THREATLOCKER®

X

Case study

ARK Technology Consultants prevents major hospital breach with ThreatLocker®.

Executive summary:

Interviewee:
Hunter Clark

Title:
Cybersecurity Engineer

Company:
ARK Technology Consultants

Industry:
Managed IT and cybersecurity services

Client industry:
Healthcare

Region:
United States

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

Outcomes:

- Blocked unauthorized remote access tool deployment (AnyDesk).
- Prevented ransomware encryption from executing.
- Stopped attackers from leveraging compromised domain admin credentials.
- Enabled hospital to remain fully operational.
- Avoiding catastrophic operational shutdown and patient disruption.

Introduction

ARK Technology Consultant's hospital client was at risk of a full-scale shutdown owing to a ransomware compromise caused by a threat actor using stolen domain administrator credentials.

The attackers identified a critical misconfiguration, gaining access through VPN connections that did not have two-factor authentication enabled. With domain admin credentials in hand, they had some of the highest-level privileges available inside the hospital's environment.

The Cybersecurity Engineer over at ARK, Hunter Clark, knew exactly what was at stake.

"Domain admin credentials are one of the highest privileges you can have in an organization." [The Attacker] having those was potentially very damaging to the hospital."

But this time, the worst-case scenario was avoided thanks to ThreatLocker®.

The initial breach attempt

The first indicator of a breach appeared around 7:30 a.m.

The attackers had already gained access using stolen credentials. Their objective followed a familiar ransomware playbook focusing on data exfiltration to steal sensitive hospital data and then threatening to leak it publicly.

For a hospital, that kind of exposure could have devastating consequences.

ThreatLocker blocks remote access deployment

Once inside the network, the attackers attempted to deploy AnyDesk, a commonly abused remote access tool used by ransomware gangs to maintain control. Thanks to their capabilities through ThreatLocker, ARK Technology was able to stop it immediately.

Unauthorized AnyDesk installation was denied.

"We could see from ThreatLocker...that they tried to run AnyDesk to get it installed on one of the machines, and it got denied."

Without the ability to install remote tooling, the attackers' operational capabilities were severely restricted.

Lateral movement attempts

After being blocked from installing AnyDesk, the attackers moved on to attempting lateral movement within the environment. However, thanks to ThreatLocker® any attempt at running tools like Rclone to begin data exfiltration was blocked owing to pre-existing restrictions in place that prevented them from leveraging Windows systems for broader compromise.

Critically, encryption never occurred, and that made all the difference.

"It was data exfiltration and extortion, as opposed to encryption — which in a lot of ways is a lot better, because it meant the hospital didn't have to shut their doors. They didn't have to turn away patients."

Unlike many ransomware incidents that cripple healthcare facilities, this situation was handled behind the scenes, without any disruption to patient care.

The unexpected confirmation

During ransom negotiations, the attackers revealed something surprising. They admitted that ThreatLocker had directly impacted their operation. In fact, they disclosed that they had encountered ThreatLocker in another organization and were unable to execute their attack as intended. As a result, they pivoted away.

"We saw you have ThreatLocker and realized we couldn't use your Windows machines for our purposes — so we moved on."

Attackers like easy targets, this was proof that the organization's Zero Trust strategy made them anything but.

The attackers were left frustrated thanks to ARK Technology and ThreatLocker

For ARK Technology Consultants, this incident reinforced the wisdom in their decision to deploy Zero Trust controls, especially working in high-risk industries like healthcare.

Because they had used ThreatLocker to deploy proactive protections, their hospital client avoided:

- System-wide encryption
- Patient diversion
- Public operational shutdown
- Catastrophic reputational damage
- Potential regulatory fallout

The hospital remained operational and patient care continued uninterrupted. Instead of becoming another headline about ransomware shutting down healthcare services, the incident became a controlled containment event.

"It was something that could be dealt with quietly and behind the scenes."

ARK Technology Consultant's challenges were matched by ThreatLocker® solutions

Challenge	Solution
Stolen domain admin credentials used to access network.	Ringfencing™ prevented unauthorized software execution.
No 2FA on VPN, allowing credential-based access.	Zero Trust controls limited attacker capabilities post-compromise.
Attempted deployment of remote access tool (AnyDesk).	ThreatLocker blocked the execution through a deny-by-default approach.
Lateral movement attempts within hospital environment.	Ringfencing™ and External Storage Device Control and Data Storage Access Control restricted application behaviors and system communication.
Risk of ransomware encryption and operational shutdown.	Default-deny posture prevented encryption payload execution .
Data exfiltration and extortion attempt.	ThreatLocker visibility enabled rapid detection and containment.
Potential hospital shutdown and patient disruption.	Hospital remained fully operational.

About ARK Technology Consultants

ARK Technology Consultants is a managed IT and cybersecurity provider committed to protecting organizations from modern cyber threats through proactive security strategies and advanced technologies. By implementing Zero Trust controls through ThreatLocker, ARK ensures their clients, especially those in high-risk industries like healthcare, remain resilient against evolving ransomware tactics.

About ThreatLocker®

ThreatLocker is a global leader in Zero Trust cybersecurity that helps organizations prevent cyberattacks through a proactive allow-by-exception approach that's straightforward to deploy, scale, and manage keeping your 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.