



# Healthcare Identity Security: What to Expect From a Solution

SailPoint's Radcliffe and Sebaugh on  
How to Accelerate Your Identity Program



### Matthew Radcliffe

Radcliffe is the area vice president of healthcare at SailPoint. He has spent the past 30 years collaborating with organizations as they plan and execute their identity security strategies. Over the past 13 years, he has led SailPoint's healthcare business through continued accelerated growth.

### Rob Sebaugh

Sebaugh is the healthcare identity strategist at SailPoint. He supports customer, partner, engineering and development organizations in addressing the challenges specific to healthcare and the growing needs for identity security in this industry. Prior to joining SailPoint, he was the senior director for identity and access management for the United States' largest provider of government-funded health insurance.



What are the key elements of a successful healthcare identity security program? SailPoint healthcare experts **Matthew Radcliffe** and **Rob Sebaugh** detail what to look for to accelerate your business and improve your security posture.

In an interview with Information Security Media Group, the two SailPoint executives discussed:

- Elements of a successful identity security program;
- How to choose a solution that can scale to your needs;
- How to solve unique healthcare identity security use cases.

**“With the reprioritization of identity, the focus at a board level and realizing that on-premises technologies can no longer scale with the business, healthcare organizations are really shifting their mindset.”**

**– Matthew Radcliffe**

## **Identity Security Program Challenges**

**TOM FIELD:** What has the healthcare industry learned from past identity security programs?

**MATTHEW RADCLIFFE:** One of the biggest challenges is that identity in the past was treated as a pure IT initiative. They didn't really consider the caregiver struggle or how caregivers participated in security programs. But identity and access for clinicians has a direct impact on patient care. The one fundamental change that's happened in the last 10 years is that identity in general is no longer just a pure IT or security initiative. More and more healthcare organizations' security departments are integrating clinicians in the design, development and employment of identity programs within their organizations.

The fact that this is now a board-level conversation helps in terms of visibility and commitment to successful identity programs. With increasing breaches and security risks across healthcare organizations, boards are starting to prioritize cybersecurity initiatives and focus on identity in particular. But you also have to think about the technology. Traditionally, identity was an on-premises initiative leveraging on-premises technologies

– and perhaps 10 or 15 years ago, that was the right kind of technology. But on-premises technologies were historically highly configurable. You could make them do whatever you wanted to do, so they became over-engineered.

As healthcare organizations' business strategies continued to accelerate the pace of businesses, they were moving faster than understaffed IT departments within healthcare organizations could maintain and grow the identity program. More and more organizations are realizing that on-premises technologies can no longer scale with the pace of business. With the reprioritization of identity, the focus at a board level and realizing that on-premises technologies can no longer scale with the business, healthcare organizations are really shifting their mindset.

## **Guidelines for Selecting an Identity Security Vendor**

**FIELD:** What should a security leader expect out of their identity security solution provider?

**ROB SEBAUGH:** A good solution provider comes forward with a standards-based approach.



The more customized we get and continue to get in our environments, the more technical debt we continue to create. If we want to scale and – especially from a security perspective – stay ahead of the bad guys, we can't always customize everything about our cyber defense practices. I understand and respect that in certain situations you need to have an adaptable fabric to support you, but organizations have to do a better job at putting forward best business processes and practices and standardizing on an approach that delivers a quality end-user experience and a quality cyber program.

Traditional infrastructure is not dying, but it's certainly being used less and less. Cloud is becoming more apparent. Cloud came about because traditional infrastructure didn't support the use cases we needed for size and scale of a SaaS or cloud solution. The same could be said for identity. We should be looking at solution providers that can scale to understand the identity context of our end users and the hybrid nature of their environment and be able to adapt to and manage those individuals and their identities across their disparate roles and organizations.

Most organizations have millions of dollars in investment in tech. And in infrastructure tech, anything you choose from an identity perspective needs to leverage those investments. We can't come in and say we're going to help you solve everything by ripping everything out. There's no way to get that done. We have to come in and be a partner. We have to be able to enhance and make use of the existing investments to provide you a better identity experience.

## Changes in the Identity Market

**FIELD:** What has changed within today's modern identity security technologies?

**RADCLIFFE:** The last four years have been an interesting window of time in identity and healthcare and identity as a market. Before COVID, 95% of our business was on-premises. Then healthcare organizations realized that they had to find ways to accelerate their cybersecurity strategies and business, and SaaS allows that.



**“We want to understand how things are being used and why someone has access. We want to help drive a more modern approach to identity that’s machine driven. We as humans can only scale so wide; that’s where the technology curve is coming into identity.”**

**– Rob Sebaugh**

The industry in the last couple of years has flipped itself upside down. Our customers are now coming to us demanding cloud deployment strategies and SaaS-based deployment strategies because they help them accelerate their business. They allow them to have a different type of resourcing pool to support these programs. No longer do you have to be a software developer to maintain an identity program. You can be a business analyst, which means they can move faster with a lower total cost of ownership.


SaaS also has to do with security. Traditional on-premises deployments and even single-tenant cloud deployments have struggled with reacting to security breaches. This is specifically why SailPoint and others in this space have focused on multi-tenant SaaS deployments. They allow our customers to accelerate their identity strategy and adapt to new cloud strategies, and they put them in a phenomenal position to more actively and proactively respond to cybersecurity threats. We can now protect thousands of customers instead of having to patch each customer one at a time.

The third element to SaaS and modern technology is leveraging AI and machine

learning – taking what was a static process of role modeling and making it dynamic.

We can help clinicians make the right decisions by arming them with the data to make sure that they are applying access in an appropriate way. Sometimes, the data even speaks for itself and removes the friction. If the technology is smart enough to help make the right decision for the organization, the clinician doesn’t have to make security decisions. We’re looking at leveraging machine learning and AI and our technology across a modern SaaS architecture.

**SEBAUGH:** We in healthcare started thinking about identity when the ink dried on HIPAA and we realized we had to govern this stuff. It’s a serious thing, but nothing in the idea of governing from a HIPAA perspective says you have to use technology. We learned that pen and paper and spreadsheets take a lot of human resources and time to manage, and they’re not always very accurate. The transition that we’ve seen is very data driven; the data will always tell a better story. If I can tell you with certainty that you don’t need this access because you haven’t used it in six months, I know I can safely take it away. These are the types of things that we want to understand.



We want to understand the data underneath. We want to understand how things are being used and why someone has access. We want to help drive a more modern approach to identity that's machine driven. We as humans can only scale so wide; that's where the technology curve is coming into identity. If I'm looking for a solution in today's modern enterprise, it has to support me in that manner.

## Identity Security Myths

**FIELD:** What are some myths surrounding today's cloud-based identity security deployment strategies?

**SEBAUGH:** Kevin Mandia said identity security is our only ability to stop what he called the first inning of the kill chain, when there's a crack in our defenses. If you can't handle identity security correctly, prevention fails. Stopping things like lateral credential theft is very difficult. Organizations are starting to look at going outside of their four walls and doing something in a SaaS solution for their identity practice. Then they think, "How can I govern that?"

There's a myth that multi-tenant is less secure than single-tenant is less secure than on-premises. The reality is that almost all breaches boil down to credential theft. And we've seen in multi-tenant environments and single-tenant environments alike that if you can pop administrative credentials, you potentially can do a lot of things. It all depends on how the other layers of security are built in your application. So if I'm a customer and I'm looking at an identity solution, I want to look for something with a security stack and protocol that I understand. I want to understand how the tenants are secured from each other and how customers are secured in a multi-tenant environment.

Any good vendor will come forward and explain how all of those things work. Without naming vendors, we've seen where administrative tokens might've been left behind that were popped, and that allowed some lateral movement. It all boils down to credential theft, and the goal is to stop that. A multi-tenant perspective gives you scale and guardrails and the ability to deliver at a rapid pace, which is the expectation of today. If you're constantly

**“SailPoint recognized that healthcare is unique and different. We started a healthcare practice 13 years ago. We focus specifically on solving the unique challenges of healthcare provider organizations.”**

**– Matthew Radcliffe**

customizing and in a single-tenant or on-premises-type disposition, you have to police yourself. You have to make sure you're not going off the guardrail. Otherwise, you will create technical debt and slow down.

## **The SailPoint Approach**

**FIELD:** How is SailPoint helping its healthcare customers overcome these challenges we've talked about and embrace a modern identity security program?

**RADCLIFFE:** Number one: SailPoint recognized that healthcare is unique and different. We started a healthcare practice 13 years ago to specifically focus on the use cases and the requirements that provider organizations have that are far different than many other verticals in the technology space. We focus specifically on solving the unique challenges of healthcare provider organizations. Two: SaaS and leveraging AI and machine learning are fundamental for us. We look beyond that: What else do we need to provide to our customers to help them accelerate their business and have the best security posture?

We don't think about just applications. If you only focus on providing identity and identity

governance around applications, you're solving one-third of the problem. Every organization has sensitive data, and you have to provide identity governance around sensitive data. Who has access to PHI? Who has access to PCI, and how is that access managed throughout the life cycle?

The second element that we focus on is cloud infrastructure. A majority of healthcare provider organizations have one to many cloud infrastructures. We manage access for a clinician population to Epic, Cerner or Meditech, and we have to recognize that there are sensitive permissions within the organization that are developing and deploying workloads within cloud infrastructure. We have to manage those sensitive permissions just like we do applications and data, so we think about cloud infrastructure as well.

We have to make it easier for our customers to deploy identity onboard applications and onboard the workflow around those applications. How do you provision users, transfer users, terminate users and govern the access? We have spent the last several years developing a workflow engine that simplifies the ability for our customers to continue to expand their identity footprint, onboard more applications and govern more access to resources.



The last point is that an identity isn't just a human. An identity can be a bot or a machine account. It has other contexts, and we have to be able to arm our customers with an identity platform that thinks about applications, data and infrastructure but also understands that an identity could be a human, a bot or some other device. SaaS is fantastic. The fact that we're on a multi-tenant SaaS platform is great. The fact that we've integrated machine learning and AI is terrific, but those other areas are just as important.

**SEBAUGH:** The name of the game for me is: Through the lens of an end-user experience, how do we simplify the ability for our clinicians to do what they're paid to do and focus on patient care? How do we not be another IT process in the way, but do it in a way that informs them that they're part of our security programs and that they understand the importance of identity? We have to make sure that our identity security approach is there; otherwise, we have a much bigger problem. So we focus on improving and supporting the cybersecurity practice. That is a goal of SailPoint in general.



## About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Each of our 36 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

(800) 944-0401 • sales@ismg.io

























