KuppingerCole Report

executive view

by Martin Kuppinger | November 2019

Identity Automation's RapidIdentity Solution

Identity Automation's RapidIdentity is an Identity and Access Management (IAM) solution that targets the specific requirements of healthcare organizations. Beyond delivering standard IAM capabilities, RapidIdentity helps healthcare organizations access a unified solution instead of relying on disparate point solutions. RapidIdentity's cohesive suite of tools reduces integration time for organizations and delivers consistent flexible functionality.

by **Martin Kuppinger**
mk@kuppingercole.com
November 2019

Content

Related Research

Leadership Compass: Identity Governance & Administration - 71135

Leadership Compass: Identity Provisioning - 71139

Leadership Compass: Access Governance & Intelligence - 71145

Whitepaper: IAM for Healthcare: It's time to act - 80029

1 Introduction

The healthcare industry is facing change and pressure in the age of Digital Transformation and ever-increasing cyberattacks. While some challenges that healthcare organizations face are the same as in other industries, many are specific to healthcare, such as Electronic Prescribing for Controlled Substances (EPCS) or the US's Health Insurance Portability and Accountability Act (HIPAA) regulations.

In order to protect access to sensitive data and assets Identity and Access Management (IAM) must become a cornerstone of IT infrastructure in healthcare organizations. Restricting and controlling access allows for focused protection down to the granular level of patient records. This requires a comprehensive IAM solution that goes well-beyond pure Single Sign-on (SSO) to support all types of users and devices and enable seamless, yet secure, access to all types of applications and data.

In KuppingerCole's view, IAM was originally a tool whose primary purpose was to prevent unauthorized access to secure resources. With a traditional focus on access administration, the IAM core technology evolved to include Identity Provisioning, as well as essential capabilities to authenticate, authorize, and audit.

The next generation of IAM solutions not only tried to prevent unauthorized access to resources, but also added the ability to detect it. As such, Access Governance with a focus on administration with business participation became a core IAM technology. The ability to detect unauthorized access was, in part, due to integrations with Security Information and Event Management (SIEM) products that were making their way into the market.

In this latest iteration, IAM built upon this ability to prevent and detect by adding the ability to respond to security threats. Many IAM technologies now include Access Analytics and Intelligence. Access Analytics makes it possible to perform analysis of historical data and uncover trends and patterns that can be used to improve decision-making processes. On the other hand, Intelligence gives the ability to make access decisions that can be acted upon based on these patterns and trends. Together, Access Analytics and Intelligence provide the ability to not only detect, but also to respond to unauthorized access attempts.

These new capabilities help to not only fulfill business requirements, but also those associated with governance, compliance, and administration. Integrations with Adaptive Authentication & Authorization, Real-Time Security Intelligence, Software Defined Environments, and Privilege Management also need to be supported by today's IAM solutions.

In regards to the healthcare industry, identity management solutions must also integrate with major healthcare applications and support the industry's specific SSO challenges. For example, doctors and nurses who use shared terminals require quick access when switching accounts.

There's no doubt IAM is essential for healthcare organizations – and when executed properly, IAM successfully mitigates security and compliance risks, supports efficiency in daily work, and enables Digital Transformation across the organization.

Identity Automation is a provider of both on-premises and cloud-based IAM solutions (Identity as a Service, IDaaS), with a specific focus on the healthcare industry. Identity Automation delivers a comprehensive IAM solution for healthcare that spans all core IAM capabilities, including Identity Lifecycle Management, Access Governance, Multi-Factor Authentication, and Single Sign-On. Identity Automation also delivers integration into major healthcare industry solutions, such as Epic, Cerner, and Meditech.

2 Product Description

Identity Automation supplies IAM solutions with targeted attention on the heathcare industry. It uses both on-premises and cloud-based deployment models. In 2018, Identity Automation acquired HealthCast, a vendor specializing in IAM solutions for the healthcare industry. By combining the two portfolios, Identity Automation now delivers a comprehensive IAM solution for healthcare organizations that spans all core IAM capabilities, including Identity Lifecycle Management, Access Governance, Multi-Factor Authentication and Single Sign-On. Identity Automation also delivers integration into major healthcare industry solutions, such as Epic, Cerner, and Meditech.

Identity Automation's IAM offering, RapidIdentity, comes as an integrated suite of IAM capabilities. This is in contrast to many of the other offerings in the IAM market, which provide a set of disparate products for various use cases, such as the SSO niche and point solution vendors. Together with support for healthcare's unique requirements, the breadth of RapidIdentity's IAM capabilities makes the solution a strong offering for healthcare organizations that can't afford the cost and complexity of integrating a range of offerings and need a solution that addresses their specific challenges.

Healthcare's increasingly complex requirements have created a need for integrated IAM solutions and structured approaches for delivering these capabilities. Such integration helps ensure efficient implementation and delivery of IAM services within mid-sized organizations that are unable to handle the complexity of a multitude of disparate tools.

Identity Automation focuses its product strategy on five key capabilities:

- Delivering a **flexible** solution with that is highly configurable for ad-hoc and complex use cases
- Providing a highly **scalable** offering, both on-premises and in the cloud, with proven support for millions of identities (users and devices)
- Enabling organizations to manage identities and access in a **secure** way with a high degree of automation, fine-grained access controls, and strong access governance capabilities
- Providing a **comprehensive** and integrated solution that supports major IAM use cases
- Making use of modern Artificial Intelligence (AI) and Machine Learning (ML) technologies for an **intelligent** solution that supports administrators in their role and helps to mitigate cyber risks

As a result of the HealthCast acquisition, Identity Automation has increased its existing strength in supporting healthcare requirements by adding a series of specific capabilities to RapidIdentity, including:

- Single Sign-On capabilities, including fast-user switching and integration with Virtual Desktop Application Access, for fast and simple, yet secure access to applications
- Support for EPCS and SSO auditing
- Drug Enforcement Administration (DEA) compliant MFA
- Tap-and-go proximity badge access to both local Windows desktops and multiple VDI solutions
- Fine-grained access to major healthcare applications
- Connectors to other leading clinical applications for provisioning and auditing integration
- Identity Verification features, which allow verification and subsequent authentication of users, including Patient Verification

These capabilities complement the broad set of features Identity Automation already delivers as part of their RapidIdentity platform. These key capabilities include:

- Identity Lifecycle Management, i.e. the ability to manage users and their accounts across systems based on well-defined and automated processes
- Access Governance as the other part of Identity Governance and Administration (IGA) that delivers access insights and as a result, enables the enforcement of the privilege of least-privilege
- Single Sign-On that delivers streamlined portal access to applications deployed on-premises, in the cloud, or in hybrid environments
- Multi-Factor Authentication with extensive support of different authentication methods, from username/password to a variety of strong authentication approaches, including push notifications, FIDO U2F, one-time passwords, fingerprint biometrics, RFID, and more
- Integrated Privileged Access Management (PAM) capabilities to restrict and control access of privileged users and in general, privilege elevation

It is the combination of specific support for Healthcare requirements and strong focus on delivering comprehensive IAM capabilities that are essential for Healthcare organizations that differentiate Identity Automation's RapidIdentity from other IAM solutions.

3 Strengths and Challenges

One obvious strength of Identity Automation's RapidIdentity is the focus on healthcare's specific IAM challenges. RapidIdentity provides several capabilities that are essential for supporting the business and fulfilling industry-specific regulatory compliance requirements. In addition, the solution comes with out-of-the-box integration into a number of healthcare-specific applications. RapidIdentity differs from standard IAM solutions in its healthcare support, and it differs from other healthcare-focused IAM solutions by providing a broad set of features that go well-beyond Single Sign-On alone.

Furthermore, RapidIdentity is a single platform, removing the need for integrating various products for different capabilities, a challenge for most healthcare organizations. It is an efficient and effective solution for these organizations.

In choosing an IAM solution, there will always be trade-offs, such as lesser features than a best-of-breed point solution. However, as an integrated suite, RapidIdentity provides a quick introduction to IAM for healthcare organizations. We strongly recommend that healthcare organizations include Identity Automation's RapidIdentity in product selection processes.

Strengths	Challenges
• Integrated suite of IAM capabilities, instead of disparate products • Focus on the major requirements of Healthcare organizations, including Single Sign-On • Out-of-the-box integration to major Healthcare applications • Scalable solution that also works well for smaller healthcare organizations • Support for major healthcare regulations	• Less depth of features than best-of-breed point solutions in most areas, but focused support for healthcare requirements • Still relatively small partner ecosystem, specifically outside of North America • Still relatively small vendor

4 Copyright

The Future of Information Security – Today

KuppingerCole supports IT professionals with outstanding expertise in defining IT strategies and in relevant decision making processes. As a leading analyst company KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

KuppingerCole, founded in 2004, is a leading Europe-based analyst company for identity focused information security, both in classical and in cloud environments. KuppingerCole stands for expertise, thought leadership, and a vendor-neutral view on these information security market segments, covering all relevant aspects like Identity and Access Management (IAM), Governance, Risk Management and Compliance (GRC), IT Risk Management, Authentication and Authorization, Single Sign-On, Federation, User Centric Identity Management, eID cards, Cloud Security and Management, and Virtualization.

For further information, please contact **clients@kuppingercole.com**