THREATLOCKER®

X

Rumberger|Kirk

Case study

# A Zero Trust operating model for modern legal work.

CIO Avi Solomon uses ThreatLocker® to enforce strict application behavior, protect sensitive case data, and gain real time threat visibility.

## EXECUTIVE SUMMARY:

**Industry:**
Legal services

**Location:**
Southeastern United States

**ThreatLocker solutions used:**
Application Control, Ringfencing™, Elevation Control, Storage Control, Detect, Cyber Hero® MDR, Configuration Manager

**Outcomes:**

- Unauthorized code execution blocked across multiple incidents.
- Containment of risky application behavior in real time.
- Minutes-level response during threat events through Detect and MDR.
- Reduced privilege exposure across attorneys, staff, and vendors.
- Stronger control over sensitive legal data without operational slowdowns.

# RumbergerKirk challenges and ThreatLocker® solutions

| Challenges | Solutions |
|---|---|
| Untrusted executables and scripts appearing on endpoints. | Application Allowlisting blocks all unapproved code by default; Learning Mode and default policies simplify approvals. |
| Trusted apps behaving unpredictably or attempting unusual actions. | Ringfencing™ confines applications to approved paths, resources, and interactions. |
| Privilege creep across attorneys, IT, and vendors. | Elevation Control grants elevation to applications, not users. |
| Sensitive legal data vulnerable to misconfigured processes or user error. | Storage Control enforces precise access boundaries. |
| Need for rapid detection and response during ambiguous or high-noise event. | Detect and MDR validate threats and provide immediate guidance. |
| Configuration drift and legacy settings increasing risk. | Configuration Manager enforces strict baseline security settings. |

## REAL-LIFE APPLICATIONS

### Application Allowlisting stops untrusted execution

Solomon runs a deny by default environment. One morning, an attorney tried to launch a utility they had downloaded without approval. ThreatLocker blocked the executable and logged the attempt in the console. No investigation cycle, no cleanup, and no chance for lateral movement.

Solomon describes Application Allowlisting as the foundation of his defensive posture because it stops untrusted code before it can ever run.

### Ringfencing contains a trusted tool behaving badly.

A legitimate application started to access files outside its normal working directories. Ringfencing kept it within its allowed paths, so the application continued to function while the unnecessary access was blocked. For Solomon, this is standard practice. Applications run only within clearly defined boundaries.

### Elevation Control eliminates privilege abuse opportunities.

A vendor needed to run an administrative utility on an attorney workstation. In Solomon's world, no one receives blanket local admin rights. He approved elevation for the specific tool only. The task completed. The environment stayed clean.

This single shift eliminates an entire category of attack surface.

### Storage Control protects high sensitivity case data.

A misconfigured workflow attempted to access protected legal matter directories. Storage Control blocked the action immediately. The system logged the denied attempt, giving Solomon the visibility he needed without exposing the firm to data leakage.

For a legal CIO, this is non-negotiable.

### Detect identifies anomalous behavior during a live issue.

During an otherwise normal day, Detect surfaced a suspicious pattern of child process spawning. Solomon used the telemetry to identify the source, isolate the behavior, and validate that no compromise occurred.

ThreatLocker® Detect adds an additional layer of context above prevention, which Solomon relies on for fast decision making.

### Cyber Hero® MDR provides rapid analyst support.

During a particularly noisy alert sequence, Solomon engaged Managed Detection and Response (MDR) to validate and interpret the event. The team responded within minutes, confirmed the threat level, and guided next steps.

MDR acts as a force multiplier for a CIO managing a distributed legal environment.

# 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.