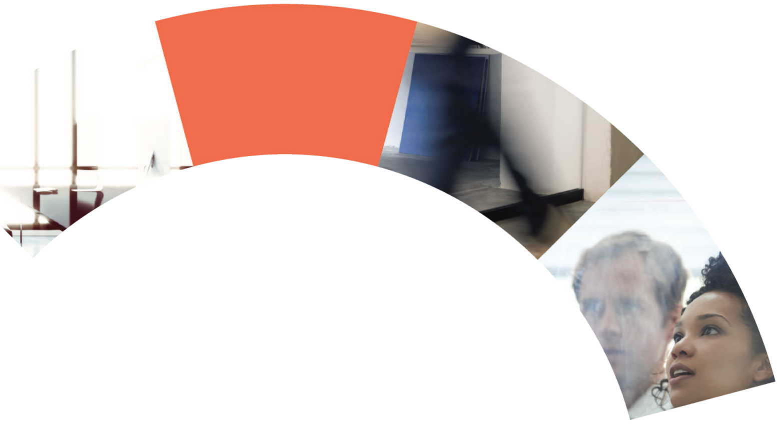
CASE STUDY



Removing the bottlenecks and blind spots in IT access

Texas A&M University's Health Science Center streamlines identity and password management to improve security and staff efficiency

Key Facts

Company
Texas A&M University Health Science Center

Industry
Higher Education

Country
United States

Employees
3,200

Website
www.tamhsc.edu

Challenges

Texas A&M's Health Science Center was spending too much time on manual processes including the management of system access privileges and password resets.

Results

- Removes 500 inactive user accounts
- Boosts efficiency with automation
- Improves insight into access rights
- Simplifies workflows and compliance
- Facilitates autonomous password resets

Products

Identity Manager

Password Manager

Students entrust universities with their digital identities, including social security numbers, academic transcripts and health information. Any system breach can jeopardize individuals' privacy, bank accounts and credit scores; damage a university's reputation; and result in noncompliance with federal regulations including FERPA and HIPAA.

To meet its security requirements, Texas A&M has always taken a proactive approach. Efficiency is also important, though, and the university's Health Science Center staff were spending significant time managing system access and users' passwords. A solution to these challenges presented itself serendipitously. Jody Harrison, associate director of systems engineering at Texas A&M's Health Science Center, happened to see a demo of One Identity Manager at a conference. "It was exactly what we'd been looking for," he says. "With Identity Manager, we could automate a lot of manual processes." He arranged for an onsite product demo and all teams agreed to implement Identity Manager and One Identity Password Manager, because of the products' capabilities and One Identity's professional services options.

“I don’t lose as much sleep at night now that we’re using **Identity Manager**.”

Jody Harrison, Associate Director of Systems Engineering, Texas A&M University Health Science Center

IT staff worked with One Identity partner EST Group to design and deploy its solution. “I’ll be the first to tell you that we don’t like to ask for help, but we’re dealing with a lot of complexity that requires a lot of coordination,” Harrison explains. “There’s no way we could’ve achieved the same results without the input of our EST Group consultants. They sat down with us and figured out all the steps between all our groups and systems, and then helped us configure Identity Manager so we’d have consistent processes.”

Improving security and compliance

To get the real-time data it needs about student, faculty and staff profiles so that it can automate workflows such as provisioning and deprovisioning access, Identity Manager ingests a live feed with information from the Banner Student and the Budget, Payroll and Personnel systems. “HR employees no longer have to manually fill out forms to request a user account,” says Harrison. “It happens automatically. And IT staff no longer have to provision and deprovision access to so many individual systems. When an account is disabled in Identity Manager, it’s disabled in all systems, including Microsoft Exchange and Skype but also in ancillary technologies like Syncplicity, our Dropbox.”

Automated processes incorporate signoffs by risk and compliance officers, and all access privileges are revoked on a specific date unless reapproved. And, if a person is removed from one system such as payroll, Identity Manager alerts IT staff so they can verify that the user’s privileges have been revoked elsewhere. “I don’t lose as much sleep at night now that we’re using Identity Manager,” Harrison says.

Increasing efficiency and cutting risk

IT staff are adding 700 Active Directory groups to the provisioning processes to standardize access and cut risk. “Giving department heads and researchers the ability to manage access to their systems instead of having IT staff do it saves time for everyone and reduces errors,” explains Harrison. “And managers can now get reports that show who has access to what, and who gave them that access. We’ve already deleted about 500 accounts that didn’t need to be there anymore using Identity Manager.”

People are also saving time via the new self-service password process. “IT staff don’t have to reset passwords 100 times a week anymore because people can do it themselves with Password Manager,” says Harrison.

The entire Texas A&M university system is now adopting Identity Manager. “My teams are now looking at how to advance our solution for broader purposes,” says Harrison. “For example, we’d like to tie it into our card reader system so when a user’s access privileges are revoked in Identity Manager, the card they use to get into buildings is also disabled. People are pretty excited about the changes we can make with Identity Manager to improve the security of our systems and our people.”

About One Identity

The One Identity family of identity and access management (IAM) solutions, offers IAM for the real world including business-centric, modular and integrated, and future-ready solutions for identity governance, access management, and privileged management.

Learn more at OneIdentity.com