Michigan Streamlines Secure Online Services for Citizens

State and local government leaders have a common question: "How can we keep our applications and private data safe?" In the past, the answer has been complicated by the various applications government agencies use — and their differing security measures and requirements.

Today, it's critical to make online security simple for citizens while maintaining strong protections for their private data. In Michigan, the Department of Technology, Management and Budget (DTMB) found an answer to these requirements with the MILogin solution for user identity management.

MILogin emerged from the department's focus on delivering secure online services. "Everything we've done in terms of next-generation digital infrastructure and cybersecurity programs is designed to deliver better services for our 50,000 employees and 9.4 million citizens," says David Behen, former DTMB director and Michigan state CIO. The department provides centralized IT services, including cybersecurity, across the state government.

ELIMINATING THE HEADACHES OF MULTIPLE LOGINS

By creating a MILogin account, users can access many state applications with a single sign-on. For example, by using MiPage — an app for smartphone and tablets developed by DTMB — a citizen gains personalized, secure access to state information and online services, including private data.

As determined by the agency that owns each application, MILogin can use tools such as credentials verified by a third party, strong passwords and multifactor authentication to further protect the user's identity. These tools also help agencies avoid sending password letters or asking users to come into an office to set up their accounts.

The state benefits from the simplicity of managing a single, secure and integrated identity for each user — whether it's a citizen, business owner or state employee. MILogin further improves security by giving DTMB centralized capabilities for access management and fraud prevention across applications and agencies. In the future, MILogin will provide the secure access necessary to allow users to view a state data profile they create, which will hold the information they have on file with Michigan agencies. User can then receive alerts about deadlines, potential eligibility for certain benefits and other useful services.

As Michigan offers more services online, especially through MiPage, citizens will be able to access more of their sensitive and regulated personal data.

CENTRALIZING MANAGEMENT OF USER IDENTITY AND ACCESS

"It was clear that we needed to wrap strong cybersecurity measures around online services to maintain citizen confidence," says Behen. Working with Deloitte, DTMB developers built on the state's already extensive cybersecurity measures to develop the MILogin solution.

MILogin was successful early on due to the Michigan Department of Health and Human Services' (MDHHS) request to manage user identities in a single location. Realizing the potential value for all state agencies, DTMB turned the MDHHS request into an enterprise-wide project.

In collaboration with Deloitte, MILogin is now a single, comprehensive system that centralizes user identity and access management across agencies,

Working with Deloitte, DTMB developers built on Michigan's already extensive cybersecurity measures to develop the MILogin solution, a single, comprehensive system that centralizes user identity and access management across agencies, applications and services.

applications and services. As adoption continues, MILogin can expand the identity components to accommodate more state services with different security requirements.

MILogin is currently deployed in DTMB's on-premises infrastructure, but the state can move to the cloud if it chooses to do so. Funding for development of MILogin was provided in part through a request from the governor's office and by federal funds through the Medicaid program administered by MDHHS.

HIGH LEVELS OF ADOPTION

MILogin has achieved positive adoption rates by both agencies and users. As of late 2016, more than 25,000 state employees and contractors, as well as 45,000 Michigan citizens and 300,000 business entities, have registered for a user account to access 156 state applications from multiple agencies. This count includes approximately 20 Medicaid software applications that contain regulated and highly sensitive personal health information. Once the MI Bridges application — which provides access to MDHHS benefits applications — is behind MILogin, more than 2 million citizens will have access to the solution.

BUILDING A NEW VISION FOR CITIZEN ACCESS TO SERVICES

The broad scope of MILogin is possible in part because the state has centralized its IT functions in DTMB. Another factor has been Gov. Rick Snyder's vision for using technology to deliver a citizen-centric state government.

To support this vision, DTMB was tasked with enhancing its IT infrastructure in four key areas:

✓ Mobility to support easier access to state services and information for citizens, businesses, visitors and state employees
✓ Cloud to provide the modern, flexible infrastructure and tools necessary for IT innovation
✓ Data collaboration to help agencies discover new insights and solutions for problems through data sharing and analytics
✓ Cybersecurity to support a unified user identity while maintaining regulatory compliance and privacy protections

"Our IT infrastructure, including our cybersecurity measures, is designed to take our services to citizens instead of citizens coming to us," says Behen.

EXTENDING CITIZEN-CENTRIC TECHNOLOGY TO OTHER STATES

The MILogin solution is available as a hosted-service offering and Michigan is working with other states to bring the MILogin identity management solution to their constituents. For example, Illinois shares Michigan's Medicaid Management Information System (MMIS). As part of that arrangement, more than 25,000 Medicaid providers in Illinois use MILogin to securely access their state's applications and data.

Cybersecurity on Many Fronts

MILogin is one of several innovative cybersecurity efforts managed in whole or in partnership by Michigan DTMB, which include:

✓ **The Michigan Cyber Civilian Corps (MiC3)**, a volunteer group of cyber professionals who provide rapid assistance to the state for response to cyber incidents

✓ **The Michigan Cyber Range (MCR)**, an unclassified, private cloud network that provides a secure environment for cybersecurity research, education, training and testing; MCR is operated by Merit Network, a regional research and education network that is owned and governed by Michigan's research universities

✓ **Co-located cybersecurity facilities**, operated in partnership with the Michigan State Police and Michigan National Guard, to allow for greater collaboration among partners from the public and private sectors
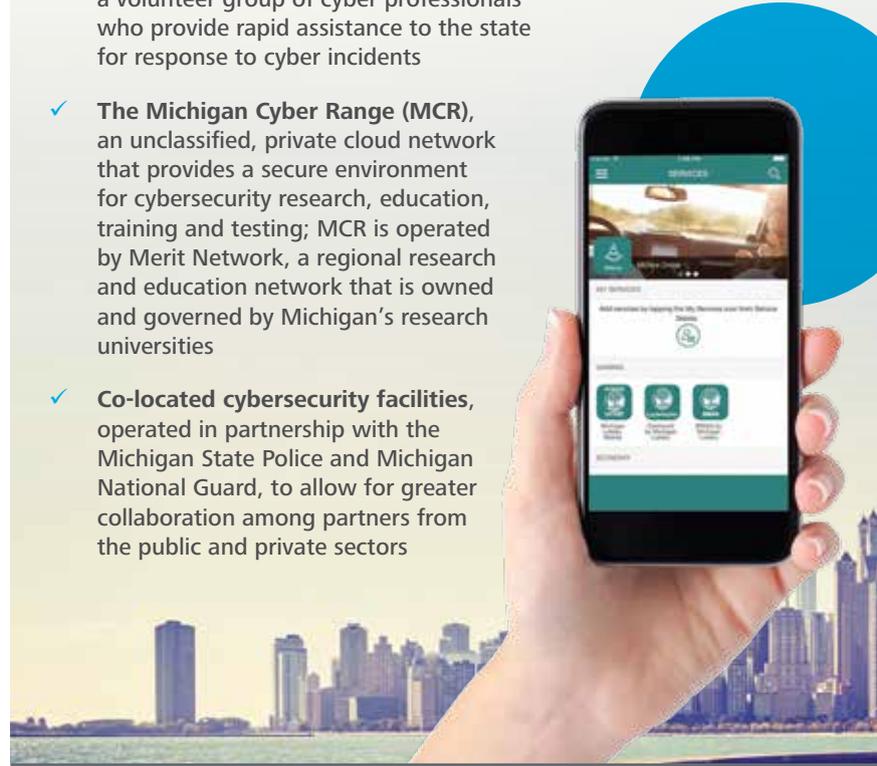
SIMPLER LOGIN WITH STRONGER ACCESS CONTROL

"Citizens expect to use more services online, without hassle but with confidence that their private data is protected by strong authentication," says Mark Ford, Principal, Deloitte & Touche LLP, Cyber Risk Services. "For governments, meeting this expectation is not so easy, given the potentially hundreds of systems — each with their own data, logins and security measures — that are involved in delivering citizen service."

Yet this challenge can be solved with a strategic vision and collaborative execution, as Michigan has found with its MILogin user identity management solution. By delivering the simplicity of a single, verified and optionally authenticated identity for users that is available across applications enterprise wide, MILogin strengthens online security while also improving the state's ability to deliver online services efficiently and effectively.

Sponsored by: **Deloitte.**

To learn more, visit:
www.deloitte.com/us/state