AI-Driven Identity Security:

Automate and secure healthcare access

Hospital and healthcare organizations experiencing rapid digital transformation, continuous cyber attacks, manual processes, and short-staffed IT teams need to reduce their cyber risk while quickly enabling their clinical workforce.

Healthcare is uniquely challenged with securing individuals with one-to-many roles and multiple authoritative sources within complex and dynamic user populations. The typical health system staffed with employees like nurses and physicians and non-employees like affiliate physicians, contract nurses, students, and researchers often need to manage a single users' access with multiple roles and many transfers.

Manually provisioning this access in such a diverse user population could be overwhelming, and error-prone, in a busy and short-staffed healthcare environment and even cause delays to patient care. Additionally, hospital and other healthcare managers that do not have the time or insight to review access properly often bulk-approve access (aka "rubber-stamp") to get the job done while unintentionally increasing their risk.

Why AI matters to healthcare

AI-driven identity security is business essential in the fight against healthcare data breaches. Gone are the days when managing identities and their permissions could be accomplished manually — today, ensuring that each identity has the right level of access can only be accomplished with significant help from artificial intelligence-based technology. AI-driven data intelligence automates the discovery, management, and control of all user access. This allows healthcare organizations to not only make better and faster access decisions, but also to quickly spot and respond to potential threats that could impact patient care and the protection of PHI.

Organizations report the lack of automation and skilled staff as the biggest challenge to managing access.

54%

of organizations are, at best, only somewhat confident in their ability to verify user access privileges.[1]

[1]Source: 2021 Identity and Access Management Report, Cybersecurity Insiders

AI key benefits

- **Speed up clinician/staff onboarding with the right access on Day 1** in a least privileged Zero Trust model.
- **Protect access to PHI data** and reduce the risk of exposing sensitive patient information.
- **Help clinician managers make faster, more accurate access decisions** so they can keep the focus on treating patients.
- **Alleviate certification fatigue** that leads to incorrect access approvals and rubber stamping.
- **Save time and cost by automating** low-risk access approval.
- **Empower C-Level and administrative staff with insights** needed to more cost effectively meet compliance requirements (HIPAA and NIST 405(d), or PIPEDA).

Product overview

Access insights

Help your identity managers and security teams save time and spot potential risks faster through data intelligence. Turn vast amounts of identity data - including user attributes, roles, access history, and entitlements - into actionable insights.

- Provides visibility to all access activity and events, including changes in access and entitlements
- Enables discovery of anomalous access and provides contextual insights for access decision support
- Standardizes the measurement of access anomaly across the organization with Identity Outlier Score and provides out-of-the-box automated workflows to remediate potentially risky access
- Provides near real-time data visualization of access date via the new Access Intelligence Center with persona-based dashboards and reports to track the effectiveness of your identity program and simplify compliance

Access recommendations

Enable healthcare managers to make quick and informed access decisions through machine learning (ML) derived recommendations. Time saving peer group analysis expedites decisioning making so the user can focus on high-risk access. Efficiencies gained alleviate clinical managers' certification fatigue and prevent delays to patient care.

- Helps maintain continuous compliance by enabling more accurate access certification decisions
- Automates low-risk IT tasks and accelerates delivery of access to users
- Offers recommended remediation steps that integrate into certification campaigns
- Provides users with personalized access recommendations

Access modeling

Reduce the need to invest in continuous 3rd party assessments to calculate, establish, and maintain role models. Alleviate short-staffed IT and security team time spent on access tasks with continuous machine learning. Provide Common Access Roles to help speed up new worker onboarding. Build and maintain user roles rapidly with the help of machine learning (ML)-generated insights to continuously monitor and adjust access across your entire organization.

- Automatically calculates, recommends, and establishes common access roles
- Establishes the ability to continuously maintain roles
- Offers wizard-based, guided process to review, and refine roles
- Provides AI suggested roles to quickly develop and evaluate an identity program

How to get started

SailPoint AI-driven Identity Security helps hospital and healthcare organizations accelerate digital transformations while reducing identity-related risk. Learn how to proactively engage clinical managers to identify and manage risky access and help security professionals intelligently create and maintain access models in today's dynamic IT environment. Visit **sailpoint.com/healthcare** and request a demo to learn more.

SailPoint

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.