



Six essential identity security capabilities for healthcare organizations



Healthcare organizations use identity security to keep sensitive data safe by ensuring users only have access to what they need. At the same time, the provisioning of user access, along with the implementation of lifecycle management best practices, is crucial for achieving compliance and reducing cyber risk. With the introduction of cloud-based identity security solutions, organizations can utilize multiple essential and innovative capabilities to ensure security and efficiency.



Six essential capabilities to look for should include:

01

Unified identity security platform which leverages time-saving artificial intelligence (AI). A unified approach, and scalable architecture is essential for healthcare organizations today and into the future. Features such as data modeling, machine learning, event-driven orchestration, clear reporting, actionable insights, enterprise-wide connectivity, and extensibility into external systems strengthen access controls with unique insights and governance simplification.

Centralized visibility because you can't manage what you can't see. For an effective identity security outcome, having all identities and the access they should have in one place is important. Maintaining one set of this information that everyone uses reduces the complexities and confusion when determining if access is needed and setting access controls. This reduces time and expense and increases confidence in security posture.

02

03

Reducing non-employee risk by managing identities beyond employees. Contractors, affiliate physicians, travel and flex nurses, as well as medical students make up a large percentage of their workforce. A unified identity security solution offers automation and constant visibility while ensuring secure access control and reporting.

Connectivity/Integration among applications and data sources. It's not uncommon for larger health systems to have hundreds of applications in use including EHR and EMR. An identity governance platform should extend core identity capabilities to the critical applications, resources, and systems that organizes use every day including clinical care applications and medical record systems.

04

05

User management and access certification through AI-driven insights to ascertain what kind of access users need, user identities, access privileges, and entitlements across cloud-based applications and services. This ensures that only authorized individuals have access to sensitive patient data, minimizing the risk of data breaches. Built-in reporting reduces the cost of compliance by automatically generating audit trails and access reports on all key applications and data.

Detection and response to suspicious or anomalous behavior in the cloud environment, including unauthorized access attempts and unusual access patterns. Real-time alerts and notifications are triggered when suspicious activities are detected, enabling healthcare organizations to take immediate action.

06

In the United States, KPMG serves over

50%
of the top 45 pediatric hospitals

~60%
of the top 150 healthcare systems

70%
of academic medical centers



KPMG and SailPoint: Delivering trust and reliability in the digital era to healthcare providers

SailPoint helps the world's most complex, sophisticated enterprises create a secure technology ecosystem that fuels business transformation. KPMG helps large, complex organizations with a wide variety of IAM services spanning assessment, strategy, implementation, and managed services.

Together we can prepare your healthcare organization for the future state.

KPMG is a top implementation alliance partner of SailPoint solutions with a focus on achieving business goals through technology enablement.

As a SailPoint Delivery Admiral since 2018, KPMG has delivered over 200 engagements including some of the largest and most complex deployments of IdentityIQ and Identity Security Cloud (ISC).



The KPMG+SailPoint implementation methodology is based on extensive experience delivering identity projects, often shaping healthcare industry-specific leading practices. We continuously refine and augment this approach as we develop better and faster ways to enable our client's identity journey.

Through investments in building an extensive catalog of intellectual property and implementation accelerators, we can tackle and accelerate the delivery of highly complex IAM programs. Ultimately designing identity programs that meet our clients' business needs today and prepares them for the future, saving time and money, and advancing long-term ROI.

Contact us

Doug LaGore
Principal, Advisory
T: 313-230-3000
E: dlagore@kpmg.com

Adam White
Managing Director
T: 949-344-5674
E: arwhite@kpmg.com

Debbie Patterson
Sr. Alliance Director
T: 512-423-6150
E: deborahpatterson@kpmg.com



SailPoint equips the modern enterprise to readily manage and secure access to applications and data through the lens of identity—at speed and scale. As the category creator, SailPoint delivers a unified, intelligent, extensible platform built to defend against today's dynamic, identity-centric cyber threats while enhancing productivity and efficiency.

KPMG Cyber Security Services

Recognized 'Worldwide Leader' in the IDC MarketScape: Worldwide Systems Integrators/Consultancies for Cybersecurity Consulting Services 2024 Vendor Assessment

Recognized 'Leader' in the IDC MarketScape: Cybersecurity Risk Management Services Vendor Assessment 2023

Named 2023 'Pacesetter' in Cybersecurity categories of Client Enablement, Value Proposition, and Service Delivery by ALM Intelligence

Ranked 'First Choice' in Financial Risk; Client Advocacy; and Third Party Assurance in Risk in Source Global Research study Perceptions of Risk Firms in 2023

Learn about us:



[kpmg.com](https://www.kpmg.com)

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.

© 2024 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization. USCS016460-1B