Fourth-Party Failure: Fenix24 Recovered Top Law Firm After a Critical SaaS Vendor Was Breached

The Challenge:

A large U.S. law firm depended on a critical SaaS application hosted in a data center that relied on a third-party software vendor. When that fourth-party vendor was compromised in a ransomware attack that impacted hundreds of organizations, the firm's data was encrypted and held for a separate ransom.

While working on the recovery, Fenix24 discovered that while all the other companies in the breach were encrypted as a block, the threat actors had identified the law firm as a high-value target and encrypted them with a different algorithm.

The Solution:

As a result of this breach, the law firm engaged Fenix24 to perform a Ransomware Backup and Resiliency Assessment (RBRA) with an expanded scope to evaluate the firm's most critical SaaS databases.

This exhaustive review uncovered a serious vulnerability: one of the firm's most important business applications was not being backed up at all. Worse, there was no technical way to back that data up outside of the provider. Based on these findings, the law firm committed to migrating away from that application to one that enabled external backups of critical data so they weren't dependent solely on the SaaS provider.

The Outcome:

In 2024, the firm purchased Grypho5 Managed Backups and began migrating to a new, more resilient application. Data volume increased significantly in 2025 as the migration continues, enabling the firm to build an assured recoverability model with control over its own backup architecture independent of any single SaaS provider.

What began as a vendor-driven crisis became an opportunity to build long-term resilience. Fenix24 turned disruption into assurance, enabling the firm to protect its data, clients, and reputation.