www.misecure.org

2025 MiSecure Legislative Report

Dear Legislators and Stakeholders,

On behalf of the MiSecure partnership, I am pleased to submit the enclosed report detailing the progress and impact of the MiSecure program during the 2024–25 fiscal year.

Authorized under **Section 97g** of the 2023-24 State School Aid Act, MiSecure was established to provide a unified defense against the increasing volume and sophistication of cyber threats targeting Michigan's K-12 infrastructure. I am proud to report that the program has successfully transitioned from a startup phase to a robust, high-impact operation that now protects **98% of Michigan's Intermediate School Districts.**

The attached report highlights several key performance milestones, including:

- **Exceptional ROI:** A **425% return** on the initial legislative investment through unified purchasing power and avoided breach costs.
- **Proactive Defense:** The prevention of **9 major ransomware attacks** that would have otherwise led to school closures and significant financial loss.
- **Equity in Protection:** The successful extension of enterprise-level security to districts of all sizes, ensuring that student data safety is no longer dependent on local budget constraints.

While we have secured Michigan's "digital front door," the threat landscape is evolving rapidly with the rise of AI-driven attacks. We look forward to continuing our work with the Legislature to ensure that our schools remain resilient, our students' data remains private, and our instructional time remains uninterrupted.

Thank you for your continued leadership and support of Michigan's educational community. We are available to meet with you or your staff to discuss the findings of this report in greater detail.

Sincerely,

Jason Mellema
Superintendent
Ingham Intermediate School District

Dr. John Severson
Executive Director
Michigan Association of Intermediate School Administrators

Michael Lilly
Associate Superintendent of IT
Ingham Intermediate School District

Matt McMahon
Director of MiSecure
Michigan Association of Intermediate School Administrators

Tammy Evans
MiCH IT Director
Michigan Association of Intermediate School Administrators

Tom Johnson
Director Michigan Collaboration Hub
Michigan Association of Intermediate School Administrators

Table of Contents

1: Executive Summary: Securing Michigan’s Future

MiSecure: A Whole-of-State Defense for K-12 Education

In 2023, the Michigan Legislature authorized **$9 million** via Section 97g to launch MiSecure—a first-of-its-kind initiative designed to provide a unified cyber defense for every K-12 school in the state. Historically, school districts were forced to defend their digital infrastructure in isolation. Today, MiSecure has fundamentally shifted that landscape from a collection of "vulnerable islands" to a **collective, statewide shield.**

Key Achievements in 2024–25:

- **Rapid Statewide Adoption:** MiSecure has successfully onboarded **98% of Michigan’s ISDs**, protecting over **37,800 devices** (servers and workstations) through a 24/7/365 Security Operations Center (SOC).
- **Direct Threat Mitigation:** The program successfully thwarted **9 major ransomware attempts** that would have paralyzed school operations. In total, over **23,000 automated detections** were recorded and mitigated before they could disrupt the classroom.
- **Massive Financial ROI:** By leveraging "whole-of-state" purchasing power, MiSecure has delivered **$38.3 million in economic impact**—representing a **425% Return on Investment** on the initial legislative funding.

The Challenge Ahead:

While MiSecure has secured Michigan’s "digital front door," attackers are evolving. Cybercriminals are now using AI-driven phishing and targeting third-party software vendors. Our data shows that **67% of incidents** still originate from compromised user accounts, highlighting a critical need to expand our focus toward Identity Management and advanced email security.

MiSecure has proven that when Michigan districts defend as one, they are stronger, more efficient, and more resilient.

> *Our district cannot afford to have someone dedicated to cybersecurity on a daily basis. The service and monitoring provided by our [MDR] implementation and the support from the MiSecure team is invaluable!*
>
> - Cory Jodoin, EUPISD

2: Background & Purpose of MiSecure

2.1 Origins and Legislative Authorization (Section 97g)

Michigan launched MiSecure in 2023 as a transformative initiative to protect K-12 schools from escalating cyber threats. Supported by **$9 million in legislative funding**, MiSecure established the state's first K-12 Security Operations Center (SOC) and deployed Managed Detection and Response (MDR) solutions to safeguard critical infrastructure. This program—driven by a collaboration between the Ingham Intermediate School District, Michigan Educational Technology Leaders (METL), the Michigan Association of Intermediate School Administrators (MAISA), and the leadership of Senator Sarah Anthony and Representative Angela Witwer—represents a vital advancement in educational security.

2.2 Michigan's K-12 Cybersecurity Landscape

Before the MiSecure initiative, districts were forced to defend against cyberattacks independently, with little to no support from peers or the state. While some districts could afford 24/7/365 software to monitor their servers, the financial burden was significant. For smaller districts, implementing these industry-leading solutions was often financially impossible, creating a dangerous gap in the state's security posture.

2.3 The Case for a Statewide Approach

By establishing a unified "whole-of-state" Security Operations Team and providing a consolidated software solution, Michigan now ensures that even the smallest districts are protected against most cyberattacks. Simultaneously, larger districts can now reallocate resources to expand their internal cybersecurity protections. The MiSecure Operations Team serves as a force multiplier for districts, providing expert training, investigative assistance, and post-incident support that complements existing technology departments.

2.4 Vision, Mission, and Goals

The MiSecure project originated in 2018, when ISD technology leaders formed a task force to advocate for cybersecurity best practices and resources. Without the legislative support provided in **Section 97g of the 2023-24 Michigan budget**, the group's ultimate aims would have remained unfulfilled: protecting instructional continuity, ensuring equity across all districts, and improving statewide cyber readiness. Through this strategic funding, these goals are now being demonstrably achieved.

> *This partnership has not only reduced risk but has also provided peace of mind to our staff, students, and families.*
>
> - Rick Webb, Kenowa Hills Public Schools

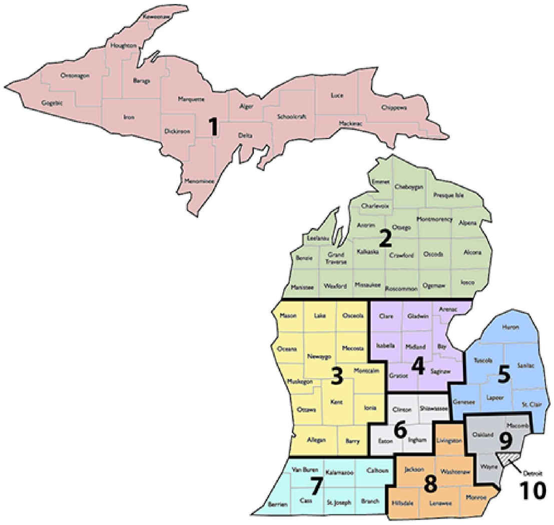
3: Governance & Organizational Structure

3.1 Oversight and Fiscal Management

As the recipient of the Section 97g funds, **Ingham Intermediate School District (ISD)** maintains primary responsibility for the fiscal oversight of MiSecure. To execute the program's statewide mission, Ingham ISD designated the **Michigan Association of Intermediate School Administrators (MAISA)** to establish and manage the MiSecure Operations Team. This partnership ensures that all key deliverables outlined in the legislation are met efficiently. Central to this oversight is the MiSecure Advisory Board, which was established to guide the project's implementation and maintain statewide accountability.

3.2 Advisory Board Composition and Activities

The MiSecure Advisory Board provides a balanced, "whole-of-state" perspective, with representatives from each of the **10 MAISA regions**. This structure ensures that resources and support are distributed equitably across all Michigan districts, regardless of size or location.



To foster a unified defense strategy, the Board integrates expertise from several key state and federal agencies:

- Cybersecurity and Infrastructure Security Agency (CISA)
- Michigan Statewide Educational Network (MiSEN)
- Michigan State Police, Cyber Command Center (MC3)
- Department of Technology, Management and Budget (DTMB)
- Michigan Department of Education (MDE)

This multi-agency collaboration ensures that Michigan's K-12 cybersecurity efforts are aligned with national standards and integrated with state-level emergency response protocols.

Appendix A provides the current list of advisors.

> *As an ISD, our overall security response strategy … relies heavily on MiSecure's active involvement. Their support includes incident response, cybersecurity awareness initiatives, training, and expert consultation, ensuring a comprehensive and resilient security posture across our environment.*
>
> - Uyi Osifo, Kalamazoo RESA

4: Work Project Review

4.1 Review: Year 1, Establishing a Foundation

During its inaugural year, MiSecure established Michigan’s first dedicated K-12 Security Operations Center (SOC) and launched a 24/7 Managed Detection and Response (MDR) service. Onboarding began in May 2024, and by year-end, the program achieved significant milestones:

- **Rapid Adoption:** Onboarded 47 of 56 Intermediate School Districts (84%), protecting over 8,800 workstations and 3,500 servers.
- **Unprecedented Cost Savings:** By leveraging state-level purchasing power, MiSecure negotiated a contract that will save Michigan districts **$5.37 million over three years** compared to independent procurement.
- **Immediate Threat Mitigation:** The system auto-mitigated thousands of detections and successfully halted six major incidents, including:
  - Thwarting a ransomware attack the night before the first day of school.
  - Stopping unauthorized attempts to encrypt district servers.
  - Blocking remote intrusions via brute-force login attempts.

This effort has fostered a statewide cybersecurity community, connecting local schools with the Michigan State Police, DTMB, and federal partners to reduce costs and, most importantly, **minimize lost instructional time.**

4.2 Strategic Objectives for Year 2: Expanding Reach

Building on the foundational success of Year 1, Year 2 focuses on achieving universal ISD participation and ensuring every district has the opportunity to protect their servers through state funding. Key objectives include:

- **Leveraging Purchasing Power:** Extending deep discounts to districts for devices not covered by the initial grant, ensuring comprehensive protection at a fraction of market cost.
- **Deepening Local Partnerships:** Moving beyond software deployment to provide hands-on support. The SOC team conducted statewide "roadshow" work sessions—from Wayne RESA to Marquette-Alger RESA—focused on risk assessments and incident response "tabletop" exercises.
- **Professional Development:** Establishing the SOC as the state's premier K-12 security resource through regular training at major educational conferences (MSBO, MAEDS, MACUL, and MASB).

4.3 Program Enhancements: 2024–25

As districts expand their coverage, the "network effect" of MiSecure strengthens statewide defense. When a threat is identified in one district, the system proactively protects all others.

Successes include:

- **Stopping Stolen Credential Attacks:** In several instances, attackers used valid but stolen credentials to enter a network. MiSecure’s MDR software detected and blocked the subsequent attempts to install malware, stopping the breach before data could be stolen.
- **Emergency Rapid Response:** Onboarding efficiency has been improved from days to minutes. This proved vital for a district that initially opted out of MiSecure but fell victim to ransomware. The SOC team provisioned protection across 90% of their devices within hours, stopping further spread and allowing the district to focus on recovery.
- **Evaluating Specialized Tools:** The Operations Team continues to vet and negotiate pricing for high-need security tools. While these are not currently grant-funded, MiSecure uses its "whole-of-state" bargaining power to make these critical resources affordable for local budgets.

> *The MiSecure [MDR] solution has disrupted multiple critical attacks targeting Wayne County schools. The MiSecure SOC and MDR solution provides tremendous value to our schools*
>
> - Bobby Hodges, Wayne RESA

5: Statewide Participation & Coverage

5.1 Participation by ISDs, Districts, and PSAs

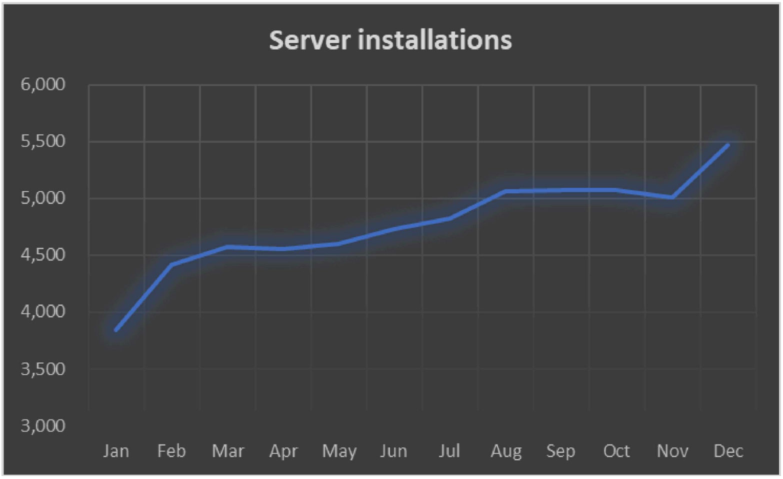
As of December, 2025, MiSecure's adoption has exceeded all projections. Growth in workstation installations increased by **367%**, server deployments reached nearly **90%** of projected levels, and **98% of eligible Intermediate School Districts (ISDs)** are now successfully onboarded.

Every Local Education Agency (LEA) and Public School Academy (PSA) in Michigan is eligible for the MiSecure Managed Detection and Response (MDR) service. While some districts are currently completing existing private contracts, **67% of all local districts** have already transitioned to the MiSecure MDR software, and **100% of districts** now have immediate access to the specialized support of the MiSecure SOC.

5.2 Device and Infrastructure Coverage

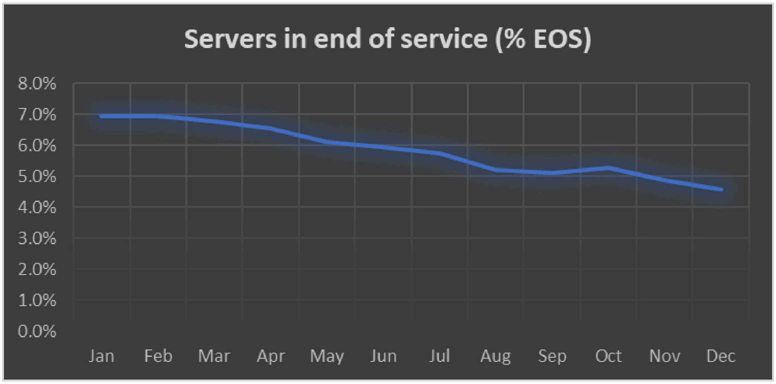
Per the legislative requirements of Section 97g 3(e), MiSecure is charged with distributing MDR licensing to protect "critical technology infrastructure." The program is currently on track to meet its long-term infrastructure goals:

Server Projections: In 2024, MiSecure projected a need for 6,140 server installations. Deployments rose from 3,532 in late 2024 to **5,469 in 2025**. Reaching 100% of the initial projection is expected in 2026 as remaining legacy district licenses expire.



> *A game changer. Having their expertise as part of our team approach has helped safeguard our systems and data.*
>
> - Paul Mulder, Allendale Public Schools

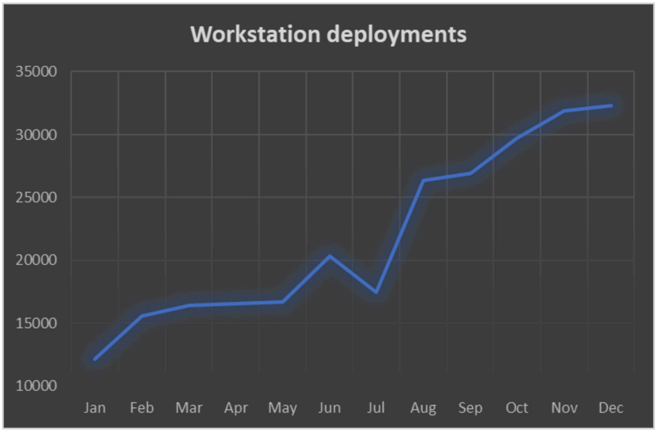
Vulnerability Insight: A major benefit of this coverage is the ability to identify "End-of-Service" (EOS) operating systems. When vendors stop updating software, those servers become easy targets for hackers. MiSecure provides districts the visibility to identify and replace these high-risk systems, demonstrably decreasing the state's overall cyber vulnerability.

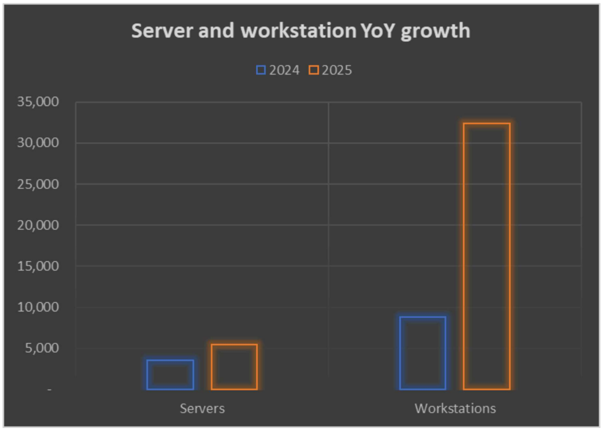


5.3 Workstation Expansion and Cloud Integration

While the primary grant focus was on critical servers, the program has seen an unexpected and rapid expansion into workstations (staff and student devices):

- **Scale of Growth:** Workstation installations jumped from 8,833 in 2024 to **32,354 in 2025**—a 367% increase.
- **The Driver:** This growth is fueled by the unprecedented "whole-of-state" pricing MiSecure negotiated, making high-level protection affordable for local budgets.
- **Strategic Advantage:** Protecting both workstations and servers on a single platform gives the Response Team superior "line of sight" into attacker activity. Often, an attacker enters via a workstation before moving to a server; unified coverage allows MiSecure to stop the threat at the doorstep.





Additionally, MiSecure is evolving alongside other state initiatives like **MiCloud**. As districts migrate from physical data centers to more flexible cloud environments, MiSecure has already adapted to protect **245 cloud-based servers**, a number expected to grow significantly in 2026.

6: Security Operations Center (SOC) Performance

6.1 Threat Trends Observed Across Michigan K-12

The MiSecure SOC analysts provide 24/7 monitoring, investigating alerts generated by the MDR software and supporting districts in both daily operations and emergency response. In 2025, the team managed **18 major cybersecurity incidents**—a 300% increase over the previous year. These incidents included:

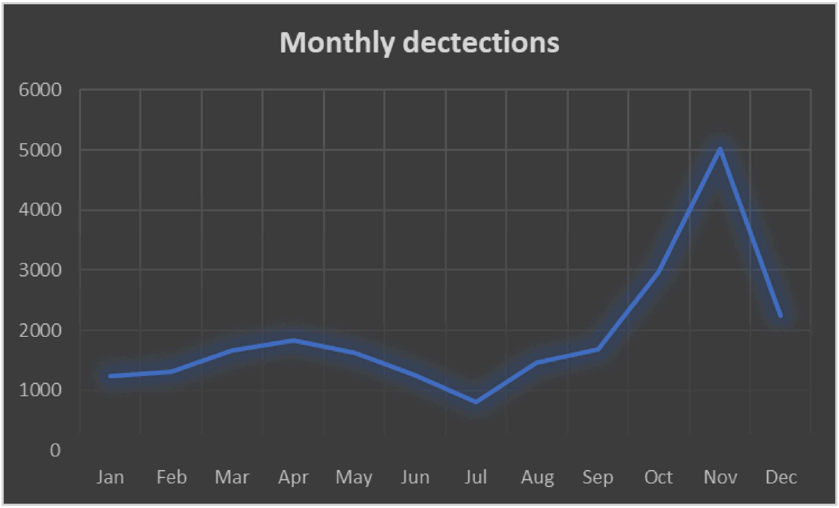
- Ransomware targeting unprotected servers.
- Compromised student and teacher laptops.
- VPN breaches and unauthorized remote access.
- Attempted electronic funds transfer (EFT) fraud.
- Theft of student and faculty personally identifiable information (PII).

6.2 The Anatomy of a Stopped Attack

The tactics of cyber attackers have remained consistent: they primarily use **phishing emails** to steal user credentials. Once an attacker gains access—even through a low-level account—they attempt to "elevate privileges" to gain administrative control and launch a full-scale attack.

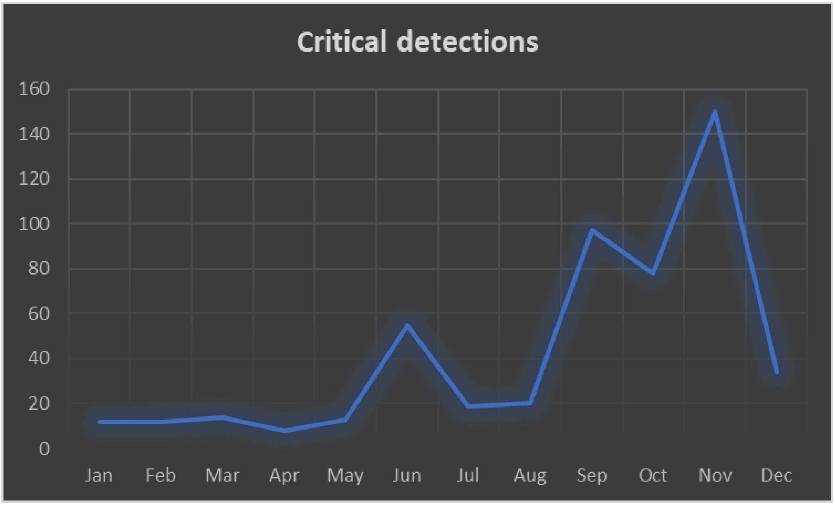
The MiSecure MDR solution is specifically designed to stop attacks at these critical middle stages.

Automated Detections: In 2025, the MDR software detected and mitigated over **23,000 detections**.



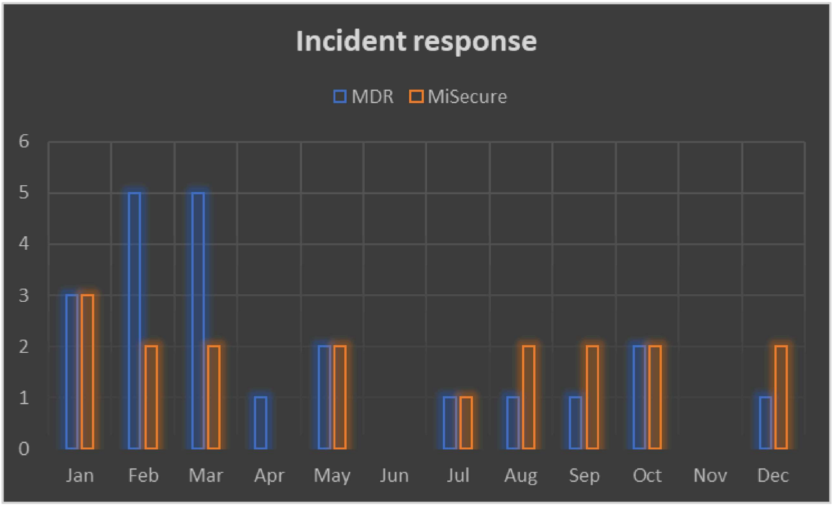
> *The interactive reports make it much easier to remedy vulnerabilities and the detailed reports allow us to dig in deep while also seeing a good top level view.*
> - Robin Paredez, Northview Public Schools

Critical Threat Prevention: Of those detections, **512 were categorized as "Critical."** These represent directed attacks or active "command and control" software that could have resulted in catastrophic system failures or data loss without immediate intervention.



6.3 Incident Response and Prevention

While the vast majority of detections are handled automatically by the software, complex threats require manual intervention by the MiSecure SOC and the MDR response team. In 2025, the team engaged in **40 high-stakes incidents** requiring direct coordination with district IT staff.



The value of this proactive model is clear: without the MiSecure solution, many of these 23,000 detections could have escalated into full-scale breaches. By stopping these threats early, MiSecure has prevented:

1. **Financial Loss:** Halting fraudulent fund transfers and ransom demands.
2. **Data Theft:** Protecting the private records of students and staff.
3. **Instructional Continuity:** Ensuring schools remain open by preventing server lockouts and network outages.

7: Incident Response Highlights

7.1 Overview of Significant Incidents

In 2025, the MiSecure Operations Team monitored thousands of automated detections. While most were resolved by software, the team provided direct, high-level intervention for **18 serious cybersecurity incidents**. The following case studies illustrate the variety, scope, and critical value of these interventions for Michigan's K-12 districts.

7.2 Case Studies: Protecting Michigan Schools

- **Case 1: Halting a 2:00 AM Ransomware Attack**
    - **The Threat:** An attacker used stolen VPN credentials to enter a district network and escalate to an administrator account. At 2:00 AM, the attacker began uploading tools to launch ransomware across the network.
    - **The Response:** The MiSecure software triggered a critical alert. The MDR team immediately isolated nine (9) servers to "contain" the attacker while notifying district staff.
    - **The Outcome:** Every malicious process was stopped. Because of this 24/7 monitoring, there was **zero impact on instruction time**. Without MiSecure, the district would likely have faced a total system lockout and canceled classes.
- **Case 2: On-Site Crisis Support during a Firewall Breach**
    - **The Threat:** An attacker compromised a district's firewall to launch an internal assault. With the local technology lead away on vacation, the district was highly vulnerable.
    - **The Response:** The MiSecure SOC detected the activity and coordinated with the ISD Technology Director. A MiSecure cybersecurity analyst traveled **on-site** to assist with the investigation.
    - **The Outcome:** The team blocked the attacker's access and confirmed no data was stolen. By resolving the issue internally, the district avoided costly cybersecurity insurance claims and restored operations quickly.
- **Case 3: Proactive Intelligence (The PowerSchool Breach)**
    - **The Incident:** When PowerSchool—a major national student information provider—suffered a breach involving sensitive data (Social Security numbers and medical records), Michigan districts were at high risk.
    - **The Response:** MiSecure was informed of suspicious activity in a Michigan district just days before the national public announcement.
    - **The Outcome:** MiSecure issued a statewide alert to Michigan contacts before the vendor's public notice, allowing Michigan schools to secure their systems ahead of the news cycle. (See Appendix B).
- **Case 4: Identifying Financial Fraud (EFT Redirect)**
    - **The Incident:** An attacker used "phishing" to monitor a business official's emails for two months, eventually impersonating a trusted vendor to divert an electronic funds transfer (EFT).
    - **The Outcome:** While the district suffered a financial loss, they partnered with MiSecure to share their story. MiSecure published a detailed forensic report (Appendix C) to educate all other Michigan districts on how to prevent similar "social engineering" attacks.

7.3 Findings & Lessons Learned

The MiSecure SOC team analyzed all 2025 engagements to identify the following strategic trends:

- **The Vulnerability of Identity:** 67% of incidents began with a compromised user account. Over half of these would have been prevented by **Multi-Factor Authentication (MFA)**.
- **The Power of Collective Defense:** In five instances, federal agencies (FBI/CISA) or the Michigan State Police alerted MiSecure to a threat. Having a single statewide SOC ensures these alerts reach local districts instantly rather than getting lost in a chain of command.
- **Preventing Panic:** The team investigated several "dark web" claims where attackers boasted of stealing student data. MiSecure's forensic audits proved these claims were false, saving districts from unnecessary public alarm and legal costs.
- **Independent Validation:** The SOC provided an "independent perspective" for districts investigating suspicious activity, confirming in two cases that suspected breaches were actually false alarms, which allowed IT staff to focus on other priorities.

Conclusion: Without MiSecure, Michigan districts would be left to defend themselves in isolation. This program provides the leadership, 24/7 visibility, and trust-based environment necessary to share intelligence and harden our schools against common enemies.

> *On July 4th of 2025, our district's firewall was breached and [attackers] managed to get to one of our servers. Fortunately, we had [the MDR] client installed on the server and immediately [it] shut all the services down and prevented any further penetrations from taking place.*
>
> *No-one knows how important this really is until it happens. Thank you for your continued support for this initiative.*
>
> - Phillip Stier, Morley Stanwood Community Schools

8. Cost Savings & Economic Impact

8.1 Strategic Licensing Savings

In alignment with Section 97g legislation, MiSecure leveraged Michigan's massive "whole-of-state" purchasing power to negotiate software contracts that were previously unattainable for individual districts.

- **Core MDR Licensing:** By purchasing on behalf of all Michigan K-12 districts, MiSecure secured a three-year contract with a **$5.3 million initial saving**—pricing that represents less than 20% of standard retail costs.
- **Optional Expansion (EDR):** MiSecure further negotiated an **80% discount** for additional endpoint licenses. In 2025 alone, this is estimated to have saved Michigan schools **$12.5 million**, enabling tens of thousands of additional student and staff devices to be protected at a fraction of the market rate.

8.2 Scaling the "Whole-of-State" Model

The MiSecure team is constantly identifying new gaps in the K-12 ecosystem. Since phishing remains the primary entry point for cyberattacks, MiSecure recently negotiated a statewide deal for an industry-leading **email security solution**.

- **90% Market Discount:** Despite not requiring a mandatory purchase, the vendor offered Michigan a roughly 90% discount from retail based on the program's reach.
- **Unified Visibility:** Both the MDR and email security solutions feed into a single dashboard. This allows the MiSecure Operations Team to monitor statewide data in real-time, providing a sanitized, "big-picture" view of threats across all participating districts.

8.3 Cost Avoidance: Preventing High-Impact Incidents

The financial impact of a successful cyberattack extends far beyond the ransom itself; it includes digital forensics, system restoration, and legal fees.

According to the **Sophos "State of Ransomware in Education 2025"** report, the average recovery cost for a K-12 organization following a ransomware attack is **$2.28 million per incident.** Based on forensic reviews, MiSecure directly prevented at least **nine (9) major ransomware attacks** that would have otherwise crippled district operations.

- **Total Avoided Costs:** 9 incidents × $2.28M = **$20.5 million in savings.**

> *As a small district, I am a one man show for 700 students and over 100 staff. It gives us that piece of mind that the servers are being watched so I can focus on just keeping the school operational. Without this software, we would be a juicy steak for one of these bad actors.*
>
> - Michael Suitor, Alcona Community Schools

8.4 Summary: Return on Investment (ROI)

The $9 million legislative investment in MiSecure has yielded a massive financial return for Michigan taxpayers and school districts.

Benefit Category	Estimated Value
Direct Licensing Savings	$5.3 Million
Negotiated District Discounts	$12.5 Million
Avoided Incident Costs (9 Ransomware Blocks)	$20.5 Million
Total Economic Impact	**$38.3 Million**

Bottom Line: For every $1 of legislative funding, MiSecure has returned **over $4.25** in direct savings and cost avoidance—a **425% Return on Investment.**

> *This year our constituent districts saved approximately $26,000 by switching to MiSecure. MAISD, at its renewal in March, will save approximately $20,000 annually by switching to MiSecure.*
>
> *The cost savings will allow MAISD and its constituent districts to further strengthen our cybersecurity posture by investing in other essential cybersecurity products and services.*
>
> - Jeff Fielstra, Muskegon Area Intermediate School District

9: Training, Capacity Building & Outreach

9.1 Strategic Partnerships and "Whole-of-State" Alignment

MiSecure leverages a robust network of state and federal partners to maximize the impact of Section 97g funding. By coordinating with existing organizations, MiSecure ensures a unified defense posture:

- **Federal Funding Advocacy:** Partnering with the **Michigan Department of Education (MDE)** and the **Michigan Statewide Educational Network (MiSEN)**, MiSecure advocates for federal E-Rate funding to offset cybersecurity costs.
- **Law Enforcement Coordination:** Regular briefings with the **Michigan State Police Cyber Command Center (MC3)** allow for the immediate exchange of intelligence on attacker tactics.
- **Insurance Cost Containment:** MiSecure collaborates with major school insurers (**SET SEG and Gallagher**) to ensure that districts utilizing MiSecure MDR maintain coverage and benefit from lower premiums due to their enhanced security posture.
- **Grant Synergy:** MiSecure worked with the federal **State Local Cybersecurity Grant Program (SLCGP)** to ensure that the $9.6M awarded to Michigan can be used to expand MDR licenses, bringing more devices under the MiSecure umbrella.
- **Unified Infrastructure (MiCHIT):** MiSecure operates within the **MiCHIT** ecosystem alongside the Michigan DataHub, MiCloud, and MiSEN. This integration allows MiSecure to protect student data and cloud environments while utilizing shared resources like the central help desk and data-sharing platforms.

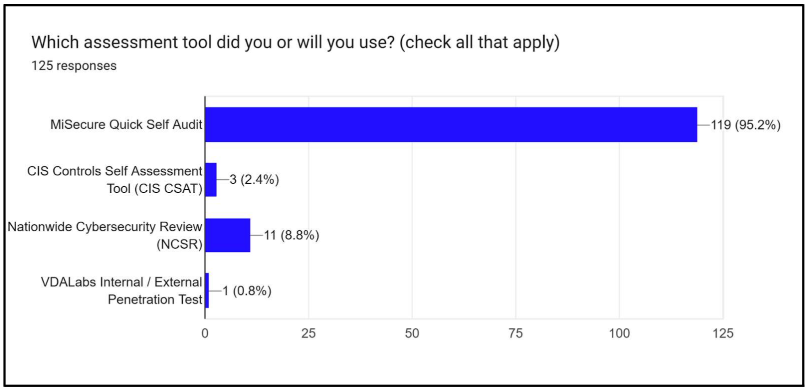
9.2 Network Monitoring and Innovation

Per legislative direction to "install and monitor intrusion detection systems," MiSecure and MiSEN have proposed a project to monitor all network traffic between the statewide educational network and the internet. This initiative will provide a critical layer of defense, identifying threats before they even reach a district's internal network.

9.3 Capacity Building and District Support

To ensure districts are not just "protected" but "prepared," the MiSecure team provides continuous professional development and support tools:

- **Direct Outreach:** The team presented to hundreds of educators through various K-12 professional organizations.
- **Technical Support:** Established a dedicated communications group for weekly security insights, monthly product training, and a comprehensive support wiki.
- **The Quick Self-Audit (QSA):** This tool helps districts evaluate their own readiness. A 2025 survey found that **95% of participating districts** utilized the QSA to guide their security improvements.



9.4 Successes and Challenges

Based on data from district IT leaders, the program has identified clear areas of progress and ongoing needs:

9.4.1 Areas of Significant Improvement

- **MFA Adoption:** Widespread implementation of Multi-Factor Authentication for staff and admin accounts.
- **Resilient Backups:** Transitioning to "immutable" backups that cannot be deleted or encrypted by ransomware.
- **Endpoint Security:** Massive growth in EDR/MDR protection across servers and workstations.
- **Awareness:** Increased frequency of internal "People and Access" conversations among IT staff.

9.4.2 Ongoing Challenges (Year 3 Focus)

- **Administrative Engagement:** Securing dedicated time with leadership to integrate cybersecurity into district-wide planning.
- **Logging & Auditing:** Managing the high cost and technical complexity of long-term data retention for forensic audits.
- **User Behavior:** Overcoming staff resistance to security protocols and addressing training time restraints.
- **Sustainable Funding:** Navigating the lack of dedicated local budgets and the need for ongoing state expertise.

> *This project has provided an incredible value to Marshall Public Schools. It has helped secure our critical data and provide a solid point of confidence for our district and constituents.*
>
> *The provided industry standard … tool, we would not have otherwise been able to afford. This is critical to our security posture now and going forward.*
>
> - Joshua Collins, Marshall Public Schools

10: Program Opportunities

10.1 Addressing Remaining Cybersecurity Gaps

While the deployment of MiSecure MDR provides 24/7/365 peace of mind for protected servers, software alone is not a total solution. Many legacy devices do not support modern MDR software, and sophisticated attackers constantly seek ways to bypass automated alarms.

To identify these hidden vulnerabilities, MiSecure promotes comprehensive **cybersecurity assessments**. These audits consistently reveal critical gaps:

- **Human Factors:** Specialized IT training and general staff awareness.
- **Policy & Governance:** Strengthening password policies and incident response planning.
- **Network Resilience:** Implementing network segmentation and "immutable" backups that are immune to ransomware encryption.

The MiSecure team actively helps districts bridge these gaps through advocacy, education, and the identification of statewide solutions.

10.2 Navigating an Evolving Threat Landscape

As Michigan’s schools harden their defenses, cyber attackers are evolving their tactics. For 2025, the team identified three major shifts:

1. **AI-Enhanced Attacks:** Attackers use Artificial Intelligence to create highly convincing phishing emails and automated hacking scripts.
2. **"Living off the Land":** Instead of using easily detectable malware, attackers now use legitimate system tools to perform malicious actions, making them harder to "catch in the act."
3. **Supply Chain Targets:** Focus has shifted toward the trusted software vendors that schools use daily to gain access to student data (PII).

In response, the MiSecure MDR solution has been upgraded to include **behavioral monitoring** (detecting unusual activity rather than just known viruses) and **SaaS monitoring** to alert districts to vulnerabilities in third-party software.

10.3 Strategic Opportunities for a "Whole-of-State" Approach

The current legislative focus on MDR has been highly successful. However, the next phase of Michigan's cybersecurity maturity requires addressing gaps that fall outside current funding limitations. By leveraging a "whole-of-state" approach, Michigan can achieve significant cost savings and security improvements in:

- **Identity & Access Management:** Securing "who" can log into the network and detecting credential weaknesses and misuse.
- **Email Security:** Blocking AI-generated phishing before it reaches the inbox.
- **Professional Services:** Statewide support for incident response planning and vulnerability scanning.
- **Lifecycle Management:** Centralized patch and vulnerability management to ensure software is always up to date.

10.4 Financial Health and Sustainability

As of the mid-point of this project, **50% of the initial funding remains**, precisely matching our original projections.

These remaining funds are strategically earmarked to:

1. **Extend MDR Coverage:** Maintaining the current shield for at least one additional year.
2. **Enhance Network Security:** Launching new detection services in partnership with MiSEN.
3. **Expand District Support:** Increasing the availability of cybersecurity assessments and improvement plans to help districts move toward a "Zero Trust" environment.

> *I firmly believe the continued support for these services is not only important but absolutely necessary for the short and long term cybersecurity safety of our K12 community.*
>
> - Joshua Hiner, Copper Country ISD and Gogebic Ontonagon ISD

11: Conclusion: A Proven Model for Resilience

The MiSecure program has reached a critical milestone. We have moved beyond the "startup" phase and have established a high-performing, fiscally responsible operations team that serves as a national model for K-12 cybersecurity.

The results of the 2024–25 cycle are clear:

1. **Equity is Being Achieved:** A student's data security no longer depends on their district’s zip code. Small and large districts now enjoy the same "industry-leading" protection.
2. **Taxpayer Dollars are Working Harder:** By centralizing licensing and monitoring, we have saved districts tens of millions of dollars that can now stay in the classroom rather than being lost to cybercrime or high software premiums.
3. **Instructional Continuity is Protected:** Every ransomware attack stopped by MiSecure represents hundreds of hours of saved instructional time and the prevention of catastrophic data theft.

As we look toward Year 3, our priority is to sustain this momentum. We will continue to expand our coverage to the "cloud," harden our defenses against AI-driven threats, and provide districts with the training and assessments they need to stay ahead of the curve.

The investment in MiSecure is not just an investment in IT—it is an investment in the safety, privacy, and future of every student in Michigan.

> *Implementing [the] MDR platform has changed how I sleep at night. Knowing that we have a team of experts monitoring our district 24/7 gives me a peace of mind I didn't have before.*
>
> - John Ross, Taylor School District

Appendices

Appendix A: Advisory Board Roster

Education Advisory Members
Mike Lilly (Chair)
Christopher Hammond
Scott Hartman
Nicholas Hay
Josh Hiner
Bobby Hodges
Dwight Levens
Nick Morse
Brandi Reynolds
Kurt Rheaume
Mark Quaderer
Corey Spade
Michael Coats (MiCloud)
Merri Lynn Colligan (MiSEN)
Tammy Evans (MiCHIT)

Strategic Partner Members
Open (CISA)
Jeff Hoffman (MC3)
Michelle McClish (DTMB)
Joe Polasek (MDE)

Staff
Matt McMahon (Director)
Eric Feldhusen
Mike Schonert
Beth Soggs
Zach Taylor
Diana Urbina

Appendix B: PowerSchool incident report

The MiSecure team has been made aware of a concern detected on a district's on-site PowerSchool servers (we haven't confirmed similar activity on hosted servers yet). On or around 12/22-12/23 the district detected that their PowerSchool servers had been accessed using **valid** support credentials. During that access, at least 2 tables were transferred back by the support user: a teacher table and a student table. This raised concerns by the district since (1) there was no active support case open and therefore no reason for a PowerSchool support technician to use their credentials, (2) the files transferred did not appear to be simple diagnostic data, and (3) at least one of the source IPs was registered to Kiev, Ukraine.

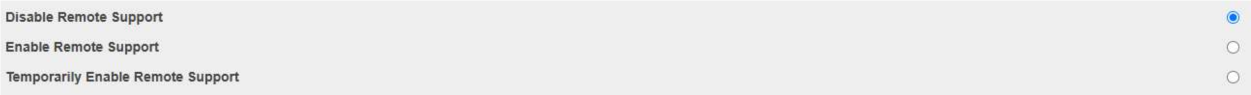
The district investigated other PowerSchool servers and found similar (nearly identical) indicators. They also contacted another district and that district had similar findings. Right now 35 districts have noticed this traffic. We are all hopeful that there is a completely reasonable explanation for this, but based on current evidence, there is concern that sensitive data may have been exfiltrated to a foreign country.

The district has opened a support case with PowerSchool and is awaiting a response. They recommend that any district with similar findings open up a support ticket for each server individually.

MiSecure is recommending that districts only enable remote support as needed:

Review remote support remote access:

1. Log into PowerSchool Admin portal
2. System Management > Security > System Security Settings
3. Ensure "Disable Remote Support" is selected



Disable Remote Support ●
Enable Remote Support ○
Temporarily Enable Remote Support ○

Furthermore, we recommend that districts review their servers for similar activity:

Review currently logged in users. Remote support users seem to stay logged in until the next server restart.

- System Management > Security > Current Users

If you have direct access to your PowerSchool server, review PowerSchool server logs

1. Log into PowerSchool server
2. Navigate to <install path>\PowerSchool\logs\tomcat-oltp
    a. Ps-log-audit.log
        i. Search for the string "supportUser". This indicates attempted access through the remote support feature.
        ii. Search for any other activity in the log from that IP address if found.
    b. Mass-data-import-export.x.log

    i. This log shows any exports done though data export manager and can be matched up with sessions from ps-log-audit.log based on the timestamps

- If you don't have direct access, there are some plugins that allow for viewing historical logins such as PSCB System Administration. You would be looking for any users with type of "Maintenance" (UserType=200 in the Logins table)

IPs Observed:

- 91.218.50.11
- 169.150.203.39
- 137.135.85.33

MiSecure is not alleging that PowerSchool is or has done anything wrong at this time. We are merely passing along a report of a concern from a district and hoping that someone can provide additional information. You can either post to the list or directly to me.

Thank you to the district that shared the information and for providing clear, actionable instructions. Please understand that our team has no first-hand knowledge of the event, nor do we have any significant experience with PowerSchool. Also, no [MDR] events or incidents were recorded during the events since the actions are all “normal.”

Appendix C: EFT misdirect

MiSecure Post-Incident Review

A local school district recently lost money in a fraudulent electronic funds transfer (EFT) after a criminal pretended to be one of the district's trusted vendors.

The incident began in October 2025, when an employee's email account was hacked through a phishing email. Because the account did not have multi-factor authentication (MFA), the attacker was able to get in easily and the employee did not realize their account had been compromised. The attacker quietly stayed in the account for nearly **two months** and logged in more than 200 times.

While reading the employee's emails, the attacker found messages about two vendor payments that were coming due: one for $69,000 and another for more than $200,000. The attacker created a domain that was almost identical to one of the real vendors and used that domain to inject a message into the ongoing email conversation. The message claimed that the vendor had changed bank accounts and asked the district to send the $69,000 payment to the new account.

Because the message used the correct names, dates, and payment amounts, the district believed it was legitimate and completed the transfer. The fraud wasn't discovered until a few days later, when the attacker attempted the same trick with the larger $200,000 payment and the employee became suspicious. IT staff investigated and uncovered the ongoing email compromise.

The district contacted its bank, but too much time had passed to recover the stolen funds. Fortunately, the district had cybersecurity insurance, which reimbursed the loss minus a small deductible. The district also reported the crime to the FBI's Internet Crimes Complaint Center (IC3) and the Michigan State Police Cyber Command Center (MC3).

Recommendations:

1. Strengthen Verification for Electronic Payments

- When sending an EFT to a **new or previously unused bank account**, even for a trusted vendor, confirm the change using a **verified, trusted method**—such as calling the vendor using the phone number already on file (not one provided in the email).
- Review internal procedures to determine **which types of EFTs the district will allow.** Whenever possible, use payment methods that provide enough time to reverse a transfer if fraud is detected.

2. Increase Staff Awareness and Training

- Provide regular training to help staff recognize suspicious emails. This should include checking the **actual sender's email address**, not just the display name, and watching for unusual requests or changes to financial procedures.

- Emphasize that phishing attempts and fake invoices have become significantly more sophisticated, making careful review more important than ever.

3. Recognize the Risks of Compromised Email Accounts

- Make users aware that if an attacker gains access to email or shared documents, they can craft **highly convincing fake messages** using real purchase orders, dates, amounts, and other details. This increases the likelihood that fraudulent requests will appear legitimate.

4. Strengthen Account Security

- Ensure that **multi-factor authentication (MFA)**, passkeys, or other secondary verification methods are enabled on all accounts to protect against phishing and password-based attacks.

5. Monitor for Unusual Account Activity

- Set up systems to detect and alert on unusual login activity, such as logins from unexpected locations or “impossible travel” events (e.g., two distant logins within minutes).
- Use any available security tools to flag anomalies and notify IT staff promptly.

Special thanks to the district and ISD for sharing this information and additional details and suggestions for districts to strengthen their cybersecurity.

Appendix D: SOC Glossary of Terms

CIS: The Center for Internet Security is an independent, nonprofit organization providing cybersecurity leadership to people, businesses and governments through leadership and the support of tools and projects such as CIS Controls® and CIS Benchmarks™.

CISA: The Cybersecurity and Infrastructure Security Agency (CISA) is a component of the United States Department of Homeland Security (DHS) responsible for cybersecurity and infrastructure protection across all levels of government, coordinating cybersecurity programs with U.S. states, and improving the government's cybersecurity protections against private and nation-state hackers.

Cybersecurity detection: Any anomalous activity that occurs in a network or device. Such activity ranges from benign end-user activity to the execution of malicious code. All detections require IT review and sometimes action.

Cybersecurity event: Any occurrence that has the potential to affect the security of a computer or network or the data it processes, stores, or transmits. Not all cybersecurity events lead to a security incident.

Cybersecurity incident: An incident is a specific type of event that negatively impacts the confidentiality, integrity, or availability of networks, devices or data, requiring an organized response.

EDR: Endpoint Detection and Response (EDR) is a cybersecurity tool that records and stores behaviors, and events on endpoints and feeds them into rules-based automated responses and analysis systems. When an anomaly is detected, security teams are alerted for human investigation.

MC3: A division of the Michigan State Police, the Michigan Cyber Command Center (MC3) investigates the criminal aspect of network intrusions for cyber incidents involving Michigan businesses and public entities, including those incidents related to ransomware, phishing, business email compromises (BEC), and malicious insiders.

MDR: Managed Detection and Response (MDR) is a cybersecurity service that combines technology with human expertise to rapidly identify and limit the impact of threats by performing threat hunting, monitoring, and response.

METL: The Michigan Education Technology Leaders are a leadership network within MAISA. Formed in October 2016, METL consists primarily of ISD/ESA/RESA senior technology leaders from across the state. The idea behind METL is how to organize and align collective efforts to work both on issues held in common and also those larger, transformative, statewide, and systemic issues.

SLCGP: The State, Local Cybersecurity Grant Program is a federal funding program intended for state, local, tribal & territorial (SLTT) governmental organizations, such as schools, to improve their cybersecurity efforts.