THREATLOCKER®

X

NILES
COMMUNITY SCHOOLS

Case study

A Zero Trust operating model for modern K-12 security.

Director of Technology Jim Tyler uses ThreatLocker® to enforce strict application behavior, secure teacher laptops, and gain real-time visibility across a resource-constrained school district.

EXECUTIVE SUMMARY:

Industry:
Education
(K-12 public school district)

Location:
Southwest Michigan

ThreatLocker solutions used:
Application Allowlisting, Ringfencing™, Zero Trust Endpoint Firewall, Privileged Access Management, External Storage Device Control, Data Storage Access Control, EDR Real-Time Threat Detection, Managed Detection and Response (MDR).

Outcomes:

- Real-time alerting on risky elevation and account-change activity.
- Malware blocked during onboarding before the district even purchased the product.
- Reduction in teacher risk thanks to controlled application behavior.
- Time-based controls on lateral-movement protocols like RDP and SMB.
- 24/7 MDR response acting as an extension of the small IT team operational slowdowns.

> We wanted to make Zero Trust a foundational principle of our cybersecurity program, and that's where ThreatLocker really came in to help us..
>
> -Director of Technology, Jim Tyler

Niles Community Schools challenges and ThreatLocker® solutions

Challenges	Solutions
Limited cybersecurity staffing and resources.	ThreatLocker Zero Trust controls reduce workload and fill staffing gaps with MDR support.
Persistent phishing and malware threats facing K-12.	Application Allowlisting blocks unapproved code and halts malicious execution.
Teacher laptops vulnerable to risky downloads.	Ringfencing™ restricts applications to defined behaviors and prevents network access abuse.
Privilege creep and unsafe elevation practices.	Elevation Control elevates applications, not users, eliminating broad admin rights.
High-risk lateral movement protocols active on endpoints.	Network Control disables protocols like RDP, SMB, VNC, and Telnet, even on schedules.
Need for immediate help during high-noise or ambiguous events.	Cyber Hero® MDR validates alerts and delivers real-time phone support.

> The challenges we experienced in securing our environment put the whole burden on our team, whereas ThreatLocker can step in and do a better job of that than we can in-house.
>
> -Senior IT Technician, Robert Schuster

REAL-LIFE APPLICATIONS

Onboarding catches malware before purchase.

During the initial rollout using Learning Mode, ThreatLocker surfaced malware activity on a teacher device. The team received the alert, investigated, and neutralized the threat immediately. For Tyler, that early detection during onboarding was a clear proof point that the platform was already reducing risk on day one.

MDR calls at 11 p.m. about a high-risk elevation.

Late on a Monday night, a user was moved into a remote users group, a change that often signals threat actor movement. ThreatLocker MDR called Tyler around 11 p.m. to verify the action. The team quickly confirmed it was a legitimate staff member working late and closed the issue. The incident validated that critical privilege changes were being monitored in real time instead of discovered after the fact.

Service account elevation flagged within 90 seconds.

On another occasion, a service account was intentionally elevated by the IT team. Within roughly a minute and a half, ThreatLocker® MDR called senior technician Robert Schuster to confirm whether the change was expected. The call confirmed the action was legitimate, but it also demonstrated how quickly the district would be notified if a threat actor tried the same move.

Detect and MDR distinguish real threats from internal tools.

Robert Schuster, Niles' senior IT technician, has seen ThreatLocker Detect surface both genuine malicious activity and internal tools that behave like malware. In each case, the team used ThreatLocker telemetry and MDR support to review what happened and decide whether to allow or block the behavior. This combination gave the district new visibility they did not have before and turned ambiguous security events into fast, confident decisions.

About ThreatLocker

ThreatLocker is a global cybersecurity leader helping organizations proactively stop cyberattacks. The ThreatLocker Zero Trust Platform features Allowlisting, Ringfencing™, and Network Control to prevent breaches before they happen, including zero-day attacks, through an allow-by-exception approach that's straightforward to deploy, scale, and manage to keep business operations running uninterrupted. Built for simplicity, scalability, and speed, ThreatLocker security stack reduces complexity, accelerates compliance, and empowers businesses to take control of their cybersecurity—before threats strike. Headquartered in Orlando, Florida with a growing global footprint, ThreatLocker protects millions of networks and endpoints worldwide. Major partners include JetBlue, Heathrow Airport, the Orlando Magic, and the Indianapolis Colts. The company was recently ranked among the top performers on the Inc. 5000 list of fastest-growing private companies.