth of best practices, experience and insights to take your identity program to the next level. IdentityIQ empowers many of the world's largest and most complex enterprises to tackle the most important governance needs they face. With best-of-breed identity governance, IdentityIQ addresses the shortfalls of first-generation solutions and manual provisioning processes while providing a robust, extensible platform to ensure that your needs are met today and well into the future.

IdentityIQ Lifecycle Manager

IdentityIQ performs complete lifecycle management of all identities. When an identity (i.e. individual) joins an organization, IdentityIQ can perform birthright provisioning (based on employee job type/role) to the appropriate applications and systems. If an employee moves roles within the organization, automatic event triggers can generate provisioning and de-provisioning requests to help ensure they have the correct access needed for their new role and any access no longer needed is disabled/removed. When an employee leaves, an automatic workflow can trigger to disable accounts and notify managers to transfer access as needed.



Benefits

Reduce Risk

Define boundaries that govern what people can request and do based on their responsibilities within the organization. Lifecycle Manager ensures users gain access to the right resources for the right reasons. When coupled with IdentityIQ Compliance Manager, organizations can then close the loop by enabling organizations to run regular certification campaigns, access reviews and having a full audit trail from start to finish on individual requests so organizations gain a tighter view on who has access to what, as well as when and where that access was granted.

Reduce IT Helpdesk Burden and Costs

End users can manage their own access requests and alleviate the burden from IT organizations. IdentityIQ offers full self-service access request capability for business users, while IT admins have complete control over what access business users can request. With a flexible workflow, IdentityIQ can be configured to create self-service portals and expedite the process of requesting and granting access for on-premises and cloud applications.

Improve Efficiencies

Automated provisioning manages the business processes of granting, modifying and revoking access throughout a user's lifecycle with an organization, whether that user is an employee, contractor or business partner. Changes to user access can be automatically provisioned via a large library of direct connectors for applications such as Workday and SAP or synchronized with IT service management solutions such as ServiceNow.

Automate Policy Management

By using IdentityIQ Lifecycle Manager in conjunction with IdentityIQ Compliance Manager you can leverage its robust policy engine to define separation of duties (SoD) policies and create other policy definitions that establish controls so you can remain compliant with internal policies and federal regulations. Robust policy definitions can be defined to prevent toxic combinations of access (e.g. Accounts Payable vs. Accounts Receivable: ensure the people that approve the checks can't write the checks in order to reduce the potential for fraud). Policies can also be written in a way to allow managers to create an exception as needed.

> **"I personally like the role-base access control feature in IdentityIQ. It helps you to find out the existing roles in the systems and assign access to those roles. That makes it easy to implement the software in large organizations.**

Privileged Access Management (PAM) Integration

The IdentityIQ PAM Integration Module integrates with existing PAM solutions to improve security and reduce risks, providing complete visibility and consistent controls over privileged accounts. The PAM Module, when used in conjunction with IdentityIQ Lifecycle Manager, allows administrators to manage and govern privileged accounts and their underlying access with IdentityIQ facilitating consistent governance. This allows administrators to certify privileged access alongside traditional access. The PAM module also helps improve productivity by streamlining the lifecycle management of privileged account access according to established business practices. With the introduction of the PAM module, SailPoint leads the development of the industry's first standard for communication between PAM and Identity Governance solutions – allowing easy integration with most PAM solutions in the market today.

Integration with Identity Governance for Files

By governing access to sensitive data, SailPoint SecurityIQ extends the SailPoint identity governance platform to provide a comprehensive approach across all applications and files. SecurityIQ delivers enterprise-level identity governance by discovering where sensitive data resides and applying appropriate access controls, as well as real-time visibility to improve security, mitigate compliance risks and support greater efficiency across on-premises or cloud storage systems.

Reflections from Customers

Mark Routh, Senior Manager of IDM Relations at Western Union: "Our users love it. IdentityIQ is very responsive which makes access requests much quicker." During the migration from the old system to IdentityIQ, they still have some applications that must be managed from the old system. "It's sort of a blessing in disguise that we have to use both systems concurrently, since we can easily tell the gains in efficiencies we'll receive once SailPoint is completely implemented."

Technical Advisor at a risk management software firm: "In an organization where you have hundreds (or in some cases) thousands of users constantly joining, leaving or moving within the company to take on complex projects, IT has the burden to assure that users have the

application access required to do their jobs. Imagine organizations that have multiple roles, job functions, geographies and regulations; accurately granting access and limiting access can be a major undertaking and IdentityIQ helps to manage the complexity of that entire process."

By leveraging IdentityIQ and its open identity platform, organizations are now able to put identity at the center of their security and IT strategy, allowing them to easily see and govern access across the entire enterprise including systems and applications found on-premises and in the cloud.

Learn what IdentityIQ Lifecycle Manager can do for your organization at
www.sailpoint.com/identityiq

SAILPOINT: THE POWER OF IDENTITY™

sailpoint.com

SailPoint, the leader in enterprise identity management, brings the Power of Identity to customers around the world. SailPoint's open identity platform gives organizations the power to enter new markets, scale their workforces, embrace new technologies, innovate faster and compete on a global basis. As both an industry pioneer and market leader in identity governance, SailPoint delivers security, operational efficiency and compliance to enterprises with complex IT environments. SailPoint's customers are among the world's largest companies.

SB1229-1805