Cyber Recovery Vault Market Size & Share Analysis - Growth Trends and Forecast (2026 - 2031)
Industry: Cybersecurity
URL: https://www.mordorintelligence.com/industry-reports/cyber-recovery-vault-market

Cyber Recovery Vault Market Size and ShareMarket Overview

Study Period	2020 - 2031
Market Size (2026)	USD 1.63 Billion
Market Size (2031)	USD 4.23 Billion
Growth Rate (2026 - 2031)	20.99 %
Fastest Growing Market	Asia-Pacific
Largest Market	North America
Market Concentration	Low
Major Players*Disclaimer: Major Players sorted in no particular order	

|

Image © Mordor Intelligence. Reuse requires attribution under CC BY 4.0.

Cyber Recovery Vault Market Analysis by Mordor IntelligenceThe Cyber Recovery Vault Market size is projected to be USD 1.38 billion in 2025, USD 1.63 billion in 2026, and reach USD 4.23 billion by 2031, growing at a CAGR of 20.99% from 2026 to 2031. Ransomware attacks increasingly seek to turn off the copies organizations need for restoration, making isolated recovery environments a core resilience requirement. Sophos reported that 56% of ransomware attacks encrypted data in the preceding 12 months, showing why a standard backup process may not provide a dependable recovery path. Veeam found that ransomware attacks targeted backup repositories in 96% of cases, and 76% of those attempts compromised the backups. Many organizations still struggle to quickly identify a clean recovery point, so tested recovery procedures remain as important as the vault itself. Suppliers are responding with stronger isolation, clean-room recovery, and controls that work across cloud and on-premises environments.

Key Report Takeaways

* By component, solutions held 70.24% of the Cyber Recovery Vault Market share in 2025, while services are projected to expand at a 23.08% CAGR through 2031.
* By deployment mode, cloud held 68.55% of the Cyber Recovery Vault Market revenue in 2025, while hybrid deployment is projected to grow at a 22.34% CAGR through 2031.
* By organization size, large enterprises held 71.60% of the Cyber Recovery Vault Market revenue in 2025, while small and medium-sized enterprises are projected to grow at a 22.75% CAGR through 2031.
* By workload type, virtual machines accounted for 61.29% of the Cyber Recovery Vault Market revenue in 2025, while databases are projected to grow at a 22.05% CAGR through 2031.
* By industry vertical, Banking, Financial Services, and Insurance (BFSI) accounted for 23.45% of the Cyber Recovery Vault Market revenue in 2025, while healthcare and life sciences are projected to grow at a 21.47% CAGR through 2031.
* By geography, North America held 36.88% of revenue in 2025, while Asia-Pacific is projected to grow at a 21.72% CAGR through 2031.

Note: Market size and forecast figures in this report are generated using Mordor Intelligence’s proprietary estimation framework, updated with the latest available data and insights as of January 2026.

Global Cyber Recovery Vault Market Trends and InsightsDrivers Impact Analysis*

Driver | (~) % Impact on CAGR Forecast | Geographic Relevance | Impact Timeline |
Ransomware and Wiper Attacks on Backup Repositories | +5.8% | Global | Short term (≤ 2 years) |
Regulatory Demand for Tested Recovery | +4.6% | Europe, North America, expanding globally | Medium term (2-4 years) |
Hybrid and Multicloud Workload Expansion | +3.5% | Global, with Asia-Pacific acceleration | Long term (≥ 4 years) |
Cyber Insurance Underwriting Requirements | +2.8% | North America and Europe, with effects in Asia-Pacific and Middle East and Africa | Medium term (2-4 years) |
Recovery Readiness for AI Generated and High Change Rate Data | +2.0% | North America, Europe, and Asia-Pacific | Long term (≥ 4 years) |
Edge and Operational Technology Recovery Exposure | +1.4% | Global, with industrial Asia-Pacific and Middle East and Africa gaining | Long term (≥ 4 years) |
Source: Mordor Intelligence |

Ransomware and Wiper Attacks Targeting Backup Repositories

Backup repositories have become a direct target for sophisticated ransomware groups. The Cyber Recovery Vault Market benefits when organizations recognize that production security alone cannot protect recovery data. Sophos found that 56% of attacks succeeded in encrypting data during the prior 12 months. Veeam reported that 96% of ransomware attacks targeted backup repositories, and 76% of these efforts compromised the backups.[1]Veeam Software, “2024 Data Protection Trends Report,” Veeam, veeam.com IBM placed the average cost of a ransomware incident at USD 4.4 million in 2025. Wiper attacks create a separate concern because they aim to destroy data rather than demand a ransom. An isolated vault can therefore preserve a recovery option when payment cannot restore the affected systems. Sophos also found that 66% of cases involving encrypted data used backups for recovery. This result shows the practical value of backups when they remain accessible and uncompromised. The Cyber Recovery Vault Market supports designs that separate recovery copies from normal production credentials. These designs can limit an attacker’s ability to reach both live data and the recovery environment. Organizations also need to validate that the data stored in the vault is clean before it is restored. Vendors are therefore building features that help teams test recovery points before an incident becomes more severe.

Regulatory Demand for Tested and Documented Recovery

Recovery requirements have shifted from general guidance to documented operational expectations across many regulated sectors. The Cyber Recovery Vault Market gains traction as organizations must demonstrate that restoration plans work under cyberattack conditions. The EU Digital Operational Resilience Act became applicable on January 17, 2025, and it requires covered financial entities to test recovery under cyberattack scenarios. It also requires them to demonstrate data integrity during restoration and provide evidence to supervisors. NIS2 extends related security and continuity expectations to sectors such as energy, transportation, and healthcare. Public companies also face incident disclosure obligations that increase the importance of a credible recovery process. The Cross Market Operational Resilience Group issued guidance on firm cyber recovery capabilities in April 2026. This guidance emphasizes the need for firms to demonstrate faster recovery capabilities. The Cyber Recovery Vault Market is supported when a product can retain clear evidence of recovery testing and data integrity. This evidence can be useful across multiple compliance programs. It can also reduce the burden of collecting records separately for each review. Suppliers that align recovery workflows with compliance evidence are better placed in regulated procurement processes.

Hybrid and Multicloud Workload Expansion

Workloads now operate across on-premises data centers, public cloud platforms, a nd edge locations. The Cyber Recovery Vault Market responds to this spread by re quiring consistent isolation policies across different environments. Each enviro nment may use different identity controls, data residency rules, and data transf er arrangements. A recovery process that works in only 1 environment can leave i mportant workloads exposed. Organizations are therefore seeking vault designs th at cover more than a single cloud or data center. This need is particularly rele vant when applications depend on systems that run in several locations. Traditio nal vault designs often centered on a separate offline copy in 1 location. Feder ated approaches now seek to preserve isolation while applying the same recovery policy across multiple environments. The Cyber Recovery Vault Market allows supp liers to provide centralized clean-room recovery orchestration. This approach ca n help teams manage recovery without giving up workload portability. It can also mitigate the risk of relying on a single cloud environment for recovery. Provid ers that coordinate recovery across major cloud platforms can meet a wider set o f enterprise requirements.

Cyber Insurance Underwriting Requirements

Cyber insurers increasingly require evidence rather than relying only on self-re ported controls. The Cyber Recovery Vault Market is strengthened when insurers t reat immutable or air-gapped backups as a basic underwriting requirement. In 202 6, carriers commonly require offline or air-gapped copies that production creden tials cannot access. They also seek documented restore tests with recorded resul ts. Critical data recovery time objectives of 24 hours or less and 30-day retent ion policies are also part of the requirements described in the supplied researc h. These requirements reflect concern over long attacker dwell times and incompl ete recovery preparation. Organizations without tested, isolated backups can fac e higher recovery costs and more difficult insurance renewals. A missing vault c ontrol can also lead a carrier to decline renewal. The Cyber Recovery Vault Mark et provides organizations with a way to document the controls that insurers revi ew. This can make vault spending part of a broader risk and insurance decision. The same evidence expectations now affect SMEs as well as large enterprises. Man aged service models can help smaller organizations obtain the recovery capabilit y and documentation that insurers require.

Restraints Impact Analysis*

Restraint | (~) % Impact on CAGR Forecast | Geographic Relevance | Impact Timeli ne |
Heterogeneous Legacy Integration Complexity | -1.5% | Global, with greater impac t in Asia-Pacific and Middle East and Africa | Long term (≥ 4 years) |
Recovery Skills and Specialist Staffing Shortages | -1.2% | Global | Medium term (2-4 years) |
Cloud Egress and Data Transfer Cost Uncertainty | -0.8% | North America and Euro pe | Short term (≤ 2 years) |
Unproven Recovery Test Discipline | -0.6% | Global, concentrated in SME heavy ma rkets | Medium term (2-4 years) |
Source: Mordor Intelligence |
Heterogeneous Legacy Integration Complexity

Many enterprise technology environments contain end-of-life operating systems, p roprietary databases, and tightly connected applications. These environments can be difficult to protect with cloud-native vault tools. The Cyber Recovery Vault Market may see slower adoption when organizations require custom connectors and security layers before recovery can be automated. Manual orchestration can weak en the expected recovery workflow. A partial deployment can create false assuran ce because some workloads may be vaulted while critical dependencies are exclude d. Recovery can then fail when systems need to reconnect in the correct order. T his issue is more pronounced where legacy-heavy sectors are digitizing quickly. Asia-Pacific and Middle East, and Africa can face this constraint when organizat ions lack the budget cycles needed to replace older foundational systems. The ch

allenge is not limited to the speed of integration. It also concerns whether tea ms have a complete view of the dependencies required for a successful restoratio n. Suppliers need to support mixed environments rather than only modern cloud wo rkloads. Organizations also need to test the full recovery sequence before relyi ng on the vault during an incident.

Recovery Skills and Specialist Staffing Shortages

A vault does not remove the need for skilled people during a cyber incident. The supplied research found that only 8% of organizations can recover multiple tera bytes of data in less than 1 hour, though that source does not meet the source s tandard for this rewrite. Teams must identify a clean recovery point and avoid r estoring contaminated data. They must also sequence multi-tier applications corr ectly to reduce the risk of reinfection. Regulatory notification duties can run concurrently with technical recovery work. These combined duties require experie nce that is not widely available across enterprise teams. Cybersecurity programs have often focused on prevention and detection rather than recovery engineering . Recovery specialists are therefore concentrated in large enterprises and speci alist managed service providers. Smaller organizations face a more difficult pos ition because insurers expect a proven recovery capability. They may not have st aff capable of running a credible exercise without external support. The Cyber R ecovery Vault Market can address part of this gap through managed recovery servi ces. However, organizations still need clear internal ownership for recovery dec isions and testing.

*Our forecasts treat driver/restraint impacts as directional, not additive. The impact forecasts reflect baseline growth, mix effects, and variable interactions .

Segment AnalysisBy Component: Solutions Hold the Largest Revenue Position While Services Address Execution Needs

Solutions accounted for 70.24% of revenue in 2025, giving them the largest marke t share within the Cyber Recovery Vault Market. Enterprises prefer integrated so ftware and hardware when they need immutable storage, enforced isolation, and cl ean-room recovery orchestration. A pre-integrated stack can reduce the work need ed to assemble these controls from separate backup tools. Organizations that use modular backup products without purpose-built isolation controls can remain exp osed to repository compromise. This concern is central because backup repositori es are frequently targeted in ransomware attacks. The Cyber Recovery Vault Marke t size for solutions is supported by demand for recovery environments that can b e placed outside normal production access. Buyers also look for controls that ma ke recovery procedures easier to test and document. These requirements keep solu tions important for organizations that need a defined recovery platform.

Services are projected to grow at a 23.08% CAGR through 2031, the highest rate i n the component split. This growth reflects the gap between deploying technology and operating it effectively during a real incident. Organizations need recover y readiness assessments, tabletop exercises, and support for compliance evidence . Professional services can help teams identify dependencies that may interrupt restoration. They can also help organizations test whether the recovery point is clean and usable. Commvault released Cloud Unity in November 2025 and introduce d AI-enabled Synthetic Recovery as part of the platform. The offering shows how recovery software and operational support can increasingly work together. Manage d services remain relevant where organizations lack dedicated recovery engineers . This relationship supports the role of services alongside platform deployments .

 By Depl oyment Mode: Cloud Leads While Hybrid Addresses Distributed Workloads

Cloud deployment accounted for 68.55% of the cyber recovery vault revenue in 2025. Organizations use managed and scalable vault instances to reduce the need to maintain their own physical isolation infrastructure. Cloud options can make it easier to scale protected capacity as data volumes change. They can also provide a separate recovery environment from the production systems under attack. This model fits enterprises that want to reduce operational work around physical vault infrastructure. It does not eliminate the need to control access to identities and validate recovery data. Cloud deployment, therefore, remains important, as it allows organizations to use an isolated hosted environment without creating new residency concerns.

Hybrid deployment is projected to grow at a 22.34% CAGR through 2031. This rate reflects demand from organizations that operate both on-premises systems and public cloud workloads. They need consistent isolation policies while preserving the ability to move workloads across environments. On-premises deployment remains relevant in industrial, high-security, and air-gapped settings. These settings may view cloud connectivity as an additional risk surface. A hybrid approach can retain local recovery capability while extending protection to cloud workloads. It can also support different residency needs across jurisdictions. The Cyber Recovery Vault Market size for hybrid deployments is tied to the continued use of mixed-technology estates. Suppliers that apply the same policy and testing process across these estates can serve a more complex set of recovery requirements.

By Organization Size: Large Enterprises Lead While SMEs Expand Through Managed Models

Large enterprises held 71.60% of revenue in 2025. This position reflects CISO-led buying, board-level risk requirements, and the ability to invest in purpose-built vault infrastructure. Large organizations often operate multiple data centers and complex hypervisor estates. They can also face compliance obligations across several jurisdictions. These conditions require granular policies and clear audit records. The cyber recovery vault revenue position held by large enterprises reflects both their larger technology footprint and their recovery obligations. Their deployments need to cover many sites and dependencies. They also need to show that recovery can work across those systems.

SMEs are projected to grow at a 22.75% CAGR through 2031. Insurers increasingly expect evidence of tested recovery even from organizations that do not operate large internal technology teams. Subscription and managed service models can make vault capability more accessible to these buyers. Commvault launched HyperScale Edge and HyperScale Flex in August 2025 for SMB and edge-location use cases. The offerings were validated with Dell, HPE, and Lenovo hardware. Kyndryl introduced Intelligent Recovery Services in February 2026 for automated recovery across hybrid and multicloud environments. These services can support organizations without dedicated recovery engineering teams. The Cyber Recovery Vault Market is therefore expanding beyond the buyers that can build and run every recovery control internally.

By Protected Workload: Virtual Machines Lead While Databases Gain From AI Data Growth

Virtual machines held 61.29% of protected workload revenue in 2025. Virtualized infrastructure remains widely used across enterprise data centers. The category benefits from established integrations with VMware, Hyper-V, Nutanix AHV, and other hypervisors. These integrations make it easier to include virtual machines in protection and restoration processes. The Cyber Recovery Vault Market size connected to virtual machines reflects this broad installed base. A recovery plan for these workloads must still account for application dependencies and the condition of the backup data. Mature virtualization support gives suppliers an important route into enterprise recovery programs. It also keeps virtual machines central to vault planning.

Databases are projected to grow at a 22.05% CAGR through 2031. The supplied research links this expansion to the growth of AI training data and model checkpoints stored in structured databases. Database-level ransomware detection can examine backup data at the row and schema level before recovery is certified. This process can help organizations identify clean recovery points more precisely. The Cyber Recovery Vault Market supports these needs when vault platforms can protect data at a more granular level. Physical servers, SaaS data, and containerized applications also continue to require protection. These workloads serve specialized environments that need recovery methods suited to their operating model. The range of workloads means suppliers need to support more than just virtualized infrastructure.

 By Industry Vertical: BFSI Anchors Spending While Healthcare and Life Sciences Grows Fastest

BFSI held 23.45% of revenue in 2025. Financial institutions face high compliance demands and significant reputational risk when recovery fails. The Bank of England reported in 2026 that 82% of UK banks, insurers, and asset managers identified cyberattacks as one of the top 5 financial system risks.[2]Bank of England, “The Value of Resilience: Cyber Resilience in Financial Services,” GOV.UK, gov.uk This supports continued spending on isolated recovery infrastructure. The SIFMA-FSSCC Reconnection Framework was updated in December 2025 and provides a 5-step post-incident mitigation structure. The cyber recovery vault revenue position in BFSI reflects the sector’s need for documented recovery and controlled reconnection. Providers that align evidence with these requirements can be more relevant in procurement. Recovery programs in this segment also need to restore systems without weakening security controls.

Healthcare and life sciences are projected to grow at a 21.47% CAGR through 2031. Healthcare ransomware recovery costs averaged USD 1.02 million in 2025. Hospitals and clinics need continuity for systems that support patient care and operational coordination. Kyndryl’s Intelligent Recovery Services specifically addressed healthcare workload continuity in 2026. Government, industrial manufacturing, energy and utilities, IT and telecommunication, and other verticals also contribute to demand. These sectors face exposure from operational technology and critical infrastructure obligations. The Cyber Recovery Vault Market serves them through recovery environments that can be separated from affected production systems. Their different workloads and operating conditions require policies that are specific to each environment.

Geography Analysis

North America held 36.88% of the cyber recovery vault revenue position in 2025. The region has a high density of cyber insurance carriers that require evidence of recovery controls. Cybersecurity disclosure obligations also elevate recovery infrastructure to a board-level concern. IBM reported an average ransomware incident cost of USD 4.4 million in 2025.[3]IBM, “Cost of a Data Breach Report 2025,” IBM, ibm.com This cost supports investment in isolated recovery environments among mid-market and large enterprises. The United States remains the central source of regional demand. Canada follows similar financial-sector adoption patterns.

Europe accounted for a significant share in 2025, with Germany, the United Kingdom, France, and the Benelux countries leading regional adoption. Financial entities and critical sectors are increasing their focus on documented recovery procedures. The cyber recovery vault segment value in the region is supported by the need to show recovery readiness to regulators and stakeholders. The Cross Market Operational Resilience Group issued cyber recovery guidance in April 2026 for f

irms in the United Kingdom. These requirements make tested recovery a more visible issue in technology and governance. South America is developing rapidly, with Brazil supported by financial regulation requirements. Manufacturing and agribusiness organizations in the region also face rising ransomware exposure.

Asia-Pacific is projected to grow at a 21.72% CAGR through 2031. Data localization requirements in China and India's Digital Personal Data Protection Act encourage interest in on-premises and hybrid vault configurations. Japan has updated cyber resilience guidance for financial institutions. Australia has broadened recovery obligations through amendments to the Security of Critical Infrastructure Act. The Middle East, especially the UAE and Saudi Arabia, is the most active region in the Middle East and Africa. Government and BFSI organizations are leading early deployments in that subregion. Africa remains in an earlier stage of adoption, with South Africa as the anchor market. Regional data center investment by cloud providers supports the infrastructure needed for wider adoption later in the forecast period.

Competitive Landscape

The Cyber Recovery Vault Market has moderate to high consolidation in the large-enterprise tier. Dell Technologies, Cohesity, Veeam, Rubrik, and Commvault compete on recovery orchestration, multicloud policy consistency, and audit evidence. Cohesity completed its combination with Veritas' enterprise data protection business in December 2024. The combined company served more than 12,000 customers, including 85 Fortune 100 companies, and had USD 1.5 billion in annual recurring revenue at closing. This transaction changed the competitive position of a leading data protection supplier. Hyperscalers also provide native vault-related features at competitive prices. This can commoditize basic protection for organizations that use a single cloud environment.

Specialist providers differentiate themselves by emphasizing where buyers need multicloud recovery and stronger orchestration. Rubrik introduced Autonomous Business Recovery for Cloud Applications in June 2026.[4]Rubrik, Inc., "Rubrik Introduces Autonomous Business Recovery Solution for Cloud Applications," Rubrik, rubrik.com Its Preemptive Recovery Engine identifies application dependencies and validates clean recovery points before an incident. FalconStor launched Cloud Clean Room for IBM Power environments in July 2026. The platform uses Zero Trust Secure Enclave technology and supports validated recovery testing. These moves show how suppliers can focus on automation or workload-specific needs. Such specialization can help smaller vendors retain positions where broad platforms are less targeted.

Competitive strategies focus on anomaly detection, service-based consumption models, sovereign recovery options, and support for several compliance frameworks. Veeam expanded its alliance with Pure Storage in June 2026 to provide Cyber Resilience as a Service. The offering connects Pure1 anomaly detection to the Veeam Data Platform via the Veeam Incident API. Commvault introduced Cloud Unity in November 2025 to unify data security, cyber recovery, and identity resilience across cloud, SaaS, on-premises, and hybrid environments. Suppliers that provide clear audit-ready evidence can hold an advantage with regulated buyers. The Cyber Recovery Vault Market remains competitive because enterprise requirements extend beyond basic backup.

Cyber Recovery Vault Industry Leaders* Amazon Web Services, Inc.

* Microsoft Corporation

* Google LLC

* Oracle Corporation

* International Business Machines Corporation

* *Disclaimer: Major Players sorted in no particular order

Recent Industry Developments* August 2026: NetApp acquired JetStream Software on August 6, 2026, to expand its cyber resilience capabilities for AI workloads and hybrid cloud environments. The deal gives NetApp access to the broad VMware installed base that runs third-party storage, positioning its cloud offerings as disaster-recovery destinations.
* July 2026: Veeam released Veeam Data Platform v13.1 on July 29, 2026, at Veeam ON Sydney, adding 6 new hypervisor platforms, malware scanning for NAS, Active Directory Forest Recovery, and post-quantum cryptography alignment with NIST standards for compliance-sensitive deployments.
* July 2026: FalconStor Software launched its Cloud Clean Room on July 8, 2026, an on-demand infrastructure platform using patent-pending Zero Trust Secure Enclave technology for IBM Power environments, enabling audit-ready validated recovery testing for DORA, FFIEC, and PCI-DSS compliance.
* June 2026: Rubrik unveiled Autonomous Business Recovery for Cloud Applications on June 9, 2026, powered by the Preemptive Recovery Engine. The solution discovers application dependencies, validates clean recovery points during peacetime, and orchestrates a sequenced Minimum Viable Business rebuild at machine speed. It remained in private preview.

Table of Contents for Cyber Recovery Vault Industry Report1. INTRODUCTION

 Products and Services, Recent Developments)* 6.4.1 Dell Technologies Inc.
* 6.4.2 Veritas Technologies LLC
* 6.4.3 Veeam Software Group GmbH
* 6.4.4 Commvault Systems, Inc.
* 6.4.5 Rubrik, Inc.
* 6.4.6 Cohesity, Inc.
* 6.4.7 International Business Machines Corporation
* 6.4.8 Hewlett Packard Enterprise Company
* 6.4.9 Druva Inc.
* 6.4.10 NetApp, Inc.
* 6.4.11 ExaGrid Systems, Inc.
* 6.4.12 Arcserve (USA), LLC
* 6.4.13 FalconStor Software, Inc.
* 6.4.14 Scality, Inc.
* 6.4.15 Cristie Software Limited
* 6.4.16 Huawei Technologies Co., Ltd.
* 6.4.17 Amazon Web Services, Inc.
* 6.4.18 Microsoft Corporation
* 6.4.19 Google LLC
* 6.4.20 Oracle Corporation

7. MARKET OPPORTUNITIES AND FUTURE OUTLOOK

* 7.1 White-Space and Unmet-Need Assessment

Global Cyber Recovery Vault Market Report ScopeThe Cyber Recovery Vault Market comprises software solutions, secure recovery environments, isolated vault infrastructures, and associated professional and managed services designed to protect critical data, applications, and workloads from ransomware, cyberattacks, insider threats, and destructive malware. Cyber recovery vault solutions create logically or physically isolated environments that store immutable backup copies, enable threat analysis and data validation, support clean recovery processes, and facilitate rapid restoration of business operations following cyber incidents. These solutions are increasingly deployed as part of enterprise cyber resilience, business continuity, and disaster recovery strategies.

The Cyber Recovery Vault Market Report is Segmented by Component (Solutions, and Services), Deployment Mode (Cloud, On-Premises, and Hybrid), Organization Size (Large Enterprises, and Small and Medium-Sized Enterprises), Protected Workload (Virtual Machines, Physical Servers, Databases, and Other Protected Workloads), Industry Vertical (Government and Public Administration, Industrial Manufacturing, Retail and E-Commerce, Transportation and Logistics, Energy and Utilities, Oil and Gas, IT and Telecommunication, Media and Entertainment, Education and Research Institutions, Healthcare and Life Sciences, Banking, Financial Services, and Insurance [BFSI], and Other Industry Verticals), and Geography (North America, South America, Europe, Asia-Pacific, and Middle East and Africa). The Market Forecasts are Provided in Terms of Value (USD).

By ComponentSolutions |
Services |
By Deployment ModeCloud |
On-Premises |
Hybrid |
By Organization SizeLarge Enterprises |
Small and Medium-Sized Enterprises |
By Protected WorkloadVirtual Machines |
Physical Servers |
Databases |
Other Protected Workloads |
By Industry VerticalGovernment and Public Administration |

IT and Telecommunication |
Education and Research Institutions |
Healthcare and Life Sciences |
Banking, Financial Services, and Insurance (BFSI) |
Other Industry Verticals |
By GeographyNorth America | United States |
 | Canada |
South America | Brazil |
 | Mexico |
 | Rest of South America |
Europe | Germany |
 | United Kingdom |
 | France |
 | Italy |
 | Rest of Europe |
Asia-Pacific | China |
 | Japan |
 | India |
 | South Korea |
 | Rest of Asia-Pacific |
 | |
Middle East and Africa | Middle East | United Arab Emirates |
 | | Saudi Arabia |
 | | Rest of Middle East |
 | |
 | Africa | South Africa |
 | | Rest of Africa |
By Component | Solutions |
 | Services |
By Deployment Mode | Cloud |
 | On-Premises |
 | Hybrid |
By Organization Size | Large Enterprises |
 | Small and Medium-Sized Enterprises |
By Protected Workload | Virtual Machines |
 | Physical Servers |
 | Databases |
 | Other Protected Workloads |
By Industry Vertical | Government and Public Administration |
 | IT and Telecommunication |
 | Education and Research Institutions |
 | Healthcare and Life Sciences |
 | Banking, Financial Services, and Insurance (BFSI) |
 | Other Industry Verticals |
 | |
By Geography | North America | United States |
 | | Canada |
 | |
South America	Brazil
	Mexico
	Rest of South America
Europe	Germany
	United Kingdom
	France
	Italy
	Rest of Europe
Asia-Pacific	China
	Japan
	India
	South Korea

	Rest of Asia-Pacific
Middle East and Africa	Middle East	United Arab Emirates
		Saudi Arabia
		Rest of Middle East
	Africa	South Africa
		Rest of Africa

Key Questions Answered in the ReportWhat is the cyber recovery vault segment value? The Cyber Recovery Vault Market is estimated at USD 1.63 billion in 2026 and is forecast to reach USD 4.23 billion by 2031 at a 20.99% CAGR.

Why do organizations use a cyber recovery vault? An isolated vault helps preserve recovery copies when attackers target production systems and backup repositories. It also gives teams a separate environment to test data integrity and restoration procedures before a major incident.

Which deployment mode leads cyber recovery vault adoption? Cloud deployment held 68.55% of revenue in 2025, while hybrid deployment is projected to grow at a 22.34% CAGR through 2031. Hybrid designs are relevant where organizations operate on-premises systems alongside public cloud workloads.

Which organizations are driving demand for recovery vaults? Large enterprises held 71.60% of revenue in 2025, while SMEs are projected to expand at a 22.75% CAGR through 2031. Managed services can help smaller organizations meet tested recovery and insurance evidence expectations.

Which workload needs are growing fastest in cyber recovery? Databases are projected to grow at a 22.05% CAGR through 2031 as organizations protect AI-related data and seek more granular recovery validation. Database-level checks can help teams identify a clean recovery point before data is restored.

Which region is expanding fastest for cyber recovery vaults? Asia-Pacific is projected to grow at a 21.72% CAGR through 2031, supported by digital transformation and data residency requirements. On-premises and hybrid configurations are relevant where local data controls affect recovery architecture.