# Healthcare Security Capabilities
## Identity Cloud

### Forging Ahead to the Cloud

To govern wisely and well, forward-thinking healthcare organizations have been looking at how they could improve efficiency and evolve the business, and shore up their resilience as an organization. Their input is reflected in key innovations like:

- Identity management for complex access models
- Automated certification as suspicious access activity is detected
- Separation-of-duties controls to prevent conflicts of interest

### Supercharging SaaS-Based Identity Security

SailPoint IdentityNow delivers identity management and governance from the cloud. This SaaS identity platform uses policies, access controls, and advanced technologies to make sure healthcare personnel see and touch only what data and applications they need to do their job. With integrated AI and machine learning capabilities to identify identity management tasks, healthcare entities can reduce the likelihood of a data breach from 30% to 5%.[1] These predictive identity capabilities include:

**Access Insights.** Each identity has a history, and data analytics provide richer context around it. When was an identity onboarded? Who approved it? What has changed about their role and access over the years? Insights like these can reveal potential risks like abnormal entitlements and dormant or orphaned accounts. They also help the organization respond to compliance and audit mandates.

**Access Modeling.** As healthcare continues to transform, the user population has become more cross-functional and fluid. One implication is that the old ways of maintaining access permissions in a spreadsheet and reviewing them periodically are no longer scalable for modern hospitals. To reduce human error, automatic access modeling lets the identity management platform suggest what the appropriate access currently should be, based on what users in similar roles have.

[1] Andras Cser and Merritt Maxim, "Making The Business Case For Identity And Access Management," Forrester, October 7, 2019.

**Recommendations.** Access approvals and certifications need to keep pace with internal compliance shifts as well as external policy changes. A recommendation engine speeds up the process by automatically provisioning low-risk access. Meanwhile, decisions around higher-risk access become easier with AI-generated recommendations based on peer group analysis, identity attributes, and historical access activity.

**Cloud Governance.** Healthcare has moved to the cloud as organizations seek more cost-effective ways to store and retrieve exponentially expanding data, especially as onsite data storage becomes increasingly expensive and vulnerable to cyberattacks. Using cognitive processing, the identity management platform can discover and protect access to all the other cloud platforms and resources in use across the organization. Healthcare entities can see who has access across their multi-cloud infrastructure, enforce access policies, and monitor accounts for suspicious activity in real time.

**To learn more about identity security and the solutions SailPoint can deliver, please visit https://www.sailpoint.com/identity-for/healthcare or contact us.**

**ABOUT SAILPOINT**

SailPoint is the leader in identity security for the cloud enterprise. We're committed to protecting businesses from the inherent risk that comes with providing technology access across today's diverse and remote workforce. Our identity security solutions secure and enable thousands of companies worldwide, giving our customers unmatched visibility into the entirety of their digital workforce, and ensuring that each worker has the right access to do their job – no more, no less. With SailPoint as foundational to the security of their business, our customers can provision access with confidence, protect business assets at scale and ensure compliance with certainty.