

TECH BRIEF

Quest® Backup and Disaster Recovery Solutions for Hybrid AD and Microsoft 365 Environments

Gain powerful, flexible and cost-effective system and data protection

Introduction

Cyberattacks are at an all-time high. Nearly 70 percent of businesses suffered a ransomware attack in 2020 alone, with an average downtime of 21 days. Your mission-critical hybrid Active Directory (AD) infrastructure and Microsoft 365 applications are highly targeted assets in these attacks. In fact, Microsoft reports that 300B threats on email and nearly 7B threats on end-points were blocked over the last 12 months.

When AD fails, either from ransomware, cyberattacks or catastrophes, the IT environment grinds to a halt, which means the entire organization stops working until AD is restored. Your Microsoft 365 data stored in Exchange and SharePoint Online, OneDrive, Teams and Calendars is just as susceptible to user errors, accidental deletion, corruption and malware. But while Microsoft may be responsible for keeping the cloud services available, you are accountable for protecting your data.

What's at Risk?

Any AD/Azure AD corruption or Microsoft 365 data loss will impact your workforce, customers and partners, negatively affecting your reputation and bottom line. In addition, to meet compliance regulations, you must demonstrate the efficacy of your backup procedures and disaster recovery (DR) plans. Thus, it's imperative to

ensure you can back up and quickly recover your hybrid AD and Microsoft 365 environment from any mistakes, corruption or disasters.

The Quest® Hybrid AD and Microsoft 365 Recovery Solution

Quest helps ensure business continuity and disaster recovery by protecting both your hybrid AD infrastructure and all your Microsoft 365 data. It's designed to help you quickly and easily restore these business-critical resources to minimize any impact on your organization.

AD and Azure AD Identity Backup and Recovery

Many headline-grabbing cyberattacks have shown that when ransomware strikes, it's critical to restore AD prior to restoring any business-critical databases and applications. According to Gartner, "The restore process from many well-documented ransomware attacks has been hindered by not having an intact Active Directory restore process." This is because many ransomware strains like SaveTheQueen and DoppelPaymer compromise AD and leverage it to spread throughout the target organization's systems. Plus, if you have a hybrid environment, it's imperative to ensure the availability and integrity of both on-premises AD and Azure AD since the two directories are closely intertwined.

Luckily, Quest can simplify, automate and accelerate backup and recovery of your hybrid AD environment with Quest® Recovery Manager for Active Directory Disaster Recovery Edition (DRE) and Quest® On Demand Recovery.

- Recovery Manager for Active Directory Disaster Recovery Edition (RMAD DRE) — covers any AD disaster recovery scenario, from attribute changes to SYSVOL corruption to full AD forest disasters. RMAD DRE automates every step of the manual AD forest recovery process, protects your AD backups from compromise and eliminates the risk of malware reinfection throughout the recovery. You'll have flexibility to choose the recovery method that works best in a given situation, whether that's phased recovery, restoring AD to a clean OS or bare metal recovery.
- On Demand Recovery — protects your Azure AD environment, including cloud-only objects not synced by Azure AD Connect, such as Azure AD groups, Azure B2B/B2C accounts, conditional access policies and more. You can run difference reports comparing your backups with live Azure AD to pinpoint specific changes or deletions. Granularly search and restore exactly what you need or recover multiple users, groups and group memberships in bulk without PowerShell.

Microsoft 365 Data Backup and Recovery

Native Microsoft 365 data protection falls short of the stringent backup requirements most IT organizations need. Versioning and replication don't protect against ransomware and other malicious attacks or even accidental changes and deletions.

Quest® NetVault Plus enterprise backup and recovery provides comprehensive Microsoft 365 protection for all your Exchange and SharePoint Online, Teams and OneDrive data. You can also use its data immutability feature to protect your backups from ransomware and other cyberattacks.

NetVault Plus provides market-leading data deduplication and compression that reduces cloud backup storage requirements and costs by up to 95 percent. You can also safely replicate backups to another cloud 10 to 15 times faster for DR purposes. With NetVault Plus, you

can truly achieve a 3-2-1 backup strategy for M365 data protection and disaster recovery. And you can use Azure Blob storage to reduce costs even more. For flexibility, NetVault Plus can be installed on premises or in the Azure cloud.

With NetVault Plus, you can back up and restore:

- Exchange Online mailboxes. Granular search and restore can recover complete mailboxes, individual emails and file attachments.
- Teams full configuration and logic at a team level, as well as individual objects including files, members, channel conversations and more.
- OneDrive user and group files and folders.
- SharePoint Online sites and sub-sites at a full site or granular level.
- Calendars, calendar groups and events.

Best of all, you can use NetVault Plus to protect your Microsoft 365 data along with all your other on-premises systems, applications and data, so you get a single solution for all your data protection needs.

Conclusion

More organizations are adopting Active Directory and Microsoft 365. But comprehensive system and data protection as well as regulatory compliance are your responsibility. Quest provides a powerful and cost-effective solution to ensure your AD system and Microsoft 365 data are protected and recoverable in case of accidental changes or deletion, viruses, ransomware and other malware.

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](#).