IT solutions and managed service provider trusts the Quest products it sells.

Phoenix Software strengthens its own security and cyber resilience with solutions from Quest.

Country: **United Kingdom**

Employees: **430**

Industry: **IT solutions and managed service provider**

Website: **www.phoenixs.co.uk**

Award-winning IT solutions and managed service provider carefully vets the solutions it offers.

Phoenix Software provides IT solutions and managed services that empower UK organisations to modernise and secure their infrastructures and to protect, visualise and manage their data. The company's excellence has been recognised with a wide range of awards, including the 2023 Microsoft Modern Endpoint Management Partner of the Year and 2021 Microsoft UK Partner of the Year.

Phoenix's obligations and commitments to customers are their highest priority. "We have a thorough onboarding process for our strategic vendors," explains Laura Banks, data protection specialist at Phoenix.

Challenges

As an award-winning provider of IT solutions and managed services, Phoenix Software only partners with vendors of the highest quality and reputation. Indeed, whenever feasible, the company's IT teams test prospective solutions in their own environment before they are offered to customers. During this process, a select few tools prove so valuable that they become part of company's own IT technology stack.

Solution

Phoenix applied its careful vetting process to Quest Active Directory security and cyber resilience solutions — which delivered with flying colours. As a result, their internal IT teams now rely on the tools for a range of crucial functions, from threat detection and response to disaster recovery.

Results or Benefits

- Blocks threats by preventing changes to critical admin accounts, GPOs and other objects
- Enhances AD security with effective Group Policy governance
- Ensures cyber resilience by slashing disaster recovery time from days to just an hour or two
- Facilitates compliance with regulations and contracts by automating privilege management tasks

"If I see an opportunity in our portfolio for a new solution, it will go to our technical team for review and testing. Before we offer it, we need for them to say, 'Yes, that's the best product out there on the market.' We will onboard only the best vendors and solutions."

Actually using these solutions in house whenever feasible provides multiple benefits. "We are very strong advocates of using the tools that we sell," notes Shaun Tosler, infrastructure and security manager at Phoenix. "Obviously, we can't do it with everything, but by verifying that a solution works well for us, we can have confidence that it will work well for our customers. Plus, it enables our teams to gain experience with the tools we offer so we can better support clients who adopt them."

As a Quest Platinum Partner, Phoenix had the opportunity to trial Quest Active Directory security and recovery solutions. Those solutions not only passed the criteria to enter the company's portfolio, but also proved so valuable that they remain vital components of its own IT ecosystem. Together, Change Auditor, GPOADmin and Recovery Manager for Active Directory Disaster Recovery Edition from Quest and One Identity Active Roles help Phoenix ensure strong Active Directory security and cyber resilience.

Change Auditor provides advanced threat detection — and can even stop attackers cold.

With Change Auditor, Phoenix enjoys real-time threat monitoring and security tracking of all key user activity and administrator changes. "For security auditing, our primary tool is Microsoft Sentinel," notes Tosler. "But we do not think it's wise to put all our eggs in one basket by having only a single tool for critical functions. What if it's wrong or gets compromised? Change Auditor provides an important secondary source of information. Moreover, because of where it sits in the technical structure of AD, it provides enriched information that the native logs do not capture."

Phoenix is even more enthusiastic about the ability of Change Auditor to block unwanted changes to critical objects, such as powerful administrative accounts and key Group Policy Objects (GPOs). "Change Auditor will stop attackers — no matter what permissions they have — if they try to modify protected objects," Tosler says. "It is our safety net against privilege escalation and AD misconfigurations. We can say that a particular account can't be touched at all, or it can be edited only from within a certain IP address range or so on. For instance, if someone accidentally made every account a Domain Admin, it wouldn't matter because Change Auditor provides a blockade to deny any critical change."

Indeed, with Change Auditor in place, Phoenix is better positioned for prompt threat detection and response. "With Change Auditor, if an attacker did get into our AD, two things are going to happen," Tosler explains. "First, they're going to make more noise, which means that our other security tooling is going to be better placed to spot them. And even if the attacker managed to disconnect our primary logging source, Change Auditor is still logging the information. In short, it gives us more time, more noise and more protection across the attack chain."

> **"Recovery Manager is brilliant — it's the only tool that automates the work of building out domain controllers after a disaster. Every other backup tool simply recovers the Active Directory database file and leaves you to do the work. Recovery Manager doesn't restore a file — it automates the entire recovery process. In just an hour or two, I can have the environment back up. Without it, we'd need days to build that out."**
>
> *Shaun Tosler, Infrastructure and Security Manager, Phoenix Software*

GPOADmin enables effective Group Policy governance.

Group Policy plays a crucial role in Active Directory security, and Phoenix utilises GPOADmin to manage its GPOs efficiently and effectively. "GPOADmin makes it easy for us to control the rollout of GPOs," Tosler says. "When we have a change that we need to put in place by a certain time, our engineers do not have to wait up until 1:00 in the morning to deploy it so it will have the least impact on users. Instead, we can make the change, stage the GPO and schedule the rollout to meet our requirements."

Moreover, GPOADmin offers robust GPO change management. "The fact is 99% of security holes come from not having proper change management — someone simply takes an action without a proper process in place," notes Tosler. "We use the approval feature in GPOADmin to ensure that one person makes a change but someone else has to approve it, which helps both prevent hasty mistakes and malicious actions. Moreover, GPOADmin tracks every event and provides clear details so we can always see exactly what was changed."

Of course, even with the most thorough processes in place, issues can arise, so GPOADmin provides advanced rollback capabilities. "Even with the most careful testing and approvals, it is possible that a GPO might be rolled out and then a problem might be discovered with it," Tosler points out. "With GPOADmin, we can quickly and easily roll back the GPO to a previous state to promptly restore Active Directory security. It's very rare that a tool does exactly what it says in terms of controlling and administering Group Policy, but GPOADmin does just that, and it does it quite well."

Recovery Manager for Active Directory is "brilliant," slashing recovery time from days to hours.

To ensure cyber resilience, Recovery Manager provides efficient and reliable AD backups, reducing bloat by omitting extraneous and risky components like boot files. Indeed, Tosler considers it "one of the best tools on the market for AD backup."

However, he says that recovery is where the solution really shines. "Recovery Manager is brilliant — it's the only tool that automates the work of building out domain controllers after a disaster," Tosler explains. "Every other backup tool simply recovers the Active Directory database file and leaves you to do the work. Recovery Manager doesn't restore a file — it automates the entire recovery process. In just an hour or two, I can have the environment back up. Without it, we'd need days to build that out. Moreover, it enables you to restore information that you simply can't rebuild, which increases its value exponentially."

> **"We have a thorough onboarding process for our strategic vendors. If I see an opportunity in our portfolio for a new solution, it will go to our technical team for review and testing. Before we offer it, we need for them to say, 'Yes, that's the best product out there on the market.' We will onboard only the best vendors and solutions."**
>
> *Laura Banks, Data Protection Specialist*
> *Phoenix*

Although Phoenix has never had to perform a disaster recovery, knowing that its speedy recovery capabilities are right at hand delivers peace of mind. "In case of a domain compromise, I'd have 1,001 things to think about, and the CEO or CTO is going be standing right there because the business would be losing money every second," says Tosler. "With Recovery Manager, I know I have one button to press to get the recovery moving, restore our identities and get services like email back up. It's invaluable, honestly."

Indeed, Tosler would recommend Recovery Manager to any organisation whose Active Directory has been wiped out by a disaster, noting that the solution would likely deliver a full return on investment immediately. “Recovery Manager will give you a solid basis to start your recovery,” he says. “Let’s say you’ve got tens of thousands of users — creating all those accounts manually could take 10, 20, 30 hours. Recovery Manager takes all the labor out of it and automates the account creation. That’s not something you can do with any other tool. The amount of time you save would probably more than pay for the solution in that situation.”

Active Roles strengthens AD security by simplifying identity management.

For identity security, Phoenix uses Active Roles, which provides management and fine-grained delegation of privileges across Active Directory domains and Entra ID (formerly Azure AD) tenants from a single console. Using role-based access control (RBAC), Phoenix can strictly enforce the least privilege principle.

“Active Roles provides the abstraction we need for identity security,” explains Tosler. “For example, we no longer have to provide admin accounts to our service desk technicians; instead, we direct them to a web interface. We can also delegate tasks like group management to the people with the necessary expertise, such as the developers of custom apps. And no one other than the break-glass accounts can make any changes directly within AD.”

Active Roles also helps Phoenix ensure compliance with the data sovereignty requirements of both company contracts and regulations like the GDPR. “Our employees need to go on holiday and access their emails, but some clients do not allow their data to be processed outside of the UK,” Tosler says. “Active Roles provides the automation we need to honor those contracts. We simply set it up so that the user will be automatically removed from certain groups when their holiday begins and added back when they return. As a result, we do not have to worry about users retaining access rights they should not have.”

A suite of solutions that work together

As valuable as each solution is individually, Phoenix recognises that they work together to deliver even more value. “If you adopt Active Roles for identity management, you may as well bring in Change Auditor to do the AD lockdown,” explains Tosler. “Similarly, Recovery Manager will create backups, and Change Auditor will watch over them and prevent anyone from tampering with them. With those types of controls in place, I can trust that the data required to get the service back online is going to be there when I need it.”

PRODUCTS AND SERVICES

Products

- Change Auditor
- GPOADmin
- Recovery Manager for Active Directory Disaster Recovery Edition
- One Identity Active Roles

Solutions

- Microsoft Platform Management

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.