Michigan.gov

Web Application Security Modernization Project

Addressing cybersecurity and operational challenges in Michigan

Award:	National Association of State Chief Information Officers (NASCIO) State IT Recognition Awards
Category:	Cybersecurity
State:	Michigan
Project Start:	March 2024
Project End:	January 2025

Contact: Dodge Howell
State of Michigan
Department of Technology, Management & Budget (DTMB)
HowellD2@Michigan.gov

EXECUTIVE SUMMARY

In March 2024, the State of Michigan (SOM) launched a Web Application Security Modernization Project to address a critical cybersecurity and operational challenge, the need to replace legacy, on-premise Application Security Manager (ASM) appliances with a scalable, modern solution capable of securing Michigan's digital public services across all executive branch agencies. The project, with our partner from Cloudflare, directly supported the Michigan Department of Technology, Management & Budget's (DTMB) four strategic IT initiatives—Cloud Smart, DevSecOps, Digital Experience, and Zero Trust—by enabling cloud-native security, automating policy enforcement, enhancing the user experience with improved service resilience while aligning protections with modern identity, and data-centric access controls.

IDEA

What problems or opportunity does the project address?
Historically, each SOM agency implemented tailored configurations for their external-facing web applications, leading to inconsistent protections, fragmented visibility, and increased risk from sophisticated cyber threats. Moreover, these legacy devices sat inside the network perimeter, allowing potentially malicious traffic to reach internal systems before inspection.

This initiative presented a transformative opportunity for the SOM to implement a cloud-native, enterprise-wide security perimeter aligned with the DTMB's Zero Trust architecture. By filtering and logging traffic at the network edge, the project modernized the state's approach to threat detection, visibility, and mitigation—before any traffic reached internal infrastructure.

Why does it matter?
Cybersecurity is foundational to public trust and service delivery. This initiative delivered a consistent, standards-based application security framework across all agencies while supporting Zero Trust principles such as least-privilege access and pre-perimeter inspection.

Key outcomes include:

- ✓ Centralized security operations: Security controls for over 500 public-facing applications are now managed through a single platform.
- ✓ Consistent policy enforcement: Changes made in one location are automatically propagated across all protected systems, reducing configuration drift.
- ✓ Improved operational efficiency: Eliminates the need for repetitive, manual updates across individual systems or devices.
- ✓ Stronger governance: Enhances visibility, auditability, and control across the entire external-facing application environment. Agency empowerment via read-only dashboards offering real-time visibility into security events.
- ✓ Proactive defense**:** Against DDoS attacks, injection vulnerabilities, and bot traffic through advanced edge-layer protections.
- ✓ Removing legacy vulnerabilities**:** Through standardizing application security statewide, the initiative elevated Michigan's alignment with federal mandates, including NIST 800-207 and CISA Zero Trust guidance, ensuring resilience in the face of increasing public-sector cyber threats.

What makes it different?
What distinguishes this project is its statewide scope, collaborative governance, and cloud-first security architecture. Rather than relying on fragmented, application-level WAF deployments, Michigan implemented a centrally managed, universally enforced security model—benefiting every executive branch agency equally.

The success of this initiative was made possible through the close partnership of:

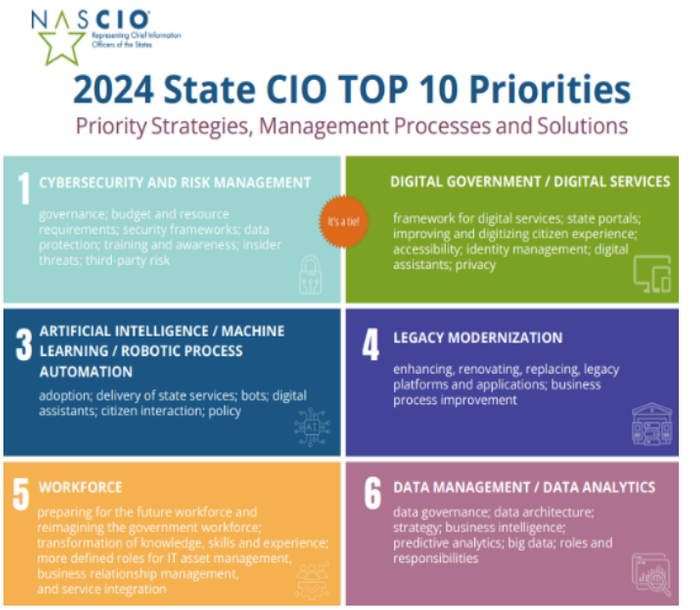
- DTMB's Office of the Chief Technology Officer (OCTO) **-** Led enterprise infrastructure design, traffic management, and Cloudflare integration.
- DTMB Cybersecurity and Infrastructure Protection (CIP) - Authored and enforced enterprise security policies aligned with Zero Trust.
- DTMB Agency Services (AS) **-** Provided project sponsors, coordinated application onboarding, managed stakeholder communications, and ensured agency-level readiness.

Together, these teams drove the development of a repeatable, scalable model for securing public-facing services—establishing Michigan as a national leader in public-sector cybersecurity innovation.

What makes it universal?
Every state faces the same urgent challenges: legacy security tools, inconsistent protections, and growing cyberattack volumes. This initiative directly addresses these issues while advancing several national priorities.

This project directly addressed those universal issues by aligning with multiple national and state-level priorities:

- ✓ NASCIO Priority #1: Cybersecurity and Risk Management
- ✓ NASCIO Priority #2: Digital Government and Services
- ✓ NASCIO Priority #3: Legacy Modernization
- ✓ NASCIO Priority #5: Cloud Services
- ✓ Supports the ongoing adoption of Zero Trust architecture in alignment with CISA guidance and NIST 800-207 Federal Alignment: Meet CISA and NIST Zero Trust guidelines



Additionally, it enhances the citizen experience by delivering customized network-edge error messaging and more transparent support paths during service interruptions. It also simplifies agency operations by eliminating the burden of managing independent WAFs, allowing security to become a shared, managed service. This replicable model empowers other states to modernize their security postures and deliver citizen services more securely, efficiently, and equitably.

IMPLEMENTATION

How does this project fit into an enterprise view and what was the roadmap?
This initiative was executed using an agile, sprint-based delivery model managed by DTMB's Enterprise Portfolio Management Office (EPMO).

The roadmap included:

- Pilot Phase (March 2024): Limited agency rollout to validate DNS, logging, and policy enforcement. Feedback from this phase informed improvements for the broader rollout.
- Phased Onboarding (April – Dec. 2024): Incremental onboarding of agency applications in agile sprints, coordinated through Azure DevOps.
- Optimization & Closeout (Dec. 2024 – Jan. 2025): Final validations, SIEM integration, dashboard access, and project documentation.

Throughout the process, DTMB ensured that Zero Trust-aligned security policies were applied uniformly across all agencies, operations remained uninterrupted, and all stakeholders were consistently engaged through structured governance and communication. This alignment with Zero Trust principles—such as least privilege, continuous validation, and centralized policy enforcement—ensured secure access and visibility without compromising usability or performance.

Who was involved?
This initiative was a coordinated effort involving multiple stakeholders, including:

- OCTO (Infrastructure & Platform Services) - Led the technical implementation, policy enforcement, and dashboard deployment.
- CIP - Developed enterprise WAF policies, ensured alignment with Zero Trust architecture, and managed SIEM integration.
- Agency Services (AS) - Provided project sponsors, coordinated application onboarding, managed stakeholder communications, and ensured agency-level readiness. To support long-term sustainability, they helped define operational ownership model, hand-off procedures, and post-launch support structures, reinforcing a strong governance framework for ongoing maintenance, operations and future scalability. Each agency contributed directly by validating applications, assisting in testing, and facilitating internal coordination—resulting in a collaborative, enterprise-wide delivery approach.
- Center for Share Solutions (CSS), EPMO - Managed timelines, sprint cadence, and enterprise stakeholder alignment.
- Cloudflare - Provided technical expertise, architectural validation, and embedded support.

How did you do it?

- Financial Resources: Leveraged existing DTMB budgets. No additional capital funding was required at the agency level due to collaboration with Agency Services, Cybersecurity and Infrastructure Protection, and Office of the Chief Technology Officer teams.

- Human Resources: Multidisciplinary team including infrastructure engineers, cybersecurity analysts, project managers, and embedded Cloudflare experts.

Timeframe: Delivered in 10 months (March 2024 – January 2025).

Centralized State Technology Agency Coordination:

- OCTO: The core implementation team, under OCTO, played a pivotal role in the design, coordination, and execution of this project. Our team led the technical architecture design, ensuring the new Cloudflare-based solution aligned with the State's Zero Trust principles and met enterprise security, scalability, and availability requirements. We developed onboarding playbooks, created repeatable workflows in Azure DevOps, and established phased deployment strategies that allowed agencies to transition with minimal disruption. OCTO also served as the primary point of coordination between Cloudflare engineers, internal infrastructure teams, and DTMB AS. Our subject matter experts facilitated configuration, troubleshooting, and policy tuning across over 500 applications. Team members who previously managed F5 WAF policies were upskilled to manage the new environment, ensuring continuity and long-term support without requiring additional staffing. This cross-functional approach enabled us to deliver a secure, standardized platform while empowering staff with modern skills and collaborative partnerships.
- CIP: CIP played a critical role in the successful implementation of the Cloudflare project by ensuring that all security controls aligned with the SOM's IT policies, standards, and procedures. From project inception through execution, CIP partnered closely with OCTO and AS to develop and enforce a standardized WAF policy framework that could be applied consistently across all agencies, while allowing for approved exceptions when appropriate. CIP provided expertise in threat modeling, policy validation, exception review, and risk evaluation to ensure that every onboarding phase met both compliance and security expectations. CIP also actively supported change control, governance alignment, and documentation processes to ensure audit readiness and long-term sustainability. By embedding security principles and controls into every aspect of the project, CIP helped advance the state's Zero Trust strategy and reinforced a secure, standardized approach to protecting external-facing applications across the enterprise.
- DTMB AS: Played a pivotal role in the project's success. AS sponsored the initiative through dedicated leadership, aligning agency priorities with enterprise goals. AS staff coordinated implementation efforts across more than 20 departments, ensuring accurate application identification, rigorous testing, and seamless migration. AS also led communication planning and stakeholder engagement—reviewing all messaging for clarity, alignment, and effectiveness. This function was critical in fostering agency buy-in, accelerating adoption, and ensuring statewide consistency.

By partnering closely with OCTO and CIP, AS helped define operational ownership models, establish scalable onboarding processes, and set a strong precedent for future enterprise initiatives.

IMPACT

What did the project make better?
This project transformed Michigan's cybersecurity landscape by implementing a centralized, cloud-native security platform that now protects over 500 public-facing applications.

Key improvements include:

- ✓ Edge-layer defense - All traffic is inspected before reaching internal infrastructure, reducing risk.
- ✓ Unified threat visibility - Centralized log streaming and agency-specific dashboards deliver real-time situational awareness.
- ✓ Consistent policy enforcement - A single set of WAF rules governs all agencies, eliminating variability and reducing management overhead.
- ✓ Enhanced citizen experience - Custom error messages now route users to agency-specific contacts for quicker support.

How do you know?
The project's effectiveness is demonstrated by measurable outcomes:

- ✓ Zero downtime for critical applications during multiple DDoS events mitigated by Cloudflare's automated response.
- ✓ 100% application coverage across agencies for externally accessible services.
- ✓ Full integration with SIEM for real-time alerting and response capabilities.
- ✓ Workforce transformation: Legacy support staff retained and reskilled, maximizing institutional knowledge while modernizing capabilities.
- ✓ This initiative also improved operational confidence, empowering agencies direct visibility into their security posture and threat activity.

What now?
Cloudflare is now a foundational element of Michigan's enterprise security strategy.

- Continued policy refinement in partnership with AS, CIP, and CTO teams.
- Expansion to include new services and applications.
- Ongoing training and onboarding using Azure DevOps.
- Integration with digital government initiatives to support seamless, secure public access.
- To support long-term sustainability, we established repeatable processes and documentation to streamline future migrations and minimize onboarding time for new applications.

Why is this project worthy of the investment?
In addition to modernizing our security infrastructure and aligning with the state's Zero Trust strategy, the implementation of Cloudflare has yielded significant cost avoidance and operational value. By centralizing protections across more than 500 public-facing applications, we've reduced the frequency and impact of cyber threats before they reach internal systems. Over a 30-day period, Cloudflare blocked more than 7.7 million malicious requests and issued 28.5 million security challenges—preventing incidents that would have required staff time, investigation, and potential remediation.

This protection translates into measurable value:

- $600,000/year in avoided incident response costs.
- $90,000/year in staff time saved through centralized policy management.
- $100,000–$260,000/year in avoided staffing costs.
- $125,000/year in deferred infrastructure upgrades.
- $30,000/year in reduced Tier 1 support calls due to improved citizen-facing error handling.
- Total estimated annual value: $945,000 to $1.1 million.

These outcomes demonstrate a strong return on investment, not solely through reduced risk, but also by improving efficiency, reducing operational burden, and supporting a scalable security framework that benefits all state agencies.

- Addressing a mission-critical security need. The project replaced an aging, fragmented WAF framework that left critical systems vulnerable to evolving cyber threats. By migrating to a modern, cloud-based security architecture, the SOM addressed long-standing exposure risks, including outdated policies, inconsistent protections, and traffic inspection gaps behind internal network boundaries.
- Standardizing protections across the enterprise. Prior to this initiative, individual agencies managed security policies inconsistently through local configurations on F5 devices. This project introduced a centralized, uniform WAF policy structure, ensuring that all external-facing applications—more than 500 across multiple agencies—receive the same level of protection, regardless of hosting environment or legacy infrastructure.
- Enhancing operational efficiency and staff capabilities. By transitioning to a cloud-delivered platform, the project significantly reduced the time and technical complexity needed to onboard new applications and apply security policies. Staff now spend less time managing device-specific rulesets and more time analyzing metrics, responding to threats, and improving overall posture. Existing F5 resources were retrained and redeployed, expanding their skillsets without requiring additional personnel.
- Improving the citizen experience. The project enabled the creation of custom error and outage pages, giving citizens timely and accurate information—including which agency to contact—when an application is temporarily unavailable. This replaced generic error messages and reduced citizen frustration, while improving trust and service transparency.
- Supporting federal compliance and Zero Trust adoption. The new environment aligns with federal Zero Trust mandates and cybersecurity frameworks such as NIST 800-207. All external traffic is now filtered through an inspectable, enforceable control point before reaching state infrastructure, closing a major compliance gap that previously allowed unaudited ingress past perimeter routers.
- The project established a repeatable governance and execution model that future-proofs the state's cybersecurity operations and positions Michigan as a leader in digital government transformation. This project created a reusable enterprise-wide model for planning, onboarding, policy governance, and cross-agency coordination. The structure developed—supported by Azure DevOps, EPMO project management, and agency engagement—can be replicated for future cybersecurity initiatives, positioning the state for faster, more agile transformation while strengthening its leadership role in digital government.

In summary, this project exemplifies the power of collaboration, innovation, and strategic alignment in securing Michigan's digital future. Through strong partnerships across DTMB and with agency stakeholders, the state has not only modernized its infrastructure—but strengthened public trust and service delivery in a measurable, sustainable way.