THREATLOCKER®

X

Case study

Executive summary

Institution: Georgia Military College (GMC)

Industry: Education sector

Location: United States

Interviewees: Matthew Keyes, Robert Johnson

ThreatLocker® solutions used:
Allowlisting, Data Storage Access Control, Ringfencing™, External Storage Device Control, Managed Detection and Response (MDR).

Twice hit by ransomware, Georgia Military College turned to ThreatLocker®.

After repeated ransomware incidents, Georgia Military College (GMC) needed more than detection. With ThreatLocker, they gained control over what could run inside of a complex academic environment and stop unauthorized executions before they could cause damage and disruption.

- K–12 + College + Cadet Corps
- 16,000 students across 8 campuses
- 2 prior ransomware incidents
- Zero Trust enforcement at the endpoint

A different kind of academic environment

Georgia Military College is not a typical school.

It combines a traditional college, a K–12 preparatory school, and a military cadet program within one organization. That means multiple user populations, different operational needs, and a broader attack surface than most academic institutions must manage.

For GMC's IT leaders, the challenge was clear: Keep systems running smoothly for students, staff, and institutional operations in an environment where even a single successful attack could create widespread disruption.

The breaking point: Recovery wasn't enough

GMC had already experienced ransomware once. They had backups and were able to recover without paying. However, the institution still suffered significant disruption.

Then it happened again.

"That was when we said, 'This cannot keep happening.'"
— Matthew Keyes

It was that second incident that changed the conversation. The team changed their focus from a faster recovery to how malicious code could be stopped from running in the first place.

Why traditional security wasn't enough

Before ThreatLocker®, GMC had what was considered a standard enterprise security stack in place: firewalls, antivirus software, XDR, Group Policy Objects, and least-privilege access controls. But these perimeter defenses only went so far, as the team had experienced.

Once something made it inside the network, the real risk began:

- Malware executing on an endpoint
- Ransomware encrypting local and mapped drives
- Unauthorized software running in the environment
- IT teams forced into reactive cleanup

In a world of increasingly convincing phishing attacks, the team knew that sometimes users will click, and when they do, security controls need to assume compromise.

> You have to assume someone will click. Your controls have to account for that.
>
> *Matthew Keyes*

Shifting from detection to Zero Trust control

At first, Zero Trust sounded like just another industry buzzword. But after more research—and more real-world pressure—GMC recognized it as the model they had been missing.

The team wanted fewer alerts and more certainty.

ThreatLocker® delivered that by enforcing Zero Trust directly at the endpoint:

- Only approved applications can run
- Unknown software is blocked by default
- Malicious payloads can land, but they cannot execute
- Control shifts from reactive detection to proactive prevention

> “If ransomware lands on a system today, it simply will not execute.” — Robert Johnson

A framework adapted to GMC’s complex environment

GMC’s environment is comprised of virtual servers with a shared storage infrastructure. During deployment, configuration changes created unexpected storage latency as systems checked in at once.

Instead of treating it like a blocker, GMC worked directly with ThreatLocker team to solve it. Together, they helped shape a delay option that staggered updates across servers, reducing load and preventing performance storms. For GMC, that mattered just as much as the platform itself.

> “They turned it around in about three to four weeks, which is incredibly fast for development work like that.” — Matthew Keyes

ThreatLocker went beyond providing security controls, working with the team to ensure that they are operationally sustainable.

What changed after ThreatLocker

The change came at both the operational and technical levels. The team was able to move with far more certainty and predictability in place than before.

They now know what is running, why it is running, and who approved it. Software requests are easier to manage. MDR support reduces burden on internal staff. And day-to-day security operations are calmer, stronger, and more controlled.

Stronger endpoint control	Only trusted applications can run
Reduced ransomware risk	Malicious payloads are blocked from executing
Less operational stress	Fewer reactive incidents and cleaner approvals
Better team efficiency	MDR support helps manage known applications while internal teams retain control

> “We know what’s running, why it’s running, and who approved it.” — Robert Johnson
>
> “We sleep better.” — Matthew Keyes

How Georgia Military College solved their challenges with ThreatLocker® solutions

Challenge	Solution
Repeated ransomware incidents created operational disruption	Zero Trust enforcement blocked unauthorized execution
Complex environment spanning K–12, college, and cadet corps	Centralized application control across diverse users and systems
Reliance on reactive tools and alert-heavy workflows	Default-deny controls reduced uncertainty and improved response
Risk of phishing-led compromise	ThreatLocker prevented payloads from executing even after user mistakes
Concern about ransomware encrypting local and mapped drives	Application Control stopped untrusted software from running
Heavy admin burden around software approvals	MDR and approval workflows streamlined application management
Highly virtualized infrastructure created deployment complexity	ThreatLocker collaborated with GMC to adapt controls to the environment

From hope to control

Georgia Military College were able to change their security model entirely thanks to ThreatLocker®. Instead of hoping existing tools would catch threats in time, GMC adopted a Zero Trust approach that prevents unauthorized software from running at all.

That shift has made the institution more resilient, more predictable, and better prepared for whatever comes next.

Ready to take control before threats strike? **Watch ThreatLocker in action.** Book a demo

About ThreatLocker

ThreatLocker is a global cybersecurity leader helping organizations proactively stop cyberattacks.

Zero Trust capabilities work to prevent breaches before they happen—including zero-day attacks—through a deny-by-default approach that's surprisingly straightforward to deploy, scale, and manage while keeping business operations running uninterrupted.

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.

> We have gone from hoping our tools will catch attacks to knowing that even if something slips through, it will not be able to run.
>
> *Robert Johnson*