



SECUREAUTH

# Case Study

## Houston Methodist



### Overview

#### Industry

- + Healthcare

#### Challenges

- + Provide secure remote access to a variety of applications
- + Eliminate the need to carry hard tokens
- + Address compliance regulations for the handling of patient information

#### Solution

- + SecureAuth IdP adaptive and two-factor authentication

#### Benefits

- + Enabled secure remote access to on-premise, web-based, and SaaS applications
- + Minimized friction and increased user satisfaction
- + Enhanced security with adaptive authentication
- + Integrated with existing technology
- + Reduced downtime associated with technology upgrades by 98 percent
- + Deployed within days

### Houston Methodist Continues “Leading Medicine” with SecureAuth

Houston Methodist is a nonprofit healthcare organization based in Houston, Texas, with seven hospitals and 2,000 beds. Following its mission of not just practicing medicine but leading it, the hospital offers the latest innovations in medical, surgical and diagnostic techniques; directs millions of dollars into research and advances in patient care; and provides financial and medical assistance to over 150,000 patients annually. The system’s flagship location, Houston Methodist Hospital, is consistently listed as “One of America’s Best Hospitals” in U.S. News and World Report.

### Business Challenges

To help its staff deliver the best patient care possible, Houston Methodist embraces new technologies. In particular, the organization enables staff to access appropriate medical records, patient data, and financial systems remotely. Doctors who float between hospitals can access medical records on their mobile devices so they can provide care even when they are not on site with the patient.

Security concerns were keeping Houston Methodist from using technology to its fullest. The organization is committed to not only meeting but exceeding HIPAA standards for securing patient information, and the IT team recognized that single-factor authentication was not sufficient to deliver the security required in today’s mobile world. But they refused to settle for a multi-factor solution that impeded the ability of staff to continue to deliver world-class care.

“It’s a tight rope to walk,” explains Matt Johnson, manager of server engineering for Houston Methodist. “You want to secure the perimeter access in the best way you can; however, you also want a solution that is easy for people to use.”

When the team implemented a two-factor solution that used hard tokens, staff complained about having to carry them. Users were happier when the hospital moved to a solution that used a question-and-answer approach; however, that solution was still intrusive to the user experience, and, critically, it was compatible with only a few of the hospital’s systems and only the most commonly used devices.

### The Solution

The problem came to a head when the question-and-answer solution proved incompatible with the new reverse web proxy that Houston Methodist deployed to facilitate access to intranet-based web applications. The hospital reached out to one of its partners, Set Solutions, who recommended SecureAuth as the fix to the problem. “We looked at several of the big name vendors, and their products were OK and easy to install,” says Johnson. “But then SecureAuth stepped in and just knocked

***“[SecureAuth] worked with not only our main Citrix-based application, but all other types of different applications, from VPN to web reverse proxy to cloud-based SaaS apps. It was a home run in every category.”***

— Matt Johnson, Manager of Server Engineering, Houston Methodist



## Case Study: Houston Methodist

---

it out of the park, both functionality and financially. They just really blew us away with their adaptability and how they've integrated with so many different types of technologies."

A proof of concept confirmed the hospital's initial impression. "We had SecureAuth up and running within a couple days, and we were really impressed," Johnson recalls. "Within about two weeks, we had it on three other systems as well. And it was done in a way that our users liked, which is pretty hard to do."

In fact, the hospital quickly discovered that SecureAuth was compatible with not only the new reverse proxy but its other systems as well. "The flexibility of SecureAuth was really nice because it worked with not only our main Citrix-based application, but all other types of applications, from VPN to web reverse proxy, to cloud-based SaaS apps," Johnson says. "It was really a home run in every category."

Moreover, SecureAuth delivered this broad security without introducing friction for users. "The users love the new system," reports Johnson. "With the old system, they had to answer questions every time they logged in. With SecureAuth, when they're on premise, they aren't even prompted for their credentials, let alone questions and answers — in fact, they often don't even realize authentication is happening. And when they're coming in from outside the network, SecureAuth creates a digital fingerprint for the device, so they have to go through two-factor authentication once and then they aren't bothered again for 90 days. That was really a big win from our user base and it allows us to still maintain security."

To further tighten security, Houston Methodist has deployed SecureAuth's adaptive authentication, which considers contextual factors such as IP address, device fingerprint, geo-location and IP reputation data, leveraging SecureAuth Threat Service. "It enables us to account for certain attack vectors, such as people who are compromising accounts from halfway across the world, based upon IP reputation or country code," says Johnson. "Data security is our main concern, but with all these different technologies, you have to make sure that you ensure accessibility in addition to security."

Houston Methodist was also pleased with the flexibility of the SecureAuth solution and staff. "Many vendors won't allow you to put your own security suite on their software appliance," notes Johnson. "SecureAuth, however, was very accommodating and let us deploy our own tools to monitor and secure the appliance." Plus, upgrades are easy and require 98 percent less downtime.

The biggest benefit of SecureAuth, according to Johnson, is that it enables the hospital to take advantage of new technologies to fulfill its mission of "leading medicine" while still maintaining security. "Previously, IT often had to block new technologies based on valid security concerns," Johnson says. "By enabling us to provide new technologies in a secure manner, SecureAuth allows us to be the good guys who provide solutions instead of closing the door on them."

### About SecureAuth Corporation

SecureAuth's identity and information security solutions deliver innovative access control for cloud, mobile, web and VPN systems to over five million users worldwide. With multi-factor authentication and single sign-on in one solution, SecureAuth IdP's unique architecture enables organizations to leverage legacy infrastructures while also embracing next generation technologies. This preserves existing investments while also meeting today's security challenges. For the latest insights on secure access control, follow the SecureAuth blog, follow @SecureAuth on Twitter, or visit [www.secureauth.com](http://www.secureauth.com).

---

***"The users love the new system. ... When they're on premise, they aren't even prompted for their credentials, let alone questions and answers — in fact, they often don't even realize authentication is happening. And when they're coming in from outside the network, SecureAuth creates a digital fingerprint for the device, so they have to go through two-factor authentication once and then they aren't bothered again for 90 days."***

*— Matt Johnson, Manager of Server Engineering,  
Houston Methodist*

---

*SecureAuth, SecureAuth IdP and the SecureAuth logo are registered trademarks of SecureAuth Corporation. All other products or company names mentioned herein are trademarks or registered trademarks of their respective owners.*

