Health care organization speeds up recovery after a ransomware attack

A large health care organization uses Quest Recovery Manager for Active Directory Disaster Recovery Edition to get their environments back up and running after a late-night ransomware attack

Large Health Care Organization

Employees: **25,000**

Industry: **Health Care**

Introduction

A few years ago, IT team members of a large health care organization got an alert in the night that there was suspicious activity going on in their Active Directory environments. A few hours of investigation later, they discovered that the organization had been attacked by ransomware.

The teams rushed onsite to start the recovery process, but they were met with various problems that brought recovery to a temporary standstill.

Growth caused gaps in recovery

The organization had been undergoing many mergers and acquisitions. While they had Quest Recovery Manager backing up a portion of their environments, amidst the rapid organizational changes, the tool changed hands to new administrators and some forests had not been backed up. In addition, the company didn't have

Challenges

After a ransomware attack left the organization in need of recovery, the organization's IT teams needed to determine which parts of their environments were backed up, which needed to be completely remade and how to get the infected portions out of their system in a timely manner to keep their health care operations as unaffected as possible.

Solution

Quest Recovery Manager for Active Directory Disaster Recovery Edition ensured that the organization's primary forest was backed up and could be recovered within a day.

Results or Benefits

- Assurance of patient care and quick restoration of business functions
- Fully backed up environments that can be recovered within a day
- Risk removal through in-depth cyber resilience

a comprehensive business recovery plan in place, meaning that their organization was offline, stressing the mission of continuous patient care at their hospitals and offsite locations. “Even though these companies will get a tool, they won’t have a plan,” said a former member of the organization’s IT security team. “It’s not just the responsibility of IT and Active Directory administrators to make sure that they have their disaster recovery plan, but also the business plan.”

The absence of a recovery plan resulted in one of the biggest issues they would face: IT administrators had no choice but to wait for the business side of the organization to determine priorities, procedure and protocol. This process took a while because legal and other branches of the organization had to be involved. “I think we as an organization weren’t prepared well enough from the business side in order for recovery to start moving really fast to not lose time and come back online and bring the environments back too,” commented another former employee.

The clock was ticking. Each minute the organization’s environment was offline and access to Active Directory was compromised, staff had to use pens and paper to maintain critical operations and assure patient care. The organization needed a recovery solution, and they needed it fast.

> **Quest being available to assist in this situation was huge because everyone was scrambling trying to figure out where to start.**
>
> *Former Employee*

Quest cuts recovery time and effort

Fortunately, the organization had already invested in Quest Recovery Manager Forest Edition to back up their biggest Active Directory forest and had implemented good practices. When Quest was alerted to the disaster the organization was facing, Quest offered an immediate upgrade to the Disaster Recovery Edition and expert guidance to get through the crisis. The Disaster Recover Edition helped IT recover that forest within the day, with automation both accelerating recovery time and improving accuracy. The former employees said that the solution’s automation, “Covered steps that we didn’t even know that we would have had to do. I can’t even imagine trying to sit there and do all these steps and read papers on how to do it natively.”

To recover the other four forests that weren’t backed up with Recovery Manager, IT teams of at least two to three people took a few days each to complete the process since they had to rebuild from scratch.

To prevent re-infection, Quest provided the organization the ability to reset privileged group accounts that were compromised, create a new administrative password and force the reset of privileged groups. With defence in depth, the stolen credentials couldn’t be used again by the cybercriminals who stole them.

> **It’s an event that created a traumatic experience for us.**
>
> *Former Employee*

Lessons learned

With the ransomware ordeal in rear view mirror, the IT and security practitioners offer these recommendations for other organizations to avoid pitfalls and get their operations back online ASAP after a disaster:

- Don’t wait for a disaster before setting up a recovery plan with both a technical and a business component. You need both to get recovery started ASAP and lower the negative impact on your business--for example, loss of revenue during the downtime, overtime costs and budget reallocation can prevent essential services, such as third-party forensics.

- Practice tabletop exercises with scenarios such as being in network offline mode so everyone can understand how applications and services will perform. The exercise should include how business and IT should respond to make timely, informed decisions.
- Think of a disaster recovery plan and best-of-breed technology as insurance. You hope that you never have to use it, but industry trends suggest otherwise. Comprehensive, practiced disaster recovery plans help you and your colleagues sleep better knowing that if disaster strikes, whether from a simple mistake to a full-on ransomware and extortion attack, your team is ready for it.
- Budget for the increased storage space necessary for recovery. As your organization recovers, you need to set aside the infected areas for forensics and other review to see how the perpetrator got through, all while you're trying to bring up the new environment. Many organizations don't expect their environment to increase in size as they're trying to recover, but it does and that's something to keep in mind.
- In the event of company mergers and acquisitions, make sure to evaluate the new additions' backup and recovery tools before IT budget decisions are made to ensure funding is available if the tools are outdated or inadequate.

PRODUCTS AND SERVICES

Solutions

- Recovery Manager for Active Directory Disaster Recovery Edition

"Quest being available to assist in this situation was huge because when everybody was scrambling and trying to figure out where to start, we had a Quest person who was totally concentrated on this one thing. 'You can't do anything until you do this, so let's get this going. Let's slowly start restoring and then we'll go from there.' That was huge."

About Quest Software

Quest Software creates technology and solutions that build the foundation for enterprise AI. Focused on data management and governance, cybersecurity and platform modernization, Quest helps organizations address their most pressing challenges and make the promise of AI a reality. Around the globe, more than 45,000 companies including over 90% of the Fortune 500 count on Quest Software. For more information, visit www.quest.com or follow Quest Software on X (formerly Twitter) and LinkedIn.