HYCU Wants to Revolutionize Data Protection

Summary

In 2023, there were 2,814 reported global data breaches, compromising over 8.2 billion records across various sectors, with expectations for higher figures in 2024.[1] As of the first quarter of 2024, more than 30 billion records have been breached in 5,360 publicly disclosed incidents.[2] Among these, a massive breach involving 12 terabytes of information exposed 26 billion records from user data platforms such as LinkedIn, X (formerly Twitter), Weibo, Tencent, and others, marking it the most significant breach reported to date. These breaches have predominantly affected the telecom, public sector, healthcare, and manufacturing industries.

Many data breaches originate from software-as-a-service (SaaS) applications. Since they emerged in the late 1990s, these cloud applications have faced data security challenges related to responsibility, complexities of data integration, and human error. More than 80% of all data breaches are due to human involvement, including individual mistakes, credential theft, and social engineering methods like phishing.[3]

A key challenge with SaaS applications is the shared responsibility for data security, often unknown to the end-customer. While the provider secures the platform, customers are, in many cases, responsible for securing their accounts and data within the application. Data security measures from providers can contain weak encryption with limited access control options for protecting sensitive data in the cloud. This paper assesses the SaaS data protection market and highlights how to protect enterprise data in the cloud. HYCU has set itself apart in this field by covering a range of environments, such as on-premises, public cloud, hybrid, and SaaS platforms.

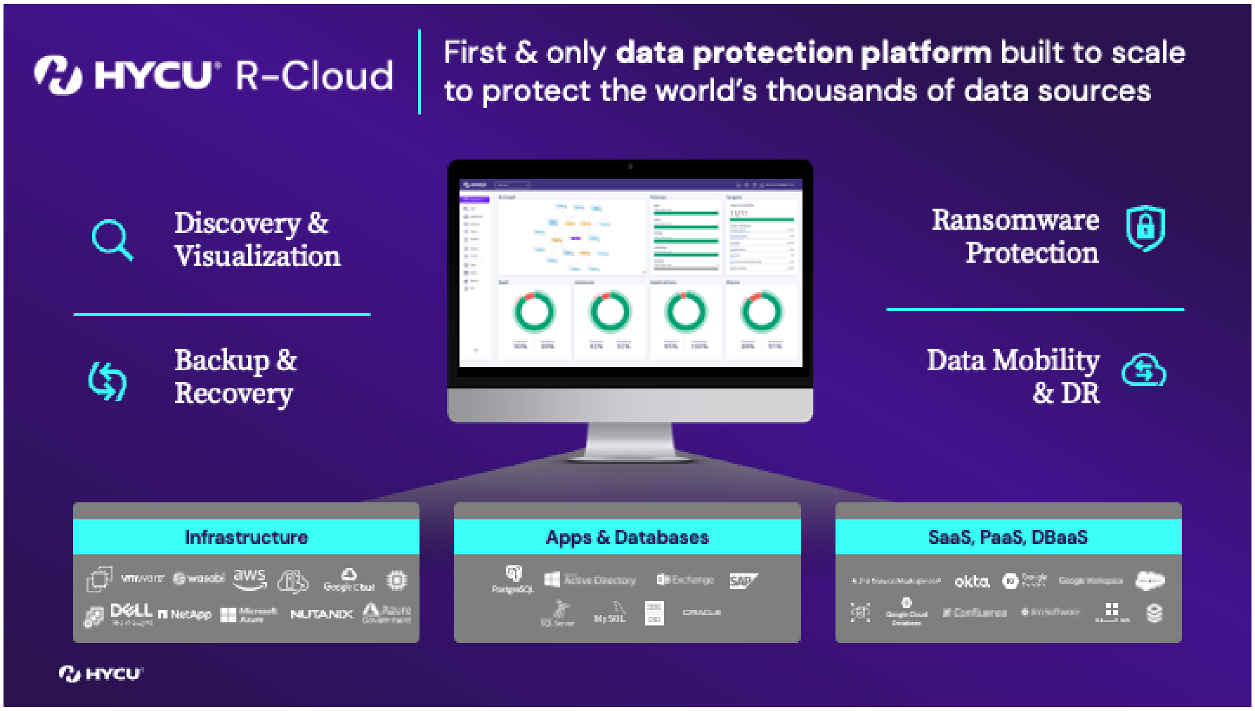
SaaS Landscape

The size and growth of the SaaS market—valued at $258.6 billion in 2023 and projected to reach $374.5 billion by 2028—underscore the need for advanced data projection technologies. On average, most midsize organizations use over 217 SaaS applications.

[1] Neil Ford, “List of Data Breaches and Cyber Attacks in 2023,” IT Governance, January 5, 2024
[2] Neil Ford, “Global Data Breaches and Cyber Attacks in 2024,” IT Governance, March 5, 2024
[3] Caitlin Jones, “50 Cloud Security Stats You Should Know In 2024,” Expert Insights, December 8, 2023

An estimated 30,000 global SaaS companies in 2023 provide applications to billions of customers for data intelligence, human resources, finance, productivity, customer service, marketing, e-commerce, supply chain, and enterprise solutions.[4]

While SaaS applications have many benefits, they also present challenges for an organization's data management strategy. Issues such as data siloing can complicate data protection and information sharing. Integrating multiple SaaS applications can create vulnerabilities by exposing data to security risks, with each integration point potentially serving as an entry point for attackers. The risks are not limited to external attackers; accidental deletions and malicious actions by internal actors also pose significant security threats. Effective data protection strategies are essential within the SaaS industry to address these concerns.



HYCU R-Cloud

First & only **data protection platform** built to scale to protect the world's thousands of data sources

Discovery & Visualization

Backup & Recovery

Ransomware Protection

Data Mobility & DR

Infrastructure

Apps & Databases

SaaS, PaaS, DBaaS

HYCU's illustration demonstrates the features and capabilities of the R-Cloud data protection platform.

HYCU Delivers DPaaS With Its R-Cloud Platform

HYCU—pronounced “haiku”—stands for Hybrid Cloud Uptime. Since its founding in 2018, the Boston-based company has distinguished itself in data protection across various environments including on-premises, public cloud, hybrid, and SaaS platforms.

[4] Ascendix, “How Many SaaS Companies Are There in the World,” May 26, 2023

HYCU provides data protection as a service (DPaaS) through its HYCU R-Cloud platform. R-Cloud's core functionalities encompass backup and disaster recovery, ransomware protection, data migration and mobility facilitation, plus data security and compliance.

In the past, the primary concern for IT departments has been securing data housed within their organization's infrastructure. However, the emergence of SaaS and public cloud platforms brought a shift in focus. As the technology landscape evolved, organizations gained access to an array of cloud-based services, including platform as a service (PaaS), infrastructure as a service (IaaS), and database as a service (DBaaS). Protecting data in these off-premises environments is just as important as preserving the data in traditional on-premises setups. HYCU has differentiated itself as a data protection company across various environments, providing DPaaS through its HYCU R-Cloud platform.

HYCU R-Cloud, with the R representing "resilience," focuses on enhancing data protection within SaaS environments. The platform is designed to help organizations protect, manage, and recover their data more efficiently and strengthen their resilience against data disruptions. R-Cloud's core functionalities include backup, granular recovery, disaster recovery, ransomware protection and recovery, data migration, mobility facilitation, and data security and compliance. The platform works hand in hand with solutions from VMware, Nutanix, Azure Stack HCI, Microsoft Hyper-V, AWS, Azure, Google Cloud, and a growing number of SaaS applications and cloud services including Asana, Atlassian Jira, Bitbucket, Box, Confluence, DocuSign, GitHub, Google Workspace, M365, Monday.com, Okta, Pinecone, and Redis to name a few.

The R-Cloud business value protects an organization's on-premises, multi-cloud, and SaaS application data. HYCU's low-code development platform facilitates the integration of backup and recovery services into various SaaS applications. R-Cloud provides a unified view of applications, platforms, workloads, and associated data protection status, enhancing data management within the ecosystem. It is recognized for its user-friendly and intuitive interface for end users as well as SaaS providers.

INNOVATIONS IN AUTOMATION AND AI

HYCU's platform utilizes AI and machine learning (ML) to automate the development of data protection tasks, reducing the need for manual coding for improved efficiency. Through a partnership with the AI startup Anthropic, HYCU has incorporated Anthropic's AI assistant, Claude, into its R-Cloud platform. Claude is designed to work with HYCU's data, understanding the specific requirements of the R-Cloud platform core concepts such as recovery protocols, compliance, and encryption. This collaboration simplifies developing data protection integrations and AI-enhanced security features for automated and user-friendly data management. As a result, what previously took weeks now takes hours or less.

Despite the speed, HYCU maintains its high standards for security and efficiency. This integration positions HYCU as a pioneer in incorporating AI into SaaS data protection. Claude helps HYCU redefine data protection strategies and simplify SaaS integrations. This collaboration delivers a new way for HYCU customers to protect SaaS applications and cloud services while still maintaining a standard with compliance, encryption, and recovery protocols.

HYCU's Technology

HYCU's technological infrastructure is designed to focus on flexibility, scalability, and security, helping it navigate the data protection landscape for hybrid and multi-cloud environments.

HYCU integrates with leading virtualization platforms, leveraging their respective APIs for agentless VM backups, migration, and restorations. This approach directly interfaces with the virtualization platforms' APIs, such as VMware's vCenter Server API, to execute essential tasks.

The API integration facilitates interactions with virtualization environments and services. It utilizes vSphere APIs for snapshot creation and Nutanix Prism APIs to backup and recover Nutanix AHV VMs. HYCU enhances storage efficiency through deduplication and compression, removing duplicate data and retaining unique data blocks. Incremental backups record only the data that has changed since the previous backup. HYCU is compatible with various storage repositories, including local storage, NAS, and cloud storage solutions such as AWS S3, Azure Blob Storage, and Google Cloud Storage. This ensures versatile and effective data storage.

HYCU encrypts backups during transmission and at rest with encryption algorithms, leveraging platform snapshots to capture point-in-time copies of VMs for quick backups without impacting production systems. HYCU's capabilities extend to public clouds, supporting cross-cloud data mobility and disaster recovery with platforms such as AWS, Azure, and Google Cloud and replicating VMs from on-premises environments to the cloud for disaster recovery.

HYCU's advanced dashboard and reporting utilities offer detailed visibility into the status of backup jobs, performance indicators, and compliance levels, complete with notifications for any arising issues. By integrating these technologies, HYCU delivers dependable data protection solutions, highlighting its dedication to assisting enterprises in securing their data throughout diverse IT environments.

COMPLIANCE STANDARDS

HYCU R-Cloud is designed with a focus on security and compliance, aligning with standards such as the Security Technical Implementation Guide (STIG), the National Information Assurance Partnership (NIAP), and ISO 27001 from the International Organization for Standardization. It ensures secure configurations and verifies security features. HYCU R-Cloud also adheres to industry-specific regulations, including the Health Insurance Portability and Accountability Act (HIPAA) for healthcare information, the Sarbanes-Oxley Act (SOX) for financial reporting, and General Data Protection Regulation (GDPR), NIS2, and DORA for data privacy in Europe, and was the first data protection solution to attain Common Criteria certification for Collaboration Protection Profile (cPP) for enhanced security, to maintain data protection across various domains.

The R-Cloud platform provides immutable backups and air-gapped recovery options to protect against ransomware attacks, utilizing write-once-read-many (WORM) technologies to certify data integrity. It features identity management with role-based access control (RBAC), offering alerting, custom reports, and job logging for increased security visibility. HYCU R-Cloud also supports multi-tenancy with instant access management, providing permissions to reduce unauthorized access risks.[5] HYCU delivers cyber resilience for various environments to ensure data protection, easy recovery, and compliance with regulations.

HYCU ECOSYSTEM EXPANDING THROUGH PARTNERSHIPS

HYCU has built its data protection solutions through a strong network of technology and reseller partners, plus managed service providers (MSPs). These technology partners include cloud providers Amazon Web Services, Microsoft Azure, and Google Cloud Platform (GCP); cloud solutions Nutanix, Okta, Qstar, Quantum, SAP, Scality, and VMware; and storage vendors NetApp, Backblaze, Cloudian, Exagrid, Wasabi, and Dell Technologies.

[5] Hycu.com, March 2024

HYCU's reseller partners have contributed to the distribution across different industries to expand market reach. MSPs incorporate HYCU's solutions into their broader offerings, providing clients with complete IT management services. These partnerships highlight the importance of an ecosystem and the value it delivers for both HYCU and its customers.

Real-World Application By Industry

HYCU's data protection spans across various industries to meet the needs of multiple industries and organizations. A few specific sectors:

- **Legal** — HYCU protects critical data for law firms, such as case files, contracts, and client information, and adheres to legal discovery regulations. HYCU partners with iManage to protect the legal and professional services industries.
- **Financial** — For organizations like the Bank of Stockton, HYCU provides secure backup solutions that comply with financial regulations, protect sensitive data, and control potential system failures.
- **Healthcare** — Medical centers such as Coastal Medical and Shrewsbury and Telford Hospital NHS Trust (SaTH) rely on HYCU to secure patient records and medical applications and maintain HIPAA compliance. Coastal Medical also requires high data availability, including protected health information (PHI). This requires dependable data backups stored in its central data center and servers located with its ISP, as well as a disaster recovery (DR) facility at one of Coastal Medical's other sites.
- **Government** — The State of California uses HYCU to secure sensitive data and provide disaster recovery, supporting FedRamp security compliance.
- **Sports** — Boston Red Sox, Callaway Golf, and others rely on HYCU to protect critical infrastructure data, analytics, and digital assets associated with games, ensuring efficient backup and recovery.
- **Manufacturing** — TT Electronics and Steel and Pipes depend on HYCU to protect production systems, supply chain data, and intellectual property, especially in preparation for a rapid recovery from disruptions. Steel and Pipes also rely on data availability and business continuity, given the company's location in the heart of "Hurricane Alley."
- **Automotive** — MATA Automotive and other automotive companies use HYCU's Nutanix full integration support for cloud adoption, data resilience, and simplified backup management for sensitive data related to manufacturing.

CHALLENGERS

HYCU faces several notable competitors. Veeam provides comprehensive backup and DR solutions, excelling in VMware and Microsoft environments while expanding its capabilities to cover Nutanix and public clouds. Rubrik is a cloud data management company offering data protection, governance, and orchestration across both on-premises and cloud environments, directly competing with HYCU in the Nutanix domain. Cohesity provides converged secondary data, including backup, disaster recovery, file and object services, dev/test, and analytics, and it supports major hyper-converged platforms. Veritas, a longstanding vendor of backup solutions that is merging with Cohesity, has shifted its focus to multi-cloud data management, with offerings such as NetBackup for SaaS protection and Beam for cloud optimization.

Commvault, another established vendor, specializes in data protection and information management, offering the Metallic SaaS platform for on-premises and cloud deployments and integrations with leading hyper-converged solutions.

CONCLUSION

Data backup and recovery is a competitive industry with established players. HYCU has made significant strides to improve its market position. In 2024, HYCU must expand its brand for additional market presence and a commitment to continuous innovation in AI and cloud technologies.

HYCU's strategic partnership with Anthropic is advantageous; by integrating advanced AI capabilities into its offerings, HYCU sets its products apart from its competitors, hoping to attract customers looking for progressive data protection solutions.

HYCU's DPaaS is developed to meet the needs of various organizations, especially those managing the complexities of hybrid and multi-cloud data protection, focusing on data privacy and sovereignty. The service is also suited for organizations needing agentless backups that do not impact the performance of on-premises tools. HYCU simplifies policy setting and offers straightforward self-service recovery options for applications, virtual machines, and files. This makes it appealing to organizations that value simplicity in their data protection strategies. With a customer base exceeding 4,200-plus globally, HYCU offers solutions that prevent data loss and minimize downtime, catering to organizations seeking a flexible, efficient, and secure data protection service that keeps pace with their evolving IT requirements.

Important Information About This Paper

Contributor

Robert Kramer, Vice President and Principal Analyst, Enterprise Data Technologies, ERP & SCM

Publisher

Patrick Moorhead, CEO, Founder and Chief Analyst at Moor Insights & Strategy

Inquiries

Contact us if you would like to discuss this report, and Moor Insights & Strategy will respond promptly.

Citations

This paper can be cited by accredited press and analysts but must be cited in-context, displaying author's name, author's title, and "Moor Insights & Strategy". Non-press and non-analysts must receive prior written permission by Moor Insights & Strategy for any citations.

Licensing

Disclosures

HYCU commissioned this paper. Moor Insights & Strategy provides research, analysis, advising, and consulting to many high-tech companies mentioned in this paper. No employees at the firm hold any equity positions with any companies cited in this document.

Disclaimer

The information presented in this document is for informational purposes only and may contain technical inaccuracies, omissions, and typographical errors. Moor Insights & Strategy disclaims all warranties as to the accuracy, completeness, or adequacy of such information and shall have no liability for errors, omissions, or inadequacies in such information. This document consists of the opinions of Moor Insights & Strategy and should not be construed as statements of fact. The opinions expressed herein are subject to change without notice.

Moor Insights & Strategy provides forecasts and forward-looking statements as directional indicators and not as precise predictions of future events. While our forecasts and forward-looking statements represent our current judgment on what the future holds, they are subject to risks and uncertainties that could cause actual results to differ materially. You are cautioned not to place undue reliance on these forecasts and forward-looking statements, which reflect our opinions only as of the date of publication for this document. Please keep in mind that we are not obligating ourselves to revise or publicly release the results of any revision to these forecasts and forward-looking statements in light of new information or future events.