

Case Study: Healthcare

Healthcare System Strengthens Security by Outsourcing Monitoring and Management

The Situation

The customer is a premier healthcare provider in the southeast U.S. Its network of leading edge facilities includes multiple acute-care hospitals and 120-plus outpatient clinics. Its nearly 3,000 doctors and over 11,000 employees, who constitute the largest medical staff of any healthcare system in the region, see several million patients each year.

Despite its size, however, the customer had a small IT team that lacked security expertise. It had minimal security measures in place and barely met HIPAA mandates to safeguard patients' data and records. To rectify this, it tasked a new Chief Information Security Officer (CISO) with building a robust security program.

The CISO understood that effective security starts with awareness of all activities on the enterprise network. **To obtain such visibility, the healthcare provider needed a security information and event management (SIEM) platform to aggregate logs and monitor processes.** Yet the CISO was unable to justify the investment without security professionals to install and calibrate the system, and then operate it around the clock. Absent this expertise, the provider could not analyze alerts, conduct investigations or garner full value from the solution.

The Solution

The CISO turned to its trusted reseller, Sayers. Sayers was able to offer HP ArcSight to the customer for a SIEM solution, but it lacked a security practice to deploy and administer the platform. To enable the sale and meet its client's need, Sayers partnered with ReliaQuest for its co-monitoring and co-management services. The reseller would continue to own and oversee the account while selling it ArcSight and earning recurring revenues from ReliaQuest's ongoing services. Moreover, the healthcare provider would keep ownership and control of its security systems. For added safety, ReliaQuest can remotely manage the SIEM without requiring logs or

→ **INDUSTRY:**
Healthcare

→ **SOLUTION:**
Co-Managed I

Benefits of Co-Man

- Advanced KPI rep
a proven track rec
value to your C-S
- Advanced Threat
integration capab
- Allows your team
key security prior
- An available team
engineers, and co
supporting your i
time
- Mitigates the risk



management team assessed the customer's environment, identified all the components that would feed into the SIEM, and conducted the necessary testing. It worked with Sayers and the customer to provide an accurate bill of materials for the ArcSight purchase and to schedule the implementation.

The ReliaQuest team then installed the ArcSight platform and optimized it for the customer's environment and security requirements. It also trained the customer's IT staff to utilize the SIEM and processes to escalate and investigate alerts. It identified, for example, who on the staff would receive critical alerts from ReliaQuest once the system was operating.

The ReliaQuest team put the SIEM solution into production and fine-tuned it further. **Today, ReliaQuest continuously monitors and co-manages the solution from its security operations centers. Its engineers immediately notify the customer's staff of potential issues and threats, and every week, the partners and the customer confer to review the prior week's events.** The ongoing communications ensure a productive collaboration.

Business Benefits

The ReliaQuest/Sayers partnership successfully deployed a sophisticated security solution. Without the alliance, the customer would have required months to certify ReliaQuest as a vendor or would have turned to a one-size-fits-all MSSP without purchasing ArcSight from Sayers. Instead, **Sayers closed a deal that it otherwise would have had to forgo and enjoys substantial margins from ReliaQuest's co-management services.** Sayers delivered the security expertise that its customer needed while maintaining ownership of the account.

With ReliaQuest's expertise, the customer, even with its modest IT staff, fully leverages its ArcSight technology, ensuring a strong return on investment. The CISO laid the foundation for a vigorous security program with enterprise-wide visibility into questionable, networked activities and processes. The provider now has the

Solution: Co-Mana

Key Takeaways

- A successful Arc deployment that the customer's e security needs
- Ongoing ArcSig and monitoring security enginee
- Data and log file the customer's e