

CASE STUDY

Ntirety Secures a Leading Healthcare Provider's IT Infrastructure - Meeting HITRUST Requirements

LEADING HEALTHCARE PROVIDER CHOOSES NTIRETY TO SECURE INFRASTRUCTURE FOR PROTECTED HEALTH INFORMATION, MEET HITRUST CERTIFICATION REQUIREMENTS



OVERVIEW

This leading healthcare provider focuses on providing comprehensive and preventative care to the most vulnerable populations in the United States. Since 2000, they have enabled the treatment of thousands of chronically ill patients through innovative health management tools.

The healthcare provider works with insurance providers to find specific individuals in need of their services and, as a result, are responsible for a large amount of Protected Health Information (PHI). To safely store this data in their warehouse and properly process the information, it's essential for the healthcare provider to guard against potential threats.

COMPANY TYPE:

Healthcare Provider

INDUSTRY:

Healthcare

SOLUTIONS:

Endpoint Detection and Response (XDR), Disaster Recovery (DR), Compliance as a Service (CaaS), Security Operations Center as a Service (SOCaaS), Network Operations Center as a Service (NOCaaS), Infrastructure as a Service (IaaS), and Database Administration as a Service (DBaaS)

CHALLENGE

The healthcare provider was growing, and in 2016 decided it would be best to reduce reliance on their own dated technology stacks by starting with a clean slate. Previous vendors they'd used lacked the database management and architecture expertise needed to manage the large amount of information the healthcare provider was responsible for. Cybersecurity was being handled by multiple partners, which increased cost, risk, and complexity.

The company utilized Virtual Desktop Infrastructure (VDI) services from another vendor but struggled with performance issues. VDI is important, as the healthcare provider has several applications that require desktops to be on the same Local Area Network (LAN) as their servers located in data centers. Thus, a functioning VDI was a requirement for the business to operate. The healthcare provider's previous vendor also failed to offer the proper level of transparency for managed security functions including logging, monitoring, and alerting. They were unable to confidently present evidence of strong security practices to assessors and auditors.

Since the healthcare provider works with large health insurance companies, an often-overlooked part of business operations is data management. To deliver quality patient-facing programs and associated technologies, data is needed to provide a solid return on investment (ROI). As a result, the healthcare provider needs to analyze vast amounts of Protected Health Information (PHI) for payers routinely - data which needs to be securely stored. This meant that the healthcare provider also needed HITRUST certification. Two years after rebuilding their IT infrastructure, the provider achieved that goal. However, additional HITRUST requirements with a higher level of compliance were added in the coming years. The provider had matured to the point where they needed to be able to scale faster, securely, to address expanding requirements related to their rapid business growth (increased staff, increased PHI data, growing compliance requirements).



SOLUTION

This healthcare provider turned to their trusted technology supplier to find the best, multi-faceted solution to their infrastructure and security needs. Their technology supplier surveyed the marketplace, and after a comprehensive selection process the healthcare provider signed the contract with Ntirety in 2020. The Ntirety solution encompassed the following:

Ntirety's database offering, with the ability to manage the provider's data warehouse while handling security in a comprehensive manner, clearly separated Ntirety from the competition. Ntirety was able to provide a complete and transparent solution that gave the provider confidence.

Ntirety's VDI fulfilled the provider's needs to properly execute business tasks. Ntirety's Endpoint Detection and Response (XDR) provided detection and protection for the business from malware. Ntirety's Disaster Recovery services additionally safeguarded the healthcare provider against attacks and downtime.

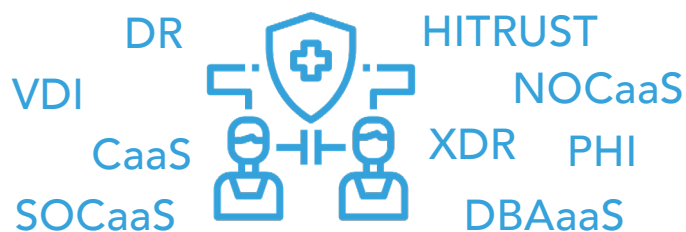
Ntirety provided a book of actionable documentation that was easy for existing employees to follow, and also approachable to new hires. Ntirety's Security Operations Center as a Service (SOCaaS) and Compliance as a Service (CaaS) helps keep the provider secure and compliant.

Ntirety's Infrastructure as a Service (IaaS) keeps the provider reliably connected to high performing servers, systems, and virtual desktops. Ntirety's Network Operations Center as a Service (NOCaaS) provides them with enterprise backend network and system support, plus updates and upgrades. Finally, Database Administration as a Service (DBAaaS) enables the provider to access database expertise with a simple email or call.

"Our data is extremely important to us and our partners, and we cannot afford for it to get in the wrong hands. We are grateful for our partnership with Ntirety, who keeps our data safe and protected from unknown threats."

RESULTS

With the help of their technology supplier, the healthcare provider was able to connect with the Ntirety team. Ntirety was able to meet all their requirements, from primary infrastructure to robust backup to Disaster Recovery (DR). Leading technology suppliers consider Disaster Recovery to be a critical part of a secure cyber environment, so this was hugely important.



With the growing amount of PHI and additional servers the healthcare provider was responsible for managing, it was a "must-have" that they work with a reliable, secure, managed services provider. Through Ntirety, the provider gained full access to activity in their security infrastructure, including reporting from the SIEM. This access led to a greater understanding of criticality levels, allowing them to properly adjust and alert. The information Ntirety provided met their exact needs:

"Ntirety's comprehensive security suite has been an impressive security shield for our business. Additionally, we don't have the budget to stand up our own internal infrastructure or internally hire the expertise required to protect against today's artful criminals."

The healthcare provider was able to comply with HITRUST requirements because of Ntirety's help securing data. Using Virtual Desktop Infrastructure (VDI) services through Ntirety, the healthcare provider felt confident operations would run smoothly. In addition to the HITRUST requirements, some customers wanted additional assurance they could entrust the healthcare provider with their personal information; Ntirety was able to serve as proof their data was safe. Clearly documented, comprehensive Ntirety "run books" contained all the details needed to understand the provider's infrastructure, giving those customers, as well as the provider's team, additional confidence in working with Ntirety as a partner.

Overall, Ntirety aided the healthcare provider with maintaining a strong security posture and provided deep domain expertise that allowed them to manage everything down to onsite assets.



Managing security and compliance is a strategic, economic imperative that directly impacts business outcomes. Ntirety is the only company that embeds compliant security throughout IT and company culture, protecting enterprises with a comprehensive compliant security solution. With over 20 years of experience and deep security expertise, Ntirety's three US-based security operations centers (SOCs) simplify risk management programs with a full protection, recovery and assurance suite of services. Learn more about Ntirety's award-winning and globally-trusted Compliant Security Solutions at ntirety.com.

Schedule a consultation to see how compliant security will protect and optimize your business by visiting ntirety.com/get-started-today.