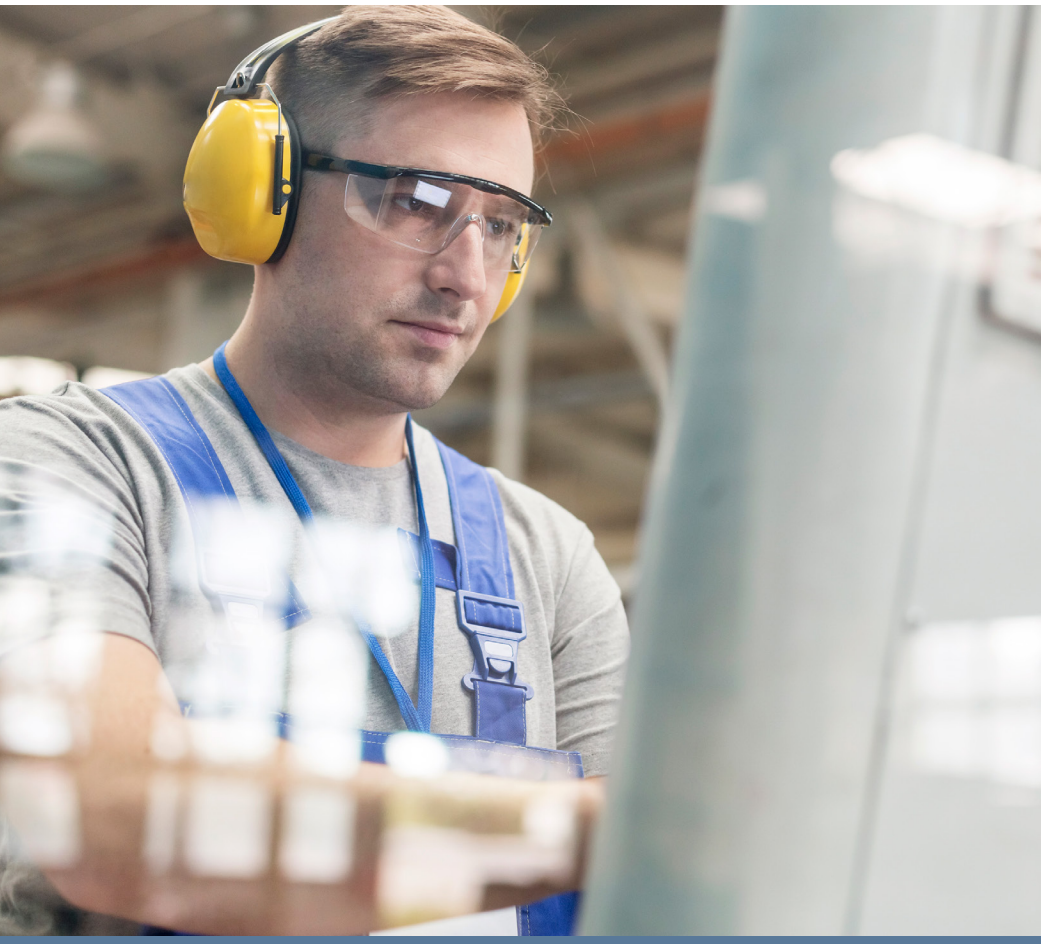
Manufacturer ensures fast and reliable AD backup and recovery

Rehrig Pacific Company gains simple and granular Active Directory disaster recovery with Quest



"The careful planning that we've put in [with Recovery Manager for Active Directory] to ensuring the resiliency of this environment means that we've bought the right insurance plan."

Brian Rowe, Director of Information, Security and IT, Rehrig Pacific Company

CUSTOMER PROFILE

Rehrig Pacific Company SINCE 1913

Company	Rehrig Pacific Company
Industry	Manufacturing
Country	United States of America
Employees	3000
Website	**www.rehrigpacific.com**

BUSINESS NEED

To maintain its position as a leader in the plastic industry, Rehrig Pacific Company needed better Active Directory backup and recovery capabilities. Native tool limitations made it difficult to recover objects at a granular level, restore objects without downtime or quickly pinpoint changes to attributes. Rehrig wasn't confident they could recover quickly or effectively enough if disaster struck.

SOLUTION

With Quest® Recovery Manager for Active Directory, Rehrig Pacific Company has the effective backup and recovery tool they need to face potential disaster. Comprehensive features allow them to quickly recover any object and attribute in their environment. Recovery Manager for Active Directory helped Rehrig reduce downtime and get users back to work quickly without restarting domain controllers. As a result, they now enjoy an AD insurance plan that gives them the ease of mind and confidence they've always desired.

BENEFITS

- Deployed Recovery Manager for Active Directory in 26 minutes and completed a full test recovery in 20 minutes
- Restored AD objects and got users back to work quickly without restarting domain controllers
- Quickly pinpointed deleted or changed objects or attributes
- Restored only the required attributes without restarting domain controllers

SOLUTIONS AT A GLANCE

- Microsoft Platform Management

Rehrig Pacific Company is one of the premier leaders in the plastic manufacturing industry. With over a century of experience, they have delivered high-quality, innovative products for various purposes, ranging from environmental to retail. A key component in supporting their successful business is a complex Active Directory environment, which the IT team keeps secure, available and protected from disasters with Quest® Recovery Manager for Active Directory.

> "One thing that really stood out for us about Recovery Manager is the deployment cycle. I think it took us about 26 minutes to get it deployed and maybe 20 minutes after that before we'd actually done a full test recovery."
>
> *Brian Rowe, Director of Information, Security and IT, Rehrig Pacific Company*

INNOVATION REQUIRES EFFICIENCY – AND SECURITY

Rehrig manufactures plastic containers for different purposes and businesses. Whether it be city-issued trash cans, recycling bins or re-usable plastic containers for logistics and supply chain solutions, they all have one common driving factor: efficiency. Rehrig understands their customers' pain points and pride themselves on solving them with high quality, easy-to-manage products. They also understand that, in order to keep innovating, their IT infrastructure – and more specifically, their Active Directory environment (AD), the lifeblood of user access, identity and authorization – needs to be secure.

"Everything we have to do has to be secure and security starts with identity," explains Brian Rowe, Director of Information, Security and IT at Rehrig Pacific Company. "As an example, you cannot log into our ERP system if Active Directory is not functional and if the key components of the role mapping and security group memberships are not there. And that's really true for every critical enterprise application that we have." Rehrig also knows the impact that a compromised Active Directory environment can have on business continuity, revenue and reputation. "If Active Directory is down, then there is no selling," says Rowe. "That means there's no order entry, that means we can't provide our customers even order status updates and it also means that we can't do any capacity planning or produce net-new work orders for any product for any customer across the company. It also means we can't ship anything."

The impact of these consequences pushed Rehrig to improving their disaster recovery plan and establishing "A firm commitment that AD has to be bare metal recoverable within 60 minutes of a complete disaster," as Rowe explains. Securing a hybrid AD and Azure AD environment is a time consuming and complex process, and when you factor in the somewhat limited, inefficient capabilities of native recovery tools, the complexity increases even further. "The only way to leverage Windows native tools is to have a full bare metal recovery image of your domain controller, and without that there's no guarantees that you can get Active Directory back and functional," explains Rowe. "It became apparent that if we were going to recover from a problem, we were really only about 50 percent confident we could do it with native functionality in our existing backup recovery tools."

PRODUCTS & SERVICES

SOFTWARE

- Recovery Manager for Active Directory
- Security Explorer

FINDING A SOLUTION WITH QUEST

For their hybrid cloud environment, Rehrig's previous backup and recovery strategy relied heavily on managed domain controllers within Amazon Web Services (AWS). Rehrig had more flexibility with AWS's infrastructure and benefited from how it can backup and restore snapshots of the server, but they were hindered because AWS is unable to make granular restores.

So, Rehrig needed a solution to back up and recover data quickly, reliably and at a granular level. This, in turn can cover the gaps that AWS cannot account for. After evaluating recovery tools on the market, they went with Quest, as they were familiar with their good reputation and their products. They felt confident that Quest had the right support and tools to help keep their AD environment safe and prepared for disaster.

Their confidence paid off when they implemented Recovery Manager for Active Directory and saw immediate results.

KEEPING THINGS SIMPLE

Specifically for Rehrig, Recovery Manager for Active Directory was installed and used to back up and restore domain controllers that are running on virtual machines in AWS. They implemented it on an EC2 instance and the process for the installation, back up or restoration was seamless. "One thing that really stood out for us about Recovery Manager is the deployment cycle," explains Rowe. "I think it took us about 26 minutes to get it deployed. It took us maybe 20 minutes after that before we'd actually conducted a full test recovery." The seamless process surprised the team, who were used to spending an agonizing amount of time developing and testing recovery tools that proved ineffective. "It really was so simple, that by the time we'd finished the POC, one of my engineers looked at me and asked if we can we just cut the PO right then and there. And we did."

Once implemented, Rowe and the rest of the team were able to take advantage of Recovery Manager for Active Directory's ability to restore specific attributes without restarting domain controllers. Being able to easily manage, backup and restore subsegments of their Active Directory environment provides Rehrig with the cost-efficient recovery method they need. "The capabilities to do that effectively and without needing a PhD in Active Directory are the things that we rely on the most," reports Rowe.

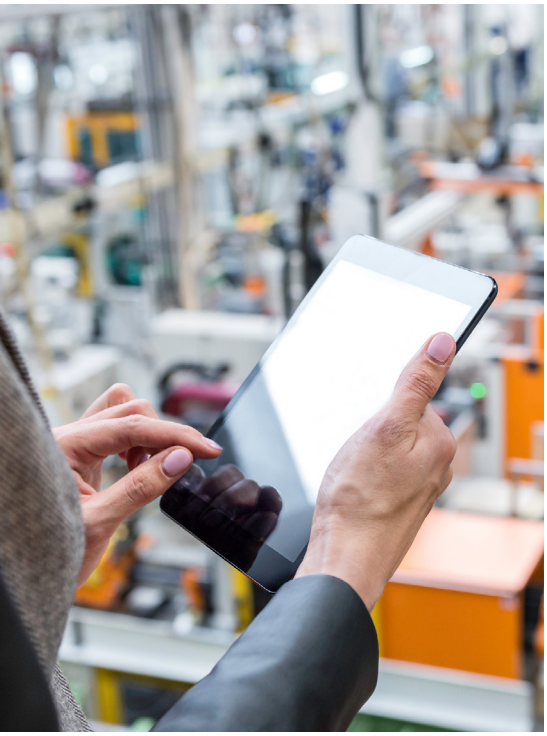
CONFIDENT ABOUT SECURITY

Throughout their various tests on the AWS EC2 instance, Rehrig's confidence in Recovery Manager for Active Directory's capabilities were solidified. Reduced downtime, along with accelerated and granular recovery of data, allowed Rehrig to feel prepared for any potential disaster. "The careful planning that we've put in to ensuring the resiliency of this environment means that we've bought the right insurance plan," states Rowe. "Hopefully it'll be the best yet least-used tool in our environment for years to come."

CONTINUED EFFICIENCY WITH SECURITY EXPLORER

With their effective disaster recovery plan coming into fruition, Rehrig wanted to focus on how they manage account privileges and permissions. With over 3,000 users in their Active Directory domain, Rehrig was having trouble determining which accounts had access to what data, especially since some of those accounts predated their modern configurations and policies. If they didn't understand each account's privileges, huge gaps in their infrastructure would be open for corruption and potential disaster. The process of going through each account's configurations was complicated, however. "I would have to send a bunch of people to look at every single asset, every group and every individual component that we wanted to evaluate, so that we could identify the problems and merge those configurations back into our current security policy and standards," Rowe states.

> "[Recovery Manager for Active Directory] really was so simple, that by the time we'd finished the POC, somebody looked at me and asked if we can we just cut the PO right then and there. And we did."
>
> *Brian Rowe, Director of Information, Security and IT, Rehrig Pacific Company*



After seeing how simple Recovery Manager for Active Directory was to deploy and operate, Rehrig decided to purchase Quest® Security Explorer, which allows them to manage access controls, permissions and security from a single, centralized console. Security Explorer will allow the team to easily manage all accounts more efficiently with features such as real-time viewing of user permissions and the ability to search for explicit or inherited permissions across their IT environments. They'll also be able to easily make targeted or bulk changes to account configurations, removing the need for manual input for every single account. These capabilities, along with the intuitive interface and controls, make Rehrig confident that they can improve their overall security. "We're hopeful that it's going to give us the opportunity to quickly hone-in and make sure our environment is clean," says Rowe. "Being able to solve things and not just keep playing whack-a-mole was really the driving force behind looking at Security Explorer."

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.

View more case studies at Quest.com/Customer-Stories

CaseStudy-RehrigPacificCo-US-KS-55841