Case Study: Preventing a Cyber Attack at an Orlando Law Firm

Client Profile (Anonymized)
Industry: Legal / Litigation
Location: Orlando, FL
Size: 25–50 employees
Environment: Cloud-first, hybrid workforce

The Challenge
Indicators of an active cyber intrusion targeting cloud identity and access controls — with zero tolerance for downtime or data exposure.

KIT's Proactive Approach
- Secure cloud configuration & least-privilege access
- AI-driven behavioral threat detection
- Automated response and containment protocols
- Tested disaster recovery and business continuity framework

Metrics Snapshot

Time to Detection	< 6 minutes
Critical Misconfigurations Remediated	11
Downtime Experienced	0 minutes
Data Loss	0%
Post-Incident DR Test Success Rate	100%

Outcome
The attempted attack was neutralized before impact. Business operations continued without interruption, and post-incident simulations further strengthened defenses.

Key Takeaway
With the right architecture, monitoring, and disaster recovery planning, cyber threats become opportunities to improve resilience — not disrupt operations.