

## DATA SHEET

# Disaster Recovery for Identity

Recover Active Directory and Entra ID 90% faster with the market's first SaaS-based disaster recovery solution

When disaster strikes your identity infrastructure, every minute of downtime costs your organization – in terms of money, productivity, and reputation. Traditional recovery approaches are slow, complex, and vulnerable to the same attacks that caused the outage. Disaster Recovery for Identity changes the game by delivering always-on, cloud-based protection that gets your business back up and running in minutes, not days.

### SaaS-based identity protection.

Disaster Recovery for Identity is the first-to-market comprehensive SaaS solution for protecting on-premises Active Directory environments. Built on the Quest unified identity cloud platform, it's always on, always updated, and always available – even when your data center isn't.

Unlike traditional VM snapshots or manual recovery processes, Disaster Recovery for Identity provides consistent, malware-free backups that can be restored rapidly from anywhere. This means you can recover critical identity services in minutes or hours instead of days or weeks, significantly reducing downtime costs and business impact.

### Benefits

- Slash recovery time by 90% — automation eliminates manual steps.
- Protect critical identities with immutable cloud backups secure from on-prem compromises.
- Launch recovery instantly without hardware provisioning or physical data center access.
- Eliminate reliance on multiple teams — identity admins can manage recovery independently.
- Reduce infrastructure costs with cloud-based disaster recovery

## Advanced recovery capabilities

### Immutable cloud backups

Protect your identity infrastructure with truly secure backups that cannot be altered or removed for a specified timeframe. Disaster Recovery for Identity provides:

- **Air-gapped storage** — that remains accessible even when on-premises storage is compromised.
- **Authentication capabilities** — that don't depend on Active Directory, creating a true recovery safety net.
- **Highly secure backups** — that are always encrypted with a randomized password only known to the system.

---

When disaster strikes your identity infrastructure, every minute of downtime costs your organization – in terms of money, productivity, and reputation.

---

### Automated recovery processes

Eliminate the risk of human error during high-pressure recovery operations with:

- **Fully automated recovery workflows** — that handle all 40+ high-level steps required for AD forest recovery.
- **Simplified recovery options** — are accessible through an intuitive interface that requires minimal specialized knowledge.
- **Consistent data restoration** — that avoids the replication conflicts common with VM snapshot approaches.

### Ideal for hybrid environments

Protect your entire identity infrastructure through a single platform:

- **Unified management** — for both on-premises Active Directory and cloud-based Entra ID resources.
- **Centralized control** — through a single console that reduces training requirements and administrative costs.
- **Flexible deployment options** — that adapt to your specific regulatory and compliance requirements.

### Enhanced security and compliance

Disaster Recovery for Identity goes beyond basic backup and restore functionality to provide comprehensive security features:

- **Malware-free recovery ensures** — that restored systems don't reintroduce the original infection.
- **Validated supply chain risk management** — practices that exceed industry standards.
- **ISO/IEC 27001, 27017 and 27018 certified platform** — built on enterprise-grade security principles.

This SaaS solution is a key component of the Quest integrated approach to the NIST Cybersecurity Framework, covering all critical pillars of identity resilience — Identify, Protect, Detect, Respond, Recover and Govern — all from a single interface.

---

Unlike manual recovery processes, Disaster Recovery for Identity provides consistent, malware-free backups that can be restored rapidly from anywhere.

---

## Enhanced security and compliance

When attackers target your identity infrastructure, traditional approaches often fall short. Consider past high-profile attacks where organizations have had to dispatch team members across continents to retrieve offline Active Directory servers unaffected by the attack. With Disaster Recovery for Identity, such extreme measures become unnecessary – you can recover from anywhere, at any time, without physical access to your infrastructure.

Our solution addresses the most critical gaps in conventional recovery strategies:

- **Immediate availability** — when on-premises systems are completely compromised.
- **Independence from virtualization teams** — who might not prioritize or understand AD recovery requirements.
- **Protection against ransomware** — that specifically targets backup systems.

For organizations in highly-regulated industries like banking, government, insurance, and healthcare that must maintain on-premises infrastructure, Disaster Recovery for Identity delivers cloud benefits without requiring full cloud migration – providing the best of both worlds for security, compliance, and operational efficiency.

Disaster Recovery for Identity changes the traditional recovery game with cloud-based protection that gets your business back up and running in minutes, not days.

### System requirements

#### Services

##### Web browser

Domain Controllers to be backed up require a DC agent installed on the Domain Controller

#### Supported web browsers

Microsoft Edge

Google Chrome (latest version)

Mozilla Firefox (latest version)

#### Supported OS for agents

Windows Server 2016

Windows Server 2019

Windows Server 2022

Windows Server 2025

### 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](https://www.quest.com) or follow [Quest Software on X \(formerly Twitter\)](#) and [LinkedIn](#).

## DATA SHEET

# Quest On Demand Migration

One simple and secure solution to migrate all Microsoft 365 workloads

Between the growth of Microsoft 365, widespread security concerns, and Microsoft's 'Cloud First' strategy, it's likely that you're considering moving parts of your business to cloud-based solutions. Gartner estimates that 96% of enterprises will rely on M&A activity for growth\* so there is a good chance you will be faced with a tenant migration now or in the near future. Additionally, you may be interested in modernizing your Active Directory environments to help mitigate risk. The importance of security is everywhere we turn -- in fact, 90% of our migration customers tell us that they are combining or considering combining their AD for more secure environments.

Migrations can reduce ongoing cost and complexity by moving all your workloads into one environment, including Active Directory, Entra ID, Exchange Online, OneDrive, SharePoint Online, Teams, and even devices. However, migrations are complex and this can create an enormous challenge since you probably have limited IT resources and don't do migrations every day. These integrations nearly always have the attention of your leadership, so you want to be sure there is little to no impact on the Business and on your users. Your IT team must maintain user collaboration and communication during the process, all while preventing downtime and data loss for the business.

## Benefits

- The Market Leader for Migration. Quest offers more than 30 years of migration expertise and a support organization that is unmatched in the industry. We have seen it all and are here to help you.
- One Solution. Many Workloads. Migrate all your Microsoft 365 workloads including Exchange Online, OneDrive, SharePoint Online, Teams, M365 Groups and Chats, Power BI, Email Domains, Active Directory, and Entra ID.
- Pre-Migration Planning. Run the ODM assessment to inventory your environments, determine migration scope, plan migration timings, and map out your target infrastructure to kick off your migration project with total peace of mind.
- Complete Control. Intuitive project management interface provides visibility and insights on the project state, progress, events, and current tasks, allowing you to stage, schedule and resolve problems in your migration project.
- Coexistence for Collaboration. Maintain user communication and collaboration throughout the migration so your users can keep working with minimal impact.
- Secure Migrations. Get the security standards, service level and scalability you need. ISO certifications include ISO/IEC 27001:2013, ISO/IEC 27017:2015 and ISO/IEC 27018:2019. [Also SOC2 Type 2 attestation.](#)

With Quest® On Demand Migration, you can forget about the complexity of migrating Microsoft 365 tenants and Active Directory. On Demand Migration allows you to simply and securely migrate all your Microsoft workloads. Through an intuitive dashboard, you get complete visibility into your migration project. You can track progress in real-time, discover and assess source accounts, groups and data — all while maintaining ongoing collaboration. On Demand Migration lets your organization continue to run smoothly throughout your migration or consolidation.

## Active Directory/Entra ID/ Device Migration

Migrating Active Directory and Entra ID is one of the most challenging components of an enterprise M&A or modernization initiative. On Demand Migration (ODM) helps you integrate and migrate users, groups, devices, and domains between Active Directory, Entra ID and hybrid directory environments. No servers, SQL, trusts, nor network connectivity required. This SaaS solution provides a management dashboard for scheduling and automation, is highly adaptable to custom configurations, and keeps migrated and un-migrated users and groups in sync during AD or Entra ID migrations.

### Active Directory, Entra ID, and Devices

Easily migrate workstations, servers, objects, settings, properties, users, groups, contacts and passwords. Migrate and integrate Active Directory, Entra ID, and hybrid directory configurations. On Demand Migration for Active Directory includes Directory Synchronization capabilities to keep migrated and un-migrated users, guests, and devices in sync during your migration.

- Establish easily repeatable processes for speed and convenience .
- Migrate remote users and their offline devices without interruptions.
- Move AD, hybrid Entra ID, and Entra ID devices from one environment to another while retaining user settings.
- Modernize and migrate your devices to the cloud without resetting the device
- Provision target users, groups and contacts, including syncing passwords for AD accounts
- Customize to fit even the most complex configurations

### Domain Move

Multiple tenants can't share the same domain at the same time. When consolidating tenants, you need a solution that migrates domains without impacting user productivity and keeps email flowing while the domain is in transit. On Demand Migration (ODM) Domain Move enables you to easily and accurately migrate your SMTP domain from one tenant to another.

- Eliminate the work of building complex scripts and mapping files
- Handle tenants that have objects synced from local domains
- Get notified when administrator action is required
- Discover and replace the migrating domain from all the source object (cloud and on-premises)
- Remove the domain from the source tenant and add the domain to the target tenant
- Select options to update target usernames and add primary and proxy addresses to the target objects
- Redirect all emails during the transition of the domain to the target tenant for seamless communication without downtime

---

“On Demand Migration is very intuitive and very simple to use, even if you don’t have much migration experience. Even though I had to dart in and out of the kickoff meetings, I was able to easily pick up how the console works, how to do the initial discovery and how to execute the migrations.”

John Windsor, Infrastructure Architect FirstGroup

---

## Active Directory/Entra ID/Mail Coexistence

Establishing coexistence is often the first step toward integration and is a crucial component you must plan for from the outset, since the migration process can be lengthy. After all, if users can't communicate between tenants, business operations become chaotic. On Demand Migration offers short and long-term coexistence services for local and cloud environments. These capabilities are particularly critical during the hybrid migration projects due to the business-critical nature of the sub-systems they are servicing, such as email and calendaring.

### Active Directory/Entra ID/Coexistence

Keep migrated and non-migrated users in sync during your migration so they can easily find each other in the directory, access required resources in both environments, and collaborate with each other. On Demand Migration (ODM) Directory Sync handles even the most complex scenarios to ensure productivity across your on-premises, cloud or hybrid environment on Day One of your merger, acquisition or consolidation project.

- Keep users, devices and applications in sync in near real time, regardless of their migration status.
- Provide a unified address book that enables effective communication and collaboration across the combined organization
- Synchronize user identities to provide migrated users access to non-migrated resources
- Enable near real-time password synchronization between two directories
- Keep groups and memberships in sync between multiple environments
- Deliver both cross-domain and cross-tenant synchronization with support for multiple environments
- Customize to fit even the most complex configurations

### Mail Coexistence

Merger and acquisition deals often task IT teams with delivering a unified email presence from Day One. On Demand Migration Domain Rewrite enables users to communicate from a common email domain, delivering a single brand to the world while facilitating internal collaboration.

- Share email domains across multiple tenants
- Enable non-migrated users to send messages using a target domain from Day One before migration
- Enable migrated users to send messages using a non-migrated source domain
- Control which users send and receive mail from common domains
- Ensure secure message handling with zero delays in delivery

---

**“In the past, we used several different tools for migrations: one for Exchange, another for SharePoint and so on. We prefer the Quest (On Demand Migration) solution because it enables the migration of all Microsoft 365 workloads.”**

Luca Radicia, Head of IT Infrastructure Fedrigoni Group

---

## User Content Migration

Preserving valuable user content during a Microsoft 365 tenant-to-tenant migration is essential to ensuring that end users can communicate and remain productive after a migration. On Demand Migration (ODM) helps you migrate user-created content in Exchange and OneDrive and helps users update their Outlook profiles and connect Office applications to the new tenant.

## Exchange & Exchange Online

Email is a vital part of communication and collaboration in your workplace. Ensure that users never lose access to their email data by migrating it to their new mailbox in the target tenant. Preserve shared email data stored in public folders. Migrate legacy archived data to meet compliance needs.

- Migrate mailboxes from on-premises Exchange or Exchange Online
- Migrate Shared Mailboxes and Exchange Resource Mailboxes
- Migrate public folders (only for Exchange Online)
- Migrate recoverable items and litigation hold settings
- Filter mail by folder, type and date to shorten migration time
- Ensure uninterrupted access by migrating permissions and delegates
- Automate the switch in mail routing before and after migration
- Schedule tasks to run immediately or at a future time
- Update Teams Links in migrated meetings to ensure continued collaboration
- Update Outlook profiles once migration completes

## OneDrive

Preserve valuable data. Migrate user OneDrive accounts to the new tenant allowing users continued access to file storage.

- Migrate file versions for each document migrated
- Preserve user and sharing permissions to allow continued access
- Filter data based on folder, type, date or size to speed migration
- Add OneDrive account on the workstation once migration completes
- Schedule migration tasks to meet your schedule

## Desktop Update Agent

To support the smoothest transition possible, On Demand Migration allows you to help users with the reconfiguration of popular Windows applications. You choose when and which applications are automatically updated, and then track the progress. These applications include:

- Outlook 2016 (32-bit or 64-bit) or higher
- OneDrive for Business
- Microsoft Teams
- Office Subscription Licensing

## Shared Content Migration

Maintaining shared content is pivotal to ensure end user productivity after a Microsoft 365 tenant-to-tenant migration. On Demand Migration (ODM) helps you keep users collaborating by migrating documents, conversations and other valuable data stored in SharePoint document libraries, Teams channels and Microsoft 365 Groups. Using this SaaS solution, you can make sure end users will continue to participate and interact in discussions, even after they have been migrated, including all historical data.

## Microsoft Teams

Preserve continued collaboration. Since Teams is the hub of communication and collaboration in Microsoft 365 it's important to ensure that users never lose valuable data stored in Teams channels, conversations, and documents. Allow users to continue to participate and interact in conversations even after they have been migrated including all historical data.

- Discover all Teams on the source including team members and M365 groups
- Provision Teams and channels — including private channels — in the target tenant
- Preserve user and group access and permissions
- Migrate files and conversations stored in Teams channels

- Rename or merge Teams while migrating
- Migrate M365 Groups and content
- Migrate 1x1 chats
- Migrate planners and tasks

## SharePoint Online

Keep users sharing. Migrate documents and other valuable data stored in SharePoint document libraries and lists. Ensure continued access by preserving site and document permissions. Preserve metadata for continued compliance.

- Discover site collections and sites to plan your migration
- Preserve site, list, library, item, and document permissions
- Configure migration of versions
- Migrate classic and modern team sites to your target tenant
- Migrate documents libraries and lists
- Preserve metadata

## Quest On Demand Solutions

Platform changes and merger and acquisition (M&A) activity are occurring more frequently than ever before. If you have Microsoft 365 and you see M&A activity in your future, you will need to consolidate tenants. On top of that, like many companies, you're likely on course to move more of your systems and processes to the cloud to support your increasingly mobile workforce. Only with Quest can you take advantage of more than 20 years of expertise migrating, managing and securing Microsoft platforms — all through an Azure-hosted Software as a Service (SaaS) portfolio. We can help accelerate your quest to Entra ID and Microsoft 365.

### 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](https://www.quest.com) or follow Quest Software on [X \(formerly Twitter\)](#) and [LinkedIn](#).

## DATA SHEET

# Quest Security Guardian

Simplify and accelerate ITDR with a  
GenAI-powered hybrid AD security solution

Powered by Generative AI and seamlessly integrated with Microsoft Security Copilot, Security Guardian accelerates hybrid AD threat detection, containment and response while minimizing downtime and exposure. From a unified workspace, it identifies and prioritizes high-risk misconfigurations and exposures and proactively safeguards critical objects to prevent threats before they escalate.

Simplify security and protect Tier 0 with the ability to:

- Benchmark your current Active Directory configuration against industry-leading security hygiene practices.
- Lock down critical objects, such as GPOs, from misconfiguration and compromise.
- Continuously monitor anomalous user activities and emerging hacker tactics, techniques, and procedures (TTPs).
- Leverage Generative AI intelligence to simplify and accelerate threat detection and response.

## Benefits

- Reduce attack surface by assessing your hybrid AD against industry best practices
- Simplify AD and Entra ID security with total visibility, control and protection of critical assets
- Leverage Generative AI, Machine Learning and Microsoft Security CoPilot to identify anomalous behavior and accelerate threat response
- Stop attacks in real time by disrupting lateral movement and persistence techniques before they escalate
- Avoid alert fatigue and identify real threats by focusing on high-value alerts
- Weave together security signals, ensuring swift threat response





With 600 million identity attacks taking place daily, securing identity is essential for maintaining business continuity, particularly in hybrid environments with Active Directory and Entra ID. The consequences of failure are dire, with Forrester reporting AD downtime costing up to \$730K per hour. Unfortunately, identity security is complex, and many organizations face a shortage of expertise and resources, making it even harder to efficiently detect and respond to threats across sprawling, misconfigured environments.

Security Guardian addresses these challenges with powerful Generative AI and Machine Learning capabilities that empower organizations to detect anomalous behaviors, reduce alert fatigue, and proactively protect critical assets. Integrated with Microsoft Security Copilot, it delivers intelligent, automated identity threat detection and response across hybrid AD.

## Hybrid AD Security Assessment

Benchmark your current configurations against pre-defined industry best practices. Surface exposures and compromises that exist within the environment. Quickly mitigate these risks and reduce your attack surface..

## Critical Asset Focus

Identify and prioritize Tier 0 assets effortlessly, ensuring that your most exploitable components receive the utmost attention. Gain full control over these critical assets, enabling you to modify the Tier 0 list dynamically, so you're always aligned with your organization's evolving needs.

## Proactive Threat Prevention

Activate dynamic, in-memory protection for Tier 0 assets, including sensitive GPOs, with the Shields Up capability. Contain incidents mid-flight by disrupting lateral movement and persistence techniques before they escalate, so you can protect critical systems in real time, not after damage is done. Get focused reports on object status, as well as the ability to effortlessly revert any unwanted changes to a previous, trusted state.

## Automated Threat Detection

Leverage Generative AI and Machine Learning to detect unusual activity in Active Directory and Entra ID, such as spikes in account lockouts, failed sign-ins, permission changes and file renames. Continuously monitor hacker TTPs (Tactics, Techniques and Procedures) and audit changes. With one click, Security Guardian GenAI Intelligence translates data into business-relevant summaries, enabling security teams to streamline investigations and effectively communicate risk to executives and stakeholders.

## Intelligent Incident Response

Quickly understand the who, what, where and when of threats by connecting anomalies and highlighting key security signals. Security Guardian's Generative AI delivers intelligent and contextual notifications, tailored remediation guidance and actionable recommendations designed for your environment, for faster, more confident risk mitigation. Seamlessly forward data collected to SIEM tools like Microsoft Sentinel and Splunk for integrated visibility and streamlined operations.

## Microsoft Security Copilot Integration

Security Guardian integrates with Microsoft Security Copilot to provide comprehensive protection for your hybrid AD environment. By combining the strengths of both platforms, you gain a powerful solution that simplifies complex security threats, accelerates your response times, and empowers your security team to operate at peak efficiency.

## Unified Security Workspace

Remove the complexity from AD and Entra ID security by focusing on core operations with a friendly user interface that provides visibility into exposures, vulnerabilities and other security signals seamlessly.

---

“Security Guardian is the best tool we could find available for identity threat hunting in Active Directory.”

CISO, Large Media Company

---

### 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](https://www.quest.com) or follow Quest Software on [X \(formerly Twitter\)](#) and [LinkedIn](#).

Explore our solutions →

