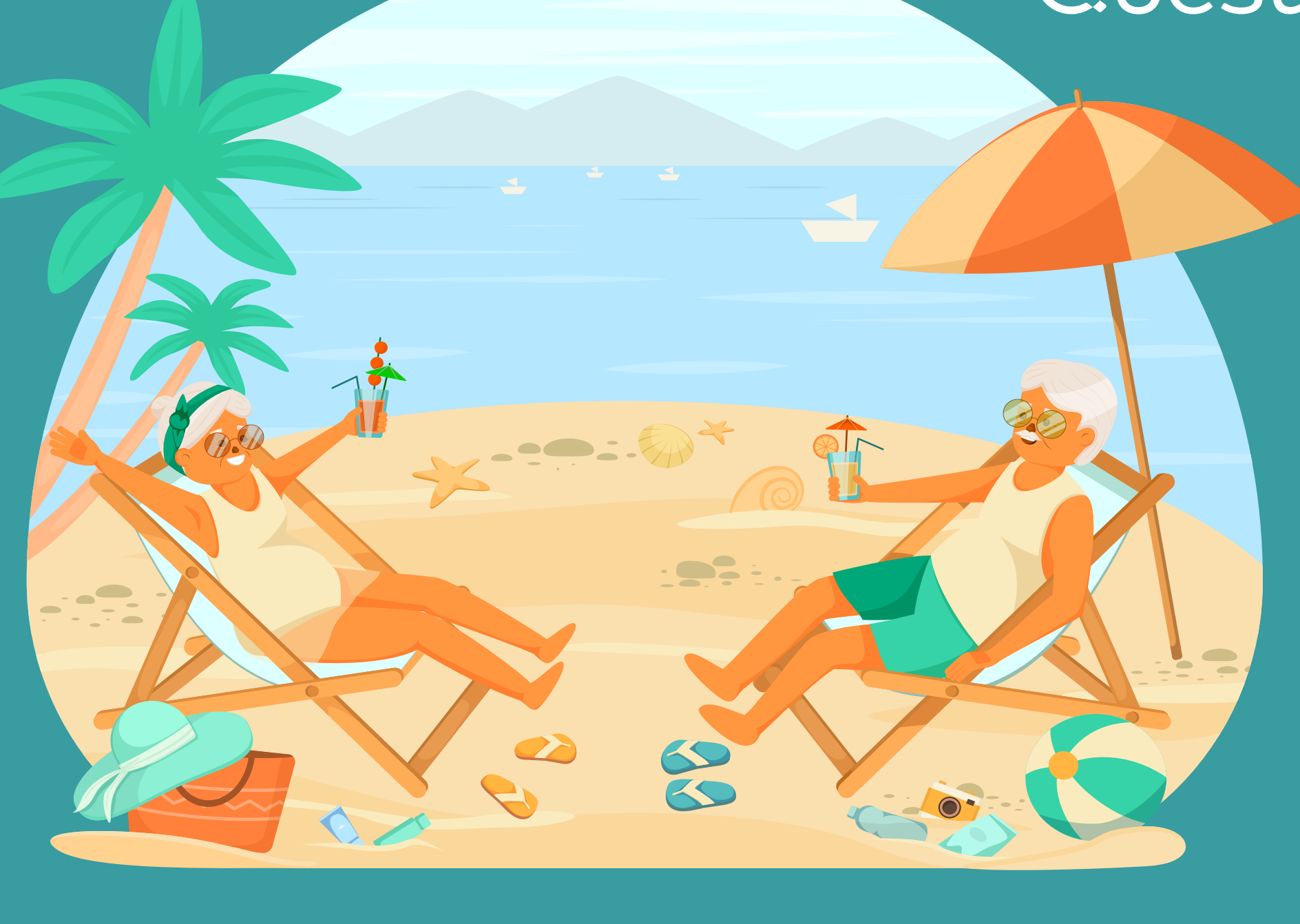
Quest



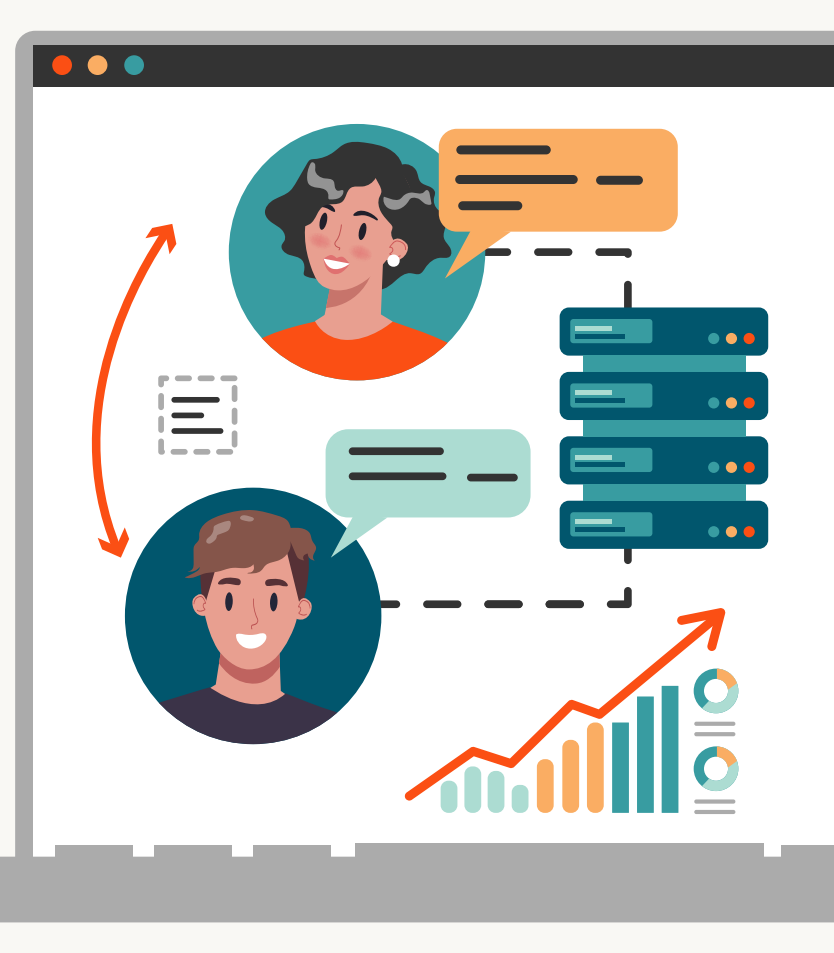
ACTIVE DIRECTORY RETIREMENT CRISIS:

SEVEN STEPS TO SURVIVING

Retirement is often considered a welcome and well-earned journey of relaxation and enjoyment. For organizations that rely on employees holding traditional on-premises Microsoft MCSE and MCSA certifications, however, retirement might be associated with panic and stress. Gen X and baby boomer employees holding these certifications will be retiring in the next ten to fifteen years, leaving organizations with a concerning hybrid Active Directory security knowledge gap. Furthermore, Microsoft retired its on-premises AD Microsoft Certifications in 2020, and the replacement focuses only on Azure – raising some fundamental questions:

Does the new workforce have the institutional knowledge to effectively manage on-premises AD?

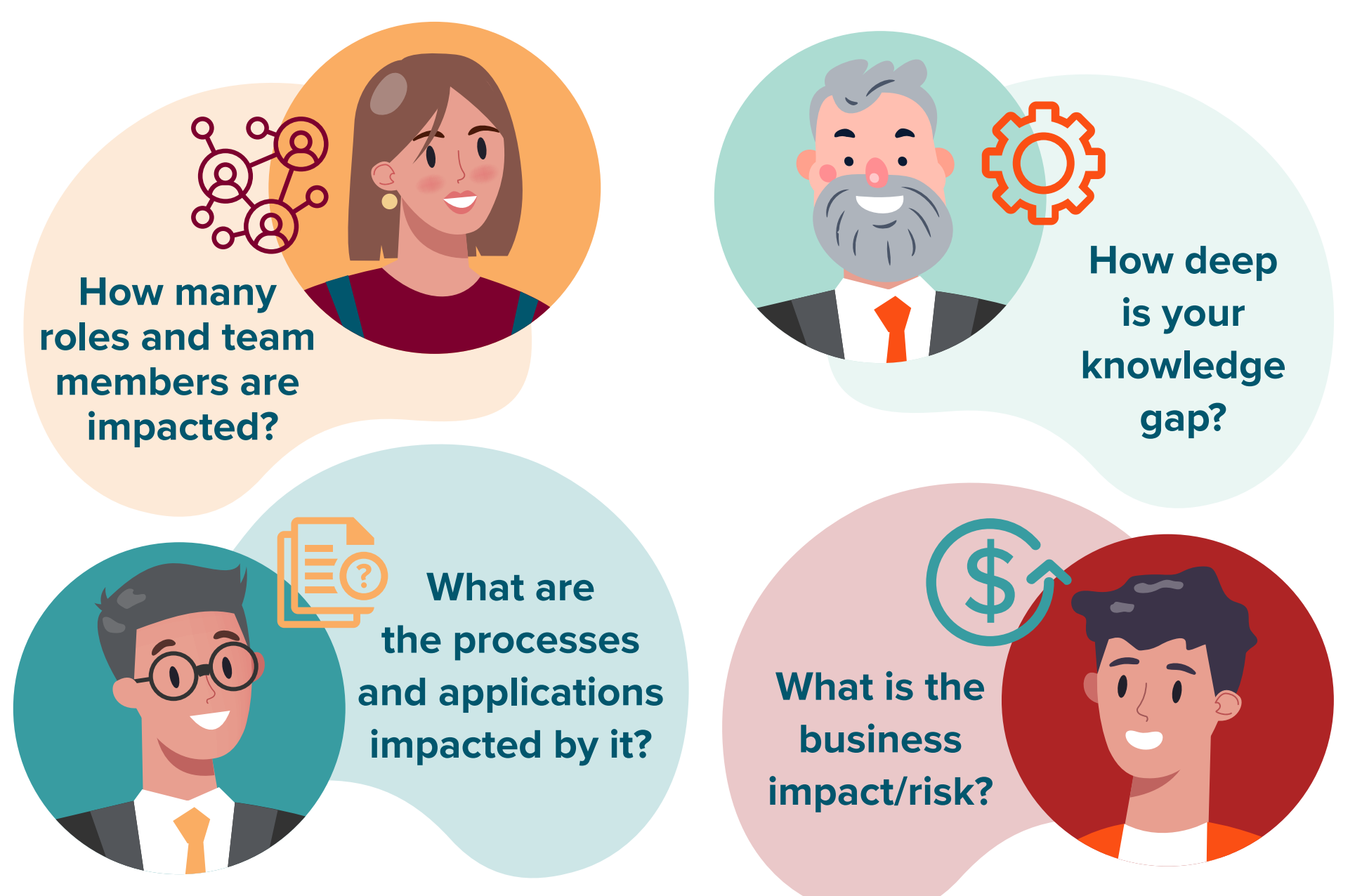
Do you have an effective AD strategy ready to keep operations alive in this changing threat landscape?



Well – sit back and relax as we provide seven straightforward steps that will help you prepare for the Active Directory retirement crisis.

1 Assess the knowledge gap

The first step is always to assess your organization's knowledge gap. To do that efficiently, you need a good picture of your infrastructure, applications, and processes. Reporting solutions can help you rapidly and automatically discover the technical pieces of the puzzle. The rest will be a mix of HR and business requirements discovery. You should have answers to the following questions:



2 Implement redundancy in roles, tasks, processes & knowledge

You need to assess your organization's roles and how they are distributed. Ensure that every team role has at least one backup. Use this as an opportunity to redistribute the roles among your team members. Too often, one team member has too many roles and responsibilities, making his departure a risk for the organization.

To mitigate that risk, pair new team members with experienced engineers. This pairing will help you with role redundancy, knowledge transfer, and talent retention. For example, promoting your senior engineers to team leader will help retain those valuable contributors and incentivize them to effectively mentor and train their teammates to reduce the knowledge gap.

3 Establish a mentoring & training plan for team members

Create a mentoring and training plan that includes the more experienced team members – not only for mentoring purposes, but also to learn new skills to increase your team's competency level in areas like cloud computing or cyber security and minimize the risk of losing a senior-level team member.

4 Standardize and automate your processes

Implementing a software solution can be an efficient way to mitigate the human dependencies of recurring tasks. Leverage solutions and tools that follow industry standards to automate and create easily repeatable and documented processes.

5 Document your processes

Step two gave you better visibility over your role distribution and the different tasks and processes in scope for each role. Step four should have helped you significantly reduce the number of tasks and processes to document. This step will leverage what you previously learned to ensure that your team creates and updates your documentation and procedures for all the critical tasks and processes that fall under their jurisdiction.

Then, have the less experienced team members test and improve the procedures. It will help your organization fix errors or inaccuracies while simultaneously training the less experienced members in executing the different tasks. Finally, it will significantly improve your onboarding and learning curve of new and future team members.

6 Retain & attract talented IT professionals

In the last few years, cybersecurity professionals have been experiencing extreme stress or burnout. According to a recent Forrester survey, 65% of cybersecurity experts considered leaving their job because of stress. To retain talented IT professionals, of course, compensation and benefits are essential, but they are only a part of the equation. A healthy work environment that offers the flexibility to work remotely or provides a comprehensible career path is, in many cases, more impactful. Finally, when recruiting new team members, instead of experience, prioritize the passion for technology and eagerness to learn.

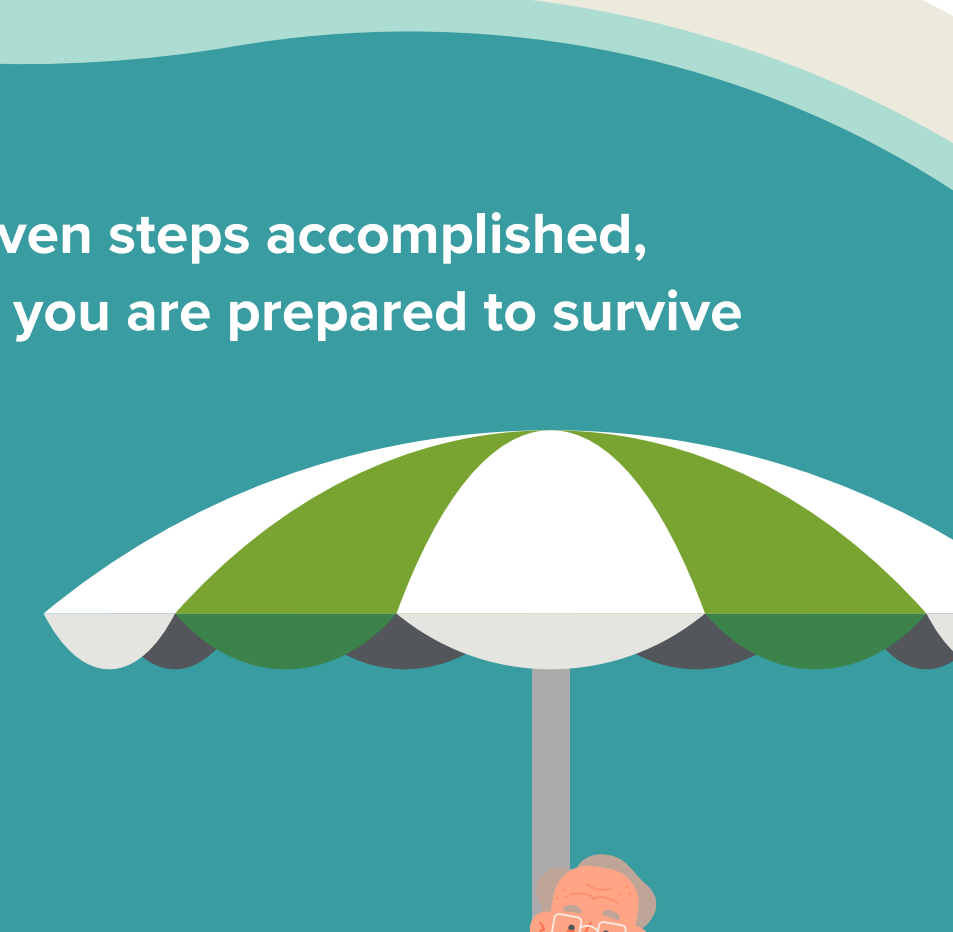
7 Deploy an Active Directory recovery plan & solution

This final step should be implemented before you modify your directory. Active Directory is a complex, multi-master database, making it extremely complicated to recover in case of corruption or a major disaster like a successful ransomware attack. That's why an AD-centric recovery solution is essential.

Implementing an AD-centric recovery solution will allow you to quickly and easily roll back any changes to your directory and enable your organization to recover from a significant disaster. Consequently, a fully automated recovery solution will not only reduce the risk of outage during an AD modernization, it will also help you reduce your effort and time to recover and simplify your recovery process and documentation.

And there you have it! With these seven steps accomplished, you can sleep a little better knowing you are prepared to survive the retirement crisis.

Speaking of preparing – think about all the changes your organization (and the industry) will experience in the next fifteen years. Active Directory is constantly evolving, and whether you are trying to automate management, stay safe from disaster, or ensure effortless migrations – you will need the right solutions and support.



Quest is the leader in managing, modernizing and securing Active Directory – from on-prem to in-cloud, and from the heart of the network to the vulnerable endpoints. Learn more about our solutions and how we can help you reduce business risk and strengthen AD cyber resilience.

Learn More

Infographic-RetirmentCrisis-US-KA-77971

Quest