

# Empowering European Healthcare with Enterprise Access Management



Silvia Piai  
Research Director,  
IDC Health Insights



Mark Child  
Associate Research Director,  
European Security



# New Compliance Requirements Are Raising the Bar for Secure Access in European Healthcare

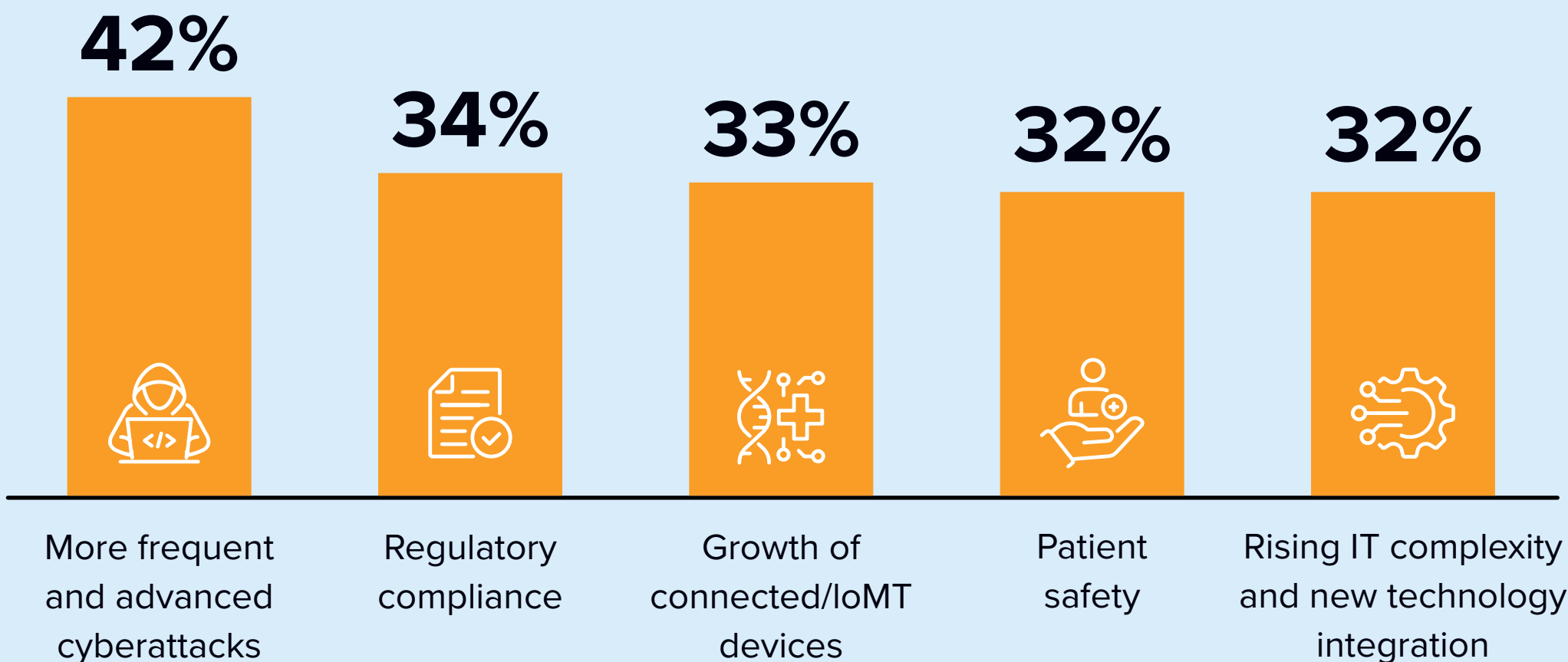
European healthcare providers are navigating an increasingly complex and regulated landscape, shaped by rising cyberthreats and the rapid digitalisation of care.

New and more stringent EU and national laws are accelerating the need for robust cybersecurity strategies, with enterprise access management (EAM) emerging as a critical component of healthcare security and data protection frameworks.

As IT environments expand and interconnected medical technologies proliferate, investing in EAM solutions, backed by strong organisational readiness, has become essential.

These investments not only ensure ongoing regulatory compliance but also help safeguard operational continuity and uphold patient safety and trust in an evolving threat landscape.

## Why Cybersecurity Is a Priority in European Healthcare: Top 5 Drivers (1)



## European key data protection and cybersecurity frameworks are requiring robust EAM capabilities.

Regulation	Core EAM Requirements
GDPR	The GDPR mandates access management as a key data protection requirement, enforcing <b>strong access controls, authentication mechanisms, including multi-factor authentication (MFA) and biometrics, and comprehensive activity logs</b> to ensure traceability and accountability, in line with “data protection by design and by default” principles.
NIS2 Directive*	It mandates a leading role for access management .Key requirements include <b>MFA, single sign-on (SSO), continuous authentication, role-based access and identity controls</b> . It also mandates regular and sometimes unannounced audits to ensure ongoing compliance.
EHDS	The EHDS regulation mandates <b>certified EHR systems for robust access logging, secure authentication, and patient-controlled access</b> .

# Overcoming Cybersecurity and Access Management Challenges in European Healthcare

With healthcare a prime target for rising cyber threats, investing in comprehensive cybersecurity, including EAM solutions, is essential to reduce risk and build resilience. Yet, healthcare organisations face several key challenges:



### Legacy Systems and Integration Complexity

Many still rely on outdated systems that lack modern security features, which makes integration with new EAM solutions difficult and operationally burdensome.



### Workforce & Resource Constraints

Budgetary constraints and staff shortages, including lack of cybersecurity specialists such as the chief information security officer (CISO), significantly hinder efforts to implement and maintain modern cybersecurity and EAM solutions.

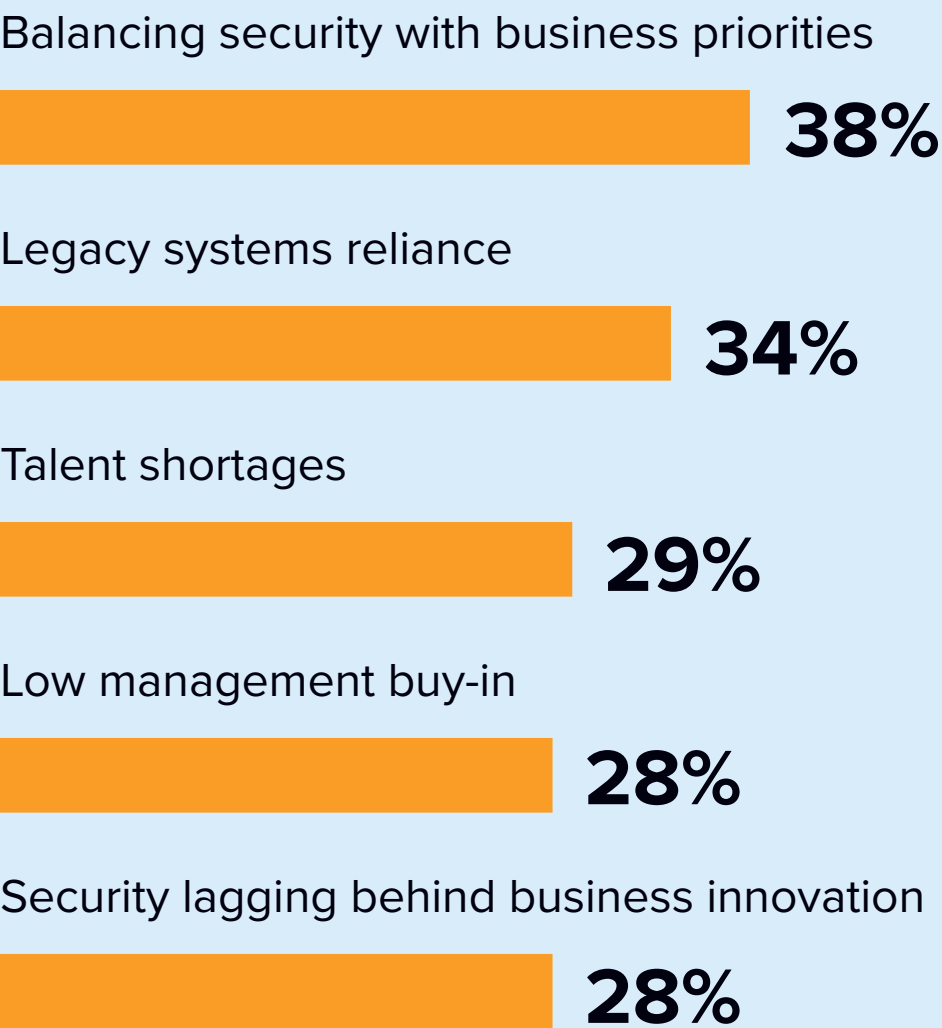


### Balancing Clinical Needs with Security

EAM must protect sensitive data while allowing seamless clinical access to critical devices, applications, and other resources. Striking the right balance between security and usability is essential to avoid disruptions and drive adoption.

These challenges underscore the need for more than technical solutions. They require **cultural change, workforce upskilling, and alignment with evolving clinical workflows and regulatory demands.**

### Key Barriers to Enhancing Cybersecurity Posture (1)



### Biggest IAM & Identity Security Challenges (2)



# Unprepared and Under Attack: The Cost of Cyber Insecurity in European Healthcare



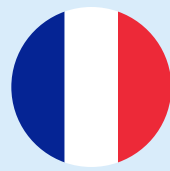
In May 2025, University College London Hospitals and University Hospital Southampton were hit by a cyberattack exploiting a known mobile device management vulnerability, prompting a joint investigation by NHS England and the NCSC. (5)



In 2024, the Dutch Data Protection Authority confirmed that health and social care remained the top sector for reported data breaches. The sector faced a sharp rise in cyberattacks, particularly ransomware. Most breach reports involved unauthorised access to sensitive personal and medical data, underscoring persistent vulnerabilities in healthcare cybersecurity. (1)



A landmark 2024 ruling by the Belgian Data Protection Authority fined a major hospital €200,000 after a ransomware attack disrupted emergency services for days and compromised over 300,000 patient records. The breach exposed gaps in risk assessment, centralised access controls, and continuous monitoring, highlighting critical weaknesses in the hospital's cybersecurity measures. (3)



In November 2024, a hacker gained unauthorised access to the electronic patient record systems of multiple French hospitals, affecting at least 750,000 patient records. The breach was traced to compromised credentials, with data later found for sale online. (2)



The 2024 breach at the Spanish Society of Medical Oncology compromised the health data of 2,622 cancer patients and led to a €42,000 fine. The incident exposed significant vulnerabilities in data management with third-party suppliers, underscoring urgent needs for stricter measures to protect sensitive patient information. (4)

High-profile cyber breaches across Europe have had real world consequences — disrupting care, damaging reputations, and triggering legal and financial fallout.

- Risks extend across workstations, mobile and connected devices, and critical health systems.
- Healthcare's interconnected nature amplifies these threats, allowing attacks to spread rapidly across the ecosystem.
- Non-compliance can lead to regulatory fines, reputational damage, and exclusion from key digital health initiatives.



Nevertheless, more than **30%** of European healthcare organisations have yet to start working on NIS2 compliance, even though the directive applies to them. (6)

Robust access management is a critical component of cybersecurity strategies to limit attack spread, protect patient data, and ensure operational resilience in this high-risk environment.

Datalekkenrapportage 2024 <https://www.autoriteitpersoonsgegevens.nl/documenten/rapportage-datalekken-2024>  
<https://www.lefigaro.fr/secteur/high-tech/cyberattaque-les-donnees-de-750-000-patients-derobees-apres-le-piratage-d-un-etablissement-de-sante-francilien-20241121>  
<https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n0-166-2024.pdf>  
<https://www.aepd.es/documento/ps-00515-2024.pdf>  
<https://www.digitalhealth.net/2025/05/two-nhs-trusts-affected-by-cyber-attack-on-mobile-phone-software/>  
IDC Survey 2025: EMEA Security Tech and Strategies 2025, European Healthcare Respondents n 65



# Meeting Compliance Demands While Building Risk Resilience with EAM



73%

of European healthcare organisations increased their identity and access management budgets in 2025. (1)

Regulatory pressure remains the top driver for access management adoption in healthcare, reflecting the sector’s need to meet increasingly stringent security and compliance standards. As frameworks like NIS2 raise the bar, organisations are prioritising solutions that not only ensure compliance but also foster long-term resilience.

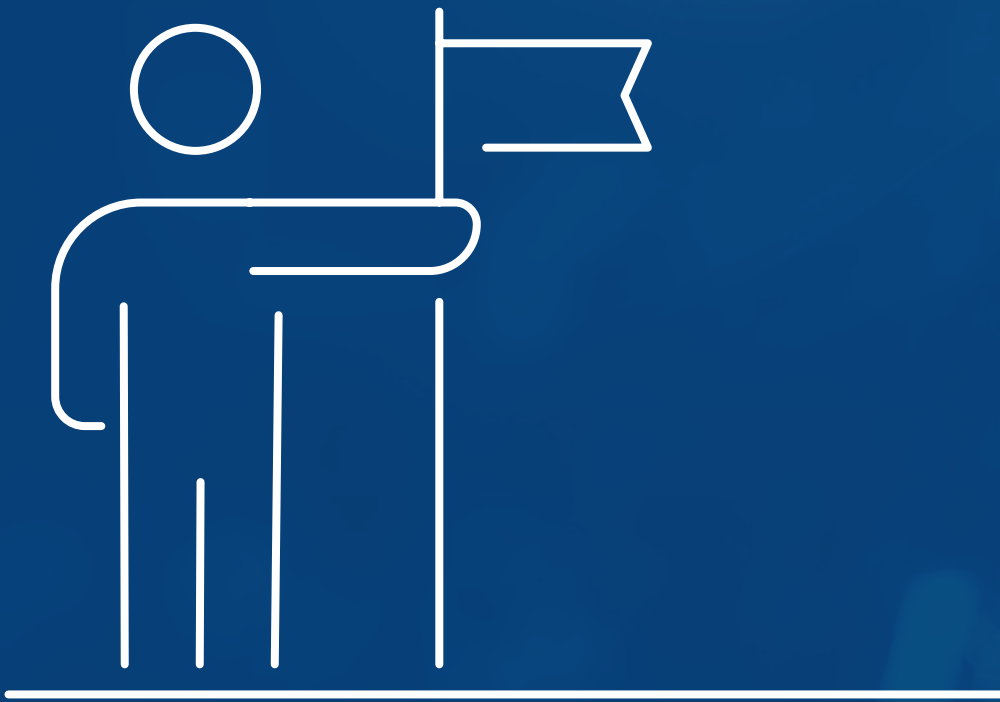
Enterprise access management is emerging as a critical enabler of proactive risk management. With automated controls, analytics, and audit trails, healthcare providers gain **real-time visibility** into access activity, **streamline audits**, and enforce **consistent policies** across complex healthcare environments. These capabilities reduce the risk of fines, data breaches, and reputational harm, while scaling effectively with organisational growth and change.

Key Drivers of Identity and Access Management Strategies in European Healthcare (1)





# Why EAM Matters: Aligning with Top Healthcare Business Priorities



Healthcare providers that strategically invest in enterprise access management position themselves as secure, efficient, and patient-focused leaders in digital care.

## Top European Healthcare Business Priorities



34%

Improving quality of care and safety



34%

Improving operational efficiency



41%

Innovating care delivery models



# EAM: Enhancing Efficiency, Enabling Digital Health, and Evolving Care Delivery

EAM delivers measurable operational efficiencies by streamlining IT processes and enhancing clinical workflows, while serving as a key enabler of digital healthcare services and care delivery transformation.



## Enhancing IT Departments Efficiency

Access management solutions automate user lifecycle processes, simplify access requests, and centralise control, reducing manual workload and helpdesk dependency.

This leads to lower support costs, fewer errors, and faster onboarding/offboarding, which frees up IT teams to focus on higher value initiatives.



## Improving Health Users Productivity and Experiences

SSO and passwordless authentication features reduce login friction and password fatigue across personal and shared endpoints (such as workstations, mobile devices, and medical equipment), allowing clinicians and nurses to access patient data and clinical systems quickly and securely.

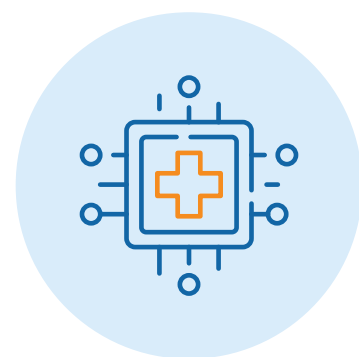
These capabilities significantly speed up login times, streamline workflow integration, and allow clinicians to focus more on patient care, rather than login issues or support calls.



## Powering Digital Health Engagement

Robust EAM strengthens security, transparency, and accountability by enforcing strong passwords and MFA, ensuring each clinician accesses patient data through their own account, and improving documentation of data access, eliminating the risks of generic or shared accounts.

It builds trust among clinicians and patients, encourages engagement with digital health services, and reinforces long-term care relationships, accelerating the shift to data-driven, digitally enabled healthcare.



## Supporting the Shift Toward Integrated Care

As healthcare models evolve from hospital-centric to community and home-based care, EAM ensures secure access across varied devices, locations, and user roles.

As staff work across multiple organisations, federated EAM models are emerging to enable seamless and consistent access, while maintaining control and compliance, laying the foundation for next-generation integrated care models.

# EAM Meets eIDAS 2.0: Unlocking Secure, Interoperable, Patient-Centric Digital Health


**eIDAS 2.0 marks a major shift in how digital identity and trust services are managed across Europe.**

With healthcare identified as a priority sector under eIDAS 2.0, European healthcare must adapt its access management strategies to align with this new framework, unlocking secure, interoperable, and patient-centric services.

## Key Implications for Healthcare EAM Strategies:


**Unified Digital Identity**

Integration of EUDI wallets, ensuring consistent, compliant authentication in all settings.




**Dynamic Consent Management**

Seamless integration with patient consent dashboards, enabling access to records based on real-time authorisations.



**High Assurance and Auditability**

MFA, biometrics, and device trust to meet “high” level of assurance, with detailed, regulatory-ready access logs.



**Vendor Selection and Interoperability**

EAM technologies, such as SSO, MFA, and session management, from vendors supporting national/ EU identity schemes and standards.




**EUDI Wallets Integration**

Healthcare staff and patients will use European Digital Identity (EUDI) wallets to verify credentials, access systems, and control data across borders and institutions.

**Cross-Border, Legally Assured Services**

eIDAS 2.0 will support legally assured, high-trust interactions for cross-border care, telemedicine, and second-opinion consultations. This will enable patient-centric, interoperable services throughout the EU.



**Aligning EAM with eIDAS 2.0 will empower providers to unlock secure cross-border digital services and accelerate the shift toward integrated, patient-centred care at the local level.**



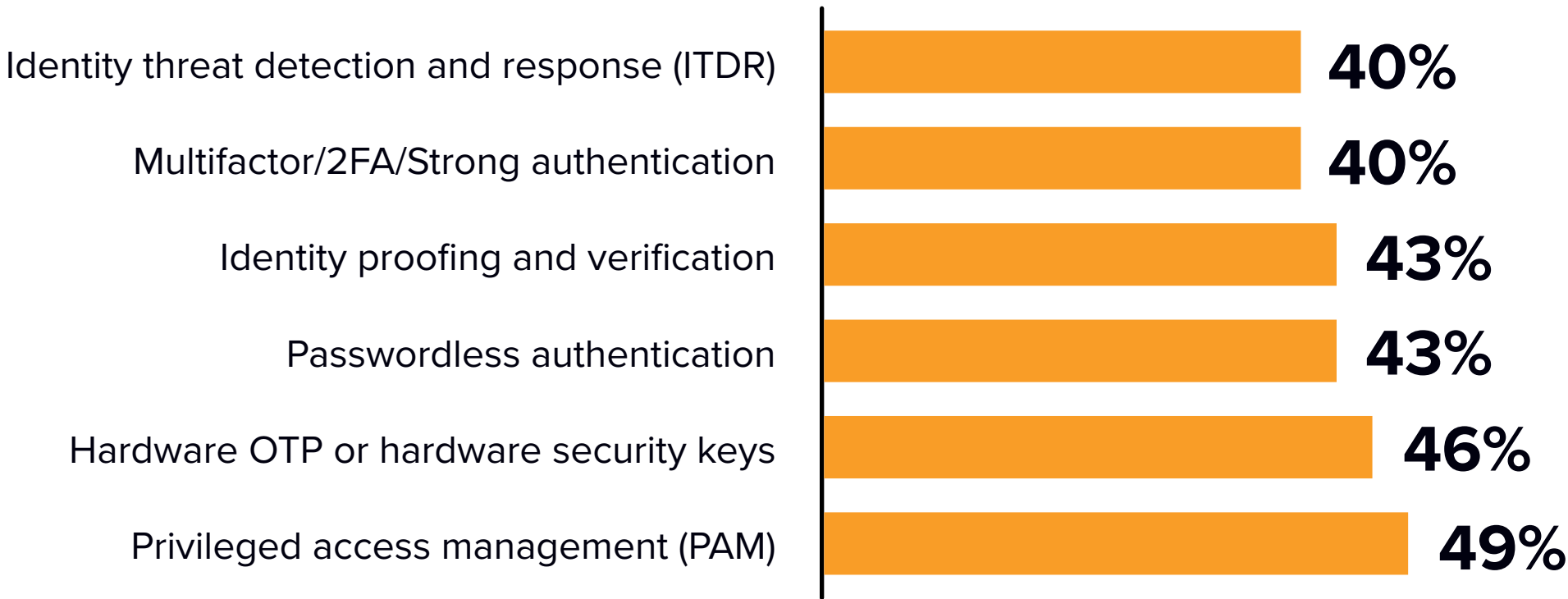
# The Evolution of EAM Investments in Healthcare: Innovation in Action

Healthcare organisations’ EAM strategies are rapidly advancing to address the key challenge of managing both heightened security requirements and clinical usability.

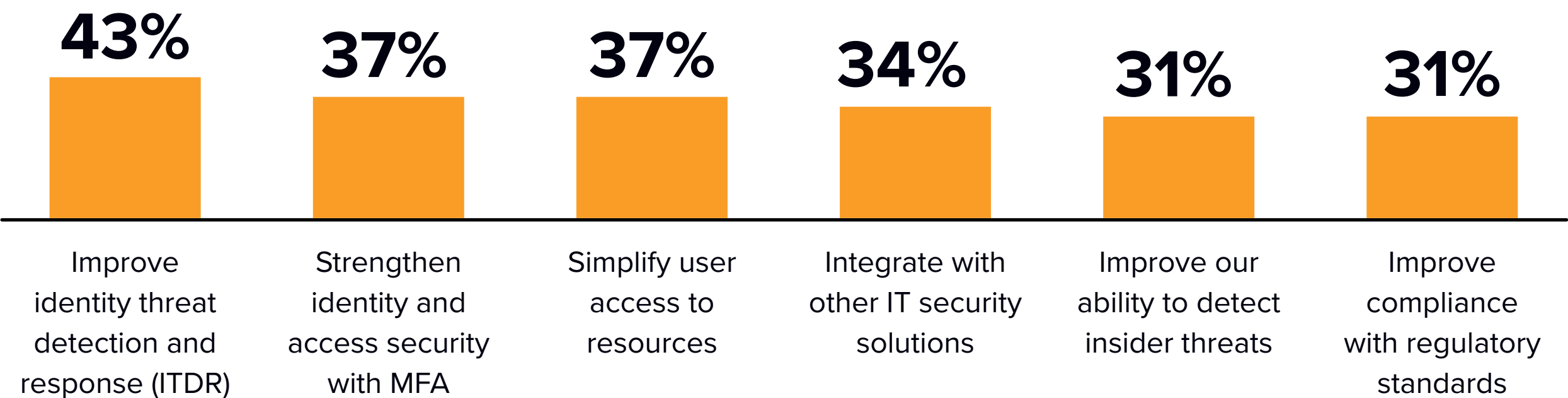
European healthcare providers’ EAM investments now go beyond fortifying SSO, also focusing on enhancing identity threat detection and strengthening MFA.

Leading solutions enable adaptive “step-up” authentication for sensitive workflows and apply privileged access controls ensuring only authorised users access critical information and systems. The industry is moving toward a passwordless future, driven by the adoption of biometrics and device trust to improve both security and the clinician experience.

## Identity and Access Management: Key Areas of Investment (1)

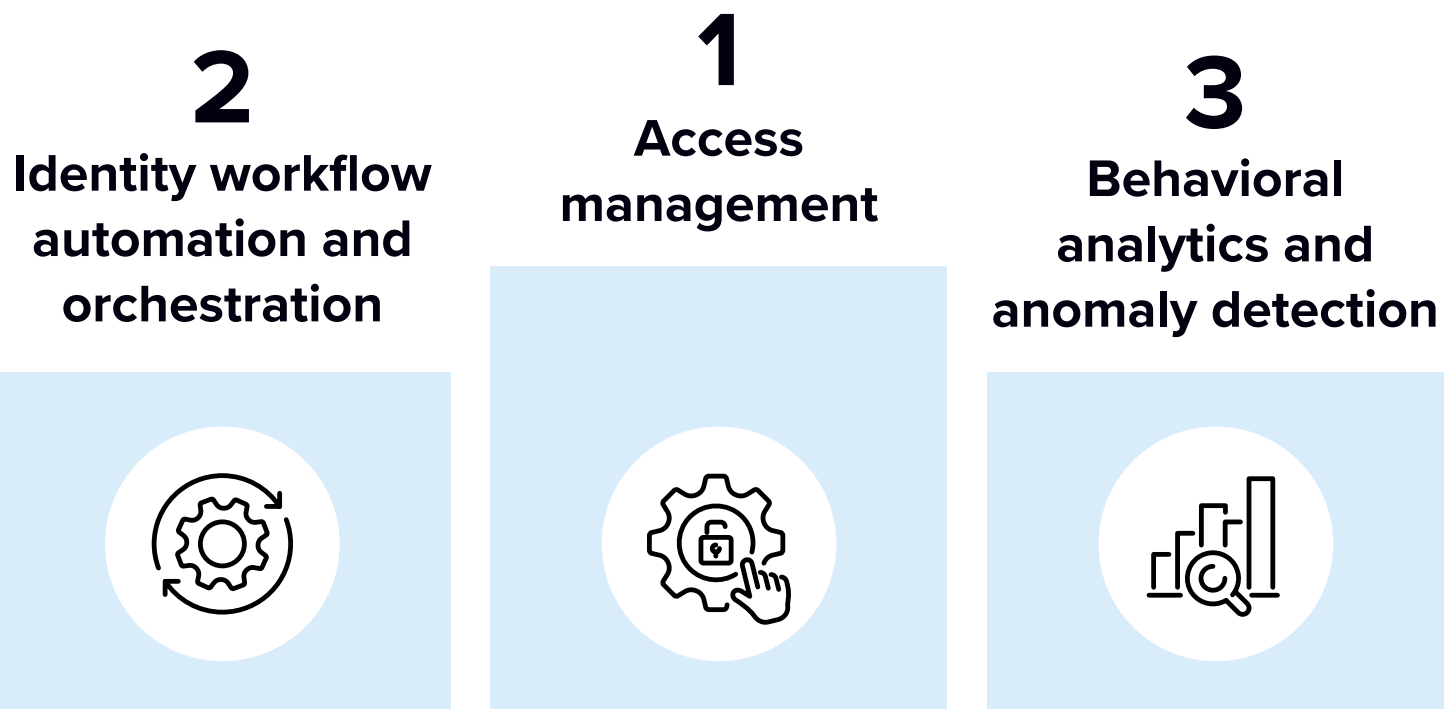


## Healthcare Organisations’ Plans to Improve Identity and Access Management (1)



Modern EAM platforms integrate with national and regional health systems, ensuring interoperability and readiness for evolving regulatory and operational demands. New capabilities such as adaptive authentication, AI-driven monitoring, and robust audit trails help strike a balance between regulatory compliance (including eIDAS requirements) and seamless workflows.

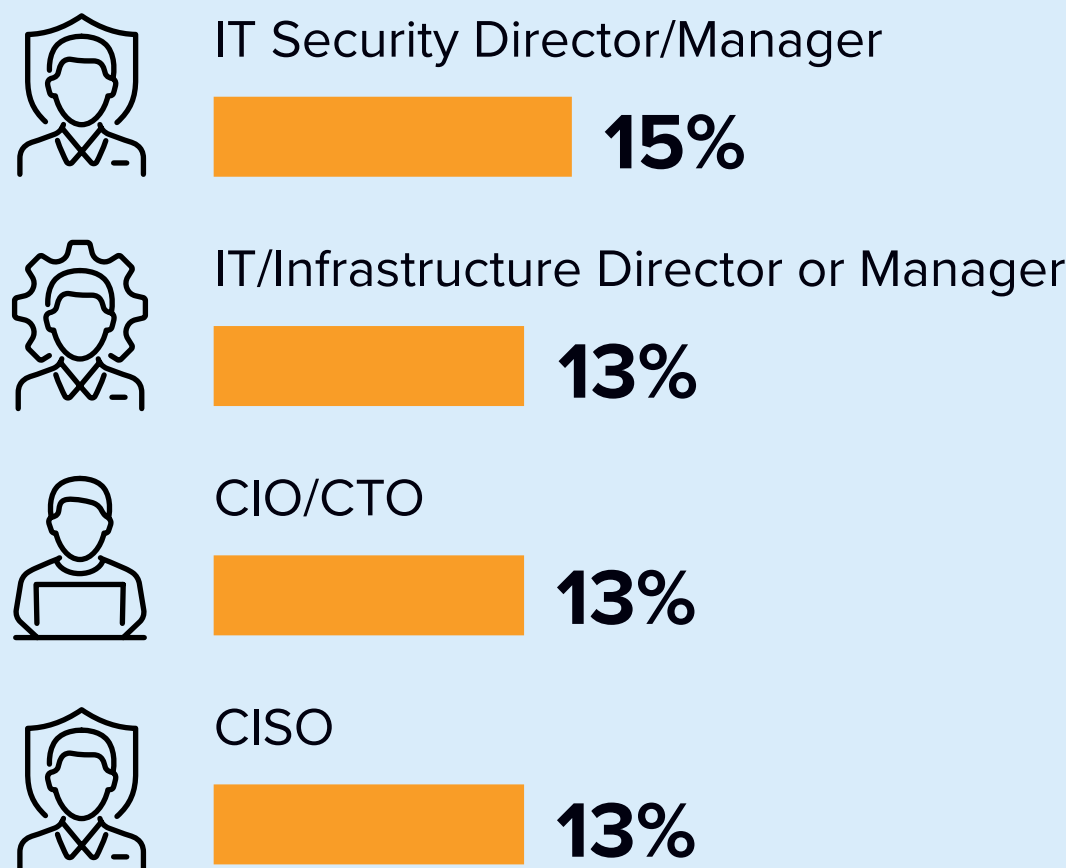
## Top 3 AI Use Cases for Identity and Access Management (2)



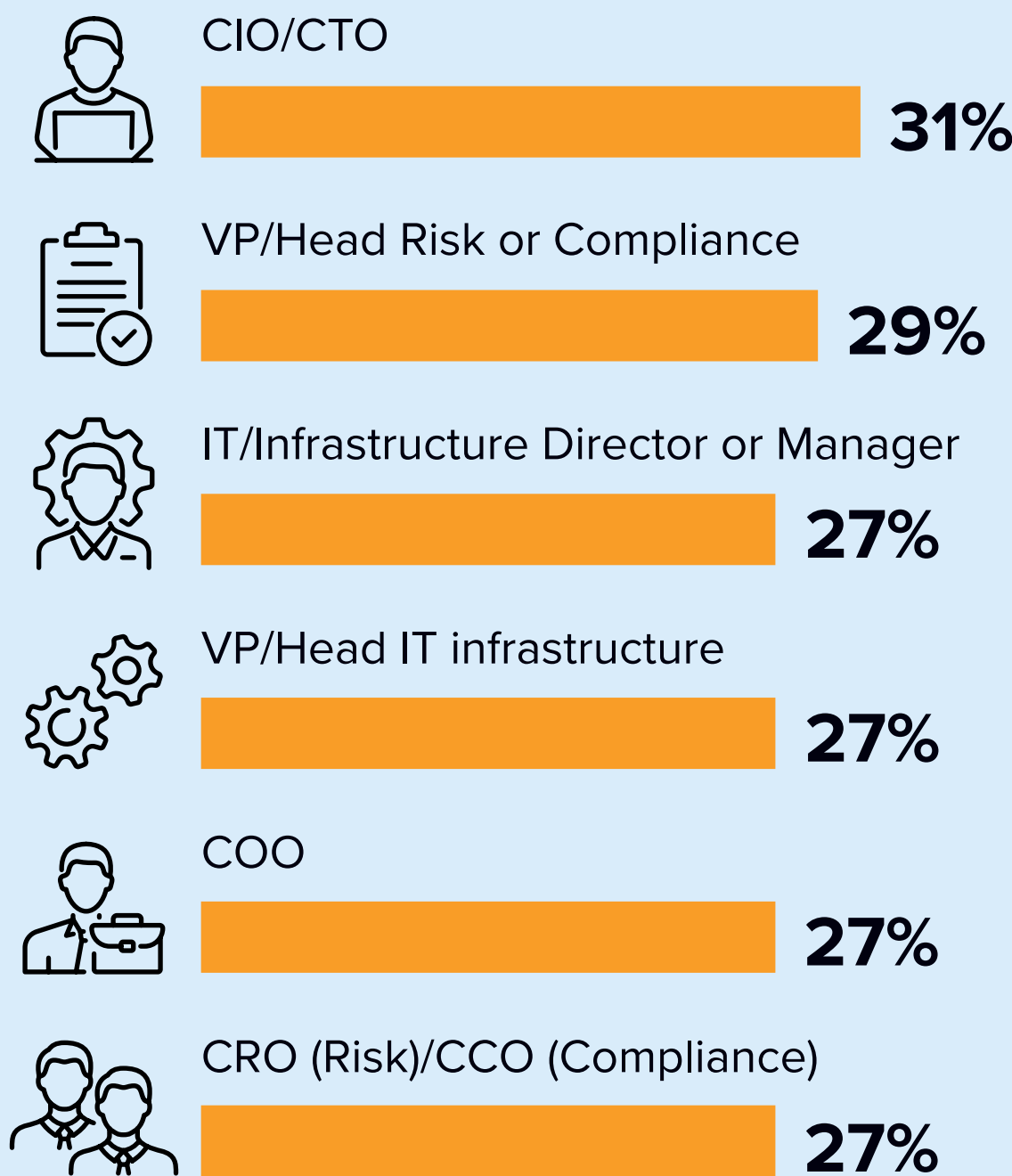


# Transforming Access Management into a Cross-Functional Healthcare Priority

## Primary Decision-Makers for Identity and Access Management Strategy (1)



## Other Roles with Significant Input into Identity and Access Management Decisions (1)



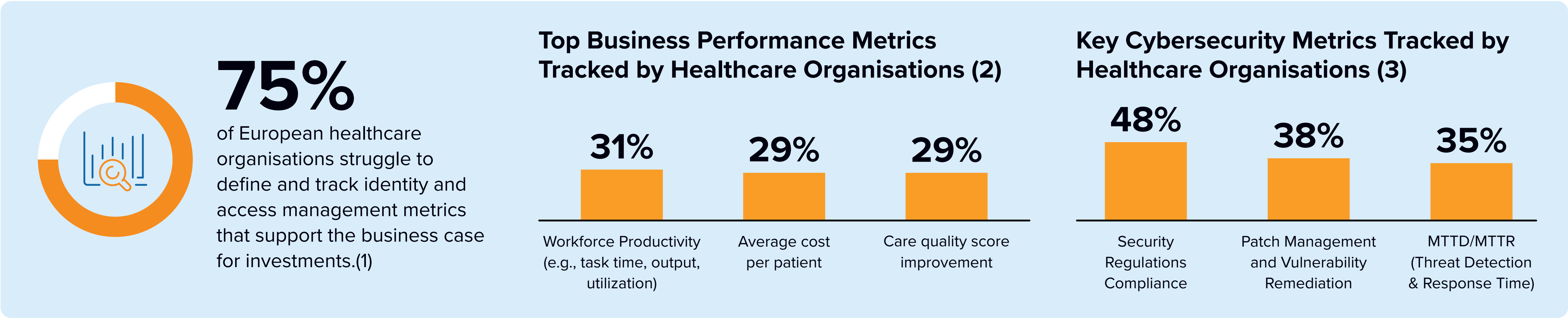
Identity and access management strategies in healthcare are predominantly shaped by IT leadership, reflecting the close link between cybersecurity and technical operations. While this ensures technical resilience, the growing complexity of healthcare delivery calls for broader strategic alignment.

As digital tools are increasingly integrated into clinical, administrative, and patient-facing workflows, access management has evolved from a back-end function into a critical enabler of transformation. Yet the influence of operational and compliance leaders in decision-making remains limited.

Unlocking the full potential of access management requires engaging staff across departments, including clinicians, to align strategies with workflows, operational needs, and the shift toward patient-centred, digitally enabled care.



# Building the Business Case: EAM as a Value Driver



Healthcare management evaluates organisational performance using KPIs that span workforce productivity, patient safety, quality of care, and, increasingly, cultural, accessibility, and environmental considerations. Cybersecurity teams, in turn, focus on compliance, threat detection, and vulnerability management. Enterprise access management bridges these domains, influencing outcomes across clinical, operational, and security objectives.

IT leaders have a pivotal role to play in championing EAM investments as drivers of organisational success. Robust access management not only reduces security risks and financial exposure but also streamlines workflows, reinforces clinical excellence, and builds enduring patient trust.

By framing **EAM’s value around the priorities of executive and organisational leaders**, IT leaders can foster sustainable buy-in and cross-functional collaboration.



Stakeholders	Impact
Executive Officers	Boost staff productivity Reduce cost of access-related support and compliance Avoid regulatory fines
Clinical Leaders	Minimise clinician time spent on authentication Ensure uninterrupted patient care Reduce patient safety events linked to access issues Improve clinician satisfaction
Operations Officers	Maximise healthcare services and operational continuity Reduce access-related delays Minimise workflow interruptions and delays
Compliance and Risk Officers	Improve compliance audit performance and avoid breaches Ensure adherence to regulatory timelines and documentation accuracy Accelerate incident response and remediation



# Next Steps : Action Plan for Strategic EAM Investment



## Define Requirements

Clearly outline the organisation’s EAM needs, addressing both compliance mandates and usability expectations from IT, clinical, operational, and administrative stakeholders.



## Assess Security Posture

Conduct a baseline assessment of current access management practices to identify gaps in compliance, vulnerabilities, and workflow inefficiencies.



## Invest in Modern Solutions

Prioritise next-generation EAM technologies such as multi-factor authentication, intelligent reauthentication, and biometrics to meet evolving security, efficiency, and regulatory demands.



## Educate and Engage

Deliver regular training for leadership and staff on data privacy, security obligations, and the tangible benefits of a robust EAM strategy for everyday clinical and operational excellence.



## Future-Proof Operations

Prepare for upcoming regulations and care delivery innovations by adopting EAM solutions that support interoperability, align with regulations like NIS2 and eIDAS 2.0, and are adaptable to integrated and remote care models.



## Balance Security and Usability

Establish cross-functional working groups to evaluate and select solutions that protect sensitive data while enabling frictionless clinician workflows and positive user experiences.

**To ensure their EAM strategy delivers maximum value driving regulatory compliance, operational efficiency, and seamless care delivery, healthcare organisations should consider the following guidance**



# Conclusions



Enterprise access management goes beyond IT: It is a strategic catalyst for secure, efficient, and patient-centred digital healthcare. As regulatory pressures and cyberthreats intensify, robust EAM solutions safeguard sensitive data, drive clinical innovation, and build trust across all stakeholders.



By adopting next-generation access technologies, European healthcare organisations can fuel sustainable transformation, ensure regulatory compliance, and strengthen defences against emerging threats.



The seamless integration of EAM into clinical workflows enables organisations to make significant strides in care quality and operational resilience, while instilling confidence in patients, clinicians, and partners alike.



Investing in advanced EAM platforms lays the foundation for secure, efficient, and future-ready healthcare across Europe. Now is the time to prioritise access management as a key driver of digital health success.



# Message from Sponsor



Imprivata delivers solutions that provide simple and secure access management for healthcare and other mission-critical industries to ensure every second of crucial work is both frictionless and secure.

Imprivata has been working with healthcare organisations for over 25 years to provide clinicians with fast, secure access to clinical systems and patient data at the point of care.

Imprivata’s Enterprise Access Management is widely used by over 50% of NHS Trusts in the UK, by healthcare organisations across the USA, and by an increasing number throughout Europe, Australia and New Zealand.

Imprivata’s range of solutions enables healthcare organisations to build on their initial investment in single sign on/enterprise access management, to deliver a comprehensive identity and access management system for both local and national systems. Imprivata’s solutions extend fast, secure user access across a variety of form factors including shared-use mobile devices, connected medical devices, multi-user desktops, and virtual desktops to support critical clinical workflows, with the same look and feel that removes barriers to technology and can significantly reduce frustration for end users.

If you would like to learn more, [book a demonstration here](#)

Or read our White Paper: [It’s all About Time](#)





# About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets.

With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries. IDC’s analysis and insight help IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives.

Founded in 1964, IDC is a wholly-owned subsidiary of International Data Group (IDG, Inc.), the world’s leading tech media, data, and marketing services company.



This publication was produced by IDC Custom Solutions. As a premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets, IDC’s Custom Solutions group helps clients plan, market, sell, and succeed in the global marketplace. We create actionable market intelligence and influential content marketing programs that yield measurable results.



**IDC UK**  
1st floor, Whitfield Street, London, W1T 2RE, United Kingdom  
T 44.208.987.7100



© 2025 IDC Research, Inc. IDC materials are licensed [for external use](#), and in no way does the use or publication of IDC research indicate IDC’s endorsement of the sponsor’s or licensee’s products or strategies.

[Privacy Policy](#) | [CCPA](#)



# Enterprise Access Management Underpins the New NHS 10-Year Plan Vision



U.K. healthcare organisations must align their cybersecurity posture with the Cyber Assessment Framework (CAF)-aligned Data Security and Protection Toolkit (DSPT). In the future, they will face stricter requirements under the upcoming Cyber Security and Resilience Bill.

## Cyber Security and Resilience Bill (upcoming)



- *Aligning to NIS2 requirements*
- *Further focusing on digital identities highlights the need for robust authentication, access control measures, and continuous monitoring to protect sensitive patient data.*



50%

One in two U.K. healthcare organisations are investing in EAM to enhance their current capabilities.

The NHS 10-Year Plan is also driving investment in EAM by demanding new, community-focused, integrated, and preventative care services, a “digital by default” mindset, and greater patient control over data, raising the stakes for digital identity and access at every level. The plan directly and indirectly positions EAM as foundational, rather an IT “add-on,” at the core of the trust and safety layer for all digital ambitions, from secure digital services to automation, AI, and flexible staffing.

## Enabling Digital-First, Patient-Powered Care



EAM, with SSO, robust identity management, and secure, contextual access, ensures only authorised professionals access the right data, with full auditability and prevention of unauthorised access, vital for building trust and adoption of key NHS Plan tools like the NHS App and the single patient record.

## Operational Efficiency and Staff Experience



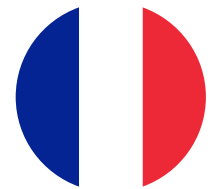
SSO, passwordless authentication, and quick access significantly reduce administrative burdens, enhance workflow efficiency, and improve the workforce experience, allowing staff to focus more on their core competency: patient care.

## Scaling “Neighborhood Health,” Flexible Staffing, and Partnerships



As care shifts to communities and multi-disciplinary teams, EAM enables portable, federated, role-based access, supporting dynamic staffing while ensuring governance, privacy, and security.

# Meeting France's 2027 Digital Health Mandates with EAM



# 70%

of French healthcare organisations are investing in EAM to enhance their current capabilities.



France's **2023–2027 Digital Health Roadmap** mandates robust access controls for compliance, workflow enablement, and clinical innovation.

Enterprise access management is essential for meeting strict health data security mandates, unlocking digital health funding, and delivering secure, innovative care in the evolving digital ecosystem.

## Cybersecurity and Compliance



National cybersecurity requirements, including the **CARE Program, HospiConnect, RIE, ANSSI best practices, and HAS certification** mandate advanced access controls, continuous authentication, strong identity management, and stricter digital criteria, with mandatory cyber exercises and audits by 2027.

## Digital identity and Access



The nationwide rollout of federated identity (**e-CPS**), high-assurance authentication (biometrics, 2FA), and integration with Pro Santé Connect requires organisations to ensure secure, seamless user experiences and compliance with evolving European (**eIDAS 2.0**) requirements.

## Digital Health Adoption



The expansion of **Mon espace santé, telehealth, and remote access** requires role-based and adaptive authentication for seamless access to medical documents and software.

With AI-driven, data-sharing initiatives in healthcare, EAM strategies should support expanded user bases, automate access reviews, and enable dynamic, consent-based access.

## Care Models and Organisations



As hospitals **consolidate IT (GHT policy)** and **interoperability** between hospital, community, and cross-border EU systems grows, providers need to advance their EAM strategies to provide secure, standardised, and auditable access to data across organisations.

The roadmap emphasises **clinician workflow enablement**, supports mobile workforces, streamlines onboarding/offboarding, minimises delays, and enables secure, context-aware access, boosting productivity and satisfaction.



# EAM: A Strategic Lever for Compliance and Modern Care Delivery in Germany



70%

of German healthcare organisations are investing in EAM to enhance their current capabilities.

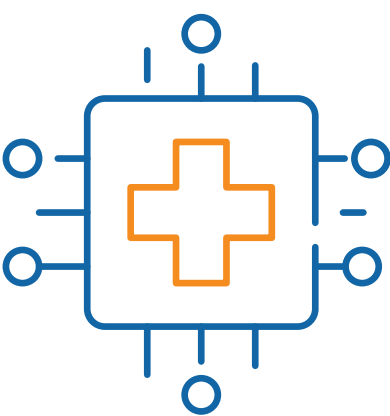
EAM investments are primarily compliance-driven, ensuring adherence to regulations through advanced encryption, MFA, and granular access controls that support reporting and audit readiness. At the same time, they enhance workforce efficiency and accelerate digital health adoption by enabling streamlined, role-based access and supporting interoperability and integrated care initiatives.



## EAM strategies support compliance with:

the **Digital Healthcare Act (DVG)** and **BSI IT Security Act**, which mandate robust cybersecurity controls for hospitals, digital health (DiGA), telemedicine providers, and IT vendors.

**BSI C5 security standards** (effective 2025), requiring healthcare providers to ensure that cloud vendors handling their health data implement strong identity and access controls to maintain compliance.



EAM investments drive workforce efficiency and digital health adoption, supporting providers in advancing key healthcare reform initiatives.

**Hospital Future Act (KHZG):** Provides major funding to boost hospitals' digital maturity, with a focus on interoperability, secure identities, and data infrastructure. Hospitals must meet requirements by the end of 2025 or face penalties.

**2025 Hospital Reform (KHVVG):** Introduces integrated care models like Level 1i hospitals, combining outpatient, inpatient, and nursing services. These new facilities require EAM to ensure secure, role-based, and auditable access to health data across care settings, ensuring privacy, data sharing, and coordinated workflows.