IDC MarketScape

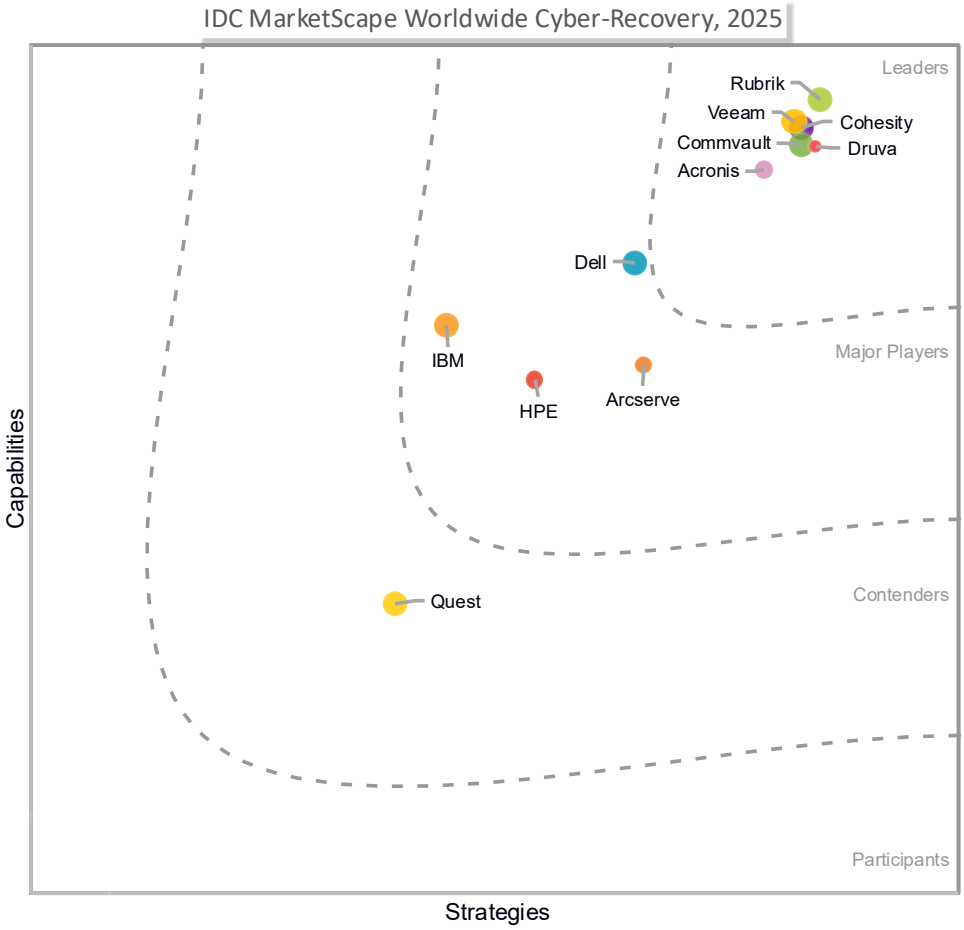
IDC MarketScape: Worldwide Cyber-Recovery 2025 Vendor Assessment

Johnny Yu Phil Goodwin

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape Worldwide Cyber-Recovery Vendor Assessment



Source: IDC, 2025

October 2025, IDC #US52040125

Please see the Appendix for detailed methodology, market definition, and scoring criteria.

IDC OPINION

Cyberattacks continue to be one of the biggest threats organizations face. A successful attack can lead to lost revenue, significant downtime, stolen data, regulatory fines, and a host of other consequences. Cybercrime is simply too organized and profitable to be completely stopped, and the ease with which perpetrators can deploy ransomware, combined with the relatively low risk of getting caught, ensures there is never a shortage of malicious actors.

Data protection and disaster recovery (DR) has traditionally been the answer to large-scale data outage events, but recovering from cyberattacks call for more than what traditional DR offers. This is where cyber-recovery comes in. Although data protection is the core component of cyber-recovery, not all data protection vendors offer a cyber-recovery solution. In addition to being able to back up and recover data, cyber-recovery requires capabilities specifically geared toward addressing the following foundational cyber-resilience needs:

- **Absolutely certain data survival:** Without absolutely certain data survival, it is highly likely that the organization will be forced to pay the ransom to get its data back. It is also likely to suffer data loss, as our research shows this to be common among victims. Organizations need to know they can get their data back no matter what.
- **Absolutely certain data integrity.** Similarly to data survival, organizations need to know that the data they recover is accurate data. Recovering data that has been modified or tampered with is as bad as or worse than not being able to recover at all, as much of the value of data lies in its legitimacy, authenticity, and validity.
- **Rapid recovery with minimal data loss.** The prospect of a long recovery may drive organizations to pay the ransom, even if they have clean, recoverable data. Being able to detect the attack early, quarantine it, assess the damage, and resume operations quickly mitigates any damage and prevents organizations from considering paying the ransom in hopes of a faster recovery.

Organizations are recognizing the threat and the importance of investing resources to defend against it. IDC research has found more than one-third of organizations plan to significantly increase their budget for cyber-recovery and resilience compared with last year. Similarly, an IDC survey found security to be one of the top 3 areas organizations say are the least likely to see budgetary setbacks.

To offer guidance to organizations looking to improve their cyberincident outcomes, this IDC MarketScape evaluates what we believe are the 11 most prominent cyber-recovery vendors. It is designed to help readers differentiate between these vendors' solutions and align their capabilities and features with their own organizational needs.

IDC MARKETSCAPE VENDOR INCLUSION CRITERIA

To narrow the list of participants to those we believe are most significant, we applied the following inclusion criteria:

- The solution must be a suite of software products (i.e., not just standalone backup/recovery).
- The solution must be primarily software, although delivery/integration with appliances is permitted as long as they are less than 50% of the solution price (as a percentage of actual selling price).
- The solution must include tools/modules specifically designed for cyber-recovery.
- The NIST cyber-recovery framework consists of five pillars: identify, detect, protect, respond, and recovery. The solution must be able to address at least the respond and recovery pillars, plus one other pillar.
- Data protection–related software revenue must exceed $100 million.
- The solution must be at least 70% "own IP" (as measured by percentage of actual selling price).
- The solution must be available worldwide (i.e., a presence in North America, EMEA, APAC, or at least 10 different countries) and have ≥20% of revenue outside of North America.
- The solution must address on-premises, multi–public cloud, and hybrid cloud workloads.
- The solution must be able to address small and midsize business (SMB) to large-scale enterprises.
- The core solution must have been in general market availability on January 1, 2024, with all features under consideration in general availability as of March 30, 2025. Features released after that time are considered road map items.

Our goal was to facilitate a head-to-head assessment with enough latitude that each vendor can illustrate its unique value and not box vendors into a one-size-fits-all evaluation.

ADVICE FOR TECHNOLOGY BUYERS

The vendors in this analysis support on-premises, hybrid cloud, and multicloud environments. However, some do so using a predominantly on-premises deployment methodology and others from a predominantly cloud-based methodology. Others will use a blend of both. Buyers need to consider which architecture fits their environment and strategic direction most closely.

Cyber-recovery vendors differentiate themselves in a number of ways. Very often, these involve trade-offs. Some of the key buying criteria are:

- **Complexity.** The solutions evaluated in this IDC MarketScape range from simple to manage to rather complex. Not surprisingly, the complex solutions may have more capabilities. IT buyers must balance between the desire for simplicity and the need for robust features/functions.
- **Breadth of solution.** Some vendors seek to supply as many capabilities as possible while others focus on specific capabilities where they believe they can excel. No vendor can supply everything, and no company needs everything. IT buyers should focus on what they need or can reasonably expect to need in the future.
- **Service offerings.** Some vendors' solutions may offer services for deployment, onboarding, technical support, day-to-day management, incident response, consultation, and training. Some buyers will want to look closely at what vendors can provide beyond tools and technology to lower their management and administrative burden or bolster their cyber-resilience knowledge and expertise.
- **Price.** While price was not an evaluation criterion in this IDC MarketScape, it certainly is an issue for every buyer. Solutions mentioned in this document will vary greatly by price, and finding that balance between cost and solution capabilities is the goal.
- **Incumbency.** Although this evaluation is conducted as if every reader has a clean slate, we know that's not true. Some IT buyers will forego some minor "nice to haves" to continue operating with an incumbent vendor. Others will insist on what they deem "best of breed," regardless of incumbency. Only the buyer can make that trade-off.

This IDC MarketScape is not intended to be a buyer's guide. We have based the evaluation on criteria that we believe to be most important for cyber-recovery, but our values and weightings may not match any specific IT buyer's needs. Its best use is as a means to begin solution differentiation and formulate a short list of vendor candidates for further consideration. Again, we believe every vendor in this evaluation could be the perfect solution in some scenarios and less optimal in other scenarios. IT buyers are

advised to use this document in the short list formulation to narrow the field and then apply their own due diligence and proof of concept prior to making any selection or purchase.

VENDOR SUMMARY PROFILES

This section briefly explains IDC's key observations resulting in a vendor's position in the IDC MarketScape. While every vendor is evaluated against each of the criteria outlined in the Appendix, the description here provides a summary of each vendor's strengths and challenges.

Acronis

IDC has identified Acronis as a Leader in this 2025 IDC MarketScape for worldwide cyber-recovery.

Acronis, headquartered in Schaffhausen, Switzerland, was founded in 2003. Its core cyber-recovery offering is Acronis Cyber Protect Cloud, which integrates capabilities spanning cybersecurity, data protection, and endpoint management. Acronis doesn't consider itself strictly a backup nor a cybersecurity vendor and instead positions itself as a champion of "cyberprotection," emphasizing unified recovery, threat defense, and operational resilience.

Acronis Cyber Protect Cloud aims to deliver seamless continuity and security for any workload, anywhere — minimizing downtime, assuring data integrity, and enabling rapid restoration after cyberincidents. Customers often consume modules for endpoint protection, backup and disaster recovery, extended detection and response (XDR), and security awareness training. Acronis stands out for its single-agent architecture, centralized policy engine, and a multitenant platform fit for both MSPs and enterprise IT.

The product includes integrations with over 300 third-party platforms across RMM, SIEM, SASE, hypervisors, public clouds (e.g., Azure, Google, and AWS), and security tools (e.g., SentinelOne, Darktrace, Fortinet, and Sophos). The portfolio is built for easy consumption, offering fine-tuned controls, compliance mapping, and automated actions through AI-driven features. Purchased modules typically span backup, disaster recovery, and endpoint management for Microsoft 365, Google Workspace, virtual machines (VMs), and diverse operating systems (OSs).

Strengths

- **Unified data protection and security:** Acronis provides a natively integrated platform where backup and recovery, endpoint protection, and threat defense

coexist within a single console and agent. This reduces operational friction and accelerates incident response, which is especially important in ransomware scenarios.

- **Integrated AI and automation:** The cyber-recovery solution leverages AI across malware detection, behavioral analytics, backup validation, endpoint anomaly detection, and security incident interpretation. Automated and AI-guided response playbooks help minimize manual triage, even across thousands of endpoints.
- **Extensive ecosystem and multicloud support:** Acronis Cyber Protect Cloud has broad integration options with support for major public clouds, popular hypervisors, legacy and modern OSs, and 300+ technology partners. The multitenant architecture is attractive to MSPs and large enterprises with distributed IT.
- **Operational technology (OT) resilience:** Acronis distinguishes itself through its purposeful support for industrial environments. It can protect legacy PC OS versions that vendors no longer support but are still widely used in industrial settings such as Windows XP and Linux 2.6.9. It does not need a cloud connection to run, making it suitable for air-gapped environments, and it features simple one-click recovery suitable for plant operators with little or no IT skill.

Challenges

- **No curated recovery:** While capable of single-click, point-in-time, and automated bulk recovery options, Acronis does not currently have the ability to build a recovery snapshot out of the last known good versions of files across multiple backups.
- **No formal data loss or ransom payment guarantees:** Acronis does not offer codified data loss or ransom payment guarantees. Remuneration is handled ad hoc, with no guaranteed recourse for catastrophic events.

Consider Acronis When

Acronis Cyber Protect Cloud is better suited for SMB organizations seeking a unified, robust cyber-recovery solution. It is also uniquely suited for OT operators with legacy OS support, simple operation, and full functionality in air-gapped environments. Acronis' channel-only approach allows customers to leave deployment and management to the company's many MSP partners — an enticing offering for companies with limited IT staff and resources.

Arcserve

IDC has identified Arcserve as a Major Player in this 2025 IDC MarketScape for worldwide cyber-recovery.

Arcserve, headquartered in Eden Prairie, Minnesota, positions itself as a pioneer in cyber-resilience with a strong focus on small and midsize organizations. Its principal cyber-recovery product is Arcserve Unified Data Protection (UDP), a comprehensive data protection solution that combines backup and recovery across multiple environments, disaster recovery, and ransomware-specific protection such as immutability and threat detection.

Arcserve UDP unifies backup, disaster recovery, and cyber-resilience into a single platform with support for on-premises, cloud, hybrid, and SaaS workloads. Key features include immutable storage in its appliances, deduplication, instant VM recovery, real-time replication, and "Assured Security" for malware and ransomware scanning at every stage (e.g., backup, at rest, and restore). Arcserve natively integrates with various public clouds (e.g., AWS, Azure, Google Cloud, and Wasabi), SaaS applications (e.g., Microsoft 365 and Salesforce), and popular hypervisors (e.g., VMware, Hyper-V, and Nutanix).

Arcserve's cyber-recovery solution can be purchased as standalone products or through backup as a service (BaaS) and disaster recovery as a service (DRaaS). On the services side, Arcserve customers have access to Arcserve Academy for training, rapid response teams for ransomware incidents, and direct-to-engineer support for troubleshooting.

Strengths

- **Simplicity and ease of use:** As SMB and midmarket is Arcserve's primary focus area, the company's cyber-recovery solution emphasizes simple deployment and management for organizations with limited IT resources and diverse infrastructure.
- **Affordability and flexible pricing:** Arcserve offers multiple licensing and deployment options to meet varying budgets and deliver the solution at a compelling price point.
- **Comprehensive cyber-resilience platform:** The Arcserve platform offers unified management for on-premises, cloud, hybrid, and SaaS environments from a single console. It also features immutable storage, tape support as an air-gap option, and near-zero RPO capabilities.
- **Global support and training:** Arcserve has a wide ecosystem of global partners in North and South America, EMEA, APAC, and Japan and provides 24 × 7

multilingual tech support, ransomware response, and an extensive training and certification platform for its customers.

Challenges

- **Enterprise depth:** With its primary focus on midmarket and SMB, Arcserve lacks some advanced features enterprises typically look for in a cyber-recovery product such as AI-based threat and anomaly detection, anomalous user behavior detection, data classification, and full runbook automation. Some of these capabilities are currently in development.
- **Direct incident response services:** While Arcserve provides a rapid response team for recovery from ransomware incidents, this team's scope is limited to the Arcserve solution and the customer's environment. Arcserve doesn't provide in-house expertise for other aspects of ransomware attacks such as ransom negotiation or cybercrisis consulting services, instead relying on its partner network for this capability.

Consider Arcserve When

Arcserve should be considered by buyers seeking cyber-recovery and ransomware resilience delivered through an easy-to-operate, cost-effective platform. It is an especially strong fit for midmarket, SMB, and regional or distributed organizations where IT staffing is limited and operational simplicity is paramount.

Cohesity

IDC has identified Cohesity as a Leader in this 2025 IDC MarketScape for worldwide cyber-recovery.

Cohesity, founded in 2013 and headquartered in San Jose, California, started in the data protection market and has since pivoted into cyber-recovery, focusing on enabling organizations to recover quickly and safely from malicious, disruptive events. The centerpiece of its cyber-recovery portfolio is the Cohesity Data Cloud, an integrated platform that combines Cohesity's DataProtect data protection, RecoveryAgent DR and cyber-recovery orchestration offering, DataHawk data security and threat scanning tool, and FortKnox immutable cybervaulting solution.

Cohesity's advanced cyber-recovery capabilities include automated clean room orchestration, AI-guided anomaly detection, threat monitoring and hunting, instant mass recovery, granular data classification, cybervaulting, and a broad portfolio of integrations with leading security vendors through the company's Data Security Alliance. Key integrations span SIEM/SOAR tools (e.g., Splunk, MS Sentinel, and Palo Alto XSOAR), endpoint security (e.g., CrowdStrike and Tenable), DSPM vendors (e.g., BigID

and Cyera), identity security (e.g., Semperis and CyberArk), and cloud platforms (e.g., AWS, Azure, and GCP).

The platform's unified Helios interface manages both on-premises and multicloud deployments, enabling centralized oversight for complex environments. Cohesity also expanded its platform in 2024 to include Gaia, a generative AI (GenAI) application that uses retrieval-augmented generation (RAG) technology to get insights and generate answers to user questions about enterprise data under the purview of Cohesity Data Cloud.

Cohesity closed its acquisition of a large portion of Veritas' portfolio at the end of 2024, which included Veritas' flagship NetBackup cyber-recovery solution. Cohesity plans to continue developing and enhancing both its own Data Cloud and NetBackup while integrating the two product lines.

Strengths

- **AI-assisted recovery orchestration:** Cohesity's RecoveryAgent delivers comprehensive, AI-powered cyber-recovery orchestration. It supports end-to-end workflows that guide users from incident detection through rehearsals, clean room setup, forensic validation, and automated restoration. Blueprints offer customizable, repeatable runbooks, and recovery can be validated non disruptively, reducing operational risk.
- **Advanced threat and anomaly detection:** The platform incorporates multiple layers of threat detection through AI/ML, signature-based scanning, and behavioral analytics for both backup and primary data. Continuous, proactive threat hunting is available, supported by integrations with leading threat intelligence feeds and third-party security platforms. The architecture includes automated quarantine of infected snapshots and robust access controls.
- **Cybervaulting and data immutability:** Cohesity FortKnox provides an air-gapped, immutable copy of critical data stored offsite or on premises, protected with advanced quorum controls and compliance-grade WORM technology. This helps ensure a surviving copy of data for reliable recovery even if primary and backup environments are compromised.
- **Extensive data security ecosystem:** The Data Security Alliance program integrates Cohesity with over 30 leading security, response, and posture management solutions. These integrations can help streamline collaboration between ITOps and SecOps and minimize time to recovery during a cyberincident.

Challenges

- **Platform complexity following merger:** Integration of Cohesity and Veritas portfolios, while well advanced, brings inherent complexity. Current customers of DataProtect or NetBackup may experience learning curves or transitional workflows as unified operations and interfaces are being fully realized.
- **Licensing and feature segmentation:** Some advanced cyber-recovery capabilities such as DataHawk, curated recovery, and in-depth operational analytics are available only in higher subscription tiers or as add-ons. This may increase evaluation time or total cost for buyers seeking specific advanced features.

Consider Cohesity When

Cohesity's cyber-recovery offering is suited for large-scale enterprises that can fully benefit from its high degree of automation. Smaller organizations can still benefit from Cohesity's Cloud Services SaaS offering to take advantage of its backup and recovery, DR, threat defense, and data security capabilities. Cohesity is especially compelling for buyers that highly value a robust security ecosystem and require collaborative response capabilities that bridge IT, security, and external partners.

Commvault

IDC has identified Commvault as a Leader in this 2025 IDC MarketScape for worldwide cyber-recovery.

Commvault, founded in 1996 and headquartered in Tinton Falls, New Jersey, delivers cyber-recovery through its Commvault Cloud cyber-resilience platform. The platform combines its on-premises data protection offerings with the SaaS and cloud-native portion of Commvault's portfolio (previously called Metallic). Uniting the two has resulted in a more cohesive offering that caters to hybrid enterprises with data and applications spread across multiple environments.

Commvault Cloud's purpose-built cyber-recovery features include immutable and air-gapped storage, curated and orchestrated recovery workflows, and deep integration with an extensive ecosystem of security vendors. Commvault was one of the pioneering recovery vendors to use decoys in its solution, simulating high-value targets such as Active Directory to detect infiltration attempts. Should Active Directory become compromised, Commvault is capable of forest-level and granular object recovery.

The platform supports the protection of a vast range of workloads, spanning files, VMs, containers, databases, SaaS, on-premises, and cloud-native applications. It has integrations across hyperscalers, data security vendors, and storage vendors. Commvault Cloud is available as SaaS, software only, and as an appliance, supporting

flexible deployment and data sovereignty needs. Commvault Cloud also offers support for several quantum-resilient algorithms through its post-quantum cryptography (PQC) solution, which serves as a quantum readiness early adopter option for regulated organizations.

Strengths

- **Cyber-recovery architecture:** Commvault Cloud combines data isolation, immutability, air gap, and orchestrated cleanroom recovery workflows under a unified control plane. This architecture supports granular restoration from verified malware-free recovery points and incorporates inline, pre-, and post-backup anomaly detection to minimize reinfection risk. Built-in data discovery and classification, cyberdeception, and AI-powered threat scanning help reduce data risks.
- **Workload and platform breadth:** The solution delivers workload coverage across on-premises, edge, SaaS, container, and cloud infrastructure. Its "any-to-any portability" enables migration and recovery of application stacks across heterogeneous platforms and cloud providers, reducing infrastructure lock-in and easing complex migrations or replatforming initiatives such as hypervisor migrations.
- **Security ecosystem integration:** Commvault Cloud features bidirectional integration with security operations platforms, such as SIEM, SOAR, XDR, and threat intelligence feeds, allowing organizations to orchestrate incident response with automated workflows, enforce least-privilege access, and maintain continuous posture assessment using familiar tools.
- **Dedicated cyber-resilience training:** Commvault addresses cyber-resilience skills gaps through offerings such as Readiverse and Cyber Recovery Range. Readiverse features training courses, workshops, certifications, and its Minutes to Meltdown tabletop exercises focused on cyber-resilience and readiness, while Cyber Recovery Range provides a simulated, but realistic, space that allows IT and cybersecurity professionals to train, practice, and validate cyber-recovery strategies.

Challenges

- **Platform complexity:** Commvault's wide functional coverage and depth, while powerful, may require significant initial investment in configuration, policy management, and skills development to fully realize value, particularly for organizations with limited IT or security staff.
- **Integration pains:** Ongoing integration of acquired products, such as Clumio and Cloud Rewind (formerly Appranix), may temporarily result in interface

disparities or workflow disruption, impacting user experience until full unification under the Commvault Cloud control plane is complete.

Consider Commvault When

Buyers should consider Commvault when seeking a single, unified cyber-recovery platform with a wide range of coverage for both legacy and modern workloads. This solution is particularly suited for large enterprises seeking to reduce technology sprawl, align data resilience strategies with evolving security and compliance mandates, and bolstering their staff's cyber-resilience skill set.

Dell

IDC has identified Dell as a Major Player in this 2025 IDC MarketScape for worldwide cyber-recovery.

Dell Technologies, headquartered in Round Rock, Texas, and founded in 1984, is an IT infrastructure provider. Within cyber-recovery, Dell's solution is anchored by the PowerProtect portfolio, with PowerProtect Data Manager and PowerProtect Cyber Recovery at the company's center. The former is Dell's cyber-resilience platform and the latter provides an isolated vault for backup data and CyberSense analytics to identify compromised data.

Dell's solution has two layers of ransomware detection. PowerProtect Data Manager's native Anomaly Detection analyzes backup data using machine learning (ML) algorithms to learn and recognize normal patterns over time to establish a baseline, then flags deviations from those patterns as potential anomalies. CyberSense is an integrated third-party tool that analyzes backup data at the content level to detect slow or intermittent encryption caused by ransomware while looking for thousands of variants of ransomware, malware signatures, and YARA patterns that indicate compromise. Combined, the tools help organizations more quickly identify data that is safe to recover from.

Dell's cyber-recovery portfolio also includes Dell Security and Resilience Services. This is divided into three categories: advisory services to help design and road map its cyber-resilience capabilities from initial deployment to maturity, managed services to provide 24 × 7 threat detection and monitoring, and incident response services to respond and recover from cyberincidents with help from Dell's internal, product-agnostic team of certified cybersecurity experts.

Strengths

- **High isolation standard:** Dell's solution is architected around a true isolated recovery vault with both physical and logical separation of data and

management planes, in strict alignment with NIST 800-209 isolation requirements and meeting Sheltered Harbor standards. The Sheltered Harbor endorsement is rare in the market and distinguishes Dell's approach to insider and advanced threat protection.

- **AI-powered detection:** Through CyberSense, Dell leverages AI/ML and deep content-based analytics beyond basic metadata both in production environments and in the isolated Cyber Recovery vault. This enables rapid identification of data corruption, malware patterns, and previously unknown threats, enabling forensics support and recovery accuracy.
- **Strong zero trust and supply chain security posture:** Dell embeds zero trust principles across identity, device, network, and application layers, including supply chain security, MFA, RBAC, hardware root of trust, and advanced NTP controls for immutability. As a storage hardware supplier, Dell can uniquely ensure that its cyber-recovery equipment is delivered to the intended recipient.
- **MDR and incident recovery services:** Dell offers a broad set of managed services, from 24 × 7 managed detection and response (with detections developed collaboratively with CrowdStrike) to incident retainer and professional recovery services. These services are supported by a global response team and flexible support models and are particularly appealing to organizations with skill shortages, complex environments, or lack a dedicated recovery vendor.

Challenges

- **Complexity:** The broad feature set and multilayered architecture may introduce operational complexity. Buyers may need considerable planning, design, and customization support, especially for smaller or less mature teams. Most customers use qualified professional services to implement and manage the Dell solution.
- **Dependency on hardware:** Dell PowerProtect's need for dedicated hardware and add-ons such as CyberSense for full functionality may result in a higher total cost of ownership and infrastructure investment compared with software-only or less feature-rich alternatives. Dell's managed service option may help mitigate this.

Consider Dell When

Dell is better suited for organizations with diverse workloads and complex environments that have the staff, skills, and resources to benefit from its PowerProtect products and leverage its expert-managed services. If the business requires immutable backup, forensic analytics, and a physically and logically isolated vault built on Sheltered Harbor–endorsed architecture, Dell's PowerProtect portfolio makes a good fit.

Druva

IDC has identified Druva as a Leader in this 2025 IDC MarketScape for worldwide cyber-recovery.

Founded in 2008 and headquartered in Santa Clara, California, Druva's cyber-recovery offering is the company's Data Security Cloud, a fully SaaS-based platform for backup, disaster recovery, and cyber-resilience. The solution protects endpoints, datacenters, SaaS applications, and cloud-native environments from a single console. As a purely SaaS-based solution, Druva uniquely provides advanced cyber-recovery capabilities without the need for traditional backup infrastructure.

Druva's key cyber-recovery features include immutable, air-gapped backups, curated recovery using the company's patented technology, AI-powered threat investigation through Dru Investigate, real-time anomaly detection, and threat hunting capabilities. The platform integrates with key security tools including CrowdStrike, Microsoft Sentinel, Palo Alto XSIAM, and Splunk. Druva uniquely includes managed data detection and response (MDDR) services at no additional cost, providing 24 × 7 monitoring by security experts.

As it is SaaS only, Druva delivers a very fast and simple onboarding process. The platform is recognized for its simplicity, rapid deployment, and a formal Data Resiliency Guarantee that provides up to $10 million in financial protection to customers.

Strengths

- **100% SaaS-based architecture:** Druva's cloud-native design eliminates the need for backup appliances, media servers, or on-premises infrastructure. This approach provides automatic scaling, eliminates hardware refresh cycles, and reduces operational overhead. It also ensures customers are always running the latest version with automatic updates every two weeks.
- **Air gapped by design:** Druva is inherently air gapped, as the control plane is Druva itself and separated from the customer's data plane. If a customer's primary data is compromised, the backups remain safe, as there is no way for an attacker to directly jump from the customer's systems into Druva.
- **Patented curated recovery technology:** Druva offers unique curated recovery capabilities that automatically analyze backup snapshots across an incident timeline to create "golden snapshots" containing the most recent clean versions of files. This patented technology minimizes data loss during ransomware recovery by avoiding the need to restore to a single point-in-time backup, instead intelligently combining clean data from multiple backup points.

- **AI-enhanced investigation and recovery:** Druva's Dru Investigate provides AI-powered natural language querying of backup telemetry, enabling both IT and security teams to quickly investigate incidents, correlate events, and identify compromised systems. The platform leverages MITRE ATT&CK frameworks and provides intelligent snapshot scoring to guide recovery decisions, significantly reducing investigation time during cyberincidents.

Challenges

- **SaaS-only model constraints:** Druva's commitment to 100% SaaS delivery, while providing benefits, may not suit organizations with strict data residency requirements, limited internet connectivity, or regulatory constraints that mandate on-premises data retention. Druva's model requires consistent cloud connectivity and may not accommodate physically air-gapped environments that some highly regulated industries require.
- **Dependency on cloud provider availability:** As a cloud-native solution storing data in AWS and Azure regions, Druva's availability is inherently dependent on cloud provider uptime and connectivity. While the platform offers cross-region redundancy and the ability to back up data to AWS and Azure, organizations concerned about cloud provider dependencies or those requiring complete independence from public cloud infrastructure may find this architectural approach limiting.

Consider Druva When

Druva's simplicity, ease of deployment, and low barrier of entry make the company ideal for small- to medium-scale enterprises, but businesses of all sizes that prioritize minimizing their datacenter footprint will find Druva's cyber-recovery solution compelling. It is less suitable for organizations committed to entirely on-premises data protection or with regulatory prohibitions against cloud storage.

HPE

IDC has identified HPE as a Major Player in this 2025 IDC MarketScape for worldwide cyber-recovery.

HPE Zerto, founded in 2009 and headquartered in Boston, Massachusetts, was acquired by Hewlett Packard Enterprise (HPE) in 2021. Its flagship cyber-recovery product is now called HPE Zerto Software, and it's supported by the HPE Cyber Resilience Vault, the HPE Alletra Storage MP B10000 storage system, and integration into the broader HPE portfolio.

HPE Zerto's core offering centers on continuous data protection (CDP), with a journal-based architecture that provides recovery point objectives (RPOs) in seconds and near-

instant recovery time objectives (RTOs). HPE Zerto also features real-time anomaly detection as data is written into the journal, automation and orchestration at scale, and support for hybrid, multicloud, and on-premises environments.

The HPE Cyber Resilience Vault is a component of the overall cyber-recovery solution. It is purpose-built for isolated, immutable data recovery, providing physical and logical air gapping, high-performance storage, and automated recovery workflows. HPE Zerto integrates deeply with HPE storage, compute, and networking, and offers direct integration with cybersecurity tools such as CrowdStrike Falcon, and backup solutions such as Commvault, Cohesity, and Veeam.

Strengths

- **Granular, real-time detection and recovery:** HPE Zerto's cyber-recovery engine is designed around CDP, capturing every data change with near-real-time anomaly detection that identifies ransomware activity as it occurs, enabling organizations to respond quickly and return to a precise moment before compromise.
- **Automation and scale:** The platform delivers built-in automation and orchestration, allowing organizations to restore entire environments or individual workloads in minutes. Granular boot order orchestration, automated network reconfiguration, and application-centric recovery minimize manual intervention.
- **Integrated ecosystem and storage performance:** HPE Zerto is deeply integrated into the HPE stack, combining compute, storage, and networking. Although HPE Zerto is storage agnostic, HPE Cyber Resilience Vault must store recovery data on the HPE Alletra Storage MP B10000 hardware platform, which provides production-grade, high-performance storage to avoid the slow rehydration process of typical backup appliances.
- **Air-gapped recovery and immutability:** The HPE Cyber Resilience Vault provides a true air gap with no network connections to the production environment. The Vault also provides immutable storage for backup data and serves as an isolated recovery environment for organizations to test their recovery and ensure it is safe before restoring to production.

Challenges

- **Complex portfolio configuration:** While highly flexible, deploying the full suite including storage and vault options can require careful planning and architecture expertise. This complexity may present challenges for organizations without strong internal resources or access to HPE's professional services.

- **Limited integration with security tools:** Although HPE Zerto has had an open API to establish third-party integrations for years, the solution's "plug-in" API integration model is still new. Current security integrations include CrowdStrike and HashiCorp Vault, with other SIEM, SOAR, and XDR offerings on the road map.

Consider HPE When

Due to its integration with HPE GreenLake, HPE Zerto is a compelling offering for HPE customers by default. Its value lies in its combination of real-time ransomware detection, near-instant and highly granular recovery, and its connection to HPE's robust portfolio. Organizations prioritizing minimal data loss during recovery will be especially interested in HPE Zerto.

IBM

IDC has identified IBM as a Major Player in this 2025 IDC MarketScape for worldwide cyber-recovery.

IBM, headquartered in Armonk, New York, and founded in 1911, has an enterprise IT portfolio that spans compute, network, storage, security, and data protection. Its cyber-recovery offering, IBM Storage Defender, takes advantage of this portfolio by using access to primary data on IBM storage to enable real-time ransomware detection before it reaches secondary storage.

Its cyber-recovery solution, IBM Storage Defender, is positioned as "cyberstorage," the vendor's term for a holistic view of storage from a cyberperspective. The solution consists of both primary storage, which is protected by SSO, MFA, MPA, encryption, immutable snapshots, I/O stream analysis for early threat detection, and backup storage, which can be provided by IBM Storage Protect software and an IBM-enhanced version of Cohesity's DataProtect. The solution has visibility across primary and backup data on IBM, Dell, and Pure Storage environments.

Other key features include multilayered threat detection using AI, anomaly detection, and hardware sensors, near-real-time ransomware and malware alerting, air-gapped protection options, and orchestrated recovery testing in isolated environments. Storage Defender supports integrations with ServiceNow and SIEM platforms such as QRadar, Splunk, and ServiceNow, as well as third-party backup and security providers including Cohesity, AvePoint, Index Engines, and Cobalt Iron.

Strengths

- **Breadth and depth of platform coverage:** IBM Storage Defender spans both primary and backup storage across distributed, mainframe, cloud, and SaaS

workloads. Its holistic approach allows for complete data estate management, giving organizations visibility and control of all data repositories.

- **Multilayered detection:** IBM Storage Defender combines real-time hardware sensors, AI and ML-enabled analytics, and host-based anomaly detection. These mechanisms operate at multiple points in the data life cycle, minimizing the risk of undetected compromise and providing rapid alerts for ransomware, malware, and other threats.
- **Ecosystem integration and open architecture:** IBM supports integration with a broad spectrum of third-party backup, security, and infrastructure tools, giving customers the ability to leverage familiar assets while adopting Defender's capabilities. Notable integrations include Dell, Pure Storage, Cohesity, Index Engines, AvePoint, and ServiceNow.
- **Strong consulting and incident response services:** IBM X-Force provides a host of cyber-resilience services including tabletop exercises, incident response, threat intelligence services, adversary simulation, and many others.

Challenges

- **Partial feature dependence on IBM hardware:** Although customers don't have to use IBM hardware with IBM Storage Defender, certain advanced features such as real-time threat detection via FlashCore sensors are only available on IBM FlashSystem storage.
- **Limited cloud deployment options:** IBM Storage Defender only supports AWS and IBM Cloud in North America, and no cloud providers in EMEA and APJ regions. IBM has plans to expand on this based on customer demand, with an EMEA offering coming in the next four to eight months.

Consider IBM When

IBM Storage Defender is more appropriate for IBM storage customers, as well as larger enterprises seeking a cyber-recovery solution that spans the full data estate. As IBM expands its integrations with third parties, the solution will improve as it gains greater flexibility.

Quest

IDC has identified Quest as a Contender in this 2025 IDC MarketScape for worldwide cyber-recovery.

Quest Software, founded in 1987 and headquartered in Aliso Viejo, California, is a global provider of enterprise IT management solutions. Its cyber-recovery solution consists of NetVault Plus at its core, complemented by the QoreStor data storage engine, Recovery Manager for Active Directory (RMAD), and a suite of other products.

NetVault Plus is architected for on-premises, hybrid, and multicloud repositories and integrates tightly with both Quest's own identity and Quest's security portfolio, which includes Change Auditor, InTrust, and BloodHound, as well as third-party backup appliances. Core features of the solution include malware detection via open source ClamAV, machine learning–based anomaly detection for behavioral and data change analytics, encryption, and robust immutability.

Quest's QoreStor storage engine serves as NetVault Plus' backup target. It is fully software defined and integrates with many major cloud providers, third-party backup appliances, and third-party data protection software. It is managed via Quest's as-a-service QorePortal interface.

Strengths

- **Advanced immutability:** Quest's cyber-recovery solution enforces strict immutability with non-bypassable policies, ensuring that mistakenly or maliciously deleted backups are recoverable. Immutability settings can't be reversed or overridden, and system time manipulation is mitigated by internal controls.
- **Active Directory recovery and forensics tools:** Between RMAD, Change Auditor, and BloodHound, Quest uniquely addresses Active Directory protection with compromise detection, forensic investigation, and granular object-to-farm recovery.
- **Instant VM recovery:** Quest's solution is capable of instant restore for VMs directly from deduplicated, encrypted storage. It also supports sandbox and physical recovery testing.
- **Highly flexible and agnostic:** Quest features broad support for major cloud providers including AWS, Azure, Google (GCP), Wasabi, Backblaze, and IBM Cloud. It integrates with third-party backup appliances such as Dell PowerProtect DD and Quantum DXi. QoreStor is data protection vendor agnostic and can serve as a backup target for Veeam.

Challenges

- **No native cyber-recovery services:** While its professional services assist with secure backup architecture, Quest does not offer dedicated cyberincident response, ransom payment negotiation, or crisis communications as native services, instead relying on partners for these capabilities.
- **No security tool integration:** Quest has no integrations with SIEM, SOAR, or XDR tools that would strengthen its capabilities beyond data protection.

Consider Quest When

Quest's cyber-recovery solution is better suited for organizations seeking a flexible solution that can support any environment, as well as for companies that are especially interested in advanced, immutable storage and highly granular Active Directory recovery capabilities.

Rubrik

IDC has identified Rubrik as a Leader in this 2025 IDC MarketScape for worldwide cyber-recovery.

Rubrik, headquartered in Palo Alto, California, and founded in 2014, delivers cyber-recovery through its Rubrik Security Cloud. It is a unified, SaaS-based cyber-recovery platform with capabilities spanning backup, recovery, data security posture management, threat intelligence, data observability, guided cyber-recovery, and more.

Rubrik Security Cloud's core features include continuous threat monitoring, AI-enabled anomaly detection, patented Turbo Threat Hunting for rapid clean snapshot identification, cyber-recovery orchestration, and identity resilience targeting Active Directory and cloud identity platforms. The solution integrates natively with a large ecosystem of third-party platforms and products including M365, Salesforce, AWS, Azure, GCP, Oracle Cloud, CrowdStrike, Okta, Splunk, and ServiceNow, among others.

Rubrik invested heavily into AI, and AI/ML is pervasive throughout Rubrik's solution. ML is used in its Data Threat Engine to identify suspicious activity and in Sentry AI to help its customer support team provide proactive service and recommendations. Ruby, Rubrik's GenAI companion, helps customers discover, investigate, remediate, and report on cyberincidents. Upon detecting an indicator of compromise by Rubrik Threat Monitoring, Ruby provides step-by-step guidance through an interactive chat interface.

Strengths

- **Extensive threat detection capabilities:** Within Rubrik Data Cloud, Rubrik Anomaly Detection uses a combination of data change, entropy, heuristics, and proprietary ML to enable continuous threat detection across backup data, and its Threat Monitoring and Turbo Threat Hunting enable proactive, rapid malware scanning at scale.
- **DSPM and identity resilience:** Rubrik's Data Access Governance is a DSPM tool within Rubrik Data Cloud that identifies user file system activity, user access to sensitive data, and changes to file and share permissions. In addition, Rubrik Identity Resilience continuously monitors for identity misuse, privilege escalations, stale or orphaned accounts, and unauthorized changes in Active Directory and Entra ID.

- **Ransomware response services included:** The Rubrik Ransomware Response Team assists organizations in responding to ransomware attacks by providing strategic and technical guidance during ransomware incidents, assisting with attack origin and blast radius analysis, and guiding teams through recovery using Rubrik Security Cloud. This is available to all Rubrik customers free of charge.
- **Deep ecosystem integrations:** Rubrik's platform unifies cyber-recovery and security operations with integrations to cloud, SIEM, SOAR, and identity vendors. Native support allows organizations to initiate threat hunts or orchestrate recovery directly from XDR, SIEM, or ITSM platforms, with all reporting, monitoring, and policy management consolidated in Rubrik's SaaS-based console.

Challenges

- **Uneven hypervisor support:** Rubrik supports data protection across multiple hypervisors including VMware, Microsoft Hyper-V, Nutanix AHV, and Red Hat OpenShift Virtualization, but some advanced security features have different levels of support across platforms. Specifically, hypervisor-level ransomware detection is currently limited to VMware environments, although VM-level encryption detection and anomaly detection capabilities are available across most supported platforms.
- **Limited view of data estate:** Rubrik's threat scanning, detection, advanced AI integration, and other security capabilities don't extend into primary storage environments. While Rubrik isn't meant to replace organizations' security tools, it nevertheless means it is only aware of data within the Rubrik Security Cloud platform. However, broader primary storage integration is in active development with some of Rubrik's strategic technology partners such as Pure Storage.

Consider Rubrik When

Rubrik's capabilities make the company broadly appealing and appropriate for medium- to large-scale organizations, especially those operating hybrid and multicloud environments or regulated industries. Any organization seeking cyber-recovery that goes beyond data backup and deeply into threat detection and response should strongly consider Rubrik.

Veeam

IDC has identified Veeam as a Leader in this 2025 IDC MarketScape for worldwide cyber-recovery.

Veeam, headquartered in Kirkland, Washington, and founded in 2006, got its start in backup and recovery for virtual environments, but has since then expanded its coverage to a broad range of environments and workloads. Its flagship cyber-recovery

solution is Veeam Data Platform, which consists of components such as Veeam Backup & Replication for data protection, Veeam Recovery Orchestrator for automated DR, Veeam Data Cloud for data protection for cloud environments and SaaS applications, and Veeam ONE for analytics, monitoring, and reporting.

Veeam's key features include inline AI-powered malware detection, immutable and encrypted data storage, rapid orchestrated recovery options, CDP with as low as 2 second RPOs, and extensive threat detection and reporting. After its acquisition of Coveware in 2024, Veeam added ransomware and cyberextortion response services to its cyber-recovery portfolio.

Veeam is only sold over its partner ecosystem, which consists of over 11,000 service providers. It has integrations with major public cloud providers, SIEM, SOAR, and other security platforms, and with Quantum DXI, Dell EMC Data Domain, HPE StoreOnce, and ExaGrid purpose-built backup appliances.

Strengths

- **Broad platform support:** Although Veeam started at protecting VMware VMs, it has expanded to multiple hypervisors including Microsoft Hyper-V, Nutanix AHV, Red Hat RHV, and Proxmox. It also protects public clouds, five physical platforms (Windows, Linux, Mac OS, Solaris, and AIX), enterprise database applications, and SaaS applications.
- **Security and cyber-recovery capabilities:** Veeam uses AI-powered, inline malware and ransomware detection during data capture and at rest. Deep forensics, including signature-based and YARA rule scanning, integrate into recovery and incident response operations. Security is further reinforced by immutable backups and air-gapped storage.
- **Incident response expertise:** The integration of Coveware by Veeam brings differentiated in-house capabilities for cyberincident response, including ransom negotiation, forensic analysis, and quarterly workshops. This enables customers to prepare for and respond to cyberextortion events with guided support and hands-on expertise.
- **High degree of flexibility:** Veeam's self-describing backup format ensures true data portability, enabling rapid recovery and migration across clouds or hypervisors. Combined with its broad integration with SIEM, endpoint security, and storage platforms, Veeam is able to accommodate most modern and legacy environments.

Challenges

- **Limited SaaS application coverage:** Although Veeam is constantly expanding its support to protect more enterprise workloads, the only SaaS applications it

currently protects are M365, Entra ID, and Salesforce. Other SaaS applications are considered critical and need data protection as well, especially in the software development tool market (e.g., Confluence, Jira, and GitHub).

- **Ransomware warranty availability:** Veeam offers a Ransomware Recovery Warranty that covers up to US$5 million in data recovery expenses if it is unable to recover data from a ransomware attack. However, it is only offered to customers that meet strict criteria and are enrolled in the Cyber Secure program, which could limit guaranteed restitution for some organizations.

Consider Veeam When

Veeam has broad appeal and should be considered by organizations looking for a robust cyber-recovery solution with unique, expert-guided incident response services. Veeam's modularity and broad partner ecosystem make the company a strong choice for environments where operational flexibility, security integration, and scalability are key purchasing drivers.

APPENDIX

Reading an IDC MarketScape Graph

For the purposes of this analysis, IDC divided potential key measures for success into two primary categories: capabilities and strategies.

Positioning on the y-axis reflects the vendor's current capabilities and menu of services and how well aligned the vendor is to customer needs. The capabilities category focuses on the capabilities of the company and product today, here and now. Under this category, IDC analysts will look at how well a vendor is building/delivering capabilities that enable it to execute its chosen strategy in the market.

Positioning on the x-axis, or strategies axis, indicates how well the vendor's future strategy aligns with what customers will require in three to five years. The strategies category focuses on high-level decisions and underlying assumptions about offerings, customer segments, and business and go-to-market plans for the next three to five years.

The size of the individual vendor markers in the IDC MarketScape represents the market share of each individual vendor within the specific market segment being assessed. In this case, because cyber-recovery is a use case for other data protection products, we have used the vendor's data protection software revenue according to IDC's research as the market share.

IDC MarketScape Methodology

IDC MarketScape criteria selection, weightings, and vendor scores represent well-researched IDC judgment about the market and specific vendors. IDC analysts tailor the range of standard characteristics by which vendors are measured through structured discussions, surveys, and interviews with market leaders, participants, and end users. Market weightings are based on user interviews, buyer surveys, and the input of IDC experts in each market. IDC analysts base individual vendor scores, and ultimately vendor positions on the IDC MarketScape, on detailed surveys and interviews with the vendors, publicly available information, and end-user experiences in an effort to provide an accurate and consistent assessment of each vendor's characteristics, behavior, and capability.

Market Definition

Cyber-recovery capabilities are built upon data replication and protection software and disaster recovery systems. Our definitions of pertinent market components follow:

- **Data protection software:** Data protection software is focused on protection, restoration, and recovery of data in the event of physical or logical errors. Products within the data protection and recovery market include data protection, continuous data protection (CDP), bare metal restore, backup/recovery software, host-based replication, and array-based replication (inclusive of snapshots, mirror/clones, and remote replication). Data protection software includes revenue from licensed software and online data protection services (aka online backup) licensed in a subscription fashion. This is inclusive of file- and image-level backup software, continuous data protection software, and backup reporting software.
- **Data protection as a service (DPaaS):** DPaaS is an umbrella term that includes backup, archive, disaster recovery, and cyber-recovery as a service. These are cloud-based services fully managed by the service provider. Most DPaaS solutions can address on-premises workloads as well as hybrid and multicloud workloads.
- **Disaster recovery and disaster recovery as a service (DRaaS):** Disaster recovery systems include all of the infrastructure, process management, and services necessary to restart an entire workload either on premises or in public cloud environment. DRaaS differs from on-premises and traditional disaster recovery in that DRaaS is a cloud-based, fully managed service. An organization may declare a disaster response based on datacenter fires or broken water pipes, power loss, and regional events such as train derailments, plane crashes, or terror events as well as earthquakes, floods, tornadoes, and hurricanes.

- **Cyber-recovery and cyber-recovery as a service (CRaaS):** Cyber-recovery builds upon disaster recovery, and CRaaS builds upon DRaaS. Cyber-recovery in both contexts includes all infrastructure, process management, analytics/forensics, and professional services to assist organizations in recovering from malware attacks in general and ransomware specifically. To qualify as a CRaaS service, we believe it must include all of the components of DRaaS (in other words, the ability to reestablish an application workload in its entirety) plus provisioning for a sanitary sandbox, forensic analysis, and curated recovery. Some vendors may go substantially beyond that with additional data security functions for value-add and differentiation.

Strategies and Capabilities Criteria

Tables 1 and 2 provide key strategy and capability measures, respectively, for measuring the success of a cyber-recovery provider.

TABLE 1

Key Strategy Measures for Success: Worldwide Cyber-Recovery

Strategies Criteria	Definition	Weight (%)
Functionality or offering strategy	Future vision — ability to forecast cyber-recovery requirements over near, medium, and longer terms and align those requirements with planned deliverables; foresight on how to meet customer requirements	16.0
Delivery	Customer success with onboarding, technical support for cybersituations, professional services related to cyber-recovery, and cyberperformance guarantees/warranties Multicloud deployments — ability to leverage broad private and public cloud environments worldwide for cyber-recovery and unique hybrid cloud/multicloud architecture or features Partner leverage — ability to develop and participate in cyber-related ecosystems	51.0
R&D pace/productivity	Vendor plan for developing cyber-recovery product requirements and solution differentiation	9.0
Innovation	Development depth and breadth, level of R&D investment, speed of innovation delivery and zero trust delivery	24.0
Total		100.0

Source: IDC, 2025

TABLE 2

Key Capability Measures for Success: Worldwide Cyber-Recovery

Capabilities Criteria	Definition	Weight (%)
Functionality or offering	Ability to ensure data survival Ability to detect malware in backups Ability to ensure clean, quick, and accurate recovery	75.0
Portfolio benefits	Unique portfolio design and the benefits it delivers	3.0
Service offerings	Added value services designed to improve cyber-recovery outcomes Crisis communications — facilitate communications with stakeholders out of band, and facilitate coordination between ITOps and SecOps	16.0
Pricing model or structure of product/offering	License flexibility to meet customer needs with the ability to "rightsize" license	6.0
Total		100.0

Source: IDC, 2025

LEARN MORE

Related Research

- *Data Protection's Importance — IT Initiatives Least Impacted by Economic Factors* (IDC #US53699625, July 2025)
- *Skill Issues When It Comes to Cyber-Response* (IDC #US53152425, February 2025)
- *Cyber-Recovery and Cyber-Resilience to Drive a Significant Increase in the Budget for 2025* (IDC #US52679424, October 2024)

Synopsis

This IDC study is an evaluation of the 11 most prominent cyber-recovery vendors on a worldwide basis. While it offers details on each vendor's capabilities and offerings, it is not meant to be a buyer guide. Instead, this evaluation is intended to help IT buyers differentiate between cyber-recovery solutions and narrow down candidates that fit their specific needs.

"No single cyber-recovery vendor offers the perfect solution for every organization's cyber-resilience needs," said Johnny Yu, research manager, Infrastructure Software Platform at IDC. "This IDC MarketScape is designed to give IT buyers the knowledge to find the solutions that best match their organizational needs, cyber-resilience skill levels, and infrastructure requirements."

ABOUT IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology, IT benchmarking and sourcing, and industry opportunities and trends in over 110 countries. IDC's analysis and insight helps IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives. Founded in 1964, IDC is a wholly owned subsidiary of International Data Group (IDG, Inc.).

Global Headquarters

140 Kendrick Street
Building B
Needham, MA 02494
USA
508.872.8200
Twitter: @IDC
blogs.idc.com
www.idc.com