# INSIDE THE BREACH THAT DIDN'T HAPPEN

**When GB Tech's trusted remote monitoring and management (RMM) platform was breached, only one tool caught it: ThreatLocker®. Director of IT Ivan Burkett shares how fast action and real-time managed detection and response (MDR) support saved the business.**

When a security breach happened, Ivan Burkett's quick action with ThreatLocker prevented major damage

When Gale and Jean Burkett founded specialist aerospace provider GB Tech in 1986, they chose a location with symbolic significance: directly across the street from NASA. Even when the Challenger disaster shook the industry, the Burketts' "mission critical" mindset helped build the Houston-based business into what it is today—a trusted provider of software engineering, managed services, and cybersecurity to commercial clients and local governments across the U.S.

Now, Ivan Burkett continues his parents' legacy, overseeing IT and managed services after working alongside them throughout his adult life. Earlier this year, he and his team faced a security breach with potentially catastrophic consequences—and their response became a testament to preparation and quick thinking. A single call from the ThreatLocker MDR team identified and neutralized the threat before it could spread. In this interview, Burkett walks us through what happened and how he and the ThreatLocker team helped avert disaster.

> “The Cyber Hero® team is the best support I’ve experienced; they jump on Zoom with you in minutes. If you’re not ready for that level of visibility and control, you’re not ready for today’s threats

**Can you walk us through what happened the day your RMM tool was breached? How did it unfold?**

It was a Tuesday morning, and we were three minutes from our weekly team meeting. 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. Around the same time, a client submitted a ticket asking why one of our techs was in their system. That tech was on the call with us, so I knew something was wrong. A user had triggered a command to steal credentials, likely prepping for a lateral attack. They were inside our RMM tool, which we use to access our clients’ systems remotely.

**Can you explain what was the cause?**

We had set up a package called ScreenConnect about 10 years ago, when there were just three of us on the IT team. At the time, no one had two-factor-authentication (2FA) or anything similar. We’ve grown to 17 people now, and everybody has 2FA—except for that original forgotten account we used to get ourselves set up. It just slipped past us. I can’t stress the importance of 2FA enough, especially now that this has happened.

**How did ThreatLocker help you to isolate the threat?**

The attack didn’t look like traditional malware. It was a script running under a trusted account. ThreatLocker Detect saw the user’s strange behavior and knew it wasn’t right. The threat actors were accessing servers and workstations, so the MDR team contacted us directly. Keep in mind, ThreatLocker never just calls, so I knew this was important. No other tool we have in place caught it. If it weren’t for MDR, we would’ve missed the window to act. That’s the power of policy-based control and real human oversight.

**What was your first reaction when you found out?**

It could’ve ended us. That RMM account had admin access. If the attack had launched from there, we could’ve lost 70% of our client base—millions in recovery costs, lawsuits, and reputational damage. Honestly, I don’t think the business would have survived.

**What did your team do after the call?**

We immediately jumped into a standup and started investigating. We shut it down and launched a four-hour forensic sweep. Fortunately, the only unlocked device the hackers accessed was actively in use. The user got annoyed, shut off the machine, and unknowingly stopped the breach.

**You were already using ThreatLocker before the incident. When did you add MDR?**

We had been using ThreatLocker for Application Control, Storage Control, and Network Control. Just months before this event, we rolled out their full MDR platform. That call proved it was the right move. ThreatLocker doesn’t just send an alert; they pick up the phone.

**How did the incident reshape your security strategy? And what were the repercussions on your team?**

It confirmed our direction. We’re retiring our other MDR tools and standardizing on ThreatLocker across the board. We’ve already started deploying it to all client environments. We trust them, and we sleep better because of it. Initially, some members of our team found ThreatLocker to be strict, but over time, they recognized its value. Now, some of our engineers are getting ThreatLocker certified. They recommend it to clients without hesitation. That’s a huge change.

**What would you say to other IT leaders who might be evaluating MDR tools?**

Don’t just compare feature lists. Look at accountability. ThreatLocker has real humans behind its alerts to back it up. The Cyber Hero team is the best support I’ve experienced; they jump on Zoom with you in minutes. If you’re not ready for that level of visibility and control, you’re not ready for today’s threats.

**Any final thoughts?**

ThreatLocker saved our business. We were lucky, but it wasn’t a matter of chance. We sleep better, and we’re doubling down on making sure our clients are protected, too.