IAM and Privileged Access Foundations for Secure Enterprise ML Platforms

Building robust identity governance for data-intensive machine learning workloads in regulated industries

Speaker Introduction

Neha Asthana

Identity Solutions Architect Abbott

Specializing in enterprise identity governance, privileged access management, and security architecture for regulated healthcare environments. Passionate about building secure foundations for data-intensive platforms and machine learning workloads.

SESSION ROADMAP

What We'll Cover Today

01

Identity Lifecycle Management

Provisioning, deprovisioning, and role synchronization with authoritative sources

02

Access Governance Practices

Certification campaigns, role-based access, and compliance alignment

03

Privileged Access Management

Securing administrative and service accounts in ML environments

04

Integrated IAM Solutions

Centralized governance with platforms like SailPoint IdentityIQ

The IAM Challenge in Modern Enterprises

As organizations scale machine learning platforms and data-intensive workloads, identity and access management becomes increasingly complex. Traditional security approaches struggle to keep pace with:

- Rapidly expanding user populations and service accounts.
- Growing regulatory requirements in healthcare and regulated industries.
- Complex data access patterns across ML pipelines and analytics tools.
- Elevated privileges needed for automation and system administration.

Access Sprawl

Uncontrolled permissions across platforms

Compliance Risk

Audit failures and regulatory gaps

Privileged Exposure

Elevated accounts without proper controls

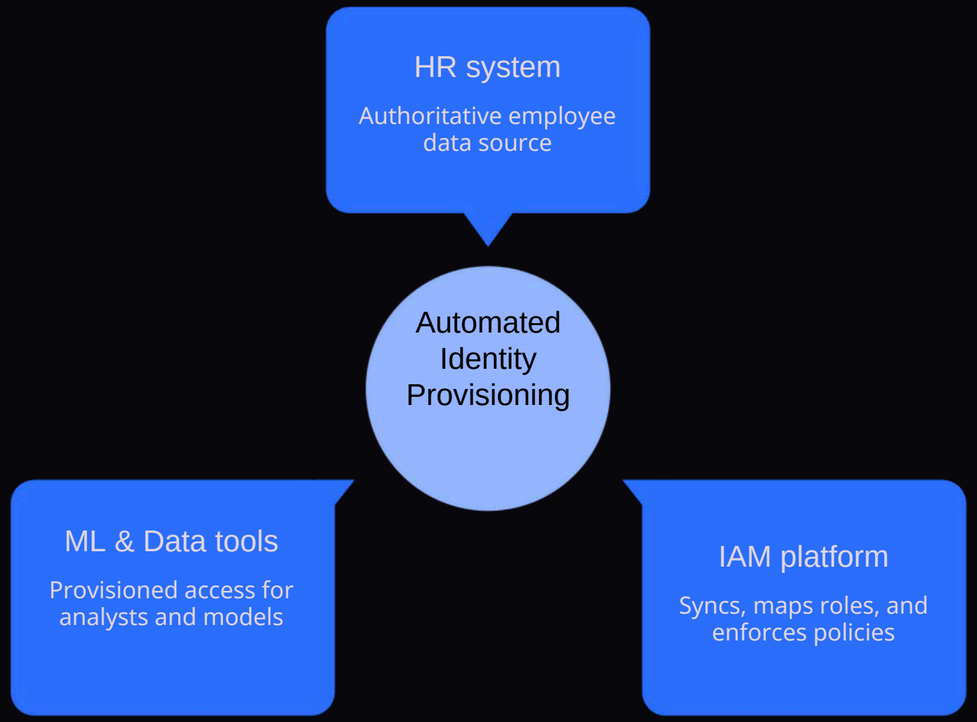
Identity Lifecycle Management

The Foundation of Access Control

Identity lifecycle management ensures that access rights remain accurate and aligned with job responsibilities throughout an employee's tenure. Integration with authoritative sources like HR systems enables automated provisioning when employees gets onboarded, role changes during internal transfers,timely deprovisioning when they leave and rehired if they come back.

This approach minimizes manual intervention, reduces security gaps from orphaned accounts, and ensures consistent enforcement of access policies across all data platforms, analytics tools, and ML infrastructure.

Connecting IAM to Authoritative Sources



Integration with HR systems creates a single source of truth for identity data, enabling real-time synchronization and reducing manual errors.

On-boarding

Automatic account creation and role assignment based on job title and department

Role Changes

Access modifications triggered by transfers, promotions, or responsibility shifts

Off-boarding

Immediate revocation of all access when employment ends or status changes

Rehire

Rehiring an employee who previously left the organization,resulting in reactivation of their digital identity and access.

Access Governance and Certification

Regular Access Reviews

Access certification campaigns are a critical control for identifying and removing excessive or outdated permissions. By requiring managers and data owners to periodically review and validate access rights, organizations can:

- Detect privilege creep and dormant accounts
- Ensure least privilege principles are maintained
- Meet audit and regulatory requirements
- Reduce insider threat risk

Role-Based Access Models

- Role-Based Access Control (RBAC) simplifies permission management by linking access rights to job roles instead of specific individuals.
- This structure enhances organizational consistency, cuts down on administrative tasks, and strengthens compliance through clear, auditable access trails.

Data Scientists

Access to ML platforms, model training environments, and approved datasets

Business Analysts

Read-only access to analytics tools and curated reporting dashboards

Infrastructure Teams

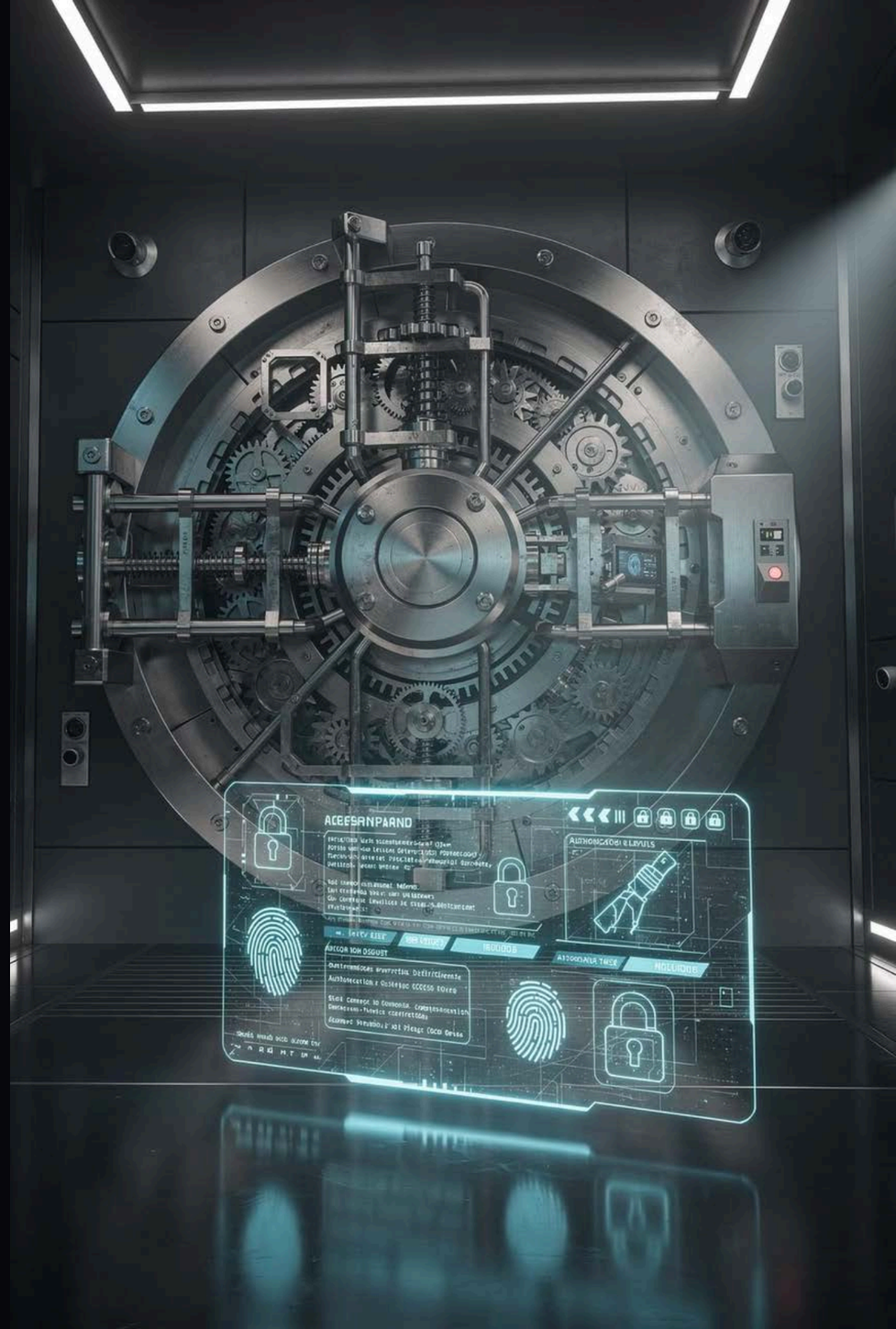
Administrative access to supporting systems with logging and monitoring

Privileged Access Management

Protecting Your Most Critical Accounts

Privileged accounts represent the highest security risk in any enterprise environment. Administrative accounts, service accounts supporting ML pipelines, and application credentials often hold elevated permissions that can expose sensitive models, data, and infrastructure if compromised or misused.

Privileged Access Management provides specialized controls to secure these accounts through credential vaulting, automated rotation, session monitoring, and just-in-time privileged access(short term) with time-bound elevation and automatic revocation.



Core PAM Capabilities for ML Platforms

Credential Vaulting

Store privileged secrets in encrypted vaults, eliminating hard-coded credentials and reducing exposure

Password Rotation

Automatically change privileged credentials on a scheduled basis to limit the window of opportunity for attackers

Session Brokering

Proxy privileged sessions without revealing actual credentials, enabling accountability and forensic review

Activity Monitoring

Record and analyze privileged sessions to detect anomalous behavior and support compliance audits

Why PAM Matters for Machine Learning

Model Protection

Prevent unauthorized access to proprietary algorithms and training data

Pipeline Security

Secure automated workflows and data transformation processes

Dataset Governance

Control who can modify or export sensitive training and validation datasets

- Machine learning environments introduce unique privileged access challenges.
- Service accounts run automated training jobs, CI/CD pipelines deploy models to production, and data engineers manage infrastructure supporting petabytes of information.
- Each of these accounts requires elevated permissions, creating potential attack vectors.
- PAM controls ensure these accounts are properly managed, monitored, and protected against misuse.

Integrated IAM and PAM Solutions

The most effective identity governance programs integrate IAM governance with PAM execution layers to provide unified visibility, policy enforcement and auditability across human and non-human identities.

1

Single Governance View

Manage all identities from one platform

2

Unified Certification

Include privileged accounts in access reviews

3

Consistent Policy

Apply the same security standards everywhere

Meeting Regulatory Requirements

Compliance in Regulated Industries

Healthcare and other regulated industries face strict requirements around data access, audit trails, and identity governance. Well-designed IAM and PAM programs directly support compliance by providing:

- Detailed audit logs showing who accessed what data and when
- Regular attestation that access rights are appropriate and necessary
- Automated controls that enforce separation of duties and least privilege
- Documentation of security controls for regulatory examinations

These capabilities help organizations demonstrate compliance with HIPAA, SOX, GDPR, and other regulatory frameworks.

Key Takeaways

1

Lifecycle Management is Essential

Integration with HR systems ensures accurate provisioning and deprovisioning aligned with job responsibilities

2

Governance Reduces Risk

Regular access certifications and role-based models help identify excessive permissions and compliance gaps

3

PAM Protects Critical Assets

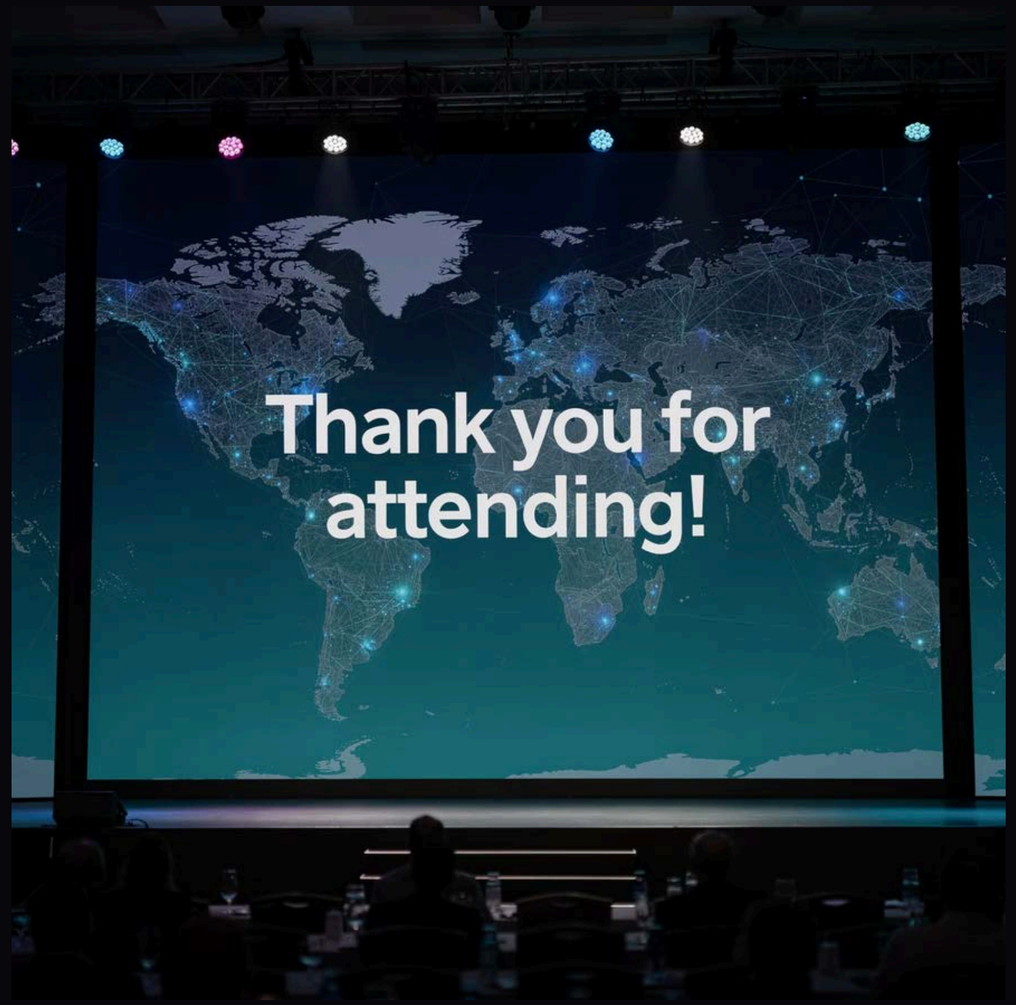
Credential vaulting, rotation, and monitoring secure privileged accounts supporting ML platforms and data pipelines

4

Integration Delivers Value

Unified IAM and PAM platforms provide centralized governance and consistent security controls

Thank You



Neha Asthana
Identity Solutions Architect
Abbott

Thank you for attending this session at Conf42 Machine Learning 2026. I hope these insights help you build stronger identity governance foundations for your enterprise ML platforms.

CONF42 ML 2026