

Commvault Identity Resilience

Radically Simplifying and Accelerating Recovery in Active Directory

By Alex Arcilla, Senior Principal Validation Analyst
Omdia

SEPTEMBER 2026

Contents

Introduction	3
Background	3
Commvault Identity Resilience	4
Omdia Technical Validation.....	5
Automated AD forest recovery	5
Granular recovery	9
Restoration for cloud-based identity providers	11
Conclusion.....	13

Introduction

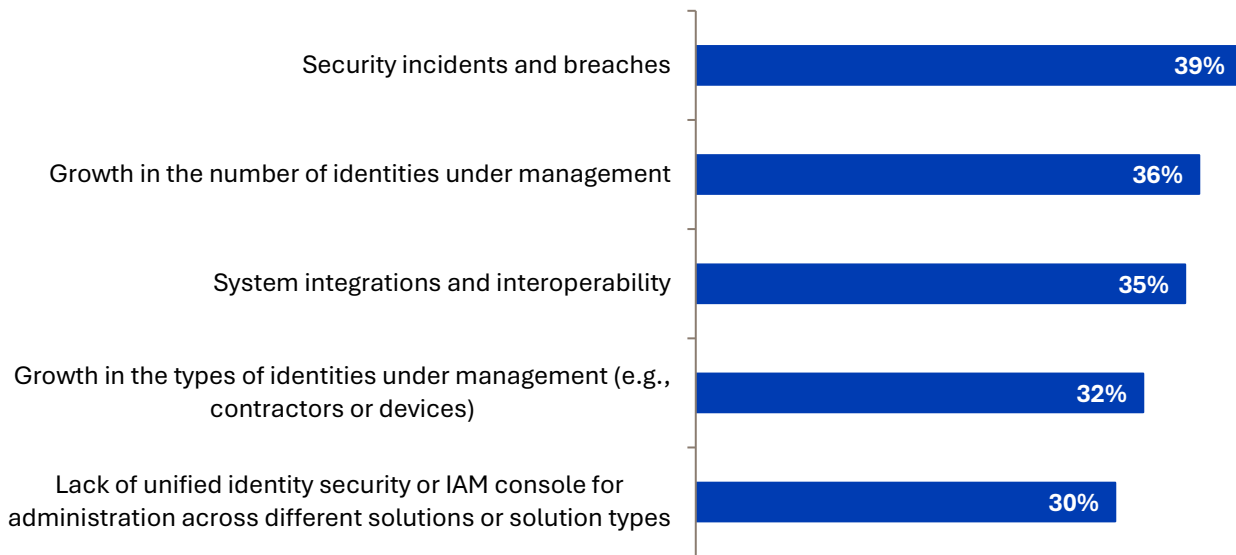
This Omdia Technical Validation documents our evaluation of Commvault Identity Resilience. We review how the solution can help organizations bolster their identity resilience as bad actors increase their attacks on compromised workforce identities. Specifically, we validate that Commvault Identity Resilience can significantly reduce both the time and manual effort typically spent on recovering from attacks and unauthorized changes using traditional prescribed methods.

Background

Growth in workforce identities is expected to continue, with nearly 80% of organizations anticipating increases in both employee identities and the number of applications and data sources to be accessed for the foreseeable future.¹ It is no surprise, then, that managing workforce identities has emerged as a critical issue, with organizations most often citing security incidents and breaches as a top challenge they face (see **Figure 1**).² Complicating how effectively organizations can prevent further attacks is the use of AI to accelerate the speed and scale of their (lateral) attacks, as bad actors steal credentials, leverage unauthorized privilege modifications and manipulate directories.

Figure 1. Top 5 cited challenges for managing workforce identities

Which of the following challenges does your organization face when managing workforce identities? (Percent of respondents, n=370, multiple responses accepted)



Source: Omdia

Microsoft Active Directory (AD) is a prime target for attacks (e.g., credential theft, privilege escalation), as numerous enterprise IT environments use this identity provider (IdP) to manage both authorization and authentication to applications and data across on-premises infrastructures. Yet, if AD is brought down by an attack, the recovery process is highly manual and complex.

¹ Source: Enterprise Strategy Group (now Omdia) Research Report, *Identity Security at a Crossroads: Balancing Stability, Agility, and Security*, September 2025.

² Ibid.

The typical recovery process is driven by rigid documented procedures, consisting of 50 to 100 or more steps that must be completed in a specific sequence. Completing these steps can take days or weeks, adding to the unplanned downtime already incurred in the attack. If security vulnerabilities are exposed during the process (e.g., AD misconfigurations, exposed credentials), administrators must close these security gaps before restarting the recovery process, leading to additional unwanted downtime. In enterprises with multiple domains and hundreds of domain controllers across geographically distributed infrastructures, multi-domain AD forest recovery becomes much more complex and time consuming, adding even more unwanted downtime.

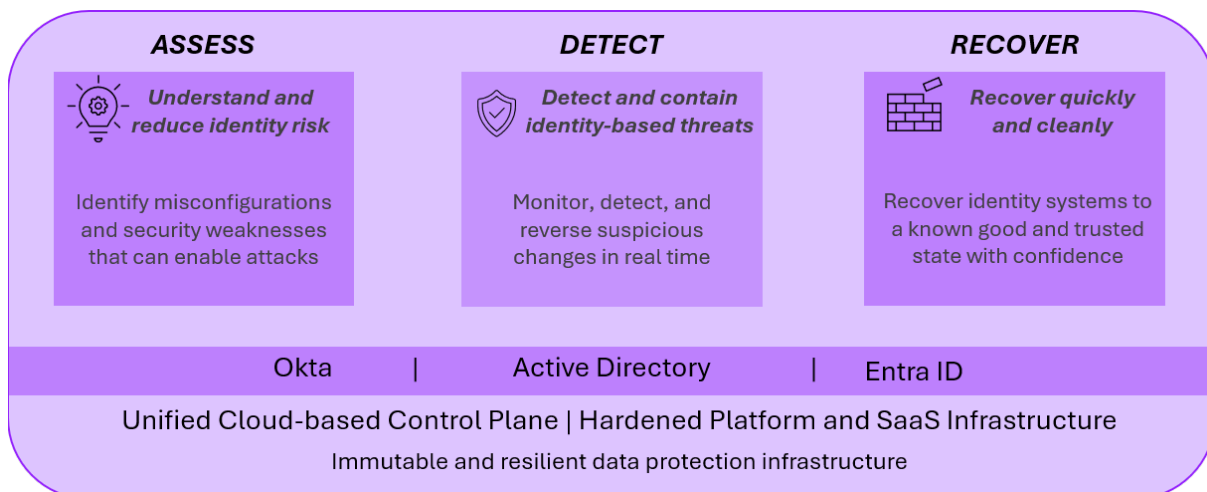
Organizations then bear the burden of slow and complex AD recovery: ceased business operations, since users cannot authenticate and applications and data are inaccessible, and financial and security risk, especially if overlooking any vulnerabilities while attempting to recover.

These challenges call for a solution that minimizes manual effort while ensuring that any security vulnerabilities in the original AD configuration are addressed.

Commvault Identity Resilience

Designed to help organizations make the identities managed and administered with Microsoft AD both recoverable and resilient, Commvault Identity Resilience is a cloud-based solution that identifies and closes identity security lapses and gaps. It backs up and recovers the AD and cloud-based IdP configurations that support an organization's often-sprawling hybrid cloud environments while providing automation for complex restoration procedures. This solution specifically helps build an overall resilient identity security posture by focusing on three key activities: proactively assessing risk, detecting and containing threats in real time, and recovering from cyberattacks, corruption, or operational failures (see **Figure 2**).

Figure 2. Commvault Identity Resilience



Source: Commvault and Omdia

With its unified control plane, the solution automatically coordinates and orchestrates tasks associated with assessment, detection, and recovery activities, eliminating the need to use the multiple tools and interfaces organizations have relied upon to date. Organizations can then reduce the time and effort spent on locating and closing identified security gaps as well as recovering from attacks or corruption, thus maximizing their

operational uptime. Commvault's unified interface is designed to work across enterprise-class hybrid cloud environments and the multiple identity providers implemented in them (e.g., AD with Entra ID or Okta).

Commvault Identity Resilience was built to help organizations recover from security events with minimal risk of error, thus saving both time and manual effort expended. Recovery can occur with increasing levels of granularity—from object level to full forest—so that the entire AD configuration can be returned to a fully trusted state validated as free from compromise, not just an operational state where security gaps and risks remain unaddressed. This approach minimizes, if not eliminates, the chances for future attacks to take advantage of any remaining vulnerabilities.

- With object-level (or granular) recovery, organizations can recover objects and their associated attributes and permissions without a complete, time-consuming rebuild of AD. Large-scale rollbacks can also be performed when unauthorized or incorrect changes affect multiple identities.
- With AD forest-level recovery, organizations can leverage the solution's automation and orchestration via pre-built runbooks. With this approach, organizations can rapidly execute the high number of necessary steps in Microsoft's prescribed sequence. This results in a return to a trusted state in the shortest possible time, while eliminating the need to restart the process if AD misconfigurations are uncovered.

Orchestration delivered by Commvault Identity Resilience ensures that specific recovery tasks are completed before moving onto the next task, while adhering to Microsoft's prescribed sequence: recovering the correct domain controllers in proper sequence, executing hygiene tasks between each domain controller restoration, coordinating parallel recovery operations across multiple geographies, and preventing replication conflicts and directory inconsistencies. During the recovery process, the solution corrects any uncovered misconfigurations and removes the need to restart the recovery process, which often risks additional business downtime. Orchestration also removes the need to manually coordinate tasks during AD recovery.

To ensure that AD recovery is done cleanly, identity backups are managed using Commvault's isolated, immutable architecture. With this solution, backups can be protected in tamper-resistant storage designed so that they cannot be modified or deleted by compromised credentials.

Organizations have the option to leverage Commvault's expertise if needed, developed through experience across multiple companies worldwide, to implement the proper recovery architecture before installing Commvault Identity Resilience. This enables the solution's runbooks to be optimized and applied repeatedly.

Omdia Technical Validation

Through online demonstrations and briefings, Omdia validated how Commvault Identity Resilience can continually reduce the time and manual effort typically spent on recovering from AD attacks, as compared to relying on traditional processes and workflows. We specifically evaluated how Commvault Identity Resilience enables organizations to recover quickly from attacks, corruptions, or accidental changes/deletions at the forest, object, and attribute levels.

Automated AD forest recovery

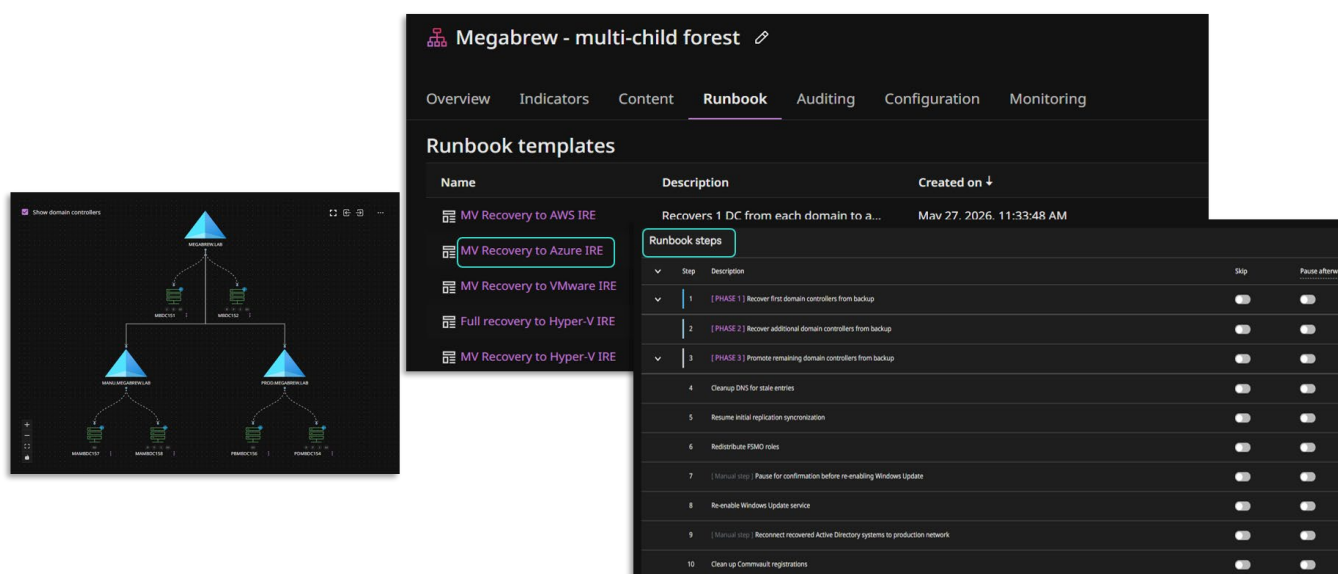
Manual AD forest recovery requires the execution of no less than 50—and frequently more than 100—sequential steps with precise timing and coordination. At the same time, any AD misconfigurations encountered must be corrected, typically requiring the recovery process to restart from Step One.

Additionally, the large amount of manual effort needed creates a high risk of human error and extended downtime. Automation and orchestration with Commvault Identity Resilience can significantly reduce the time and effort typically required for manual AD recovery, potentially down to a few hours, without the risk of incurring human error.

To evaluate how recovery time decreases with Commvault Identity Resilience, Omdia observed how to execute an AD forest recovery for the “Megabrew” company (see left side of **Figure 3**). We should note that a full forest recovery performed by Commvault’s solution recovers every domain controller in the forest, not just a single DC. In this case, we also chose to run a “minimal viable” recovery (i.e., restoring the minimum set of DCs required to keep the business operational) to determine if the AD forest can be fully restored without encountering any additional issues.

From the Commvault interface, we chose to recover to an isolated recovery environment (IRE), as recommended by Microsoft. We selected the runbook “MV Recovery to Azure IRE” and clicked to reveal the steps within it (see right side of **Figure 3**).

Figure 3. Selecting the runbook for recovery of Megabrew multi-child forest



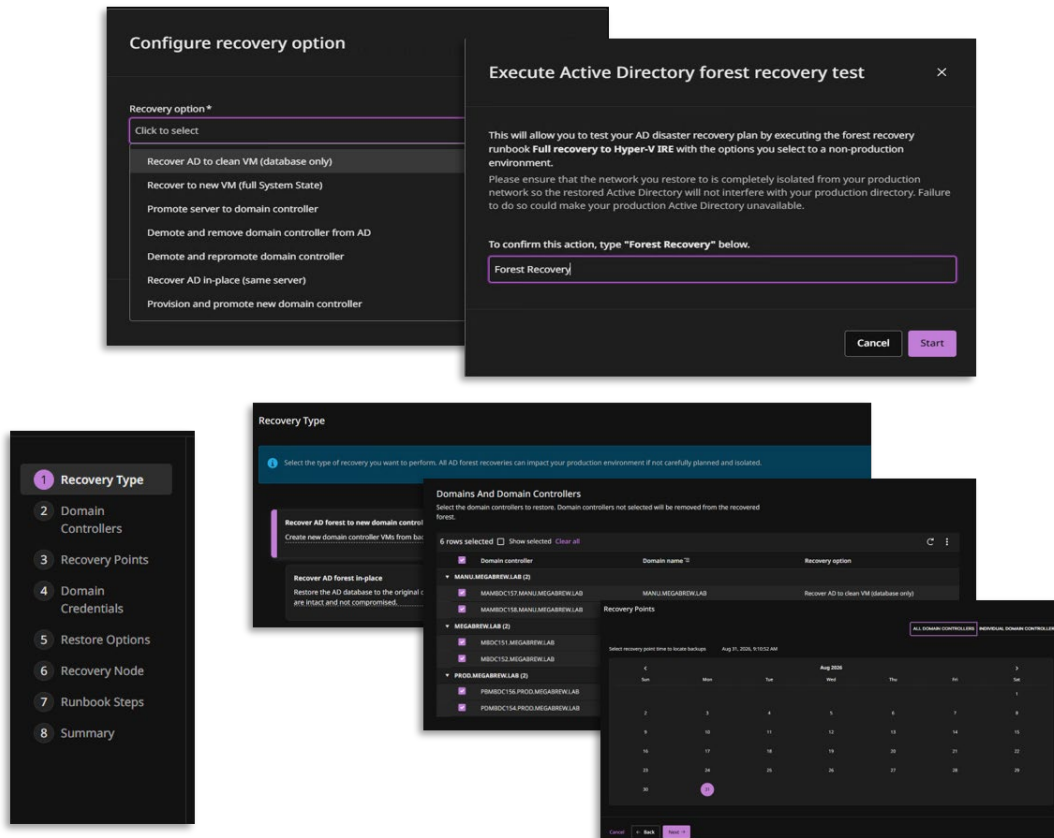
Name	Description	Created on
MV Recovery to AWS IRE	Recovers 1 DC from each domain to a...	May 27, 2026, 11:33:48 AM
MV Recovery to Azure IRE		
MV Recovery to VMware IRE		
Full recovery to Hyper-V IRE		
MV Recovery to Hyper-V IRE		

Step	Description	Skip	Pause afterward
1	[PHASE 1] Recover first domain controllers from backup	☐	☐
2	[PHASE 2] Recover additional domain controllers from backup	☐	☐
3	[PHASE 3] Promote remaining domain controllers from backup	☐	☐
4	Cleanup DNS for stale entries	☐	☐
5	Resume initial replication synchronization	☐	☐
6	Redistribute FSMO roles	☐	☐
7	[Manual step] Pause for confirmation before re-enabling Windows Update	☐	☐
8	Re-enable Windows Update service	☐	☐
9	[Manual step] Reconnect recovered Active Directory systems to production network	☐	☐
10	Clean up Commvault registrations	☐	☐

Source: Omdia

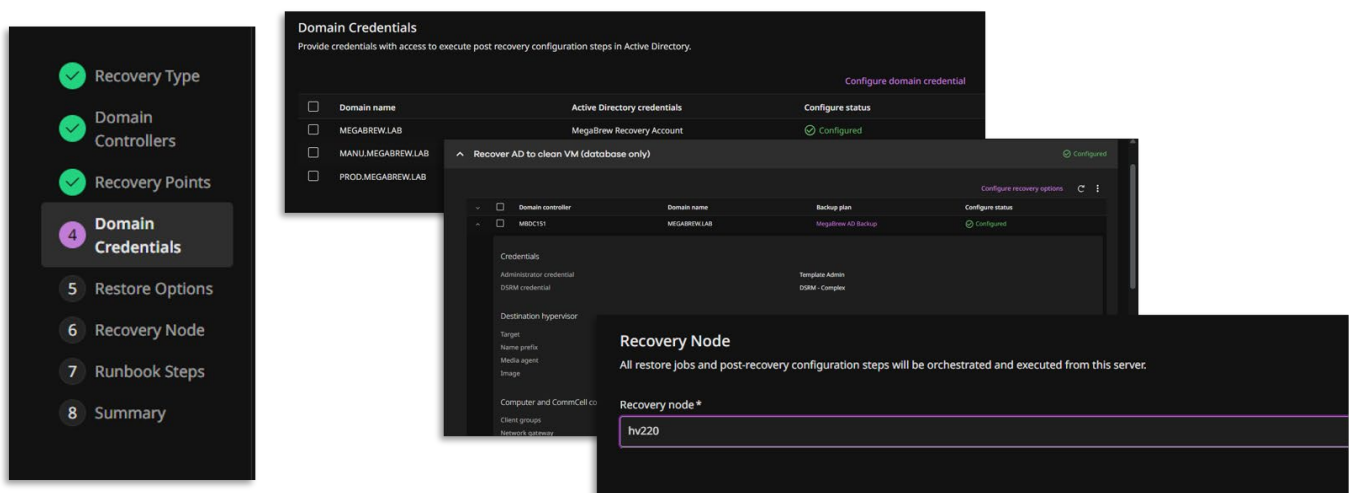
Before running the playbook, we were prompted to choose a recovery type: “Recover AD forest to new domain controllers” or “Recover AD forest in place.” After selecting the first option, the solution prompted us to configure the recovery settings. **Figure 4** displays the steps to select domains and DCs to be recovered and the date of the recovery point to be restored, while **Figure 5** displays the steps for selecting the domain credentials to permit the recovery to proceed, restore options (e.g., the destination hypervisor), and the recovery node (i.e., the server from which the recovery will be initiated).

Figure 4. Selecting the scope of the AD recovery and the recovery point



Source: Omdia

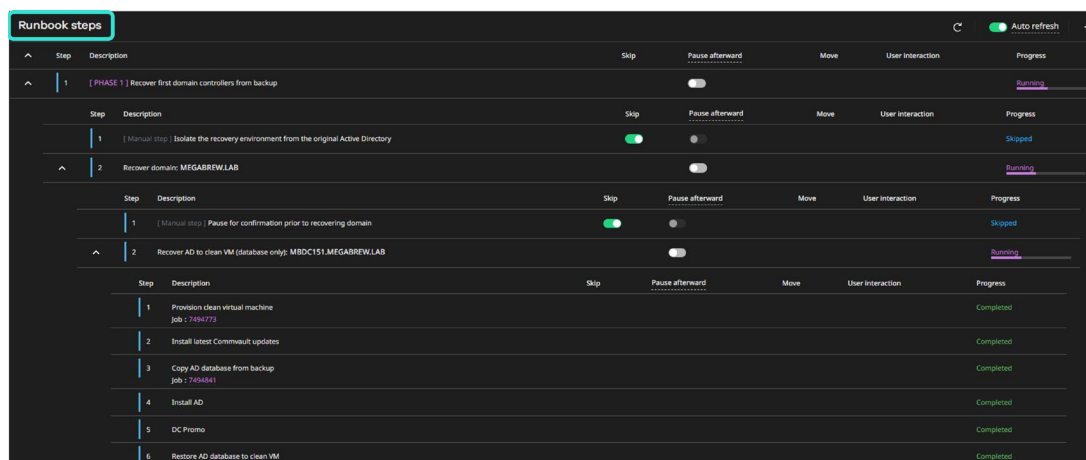
Figure 5. Selecting the domain credentials, restore options, and recovery node



Source: Omdia

After all settings were selected, we executed the runbook as shown by the progress bars displayed by each step in **Figure 6**. Progress was noted as “Pending,” “Completed,” or “Skipped.”

Figure 6. Runbook executing the AD forest recovery



Source: Omdia

While the runbook automated and orchestrated each step, we also noted that the recovery settings inputted previously dictated whether some steps were omitted (as denoted by the “Skipped” label). Once the runbook was executed, we also noted that the solution automatically performed critical post-restoration tasks, such as computer password resets and replication health checks.

By automating and orchestrating the necessary AD recovery steps, while addressing any security vulnerabilities encountered, Omdia saw how Commvault can significantly decrease recovery time from days or weeks to hours. This represents a huge improvement over an administrator manually executing the 50 to 100-plus steps, *assuming that the AD environments have been configured properly prior to the recovery attempt*.

Omdia also noted that the selected runbook and recovery option (and related settings) prompts Commvault Identity Resilience to skip steps that are unnecessary to execute or run specific steps in parallel (e.g., multiple domain controllers can be restored simultaneously across different domains). We should point out how these approaches can further reduce recovery time. When attempting an AD forest recovery manually, knowing which steps can be skipped or attempting to execute steps in parallel can be difficult. Commvault’s orchestration removes the guesswork and uncertainty, as well as the additional manual effort.

Additionally, the runbook configuration and ability to recover into an IRE provide organizations with the capability to practice their recovery strategy regularly. To build confidence in executing recoveries and help satisfy compliance requirements, organizations can execute their recovery runbooks in isolation. This goes far beyond validating that backups exist or that recovery settings are correctly configured. It performs the recovery of the AD forest itself, enabling teams to validate the complete recovery process, measure recovery times, identify gaps, and gain hands-on experience before a real incident occurs. A recovery plan should not be something an organization executes for the first time during a crisis.

Why this matters

Restoring an AD forest from a cybersecurity attack is manually tedious. While existing Microsoft documentation can guide the recovery process, the 50 to 100-plus steps must be executed in a prescribed manner, assuming that the AD forest was configured correctly prior to the attack. Performing these steps manually already consumes more time and effort than desired, with typical recoveries lasting days or weeks. Time is also consumed when needing to restart the process should any AD misconfigurations need to be corrected.

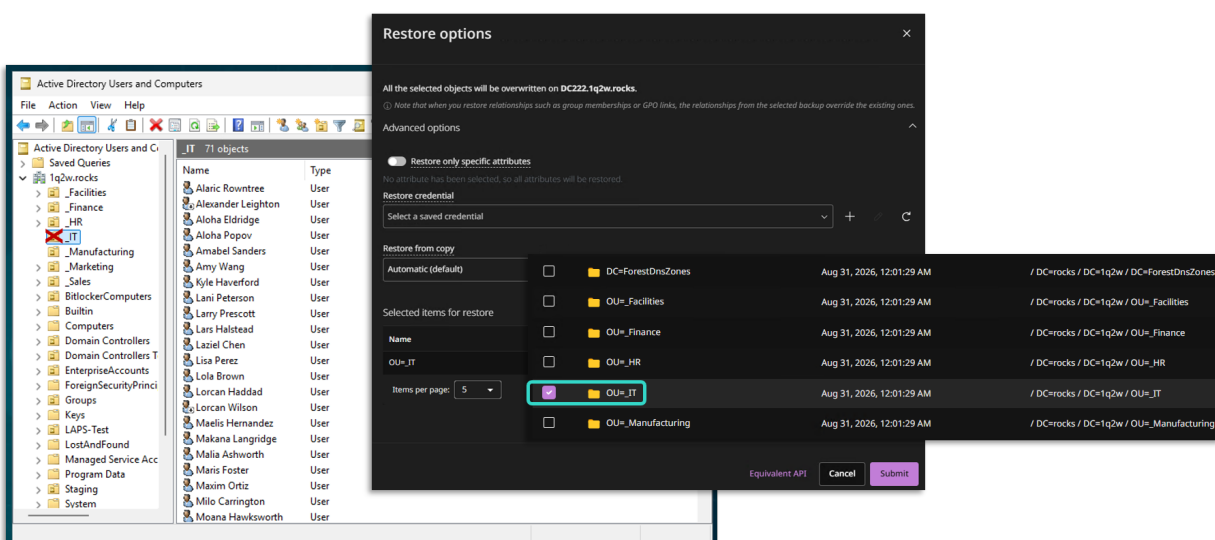
Omdia validated that Commvault Identity Resilience can significantly reduce the time and manual efforts spent on AD forest recoveries. We observed how the automation and orchestration of the recovery steps prescribed by Microsoft helped to decrease the overall recovery time. We also observed how Commvault Identity Resilience determines the most efficient way to execute the process, such as skipping unnecessary steps and performing tasks in parallel. Recovery times can be as low as a 1.5 hours based on reported recovery times. Lower recovery time maximizes operational uptime and decreases business and financial risk.

Granular recovery

Common scenarios, such as accidental deletions, attribute changes, or the corruption of specific objects, only require a few recovery steps, unlike an AD forest recovery. However, those steps must be completed manually (such as writing scripts), along with post-recovery steps to ensure that security remains uncompromised. Commvault Identity Resilience can help organizations accomplish this level of granular recovery quickly and easily while reducing the manual effort typically required.

To illustrate the simplicity of an object-level recovery, Omdia navigated to an AD domain named “1q2w.rocks.” We considered a scenario in which the “IT” organizational unit, containing 71 objects, was accidentally deleted (see left side of **Figure 7**). Using the Commvault interface, we located the last known backup named “OU=_IT” in the DC named “DC222” and restored it (see right side of **Figure 7**). Omdia observed that the time for restoration of 71 objects (or names of people within the IT organization) in the “IT” OU was under a minute.

Figure 7. Restoring the accidentally deleted IT OU from ‘1q2w.rocks’



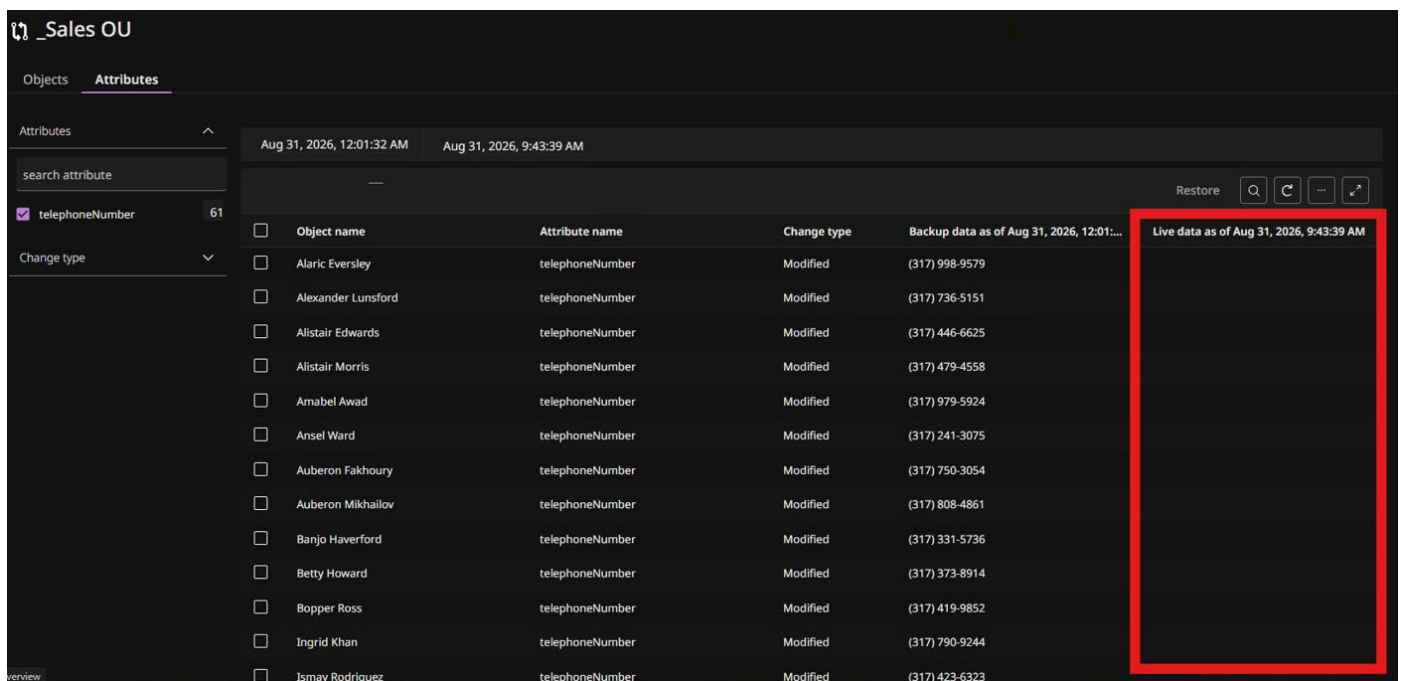
Source: Omdia

Omdia then reviewed how organizations can use object comparison to quickly detect specific attribute changes (e.g., phone numbers, office locations, group memberships) that were not supposed to occur. Instead of resorting to the recovery of entire objects, Commvault Identity Resilience enables selective restoration of individual attributes without affecting other object properties.

We observed how we could examine the “before and after” of attribute changes at the OU and user level by comparing the latest backup with live data. **Figure 8** shows a comparison of changes in phone numbers of members within the “Sales OU” between a backup from a specific date and live data. Any differences between backup and live data can instantly flag what needs to be updated. Backups taken at different times can also be compared.

After discovering these discrepancies, Omdia observed that the recovery only required a few clicks and selections from the options presented by Commvault Identity Resilience. With the granular recovery capability, Omdia saw how an administrator can eliminate the need to perform a more extensive recovery, translating into minimal downtime for the business.

Figure 8. Comparing attributes using backup and live data



Attributes		Aug 31, 2026, 12:01:32 AM	Aug 31, 2026, 9:43:39 AM
☒ telephoneNumber	61		
Object name	Attribute name	Change type	Backup data as of Aug 31, 2026, 12:01:32 AM
☐ Alaric Eversley	telephoneNumber	Modified	(317) 998-9579
☐ Alexander Lunsford	telephoneNumber	Modified	(317) 736-5151
☐ Alistair Edwards	telephoneNumber	Modified	(317) 446-6625
☐ Alistair Morris	telephoneNumber	Modified	(317) 479-4558
☐ Amabel Awad	telephoneNumber	Modified	(317) 979-5924
☐ Ansel Ward	telephoneNumber	Modified	(317) 241-3075
☐ Auberon Fakhoury	telephoneNumber	Modified	(317) 750-3054
☐ Auberon Mikhailov	telephoneNumber	Modified	(317) 808-4861
☐ Banjo Haverford	telephoneNumber	Modified	(317) 331-5736
☐ Betty Howard	telephoneNumber	Modified	(317) 373-8914
☐ Bopper Ross	telephoneNumber	Modified	(317) 419-9852
☐ Ingrid Khan	telephoneNumber	Modified	(317) 790-9244
☐ Ismay Rodriguez	telephoneNumber	Modified	(317) 423-6323

Source: Omdia

Why this matters

Recovering from small yet significant events that affect regular business operations, such as accidental deletions, attribute changes, and object-level corruption in AD, still requires some manual effort (e.g., scripting), along with post-recovery work to maintain AD security going forward. While not a full AD forest recovery, such efforts still consume time and delay the business from completing its tasks.

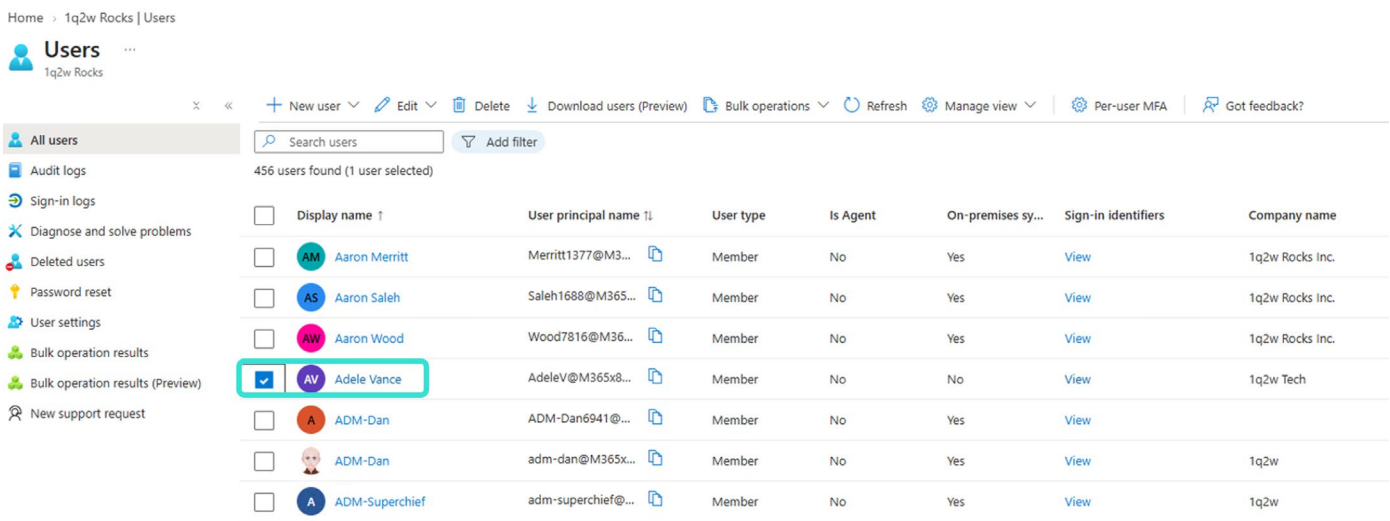
Omdia validated that Commvault Identity Resilience can simplify how organizations recover from errors, deletions, or corrupted objects and attributes before they are reported. We observed how organizations can compare data associated with objects and attributes to confirm that the latest and correct data is reflected, such as comparison between backup and live data or between backups. Recovering only requires a few clicks to resolve discrepancies, along with any post-recovery steps.

Restoration for cloud-based identity providers

When AD is installed on-premises along with cloud-based IDPs, specifically Entra ID and Okta, restoring the appropriate policies is paramount so that access privileges remain intact and consistent across hybrid clouds. However, different processes and workflows (with the associated tools) are in place when recovery needs to occur, easily leading to unwanted downtime when working with more than one IdP. With the unified control plane of Commvault Identity Resilience, organizations can recover across on-premises and cloud-based IdPs in a uniform manner.

To review this capability, Omdia first navigated to Entra ID, the cloud version of AD for Microsoft Azure associated with the Megabrew company. Since both AD and Entra ID are synchronized, we saw that the user “Adele Vance” was also recovered in Entra ID after initiating the recovery in AD (see **Figure 9**). We noted how quickly the recovery took place, as this was a cloud-to-cloud recovery (between Commvault and Azure).

Figure 9. Simultaneous recovery of user in AD and Entra ID

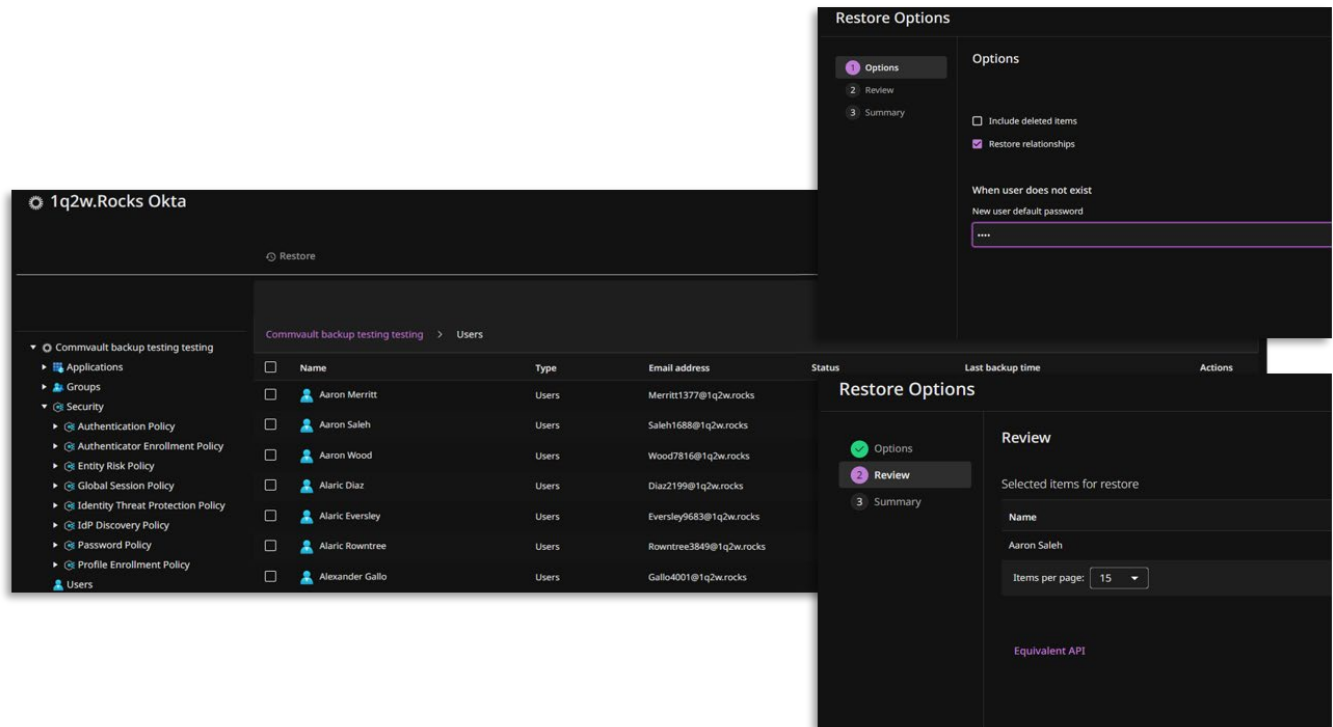


Display name	User principal name	User type	Is Agent	On-premises sy...	Sign-in identifiers	Company name
☐ Aaron Merritt	Merritt1377@M3...	Member	No	Yes	View	1q2w Rocks Inc.
☐ Aaron Saleh	Saleh1688@M365...	Member	No	Yes	View	1q2w Rocks Inc.
☐ Aaron Wood	Wood7816@M36...	Member	No	Yes	View	1q2w Rocks Inc.
☒ Adele Vance	AdeleV@M365x8...	Member	No	No	View	1q2w Tech
☐ ADM-Dan	ADM-Dan6941@...	Member	No	Yes	View	1q2w
☐ ADM-Dan	adm-dan@M365x...	Member	No	Yes	View	1q2w
☐ ADM-Superchief	adm-superchief@...	Member	No	Yes	View	1q2w

Source: Omdia

We then worked with Okta to view the identities associated with our previous domain, “1q2w.rocks.” We chose the same user from the previous demo and proceeded to restore the related identity (see **Figure 10**). As we saw in previous demos, restoring this identity simply required right-clicking on the identity to be restored and choosing the parameters to guide how the recovery would proceed.

Figure 10. Restoring Okta identity within the ‘1q2w.rocks domain’



Source: Omdia

Without Commvault Identity Resilience, an administrator would need to work directly with Okta and its processes and workflows, leading to unwanted additional effort.

Why this matters

In situations where an organization works with both AD on-premises and cloud IdPs, recovering from an attack can be difficult, as each IdP offers its own unique tool sets and processes. However, the lack of uniformity can lead to complexity when needing to recover identity-related information, either at the granular or forest levels.

Omdia validated that Commvault Identity Resilience provides a uniform recovery experience in hybrid environments where AD and Entra ID or Okta are in place. The unified control plane provides a consistent way to initiate recoveries, resulting in less operational complexity and less time needed for recovery.

Conclusion

Securing identities is a critical issue to address, as employees require access to critical business applications and data. Bad actors seek ways to infiltrate organizations via compromised credentials, privilege manipulation, and backdoor accounts. With AI in the mix, such (lateral) attacks can now occur faster than ever before, making recovery that much more important to achieve as quickly as possible.

Since AD remains the predominant IdP for a majority of IT environments, it remains a prime target for cyberattacks. However, the typical recovery can last days, if not weeks or months, as the prescribed recovery process consists of multiple steps that must be completed as sequenced. Unfortunately, recovery then becomes a time-consuming and tedious manual process. Moreover, the prescribed sequence assumes that AD has been configured properly when first installed; if not, misconfigurations must be corrected, and the process must restart. With the threat of unwanted downtime, organizations need a better and more efficient way to recover from an AD attack.

Commvault Identity Resilience is designed to help organizations minimize downtime from an AD attack by greatly simplifying how recovery can occur. By automating and orchestrating prescribed tasks defined by Microsoft's prescribed process, this solution can drastically decrease the time and manual effort required. By minimizing recovery downtime, business operations can recover more quickly, decreasing both business and financial risk.

Throughout this evaluation, Omdia validated that Commvault Identity Resilience can recover easily from both full-scale security attacks as well as granular events, such as accidental deletions or object-level corruption. We found that this solution can:

- Drastically reduce the time and manual effort traditionally spent on recovering an AD forest if attacked by leveraging Commvault's automation and orchestration of the 50 to 100-plus prescribed steps.
- Simplify how granular recovery can be accomplished at both the object and attribute level using a comparison between backup and live data or between backups.
- Restore cloud-based identities in a consistent and uniform manner, eliminating the need to work with different tool sets.

If your organization is facing the challenge of reducing recovery time for AD and associated IdPs in hybrid cloud environments, we strongly recommend looking more closely at Commvault Identity Resilience.

Copyright notice and disclaimer

The Omdia research, data, and information referenced herein (the “Omdia Materials”) are the copyrighted property of TechTarget, Inc. and its subsidiaries or affiliates (together “Informa TechTarget”) or its third-party data providers and represent data, research, opinions, or viewpoints published by Informa TechTarget and are not representations of fact.

The Omdia Materials reflect information and opinions from the original publication date and not from the date of this document. The information and opinions expressed in the Omdia Materials are subject to change without notice, and Informa TechTarget does not have any duty or responsibility to update the Omdia Materials or this publication as a result.

Omdia Materials are delivered on an “as-is” and “as-available” basis. No representation or warranty, express or implied, is made as to the fairness, accuracy, completeness, or correctness of the information, opinions, and conclusions contained in Omdia Materials.

To the maximum extent permitted by law, Informa TechTarget and its affiliates, officers, directors, employees, agents, and third-party data providers disclaim any liability (including, without limitation, any liability arising from fault or negligence) as to the accuracy or completeness or use of the Omdia Materials. Informa TechTarget will not, under any circumstance whatsoever, be liable for any trading, investment, commercial, or other decisions based on or made in reliance of the Omdia Materials.

Get in touch: www.omdia.com askananalyst@omdia.com

