

CUSTOMER CASE

NHS Blood and Transplant cuts AD disaster recovery to one hour with Quest Software



NHS Blood and Transplant (NHSBT) manages England's blood supply chain and the UK's Organ Donor Register, serving around 65 million people. To address vulnerabilities in their Active Directory and Entra ID backup and recovery, NHSBT deployed Quest solutions, cutting full environment restores from an estimated half a day to just one hour.

As a life-critical organization, NHS Blood and Transplant cannot afford disruptions to its identity environment. With roughly 8,000 people waiting for an organ transplant each year, any outage could have devastating consequences for patient care.

NHSBT runs a single Active Directory forest and Entra ID tenant supporting 7,000 staff across 100 sites, including production centers, distribution centers, and laboratories where blood products are made. Built to support mission-critical blood production, the enterprise environment reflects nearly 20 years of continuous service, integrating specialized laboratory instruments with established operational frameworks. "Our mission is to save and improve lives," said Daniel Bhatoa, an identity and access management engineer within NHSBT's technology and services department. Doing so depends on reliable identity services and the ability to restore quickly.



Country: UK



Employees: 7,000

People Served: 65 million



Industry:
Healthcare Services

Challenges

NHSBT had been using a third-party backup tool that required staff to follow lengthy Microsoft documentation to complete an AD restore, a cumbersome process that the team couldn't reliably test or validate. A full AD restore could take half a day or longer, leaving NHSBT exposed during ransomware attacks and without strong evidence to support mandatory compliance frameworks.

Solution

The security team selected Quest backup and recovery solutions to close the gap across their on-premises Active Directory and Entra ID environments. The wizard-driven, automated approach gave NHSBT granular, item-level restore, backup-to-live comparison, and encrypted, malware-scanned, off-site backups, all validated through a dedicated lab environment and ongoing support from Quest's Recovery as a Service consultants.

Benefits

- **Half a day+ to ~1 hour**
Full Active Directory recovery
- **Hours to minutes**
Single-item recovery
- **Stronger audit evidence**
Tested, documented recovery processes support the Cyber Assessment Framework and Data Security and Protection Toolkit compliance audits
- **Greater operational resilience**
Faster recovery helps protect identity services supporting 7,000 staff across 100 sites

The pressure of manual recovery

Before, NHSBT relied on a generic, third-party backup tool. Restoring Active Directory meant using that tool and then working through Microsoft's own documentation, command by command, each one needing to be typed correctly and checked by hand. "In such a stressful situation where the entire identity plane doesn't really work, you're prone to make mistakes," said Jakub Witkowski, an identity and access management engineer at NHSBT. "One typo can cause the command not to work."

Beyond the manual recovery process, the team had never been able to properly test or validate that their backups would actually work. "It was just a case of we've got some backups; we don't know how good they are until we actually come to test them," said Daniel. Based on modelling exercises, NHSBT estimated that a full Active Directory restore could take half a day or longer using the previous approach.

Day-to-day, smaller mistakes caused considerable disruption, too. On one occasion, a team member accidentally deleted the wrong Active Directory group. "We had to find the group that was deleted, find out who all the members were, re-add them in, and then reassign permissions," said Daniel – all without a reliable, validated state to restore from.

Choosing a specialist for identity recovery

Having used Quest's migration technology in a previous role, Daniel had already seen what a dedicated solution could do. He pushed for the same rigor in backup and recovery, looking for a solution that reflected Microsoft best practices, was easy to use, and came with a strong reputation and expert support.

“With Quest in place we can restore our Active Directory in around an hour. Prior to that, we estimated it would take half a day or longer to actually restore”

Daniel Bhatoa, Identity and Access Management Engineer

The team found Quest's recovery capabilities went well beyond competitors', including granular restores down to a single attribute, side-by-side comparison of a backup against the live environment, online restore, and built-in validation checks. Quest's Gartner-recognized standing, its track record dating back to the 1980s, and its ISO and SOC 2 accreditations gave the team additional confidence. “Quest is a top-tier solution available on the market, with years and years of experience helping other customers and organizations make sure their Active Directory is resilient enough,” said Jakub.

NHSBT deployed Quest recovery solutions across Active Directory and Entra ID, giving the team, as Jakub described, “a complete package” that covers identity recovery across their environments. Choosing a combined on-premises and cloud offering meant the team no longer had to stitch together separate tools for Active Directory and Entra ID.

The difference in day-to-day use was significant and immediate. Instead of manually typing and verifying individual commands, the team was able to follow a guided, largely automated process. “There's no typing in there,” said Jakub. “When everything is

prepared, and the product is in place, you just pretty much follow the steps that the tool gives you.”

Backups themselves are encrypted, malware-scanned, and stored off-site, capabilities that NHSBT didn't have with their previous solution. The security team also uses Quest's dedicated lab environment to run regular fire drills, testing and refining their restore runbooks under realistic conditions. On top of the technology itself, NHSBT has taken advantage of Quest's Recovery as a Service offer, giving them ongoing access to Quest consultants who review configuration and suggest enhancements over time.

Recovery in hours, not days

Through regular recovery fire drills, the team has been able to validate and document its recovery capabilities under realistic conditions. “With Quest in place we can restore our Active Directory in around an hour,” said Daniel. “Prior to that, we estimated it would take half a day or longer to actually restore.”

The same capabilities also simplify day-to-day recovery tasks. A deleted group that once meant hours of manual reconstruction can now be restored online within minutes by comparing the backup to the current state. “We can actually do an online restore of that particular group within a few minutes, saving hours of time,” said Daniel.

With encrypted, malware-scanned, off-site backups, and a phased recovery capability that lets the team prioritize their most critical systems first, NHSBT is better prepared for a serious event. In the case of a ransomware attack or a compromised domain controller, the team can now restore to a clean operating system, original hardware, or a virtual machine. NHSBT can also evidence its recovery capability for the Cyber Assessment Framework and Data Security and Protection Toolkit audits, backed by tested, documented processes.

“Quest is a specialist solution that allows you to restore identities in a fast and auditable way that is actually intuitive and easy to use,” said Jakub. When NHSBT’s supply chain of blood and organs is disrupted, it has a massive impact on people’s lives. Having a fast, reliable, and auditable way to restore identity services gives the whole organization, as Daniel put it, “a lot of reassurance.”

“Quest is a top-tier solution available on the market, with years and years of experience helping other customers and organizations make sure their Active Directory is resilient enough.”

Jakub Witkowski, Identity and Access Management Engineer

Products

- [Quest Identity Recovery](#)
- [Quest Recovery Manager for Active Directory](#)

Results at Glance

- Full AD recovery validated in around one hour
- Deleted groups restored in minutes instead of hours
- Recovery processes regularly tested and documented for audit readiness

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](#).

Explore our solutions →