THREATLOCKER®

X

CB TECH

Case study

Executive summary

Interviewee: Ivan Burkett – Director of IT

Company name: GB Tech

Industry and services:
Founded in 1986 by Gale and Jean Burkett, GB Tech is an IT service provider specializing in the aerospace industry. Located directly across the street from NASA, the company delivers software engineering, managed services, and cybersecurity to commercial and local government clients across the United States.

Location: Headquartered in Houston, Texas

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

Outcomes:
ThreatLocker MDR identified and stopped an active breach inside GB Tech's RMM platform, preventing lateral movement, client impact, and potentially catastrophic financial and reputational damage.

Introduction

The breach that wasn't: How the speediness of the ThreatLocker® EDR and MDR solutions averted disaster for GB Tech.

Breaches that operate under the radar, hidden within trusted or forgotten tools, can be amongst the most dangerous. Visibility and human response become just as critical as preventative controls to avoid heavy consequences.

At GB Tech, Director of IT Ivan Burkett experienced this firsthand.

His Tuesday morning began like any other, but then, three minutes before a routine team meeting, he received an unexpected phone call.

"I got a call from the ThreatLocker MDR team. They said, 'We're seeing unusual activity on your server. Is this normal?'... It wasn't."

That call marked the beginning of what could have been a devastating breach.

How the incident unfolded

Almost simultaneously with the MDR call, a client submitted a support ticket asking why a GB Tech employee was accessing their system. The employee that was supposedly accessing a client's system individually was already on GB Tech's internal call.

Something was clearly wrong.

Threat actors had gained access to GB Tech's remote monitoring and management (RMM) platform and triggered a command designed to steal credentials, likely preparing for lateral movement to execute a ransomware attack.

"They were inside our RMM tool, which we use to access our clients' systems remotely," Burkett explained.

No alerts fired from other security tools and no malware was detected. The activity didn't flag up internally...

But it did not pass by the Threatlocker® MDR.

How ThreatLocker EDR helped stop the breach from progressing

ThreatLocker Endpoint Detection and Response (EDR) identified abnormal behavior tied to a trusted process and escalated it to the MDR team.

"ThreatLocker never just calls, so I knew this was serious."

Within minutes, GB Tech and ThreatLocker worked together to isolate the activity and begin an investigation. A four-hour forensic sweep confirmed the breach had been stopped before it could spread.

The root cause traced back to a decade-old configuration oversight.

"We had set up ScreenConnect about ten years ago, when there were just three of us. Everyone has two-factor authentication (2FA) now—except for that original forgotten account. It slipped past us."

That single missed detail nearly opened the door to catastrophic consequences.

A successful attack could have had the ultimate consequence

The compromised RMM account carried administrative access across client systems.

"It could've ended us," Burkett said. "If the attack had launched from there, we could've lost 70% of our client base—millions in recovery costs, lawsuits, and reputational damage. I don't think the business would have survived."

Because ThreatLocker® EDR and MDR detected the activity early and engaged immediately, that outcome was avoided entirely.

Extensive visibility and rapid response save the day

GB Tech had already deployed ThreatLocker Allowlisting, Data Storage Access Control, and Zero Trust Endpoint Firewall. Just months before the incident, the company added MDR to their toolkit.

That decision proved decisive.

"That call proved it was the right move. ThreatLocker doesn't just send an alert—they pick up the phone."

Following the incident, GB Tech began retiring other MDR tools and standardizing on ThreatLocker across both internal and client environments.

"We trust them. We sleep better because of it."

What began as a security incident ultimately boosted internal confidence and validated GB Tech's investment in ThreatLocker to strengthen visibility, awareness, and subsequent response.

"That call proved it was the right move. ThreatLocker doesn't just send an alert—they pick up the phone."

Summary

GB Tech challenges and ThreatLocker® solutions

Challenge	Solution
Attackers operating inside trusted tools and credentials	ThreatLocker Zero Trust policies identify abnormal behavior
Silent breach inside RMM platform	ThreatLocker MDR detects and escalates threats in real time
Risk of lateral movement into client environments	Zero Trust Endpoint Firewall restricts unauthorized access paths
Limited internal resources during critical incidents	The ThreatLocker Cyber Hero® Team acts as an extension of the internal security team

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.