Supporting Easy Access & Customer Control *with* Centralized Identity Governance

CATEGORY
Cybersecurity

START DATE
July 2018

END DATE
July 2020

NASCIO STATE IT RECOGNITION AWARDS

COLORADO
Governor's Office of Information Technology

Brandi Simmons
Chief Communications Officer
Brandi.Simmons@state.co.us
303.764.6897

Executive Summary

For most people, creating a new email account or opening an online account to shop, book travel or any other consumer activity is pretty easy. So it's understandable why people think it should be just as easy to get their accounts set up when they start working for the State of Colorado. What they likely don't know is that behind the scenes at the Governor's Office of Information Technology (OIT) is a team that is dedicated to making sure that every account created gives a person the right access to the right information at the right time, ensuring that the data of Coloradans within state applications and systems is securely in the hands of only those who need it for legitimate business purposes. This is no easy task.

OIT has been the enterprise provider of information technology services and support to executive branch agencies and approximately 31,000 state employees since 2008. Our Office of Information Security (OIS) is also statutorily responsible for developing the information policies, standards and guidelines necessary to safeguard state systems and the data they hold. The Identity and Access Management (IAM) team manages access for not only the executive branch state employees but thousands of others who work outside of Colorado state government and have a business need to have access to state systems.

Managing the ongoing requests for account creation, closure and access for a growing number of systems and applications was a struggle no matter how many staff members IAM was able to hire. With identity-centric security being a critical part of OIT's Secure Colorado strategy, there was a need to make sure that the best technology was in place to secure state data as well as provide state staff the access they needed efficiently and without delay.

The decision was made to establish a centralized system for secure access, authentication, authorization and user account administration for all systems managed or supported by OIT. This was an exciting step forward in the maturity of the state's identity and access management. The new solution put the decision and control of access in the hands of the state agencies and business units responsible for the state data in their applications. After all, state agency staff are the experts when it comes to understanding who should have access to an application and at what permission level. A bonus was that this new solution would automate processes, speed up the time spent on account creation, reduce errors and provide new state employees the access they needed faster so that they are then ready to get to work on their first day on the job.

Project Narrative

Idea

Managing identity and authentication for the thousands of people (35,000+) who need access to state systems is complex. OIT's Identity & Access Management (IAM) team needed a state-of-the-art solution that was a true advancement in identity and security management to better protect state data by making sure that only authorized individuals have access to state accounts.

Prior to implementing a modern identity management solution, OIT's IAM team had a backlog of access requests, many orphaned accounts to analyze and there were audit findings for not removing access in a timely manner or for not performing access reviews. Additionally, customer satisfaction and user experience were at risk because of inadequate notification for accounts that were expiring; access request forms were electronic with digital signatures but lacked the true digital experience and automation with the workflow processes. Improvements were made through leaner processes and better alignment of staff but it still wasn't enough to meet the demand at the level OIT needed to attain.

Increasingly, organizations are taking a holistic approach to identity management and access management to improve security and risk posture; maintain sustainable compliance with government regulations; standardize and optimize business processes, policies and procedures; reduce time and cost to address both physical and logical security incidents; improve protection of sensitive data; and increase management visibility through the centralized collection, normalization and correlation of both logical and physical security information and events. OIT needed a technology that would help the state realize all of these benefits and more.

The decision was made to implement the Identity Manager solution from One Identity. Identity Manager is a system that allows automated account provisioning (onboard, offboard, access management) throughout the life cycle of state employees and others working for or with the State of Colorado. The automation happens in near real-time or on a future date if requested. The system provides audit and report, attestation and certification, and is accessible 24x7.

Implementation

Since 2012, the Secure Colorado initiative has been the strategic plan for ongoing security improvements, setting the budget and enabling strategic decisions and investments to protect state data. It provided funding for the statewide deployment of Identity Manager and for user licenses. The ability of OIT to manage access for 16 Colorado executive branch agencies along with access into state systems for 64 counties was part of the initial implementation.

The Challenge

After the decision was made to implement an enterprise solution for identity management, the challenge was to help each of the state agencies using the solution understand how it would work with their current processes for requesting accounts, changing access or removing access.

The Training

The solution was rolled out to agencies using a measured approach that provided the opportunity for small groups of staff to receive system training from OIT's Identity and Access Management team and then offer feedback for the next group of trainees. Concerns over system use were allayed through training on the three different user roles. Anxiety over access decisions was relieved through communication explaining that this was a digitization of the paper forms they had been using. Agencies were making the decision over who had access to their systems; Identity Manager was just going to make it easier to make the request.

The first group of trainees was made available to help staff within their agencies as the solution rolled out to larger groups of users. Understanding that not everyone could attend in-person training, a user guide, job aids and short how-to videos to walk a user through the steps for each available function were provided. Identity Manager is very intuitive and user-friendly but we were conscientious to offer diverse training as well as a marketing and communication plan to achieve widespread adoption and utilization across state agencies.

The Success

Release One launched with 16 Active Directory domains integrated into Identity Manager meaning that access to the more than 30 agency applications that use Active Directory authentication could be centrally managed throughout the lifecycle of an employee. Release One integrations also included enterprise Google Workspace which is the state's primary communication and collaboration platform, enterprise Information Technology Service Management system, and the enterprise Customer Service Portal and Project Management. This was immediately followed by the human services line of business applications for Child Care and Child Support. Many other line-of-business applications have already been added to the development roadmap.

Impact

Requesting an account for a new employee, changing access to applications and systems or removing access to accounts for departed employees was previously conducted through processes and tools that varied by agency. The routing and approval processes added to the time that it took to fulfill requests. Many times the demand outweighed our resources which impacted customer satisfaction, created risk and allowed for audit findings around security and access.

Identity Manager standardized the process for requesting new accounts, changing access or removing accounts. It reduces the amount of time for requests to be processed from weeks and days to minutes while reducing the risk for human error by eliminating manual processes. The service has been digitized with manual processes automated and paper forms retired. The solution is now self-service at any time. This is especially valuable when there is a need outside of the Identity & Access Management team hours of Monday through Friday from 7 a.m. to 5 p.m. Since some of the agencies that OIT supports operate 24x7, this is an added value.

Identity Manager has improved the state's security and improved regulatory compliance through reduced audit findings. Account provisioning is based on roles and the concept of least privilege, which further reduces risk by allowing only the minimum system permissions necessary to perform job functions. The ability to immediately disable an account of a departed employee prevents former employees from accessing state data.

Identity Manager is easy to access through a URL and does not require a user to be on the state network or using VPN. So far, the response from our customers has been positive.

What our customers are saying about Identity Manager

- ★ It is SOOOO much faster!!! I LOVE IT!!!! THANK YOU THANK YOU THANK YOU!!!!!
- ★ What I have used has been excellent! Thank you so much for developing this much-needed upgrade.
- ★ Appreciate where this is going and when the applications are integrated, this will be great and provide quicker access.
- ★ You all are so appreciated for doing this. Makes our lives so much easier.
- ★ I used it to offboard employees and that was easy to do.

Future releases

There are currently more than 1,100 OIT managed applications with identity and access needs and Identity Manager integration will be considered for all new application development creating an extensive roadmap for the future of the State of Colorado's centralized identity governance solution.