Case Study

Seattle Cancer Care Alliance

SECUREAUTH

Seattle Cancer Care Alliance
Fred Hutch · Seattle Children's · UW Medicine

Overview

Industry

+ Healthcare

Challenges

+ Low-friction authentication for physicians at partner sites
+ Secure remote authentication for physicians at home
+ Flexible authentication options for users who are not employees

Solution

+ SecureAuth IdP
  - Flexible multi-factor authentication with device recognition technology
  - Self-service password

Benefits

+ Minimized friction for low-risk physician access, speeding patient care
+ Secured remote access with multi-factor authentication
+ Offered knowledge-based authentication options that do not require tokens or specific smart phone apps

Seattle Cancer Care Alliance Enhances Both Patient Care and Security with Adaptive Authentication from SecureAuth

Seattle Cancer Care Alliance (SCCA) is a world-class cancer treatment and research center that combines the power of science with the power of collaboration. Together, the devoted healthcare professionals at its partner organizations provide advanced therapies and clinical studies that turn cancer patients into cancer survivors.

Business Challenges

Like many organizations today, SCCA needed to enable secure remote access to its systems and data — without unnecessarily burdening on-premises users with additional authentication steps.

For example, SCCA hosts an application that helps physicians manage radiation oncology treatment plans for patients. This application is available to physicians both when they are treating patients at partner sites and when they are at home. "We needed a solution that could differentiate between those two situations," explains Chad Hoggard, Manager, Information Security Architecture at SCCA. "Basically, we wanted to require two-factor authentication when users are accessing the application from home but not when they are at a patient's bedside at any of our partner facilities."

Moreover, not just any second authentication factor would work. "We wanted a variety of second factors because the various applications we use all have different requirements," says Hoggard. "Plus, users across the board are very happy to have options like knowledge-based authentication, SMS messaging, and device recognition."

A team was tasked with researching a range of products on the market, including tools from RSA, SafeNet, Duo Security, and SecureAuth. They whittled the contenders down to three based on high-level requirements; for example, they eliminated Duo Security because SCCA did not want a strictly cloud-based solution.

The Solution

Because SCCA needed a solution in place quickly, the team decided to ask the three finalists to demonstrate their ability to integrate with several specific applications, including Cisco VPN, VMWare Horizon View, Microsoft Outlook Web Access (OWA), Citrix, and the video conferencing system Lifesize.

"SecureAuth's presales team was excellent," says Hoggard. "They really went after our use cases and successfully integrated the first four. Moreover, only SecureAuth went to the effort to contact vendors to investigate what it would take to integrate Lifesize. With the other vendors, we would have had to go on faith that they could do everything we needed."

"SecureAuth minimizes the impact on the physicians and makes the process as painless as possible. When a user comes in consistently from the same device, such as their home computer, the device recognition technology provides a high degree of confidence that it is the right user."

— Chad Hoggard, Manager, Information Security Architecture, Seattle Cancer Care Alliance

Moreover, most other vendors have limited authentication options while SecureAuth IdP offers more than 20 factors that can be associated with an authentication attempt. Options include not just passwords and USB keys but also push notifications, one-time passwords (SMS, telephony, and email), a variety of OATH tokens, and device recognition. Therefore, SCCA is able to choose the factors that meet its unique requirements now and into the future, while minimizing friction for legitimate physician authentications.

"Because not everybody has a smart phone, having the ability to use a knowledge-based second factor rather than requiring a device was a big selling point for SecureAuth," Hoggard notes. "In addition, SecureAuth minimizes the impact on the physicians and makes the process as painless as possible. When a user comes in consistently from the same device, such as their home computer, the device recognition technology provides a high degree of confidence that it is the right user."

Deployment was far quicker and easier than SCCA had dared hope. "Our idea of how long it would take to get an authentication solution in place completely changed when we started working with SecureAuth," says Hoggard. "We were delighted when we realized it would take hours, not days or weeks."

In addition to streamlining access for physicians and blocking risky authentication attempts, SecureAuth IdP has also helped SCCA reduce help desk workload and improve user productivity. For example, although many organizations have to handle a high number of password resets, the problem was worse for SCCA.

"We used to have 50–80 calls a month to the help desk for password resets," recalls Hoggard. "Because SecureAuth delivers self-service password reset out of the box, we were able to retire our dated password change system altogether."

SecureAuth has not only met SCCA's current needs but also positioned the organization for the future. "We did not want rely on proprietary two-factor methods like RSA has historically done," Hoggard says. "It's better to have a solution that uses open protocols and methods. For example, SecureAuth gives us SAML possibilities we didn't have before. If I could do it over, I would absolutely make the same decision. I am very, very happy that we chose SecureAuth."

"Our idea of how long it would take to get an authentication solution in place completely changed when we started working with SecureAuth. We were delighted when we realized it would take hours, not days or weeks."

– Chad Hoggard, Manager, Information Security Architecture, Seattle Cancer Care Alliance

About SecureAuth Corporation

SecureAuth is the leader in adaptive access control solutions, empowering organizations to determine identities with confidence. SecureAuth™ IdP provides authentication security, Single Sign-On, and user self-service tools together in a single platform, allowing strong identity security while minimizing disruption to the end-user. Flexible Adaptive Authentication workflows can protect on-premises, cloud, mobile, and VPN applications that can detect the use of compromised credentials allowing our customers to quickly respond a security breach. Currently protecting over 5 million users worldwide including Western Union, Unisys, FBI, Toshiba, Ticketmaster, General Mills, and more, SecureAuth provides adaptive access control to some of the largest and most respected companies in the world. Learn more about how to determine identities with confidence at secureauth.com.