eBOOK

Prioritizing Identity within Higher Education Institutions

SailPoint

Competing priorities coupled with limited resources create a conundrum for higher education IT – that is where do you put your finite dollars when it comes identity management? Often, institutions must juggle with whether to prioritize between single sign on (SSO), multifactor authentication (MFA), identity governance, privilege account management (PAM), etc.

Understanding Identity Management

Identity management helps organizations verify, authenticate and authorize user access and there are various solutions to address each aspect. The following provides a quick explanation of each:

Access Management. "Getting in through the front door."
Validating and authenticating users to ensure that they are who they say they are helps to ensure proper entry is gained by each user. This is done using technologies such as:

- **Single Sign-on (SSO)** – A session and user authentication service that permits a user to use one set of login credentials (e.g., name and password) to access multiple applications.
- **Multifactor Authentication (MFA)** – Requirement of more than one source of authentication to confirm a user's identity for a login or other transaction.

Identity Governance. "Controlling what users can access once they've gained entry."
Validating and authenticating users to ensure that they are who they say they are helps to ensure proper entry is gained by each user. This is done using technologies such as:

- **Provisioning** – Automatically grant, modify or revoke access to applications and data as users join, move or leave the organization.
- **Access Certification** – Validate that all types of users have the appropriate access to corporate resources.
- **Self-service Access Request and Password Management** – Enable users to request and receive access to new applications or data, and change or reset passwords on their own.
- **Policy-based Access Controls** – Implement a set of policies that detect and prevent conflicts of interest and potential fraud such as separation-of-duties.

Privileged Access Management (PAM). "Protect the keys to the kingdom."
PAM solutions enable organizations to provide secure privileged access to critical assets and meet compliance requirements by managing and monitoring privileged accounts and access.

- **Privileged Credential Management** – Centralize and isolate the use of privileged accounts to reduce the risk of those credentials being stolen.
- **Secure Privileged Access** – Control who is accessing privileged accounts, log all access and monitor for any suspicious activity.

Starting Your Identity Journey with Identity Governance

Identity governance is a core component of a successful security and compliance program. Its ability to govern all digital identities, including disparate user types found across higher education institutions such as students, faculty, and staff, make this a fundamental component that integrates all aspects of your identity program. IT and security teams can centrally manage access to all apps and data while ensuring access rights are appropriately reviewed and scrubbed, thus creating the foundation for other identity-centric functions such as single sign-on, multi-factor authentication, and privileged access management.

See Rapid Results

Contrary to general belief, an identity governance solution can be rapidly deployed – enabling institutions to quickly on-board critical applications and bring all user access under centralized view and control.

- Based on an institution's use cases and environment, an identity governance solution can be **deployed in as little as three months.**

Protect Against Breach

A data breach can happen anytime. Identity governance significantly reduces the threat surface by ensuring users only have the least access and privilege needed to perform their job successfully. Access is automatically adjusted when users change roles or jobs, minimizing risk and enforcing a least privilege model.

- **Reduce risk from 30% to only 5%. Ultimately, this potentially saves millions of dollars** in remediation costs resulting from a data breach.

Automate Critical Processes

IT teams are overburdened and need to automate to reduce risk and enable growth. Identity governance provides the automation that increases IT efficiency, improves user the access experience and boosts productivity. With the constant onboarding/offboarding of students, faculty and staff in higher education, this has proven critical.

- The time required for access requests to be granted per user **plummets 80% from an average of 60 minutes to 12 minutes.**

- Users wait on average more than 300 minutes throughout the year for help desk to correctly provision or change access. **With automated identity, the wait drops by 200 minutes.**
- Reduce the IT burden by **cutting the number of password-reset calls by 60%.**
- Decrease average cost per password reset call **from $30 down to $12.**

Ensure Continuous Compliance

Various regulations call for establishing demonstrable access controls. Identity governance improves audit performance by enabling organizations to control who has access to what IT resources, who should have access, and how access is used. In addition, identity governance assists in NIST Compliance for research institutions, especially when it comes to addressing government-based research, which requires separation of duties, workflow processes for control and access, and identification of structured & unstructured data whether on-premises or in the cloud.

- By leveraging identity governance, higher education institutions can perform access entitlement reviews in **only 1/3 the time compared to the industry average.**

What Makes SailPoint an Ideal Partner?

SailPoint is purely focused on identity governance and is acknowledged by top industry analysts as an identity leader and innovator. Higher education institutions across the globe build their identity program on SailPoint's Predictive Identity Governance Platform because it is:

Intelligent
Leverage artificial intelligence and machine learning to help multiply your efforts, without multiplying the cost. In addition, spot risky users and suspicious access before it becomes an issue.

Flexible
Deploy identity governance in the cloud or on-premises to efficiently and affordably address the various financial and operational requirements of the higher education institutions.

Automated
Reduce burden on IT by automating critical processes for governing user access rights to applications and data files.

Are you ready to improve identity security, reduce compliance risk, and improve the user experience? With SailPoint you can. Contact SailPoint to request a complimentary business value assessment specifically for your institution.

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.

EB1336-1911