CASE STUDY

Protecting and monitoring access to a state's systems

A state improves security, efficiency and insight into who accesses which systems by replacing 18 IAM solutions with a comprehensive platform from One Identity

Key Facts

- **Industry**
  State & local government
- **Country**
  United States

Challenges

A state government needed to quickly comply with a new federal mandate that requires it to use a unified framework for identity and access management (IAM) in all its agencies.

Results

- Ensures compliance with federal IAM regulations
- Improves security
- Increases insight and control over IAM — statewide
- Boosts staff efficiency
- Supports needed flexibility in users' profiles and access

Solutions

- Active Roles
- One Identity Manager
- Password Manager
- One Identity Safeguard
- Starling Two-Factor Authentication

To protect citizens' data and improve homeland security, in 2017 the United States government issued the Cybersecurity Executive Order. It outlines new data-protection regulations that include having each state use a consistent framework for identity and access management (IAM) in all its agencies.

To comply with the mandate, one state needed to replace the 18 disparate solutions used by its agencies to govern access for more than 17,000 people — including employees and contractors — with one platform. It had to give administrators a complete view of all users and their privileges. And the state wanted to automate some of the manual workflows that hindered efficiency and introduced risk. Given the complexity of the job and the urgent deployment timeframe, the state engaged third-party IAM expert EST Group for help. Nathan Wiehe, vice president of identity and security services at EST Group, says, "We have a long history of working with state and local organizations. We came in and walked beside staff to understand their specific needs." After doing so, EST Group designed and implemented a comprehensive solution using One Identity technologies.

Statewide user views and flexible controls

Today, from a single dashboard, authorized administrators can instantly see a list of every user who can access any of the state's IT systems or cloud services, regardless of their location or platform. Plus, agency administrators have appropriate insight and control over their users and access privileges. "Creating a central identity repository with One Identity Active Roles provides the foundation for compliance," says Wiehe. It gives administrators a single solution for managing all the users' profiles in all the agencies' Active Directories and Azure Active Directories.

And even though the state replaced 18 solutions with one, it can meet all its extremely diverse IAM requirements. "Agencies are more efficient with the One Identity solution because they have a consistent, flexible framework that supports unique user roles and access privileges across all domains," Wiehe explains.

> **"Creating a central identity repository with One Identity Active Roles provides the foundation for compliance."**
>
> Nathan Wiehe, Vice President of Identity and Security Services, EST Group

Boosting the efficiency of state workers

Today, when an employee or contractor needs to create or reset a password, they can instantly do so from a central portal supported by One Identity Password Manager, instead of contacting the appropriate agency's help desk. The state has also created automated provisioning and deprovisioning processes using One Identity Manager that are triggered by specific changes to user profiles in any of its repositories.

Providing additional layers of security

The state has increased protection for citizens' data as well as sensitive information relating to operations. Having agencies use one IAM solution along with automated workflows ensures consistency and immediacy of action, which is especially important when it comes to system access. Plus, the state can ensure IT administrators have appropriate IT privileges and are complying with regulations by monitoring their profiles and actions via dashboards and automated reports supported by One Identity Safeguard. In addition, One Identity Starling requires people who access sensitive data to enter a unique security code — also known as two-factor authentication — whenever they log into systems.

Resolving risks around supply chains

EST Group also helped the state minimize other risks by establishing a single platform for supply-chain transactions. "The state can now bring in new buying organizations and purchase from them through a single portal that's supported by its One Identity solution, increasing efficiency and improving security," says Wiehe. Commenting on the success of this engagement, he says, "One of the reasons this state enjoyed working with EST Group is that we asked questions like why does this happen and why are you using that process? Asking these kinds of "why" questions made it possible to build a seamless solution that helps this organization effectively overcome its IAM challenges — at every level."

Agencies are more efficient with the One Identity solution because they have a consistent, flexible framework.

Nathan Wiehe, Vice President of Identity and Security Services, EST Group

About EST Group

EST Group is an IT solutions company, with a strong focus in providing integration and consulting services tailored around automating, managing and securing organizations' IT environments. Our goal is for our clients to achieve maximum efficiency and productivity.

About One Identity

One Identity helps organizations get identity and access management (IAM) right. With our unique combination of offerings, including a portfolio of identity governance, access management, privileged management and identity as a service solutions, organizations can achieve their full potential – unimpeded by security, yet safeguarded against threats. Learn more at OneIdentity.com