Commvault's Cloud Rewind & New Cyber Resilience Capabilities

STEVE MCDOWELL, CHIEF ANALYST
10/14/24

CONTEXT

Commvault announced a series of updates at its London Shift customer event. The key updates include the launch of Cloud Rewind and the general availability of Commvault Cloud on AWS, alongside enhanced cyber recovery capabilities.

CLOUD REWIND

Cloud Rewind integrates several advanced capabilities to improve cloud cyber recovery and resilience.

The most critical aspects of the solution include:

- **Application and Infrastructure Rebuild**: Cloud Rewind automates the recovery and rebuild process across multi-cloud environments, focusing not only on data but also on the infrastructure and configurations that support that data. The feature supports full cross-account and cross-region replication.
- **Dependency Mapping** analyzes and defines relationships between cloud components, providing automatic restoration of interdependent services, minimizing manual intervention, and decreasing mean time to recovery (MTTR).
- **Drift Analysis**: By monitoring and identifying deviations from original configurations, Cloud Rewind helps ensure that restored systems are aligned with their pre-incident states.
- **Multi-cloud visibility** offers continuous monitoring of cloud resources across all environments, allowing real-time visibility into potential vulnerabilities and necessary recovery points.

- **Cloud Map** maintains historical snapshots of dependency maps and configuration data, offering the ability to rewind and restore to a clean state in the event of a cyberattack or failure.

CYBER-RESILIENCE DASHBOARD

A new Cyber Resilience Dashboard complements Commvault's cloud-native rebuild capabilities, offering continuous ransomware readiness assessments. This includes:

- **Visibility Across Data Estate** by providing a comprehensive view of resilience readiness, covering areas such as frequency of testing, success rates, and availability of immutable, air-gapped backups.
- **Recovery-as-Code** automates the testing and recovery process by capturing data and operational blueprints of applications, infrastructure, and networking configurations.

DORA COMPLIANCE WITH PURE STORAGE PARTNERSHIP

DORA is a new EU regulatory framework designed to improve the cyber resilience of financial institutions. Commvault is collaborating with Pure Storage to ensure that financial institutions have the tools to meet the stringent requirements of the new regulations. This includes:

- **Continuous Testing**: By enabling recovery tests in isolated environments, Commvault ensures compliance with DORA’s requirement for continuous operational testing.
- **Rapid Restoration**: The solution offers flexible recovery of clean data in isolated environments, ensuring data sovereignty and operational resilience.

EXPANDED AWS OFFERINGS

Commvault's Cloud Rewind on AWS, built on Appranix technology, serves as an automated recovery solution designed to mitigate the complexity of restoring distributed cloud applications and infrastructure after a cyber incident.

The expanded capabilities available to AWS customers include:

- **Cloud Rewind**: This tool enables organizations to "rewind" to the last clean state of their data and cloud configurations, offering automated rebuilds of applications and infrastructure across regions and accounts. This significantly reduces the mean MTTR from weeks or days to what Commvault claims is “minutes.”

- **Cyber Resilience for Amazon S3**: With the introduction of Clumio technology, Commvault adds the ability to rapidly restore clean data in Amazon S3 environments after a malware attack, benefiting enterprises handling large datasets such as AI and ML workloads.

- **Air Gap Protect**: This solution provides AWS customers with immutable copies of their data stored in an isolated Commvault tenant.

- **Cleanroom Recovery**: Extending this feature to AWS, Commvault allows organizations to provision isolated recovery environments for forensic analysis and secure testing of their recovery plans, enhancing preparedness and compliance.

EXTENDED GOOGLE WORKSPACE & SAAS INTEGRATION

Commvault's extended support for Google Workspace protection is another strategic step in strengthening its position as a cloud-native resilience provider. Protecting Gmail, Google Drive, Shared Drives, and built-in Google Cloud Storage enables organizations to meet compliance mandates while maintaining business continuity across cloud environments.

In addition, the new Cloud Rewind integrates with Google Cloud, offering rapid recovery of applications and infrastructure. This reflects Commvault's commitment to addressing cloud complexity through automation and infrastructure rebuild.

ANALYSIS

Commvault's announcements highlight its cloud-first approach. Whether using AWS, Google Cloud, or a hybrid cloud infrastructure, Commvault is increasingly focused on ensuring its solutions are cloud-native and capable of operating seamlessly in multi-cloud environments.

Here are some key observations about the announcements and Commvault's recent moves:

1. **Cloud Rewind is a Market Differentiator**

    - Commvault's focus on rapid, automated recovery of cloud environments sets it apart from traditional data protection vendors, which often emphasize data backup without addressing the more complex recovery challenges involving applications and infrastructure.

- In the current environment, where cloud configurations are constantly evolving, the ability to automate the rebuild process through dependency mapping and drift analysis significantly reduces downtime. This places Commvault ahead of competitors like Veeam and Rubrik, which may still rely on more manual processes for full cloud environment recovery.

2. **Multi-Cloud Support and SaaS Protection**
    - A unified recovery solution becomes critical as organizations diversify their cloud deployments across multiple providers (AWS, Google Cloud, Azure). Commvault's multi-cloud approach and protection for major SaaS applications like Google Workspace address this market gap.
    - With the integration of Appranix technology, Cloud Rewind offers a more robust cross-cloud recovery solution. This allows organizations to manage complex, distributed environments with confidence, a strong differentiator in an increasingly multi-cloud world.

3. **Strategic Focus on Cyber Resilience**
    - With DORA set to arrive in January 2025, Commvault's partnership with Pure Storage to offer continuous testing and recovery for financial institutions should resonate with organizations under regulatory pressure within the EU. The ability to test recovery in isolated environments aligns well with the operational resilience mandates in financial services, giving Commvault an edge as these institutions seek compliance solutions.
    - Beyond the financial sector, its focus on operational resilience and regulatory compliance may appeal to other industries facing similar pressures, including healthcare and critical infrastructure.

4. **Shift from Data Recovery to Operational Recovery**
    - Commvault’s narrative, particularly around Cloud Rewind, reframes recovery from being solely about data protection to focusing on operational continuity. This shift is essential as

organizations increasingly view downtime as the real threat in the event of a cyberattack.

- Traditional recovery processes focusing on restoring static data do not fully address the challenges of rebuilding dynamic cloud environments. Commvault's approach acknowledges that recovery today must account for rapidly changing cloud configurations and interdependencies between applications. This evolution will likely resonate with large enterprises looking to minimize disruption in complex IT environments.

Commvault’s strategic push for cloud-native recovery sets it apart from competitors like Veeam and Rubrik, which focus heavily on traditional backup and recovery but offer different levels of automation for restoring cloud infrastructure. By combining data recovery with full cloud application rebuild capabilities, Commvault addresses the complexity of modern cloud environments with a robust set of rapidly expanding capabilities.

The impact of the company's acquisition of Clumio, completed just a week before the Shift event, is felt throughout these announcements. Commvault is moving with lightning speed to integrate Clumio’s technology into its core offerings, and the results are already creating significant differentiation for the company. That bodes well for the long-term success of the integration.

Commvault is rapidly advancing the state of cloud-native cyber resilience. With its focus on automation, multi-cloud flexibility, and regulatory readiness, the company addresses the most pressing challenges facing cloud-first IT organizations. The ability to restore entire cloud environments—not just data—after a cyberattack is a critical capability.

As businesses continue to move critical workloads to the cloud, Commvault’s solutions will be instrumental in ensuring operational continuity and protecting against the rising tide of cyber threats.

The information contained within this document was believed by NAND Research to be reliable and is provided for informational purposes only. The content may contain technical inaccuracies, omissions, or typographical errors. This document reflects the opinions of NAND Research, which is subject to change. NAND Research does not warranty or otherwise guarantee the accuracy of the information contained within.

NAND Research is a technology-focused industry analyst firm providing research, customer content, market and competitive intelligence, and custom deliverables to technology vendors, investors, and end-customer IT organizations.

Contact NAND Research via email at info@nand-research.com or visit our website at nand-research.com.