CASE STUDY

MOXFIVE

Healthcare Ransomware Response:

50% Ransom Reduction, 650K Files Restored

The Situation

Growing by acquisition comes with a cost that rarely shows up on the balance sheet. For this healthcare group, years of M&A activity had built a sprawling, multi-entity operation with a distributed infrastructure that served the business well. Yet, building a company through acquisition is a little like renovating a house while people are living in it. Things get patched, systems get inherited, and somewhere in the shuffle, details fall through.

For this organization, that detail was three servers: file transfer, SFTP, and remote access. Endpoint protection covered most of the environment, the standard toolkit for a company of their size and complexity. But these three hosts had never made it onto the coverage map. No EDR and no firewall, meant no visibility. In the healthcare sector, where sensitive patient data and regulatory obligations compound every breach, that kind of quiet gap tends to stay quiet right up until it doesn't. The Anubis ransomware group found it first. Compounding this challenge were several simultaneous crises:

- Encrypted systems halting business functions across the enterprise
- A ransom demand requiring immediate strategic decision-making under extreme pressure
- 800 GB of potentially exfiltrated sensitive data reviewed, including database files containing PII and PHI.
- Regulatory notification obligations under HIPAA and applicable state breach notification laws, with clocks already running
- A legally defensible forensic investigation needed to determine what happened, what data was accessed, and who needed to be notified

RESULTS

50% ransom reduction negotiated

650,000 files restored to production

3.75 TB of data recovered

5 MOXFIVE service lines deployed

The MOXFIVE Response

MOXFIVE deployed five service lines within 24 hours of the intake call. One firm with ownership of every workstream, with no handoffs and no subsequent context loss.

- **Ransomware Negotiations:** With prior Anubis experience on the team, MOXFIVE was able to secure approximately a 50% reduction from the initial ransom demand. The decryption tool was secured following payment, enabling immediate recovery operations to begin.

- **Investigation**: The full timeline of attacker activity was reconstructed from initial access through lateral movement and exfiltration. Three servers were identified as primary breach vectors, all without EDR or firewall coverage. Ultimately, hundreds of gigabytes of data were confirmed as potentially exfiltrated, and a VPN anomaly was flagged and investigated. The full forensic report and executive summary were delivered to the organization's breach counsel

- **Restoration & Recovery:** MOXFIVE managed these efforts, restoring from DR to production 650,000 files totaling 3.75 TB.

- **Data Mining:** The hundreds of gigabytes exfiltrated from three unprotected servers created a notification obligation that required precision. As part of the project, MOXFIVE oversaw programmatic search and manual review of the full in-scope dataset, identifying PII and PHI scope, and determining the notification population. Findings were delivered to the heathcare firm's breach counsel with chain of custody intact and HIPAA obligations supported.

- **Proactive Resilience:** While the forensic investigation had already conducted the diagnostic work, what followed was a prioritized roadmap with specific recommendations tied directly to the failure points the investigation surfaced, including rationalizing M&A-inherited environments, addressing architecture gaps, and building proactive monitoring across previously uncovered hosts.

Results

In addition to 50% off the initial ransom demand, the decryption tool was secured and recovery began without delay. By the time the restoration workstream closed, 650,000 files totaling 3.75 TB had moved from the disaster recovery site back into production. The exfiltrated dataset had been reviewed in full, PII and PHI scope confirmed, and the notification population identified with enough precision to satisfy HIPAA and applicable state obligations. Approximately 50 critically defined systems were restored within seven workdays, and a legally defensible forensic report and executive summary were in breach counsel's hands.

Why MOXFIVE

Most post-breach assessments start with a framework. This one started with evidence. The three unprotected servers at the center of this incident weren't identified through a compliance checklist or a theoretical risk model. They were identified because MOXFIVE's forensic team reconstructed exactly what the attacker did and traced it back to its source. That distinction matters when the findings have to hold up in front of breach counsel, a carrier, and a regulator simultaneously.

The structure of the engagement mattered as much as the findings. Negotiations, forensics, restoration, data mining, and resilience planning ran concurrently, under unified leadership, from the same incident data. The resilience recommendations that followed were built on the same forensic foundation, providing a prioritized set of changes derived from what the breach actually revealed about the environment. That's a different kind of advice, and it comes from a different kind of relationship with data.

www.moxfive.com
(833) 568-6695
info@moxfive.com