CASE STUDY

Healthcare Organization Recovers from Ransomware & Builds a Future-Ready IT Environment

AT A GLANCE:

CUSTOMER CHALLENGES

- Legacy systems and outdated security tools
- Ransomware attack via third-party VPN exploit
- No EDR/MDR or MFA in place
- Full domain compromise and operational downtime

OMEGA SOLUTIONS

- Rapid ransomware containment and recovery
- Deployed next-gen endpoint protection and AMTD
- Rebuilt and segmented network infrastructure
- Migrated to Omega's SOC 2 certified private cloud
- Implemented HIPAA-aligned security controls

OUTCOMES & BENEFITS

- Core operations stabilized within 2–3 weeks
- Full IT modernization in under 2 months
- 24×7 IT support, MDR, and vCISO oversight
- Stable, compliant, and future-ready IT environment

DISCLAIMER

This case study has been anonymized at the customer's request to protect the privacy and security of the healthcare organization involved. Certain details have been modified or omitted in accordance with HIPAA and other applicable privacy and security regulations, due to the sensitive nature of the incident and to maintain compliance with confidentiality obligations.

In today's sophisticated cyber landscape, organizations can face devastating consequences if legacy systems and outdated practices are left unchecked. Ransomware, in particular, continues to be one of the most damaging threats to healthcare providers, where **data shows downtime can directly impact patient care**.

This case study highlights how Omega Systems responded to a critical ransomware attack against a mid-sized healthcare organization and helped the customer not only contain the breach and recover essential systems but ultimately modernize their IT infrastructure into a resilient, future-ready environment.

The Challenge: Ransomware Penetrates Legacy Infrastructure

A healthcare organization with approximately 160 users faced a critical cybersecurity incident early in 2024. At the time, their reliance on Omega Systems for security support was limited. The organization experienced a ransomware attack after a third-party vendor's VPN access was exploited by a threat actor. The attack led to the exfiltration of domain keys and complete control over the organization's [Windows based] systems, limiting some of the organization's operations.

The Solution: Rapid Response & Complete Modernization

Upon receiving Security Incident and Event Management (SIEM) alerts, Omega's team quickly identified the nature of the threat and immediately engaged with the customer to contain the breach. They equipped the organization with robust endpoint security tools, including next-generation automated moving target defense (AMTD) capabilities, which helped stop any further spread of the ransomware. After determining the attack's origin and scope, Omega's Security Operations Center (SOC) spent several days containing the threat.

To rebuild the operational environment, Omega repurposed existing servers from an ongoing project, helping the customer to avoid immediate capital outlays for new hardware. The repurposed servers were used to establish new domain controllers, and Omega implemented a segmented network and sanitized the impacted servers in the ensuing days and weeks. During this period, Omega coordinated closely with the customer's legal counsel and various stakeholders, including software vendors and internal IT teams, to ensure alignment and effective communication.

Understanding the need for modernization, Omega recommended the customer move its infrastructure permanently to Omega's secure, SOC 2 certified data center, integrating additional advanced security measures such as private cloud storage, HIPAA compliant controls, comprehensive threat detection & response, multi-factor authentication, zero trust architecture, and 24×7 IT support.

"When the SIEM alerts came through, our priority was immediate containment. Within hours, we had new defenses in place and were working side by side with the customer's IT and legal teams to stop the spread and begin recovery. Our goal wasn't just to restore operations, but to ensure the customer came out of this event stronger and better protected than before."

— Omega Systems' Incident Response Team Lead

The Outcome: Stability, Security & Ongoing Partnership

Through Omega Systems' intervention, the healthcare organization gradually resumed limited operations within 2-3 weeks. Due to the extensive nature of the ransomware threat, the complete restoration and modernization process took close to two months. In the end, Omega's collaborative approach ensured the organization reemerged with a stable, efficient, and secure IT environment.

"The Omega team was invaluable during one of the most challenging times in our organization's history. When the attack hit, our backs were immediately up against the wall, but Omega stepped in immediately to take control and made sure we understood what was happening every step of the way. They helped us recover, but more importantly, they gave us the tools and support we needed to feel secure moving forward."

— Grateful Healthcare Customer Post-Security Incident

Post-incident, the organization transformed its IT infrastructure, maintaining an internal IT function focused on application management while relying on Omega for day-to-day IT support, managed security services, and ongoing advisory. Regular technical business reviews (TBRs) helped continually improve the environment's stability and security in the subsequent months.

Today, the organization benefits from a modernized IT infrastructure and robust security framework, allowing them to focus on expanding their healthcare business while ensuring compliance and operational efficiency.

Ready to achieve similar results?

Let's Connect: **omegasystemscorp.com** | connect@omegasystemscorp.com