Quest

CUSTOMER PROFILE

Company
Global Manufacturer

Company Size
7,000 employees

Global Manufacturer Overcomes Ransomware Attack with Quest Recovery Manager for Active Directory Disaster Recovery Edition

Ransomware recently plagued a global manufacturing customer, impacting 17 Domain Controllers (DCs) across multiple continents. The attack also scrambled Active Directory (AD) passwords for a majority (98%) of their users, including untold numbers of service accounts, which can obviously hinder recovery ability.

At first, one of the 17 DCs appeared untouched. But after isolating this DC on the network, they later discovered encrypted files in SYSVOL. This may have simply replicated from another DC, but since ransomware does like to propagate via Group Policy, it was critical to ensure malware wasn't hiding somewhere else on the server. Therefore, the team had to both restore and protect their network from a repeat attack, at the same time. A daunting task indeed, but that's the reality of ransomware recovery.

Luckily, the organization was able to use Recovery Manager for Active Directory Disaster Recovery Edition (RMAD DRE). This solution gave them the flexibility to utilize multiple recovery methods, including a phased recovery and restoring AD to a clean OS to minimize the risk of malware reinfection. RMAD DRE also provided their recovery team with more control over the entire disaster recovery process, saving time and resources by eliminating dependencies on cross-departmental teams.

According to the consulting services project manager on-site, "The customer was feeling hopeless until Quest stepped in and got things rolling. Then you could hear it in their voice that the hope started to return."

They were also able to achieve better control over the recovery process by implementing a phased recovery approach. The customer prioritized the order in which DCs were recovered in order to allow critical services to begin their recovery operations faster.

First, all the impacted user accounts were recovered from a backup from five days earlier. RMAD DRE even enabled the team to reset the passwords for all privileged accounts, which was essential since they believed at least one privileged account had been compromised.

Then the recovery proceeded as follows:

- Phase 1 — The first DC was recovered in one hour.
- Phase 2 — The second DC was recovered in 12 minutes.
- Phase 3 — Three additional DCs across two continents were recovered in 36 minutes.
- After the project team recovered the first five DCs, they planned the recovery of less critical locations for later phases.

The bottom line is that the global manufacturing organization drastically minimized downtime using RMAD DRE, so much so that the project manager raved, "There's no way that they would have recovered so quickly if they did not have the Quest tool!"

Quest
4 Polaris Way, Aliso Viejo, CA 92656 | www.quest.com
If you are located outside North America, you can find local office information on our Web site.

CaseStudyBrief-MPM-RMADDRE-US-LR-68528