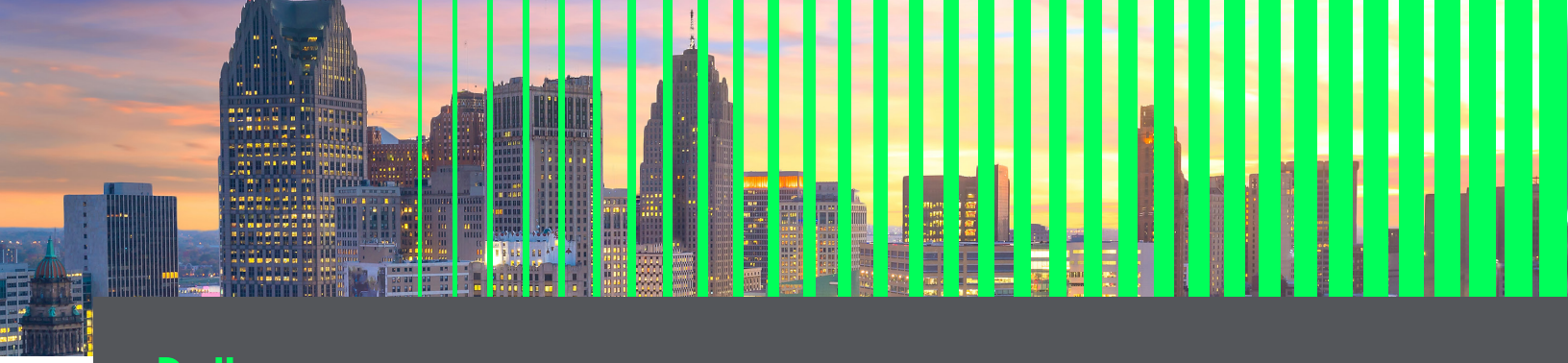

Delinea

STATE OF MICHIGAN **CASE STUDY**

Delinea Zero Trust Privilege Services

Helping the state of Michigan simplify audits, strengthen compliance posture and reduce risk of a breach

Challenges

Within a rapidly-growing heterogeneous server environment, too many users had too much privilege. Lack of visibility resulted in difficulty proving access control compliance for regulations, standards, and policies such as CJIS, CMS, HIPAA and PCI.

In 2012, DTMB was undergoing considerable change. One year earlier, former Gateway, Inc. Chairman Rick Snyder was elected governor of Michigan, and he called for the state's reinvention. Snyder knew that cutting-edge technologies delivered through the DTMB could provide the automation, security, and information accessibility necessary to bring the state into the 21st century.

At the same time, DTMB was busy responding to new security boosting federal regulations. DTMB was required to comply with many government and industry regulations/policies, including Criminal Justice Information Services Security Policy (CJIS, FBI security policy), Centers for Medicare & Medicaid Services (CMS), Health Insurance Portability and Accountability Act (HIPAA), and Payment Card Industry Data Security Standard (PCI -DSS).

With the goal of protecting the people of Michigan from cyberthreats, adhering to federal regulations and industry standards/ policies, as well as defining its role as an active participant in Governor Snyder's statewide reinvention, DTMB turned its focus toward identity management.

Background

The Department of Technology, Management and Budget (DTMB) is an arm of the Michigan State government responsible for the management of technologies for 19 peer agencies and several non-governmental entities.

DTMB

> Upon implementation, Delinea immediately began to solve a number of compliance issues by providing us with three key ingredients: Centralized privileged identity management, granular access controls, and privileged activity auditing."
>
> → Brad Settles, Technical services administrative manager

DTMB initially developed its own homegrown system designed to leverage the native Lightweight Directory Access Protocol (LDAP) client inherent to UNIX and Linux systems, often along with the open source security application sudo (Superuser Do) for managing privilege. But without the ability to manage access centrally and with granularity, audit findings indicated the department was falling short. "Centralized privileged identity management is a requirement of most of the regulations we follow," said Brad Settles, Technical Services Administrative Manager.

The homegrown solution used sudo to manage privilege locally on each system. Native to Linux, the sudo command line allows users to run programs with the security privileges of another user or a root password. This can be convenient in terms of distributing privileges, but can also introduce administrative and security challenges.

"Each system had a separate password file and a separate sudoers file, so each had to be manually updated and managed. This created an enormous challenge," said Peter Manina, IT Specialist and UNIX Systems Architect for the State of Michigan. "And once we incorporated 30-day password expirations — a key requirement of regulatory audits — it got complicated fast."

With sudo, privilege management data is stored locally on each system, which works when there are a limited number of systems. But the need for Medicaid compliance caused the number of Linux systems in scope to increase from 100 to over a thousand in just a few months.

"When we found ourselves managing a thousand servers, there was no way to be sure what was in each sudoers file on every system," said Manina. "We needed to store and manage roles and rights from a central point of control, from which we could provide access to contractors, remove old user IDs, and manage privileges."

> Delinea Zero Trust Privilege Services allowed us to create templates that could be assigned to groups of systems and groups of admins. And that made the whole process of privilege management that much easier – and that much more secure."
>
> → Peter Manina, IT Specialist and UNIX Systems Architect

Solution

DTMB selected Delinea Zero Trust Privilege Services to help meet federal/industry compliance, increase security, and improve audit performance using centralized privileged identity management.

After struggling with its home-grown solution for two years, DTMB reevaluated several commercial options and chose Delinea Zero Trust Privilege Services — delivering one of the critical pillars of Zero Trust Security — based on its ability to help achieve three main goals:

- Implement a model of least privilege across a hybrid environment of Windows and Linux servers to ensure compliance with government/industry regulations.
- Ensure audits pass and the process is simple by implementing the required password expiration, complexity, and privilege escalation mechanisms.
- Reduce the time required to investigate and report on incidents.

While evaluating Delinea Zero Trust Privilege Services, DTMB approached auditors for insight. While they cannot pre-approve solutions, auditors will look at the issues departments are trying to solve and provide perspective on the solutions under consideration. When presented with the Delinea Zero Trust Privilege Services, auditors signaled that the solution would likely help achieve many of their identity management goals, including to give just enough access and privilege across environments.

DTMB was confident that the cloud-ready Delinea Zero Trust Privilege technology would allow it to move away from the less secure sudo approach, ensure that privileges could be managed with granularity, provide time-limited elevation of privileges, and prove what each administrator did or did not do while inside a system.

"Delinea Zero Trust Privilege Services presented us with all the centralized user identity management we'd been trying to build for years," said Settles. "It would allow us to eliminate both the hodgepodge of password files that had existed across the environment and the sudo files that had been usurping IT resource time."

Results

DTMB replaced a less-secure system based on LDAP and sudo, instituting centralized privilege information management with Delinea. Now, DTMB effectively addresses federal/industry compliance and can easily provide identity-related data to auditors upon request.

Delinea Zero Trust Privilege Services met all existing project requisites. It provided a strong foundation for the future, which enabled DTMB to move away from its home-grown, high-maintenance, and less secure privilege management solution and implement a centralized model of least privilege across its Linux and Windows servers. Delinea's sudo migration wizard made it quick and easy to move away from the local sudoer files and adopt a centralized authorization model. It supports multiple user identifiers (UID) and group identifiers (GID), avoiding the typical UID/GID rationalization and normalization via cross-mapping.

> One of the biggest benefits of Delinea Zero Trust Privilege Services is that Delinea maintains all the clients for all the different platforms, allowing us to handle future upgrades, patches or any other changes more efficiently."
>
> → Peter Manina, IT Specialist and UNIX Systems Architect

DTMB is now able to centrally manage user roles and granular privileges across all platforms from Active Directory. Active Directory group policy is also extended to its Linux servers for enhanced management and control. With least privilege access control now ensuring full accountability to individual users, Delinea auditing and session recording can prove exactly what each administrator did during a privileged session.

Both access management and password management were simplified, making provisioning and de-provisioning users, and even revoking specific user privileges, much easier. "I'm an example of an administrator that once had continuous access to 140 servers across our environment," said Manina. "With Delinea, I no longer need blanket access — it takes just minutes to elevate my privilege when necessary. Afterwards, there's a record of everything: access was granted, my privileges were escalated, and my access was terminated. It ultimately protects the State of Michigan."

Delinea simplified the audit process and allows DTMB to comply with all the required federal/industry regulations. "There isn't a regulation that Delinea hasn't helped us to meet. Every time an administrator touches a server, I have a record of it. I can pull up a report, print it, and hand it to the auditor," Manina said. "Delinea's reporting capabilities have simplified the entire

auditing process. Now, we go to Active Directory and say, 'here are the settings for password expiration, password complexity and escalated privileges,' all from one central console."

"Prior to Delinea, if there was an incident we needed to investigate, we'd have to go through syslog and a user's shell history to figure out exactly what happened," continued Manina. "When you've got a system that 20 different admins have access to, it can take days to resolve. With Delinea, we can leverage session recordings to reconstruct the incident and deduce root cause in a matter of minutes."

Implementing the Delinea Zero Trust Privilege Services helped CHAMPS receive special approval from the U.S. government, allowing DTMB to create an alliance with the state of Illinois to execute their Medicaid processing as well. Additional states have since inquired about joining the compact.

Michigan is regularly cited among the top three states in the U.S. for successfully executing IT best practices, and the state boasts several National Association of State Chief Information Officers (NASCIO) awards. DTMB expects that Delinea will assist in continuing Michigan's time-honored tradition of achievement in IT.