yubico

CASE STUDY

Michigan Office of Child Support

Industry

State and local government

Benefits

Enables Michigan OCS workers statewide to securely access state IT systems while working in the field.

Protocols

Webauthen

Products

YubiKey 5 Series

Deployment info

Accessible to OCS workers across all Michigan counties.

The Michigan Office of Child Support secures and streamlines access to statewide systems with the YubiKey

Promoting the health and success of Michigan's youngest residents

The Michigan Office of Child Support (OCS) is a key division within the Michigan Department of Health and Human Services, dedicated to ensuring that children receive the financial support they need to thrive. Serving over 800,000 children annually, OCS oversees the administration of child support enforcement across the state, working closely with county and state agencies to establish, enforce, and distribute child support payments.

At a glance

- 800,000+ children served annually
- 1,900+ county and state workers

Key results

- Developed a single authentication process for users in 83 counties
- Streamlined, passwordless authentication
- Began the journey to single sign-on

> "I didn't want to introduce something that would take away from what they need to do for Michigan families. We needed to make MFA simple and easy so that they can do their complex work without having to add more friction to their jobs."

Jenny Marlatt | Help Desk manager | Michigan OCS

A need to secure and streamline access to critical systems

The State of Michigan's Office of Child Support (OCS) is a critical lifeline for families because it establishes, enforces, and distributes child support payments throughout the state and helps parents establish a financial partnership through structured child support. In 2023 alone, they provided services for 819,000 children and their families, and collected and distributed $1.04 billion.[1]

From a cybersecurity perspective, OCS faced daunting challenges. The Michigan Child Support Enforcement System, the state's computer system, supports the work of over 1,900 county and state workers in providing child support services. However, each of the state's 83 counties has its own separate IT and security policies, and adding to the complexity, there are people who need to access OCS' applications who are not state employees. However, no matter who the users work for, it is OCS' job to bring all of them together in one secure online "hub of child support."

> "We're talking about 83 potentially different policies and approaches to security. We have to be the big umbrella to make sure that they're complying with what we need to comply with in order to access our applications."
>
> **Jenny Marlatt** | Help Desk manager | Michigan OCS

With such variety in users, policies, and levels of technical expertise, OCS had difficulty ensuring secure, streamlined access to critical systems. That presented a significant threat, as 49% of ransomware attacks in SLTT governments begin with phishing and the use of compromised credentials.[2]

The imperative for multi-factor authentication (MFA)

The catalyst for change was OCS' transition from an on-premises SharePoint platform to a cloud-based solution that required multi-factor authentication (MFA). OCS needed a solution that could accommodate a wide range of needs without overwhelming users.

Enter the State of Michigan's Department of Technology, Management and Budget (DTMB), OCS' liaison for all things technical, with DTMB taking a problem-solving approach on how state agencies think about technology so it can bridge the state and its end users together in the most effective, efficient ways possible.

In this case, DTMB's search for a solution was unique. Many OCS users were unfamiliar with MFA altogether, and some county-managed offices had restrictions on the use of personal devices, which limited the MFA options available to them. There was also a disruption factor, as many users were used to simply opening their browser and starting work—DTMB knew that any extra steps for authentication was going to be jarring. Dean Krispin, a project manager within the State of Michigan's Enterprise Portfolio Management Office which handles IT project management for DTMB, knew that overcoming user mental hurdles was going to be important.

[1] Michigan Department of Health and Human Services, Child Support in Michigan: Facts & Figures

[2] Sophos, The State of Ransomware 2024

> The challenge was dealing with the end user and their adoption in getting them to feel comfortable with at least trying to make a change."
>
> **Dean Krispin** | Project Manager | Michigan DTMB

All of the challenges made the goal crystal clear: implement a multi-factor authentication solution that would work across varying environments and a large user base, that maintains the highest security standards, and also be user-friendly.

Delivering flexible and simplified phishing-resistant MFA

The ideal solution to meet all of these requirements was the YubiKey, a hardware security key that delivers phishing-resistant MFA and passwordless authentication at scale with an optimized user experience. Unlike other options, the YubiKey offers a unique combination of strong security and a simple authentication process that merely involves a simple tap or touch.

Part of DTMB's work is exploring technology options, which is how Krispin first became aware of the YubiKey. He learned that a security group within the DTMB had already granted permission for a few YubiKey pilots, and they decided to add this project to the list.

What came next was a detailed testing and phased rollout process. The OCS Help Desk was the first to test out the YubiKeys. "My role was to play Devil's Advocate," Marlatt explained. "Are we going to be able to teach them how to use it? Is it going to be simple getting it to them? What happens if they're lost?"

Once the YubiKey passed that initial test, OCS opted for YubiKey as a Service, Yubico's enterprise subscription model that provides a lower cost to entry for the highest assurance MFA along with assistance from Yubico's Professional Services Team, along with a dedicated Customer Success Manager and Priority Support. For less than a cup of coffee per user per month, OCS' journey to phishing-resistant MFA had begun.

To simplify and streamline shipping logistics, OCS used YubiEnterprise Delivery, a turnkey delivery service that sends YubiKeys directly to users, at both corporate and residential addresses. Marlatt was able to get instant visibility into inventory and shipments with the YubiEnterprise Console, a dashboard she used "exclusively" during the distribution process to keep track of YubiKey shipment statuses, view purchase order information, and contact customer service. "Sending them out was really easy," said Marlatt.

> Being able to send YubiKeys directly to the users themselves and being able to manage the logistics and management from procurement to distribution was a huge benefit."
>
> **Dean Krispin** | Project Manager | Michigan DTMB

YubiKey rollout best practices for widespread user adoption

To make adoption just as seamless, OCS developed much of its rollout plan from Yubico's documented best practices and insights from their Customer Success Manager. OCS started with an initial activation of internal champions, followed by a rollout to statewide users.

However, only a small portion of OCS' users are managed directly. The others are not required to follow OCS policies, so YubiKeys were offered as an option, not a mandated solution, to those users. To encourage adoption, Marlatt actively engaged with county IT leaders, explained why the shift to phishing-resistant MFA was happening, and how YubiKeys optimized both security and convenience. When she followed up with an email to each county asking how many YubiKeys they wanted, bulk requests began flooding in.

OCS then expanded its communication strategy beyond IT leaders to encompass user education for individual YubiKey users. They hosted a webinar, Q&A and training sessions to help build familiarity. OCS also temporarily stood up Help Desk employees for dedicated YubiKey support, ensuring that users' initial questions were answered quickly.

> "The number one plan was: communicate, communicate, communicate, to gather user feedback and their thoughts. You need to read the room or get the temperature of the people who are going to be dealing with this."
>
> **Jenny Marlatt** | Help Desk manager | Michigan OCS

> "They can basically eliminate how many times they need to reauthenticate and reduce the number of steps that are required. It makes them more efficient without dealing with frustrations or inconveniences of having to log in constantly throughout the day."
>
> **Dean Krispin**
> Project Manager | Michigan DTMB

The phased rollout, coupled with a comprehensive communication strategy and ongoing support from Yubico, led to a smooth and successful implementation, with most counties adopting the YubiKey. Only six counties needed additional assistance, and on the rare occasion help was needed, Yubico's engineers jumped in. "The Engineering support was there when I needed to have them jump on calls with directors," said Krispin. "They were able to walk IT managers through and get them configured for YubiKeys in less than half an hour every time."

Currently, the majority of YubiKey users are county-managed partners. With YubiKeys, these users can access OCS' systems securely, quickly, and easily. It is the first step in OCS' move towards single sign-on (SSO), as the YubiKey provides multi-protocol support for Smart Card/PIV, FIDO2/WebAuthn, FIDO U2F, OTP and OpenPGP on a single key, ensuring maximum protection against phishing attacks.

After the initial rollout, Marlatt used a unique metric to determine how the YubiKeys were received: a lack of complaints.

> "Sometimes not hearing anything is good. What I have heard has been positive—they're using the keys. We've received some thank-yous, specifically from IT staff saying, 'Thank you for helping us,' or small emails, things like that. But I think no news is probably the best news."
>
> **Jenny Marlatt** | Help Desk manager | Michigan OCS

Future-proofing and protecting Michigan's families

As the threats against state and local governments increase in quantity and sophistication, OCS' successful YubiKey implementation has been a significant step forward in securing and streamlining access to critical systems. With this innovative approach the diverse user base of employees and partners can work more efficiently to serve Michigan's children and families. The YubiKey has become a vital tool in OCS's ongoing fight against cyber threats, providing the reliable and scalable solution needed to safeguard both their operations and the sensitive data they manage. The work isn't done yet, though. OCS is already looking ahead to future advancements, and thanks to their work with Yubico, there is a shorter and smoother path to large goals such as single sign-on.

Learn more | yubi.co/customers

yubico