IDC ANALYZE THE FUTURE

White Paper

The State of Data Protection and Disaster Recovery Readiness: 2021

Sponsored by: Zerto

Phil Goodwin
April 2021

IDC OPINION

The demand for data has never been greater and the value of data never more powerful. IDC research has found that 60% of organizations have taken steps to be "data driven" – that is, they have implemented tools and methods to utilize data more effectively to make decisions faster and with greater accuracy and certainty.

For those organizations genuinely pushing to become data driven, the key foundational element is obviously data availability. Without data availability, data use simply is not possible. Data availability has a number of aspects, starting with online access. Organizations that suffer disproportionally high downtime – whether planned or unplanned – will be at a competitive market disadvantage relative to those companies that have "always on" systems. Data loss, often regarded as the cardinal sin of data protection, further erodes an organization's ability to harness the power of data. Data loss can lead to lost customers, lost revenue, lost opportunity, and staff overtime.

Previous generations of data protection software and storage systems simply did not have the capability to prevent data loss or downtime. Organizations had to accept data loss and downtime as unavoidable. However, this situation has become increasingly unacceptable as the consequences become more costly and severe. Thus IT organizations are looking for solutions that can drive downtime SLAs (i.e., recovery time objective [RTO]) and data loss SLAs (i.e., recovery point objective [RPO]) to near zero, equating to no downtime and no data loss.

The proliferation of applications and the data they create are making the effort to make data always available more difficult. Organizations use a variety of interleaved data protection products (i.e., backup and recovery software, snapshots, mirrors, and replicas) along with disaster recovery (DR) strategies as a means to ensure data recovery in the event of any failure. However, new applications at the core, cloud, and edge create data that is structured, unstructured, and containerized; this data resides in geographically dispersed object storage services such as AWS S3 and Azure Blob. As a result, IT organizations are facing ever-increasing complexity in providing data protection and disaster recovery.

Our research also indicates that more than 80% of new applications will be deployed in the cloud or at the edge. Most cloud applications will be either SaaS or cloud-native containerized applications. SaaS application data, in particular, can create a data management gap. This is because the data is managed by the SaaS provider and not the IT group and thus does not have the governance or data protection policies of the IT organization. These factors further contribute to data becoming siloed and requiring separate data protection, DR, orchestration, monitoring, and management solutions. These overlapping solutions contribute to additional infrastructure costs and staff inefficiency.

In early 2021, IDC conducted a research study, sponsored by Zerto, to learn about evolving requirements for backup and disaster recovery and how organizations are dealing with emerging challenges. The top IT priorities include:

- Cloud-first deployments
- IT transformation (ITX)
- Implementing cloud-based disaster recovery

In addition, other key findings include:

- 95% of organizations have had to rethink data protection due to the sudden emergence of work from home (WFH).
- New workloads, including containerized applications and SaaS, are driving data protection modernization.
- Malware and ransomware attacks are so pervasive that organizations must provide protection from them and ensure recovery.
- 43% of organizations suffered unrecoverable data within the past 12 months.
- 63% of organizations have suffered a data-related business disruption within the past 12 months.

One of the key technologies now emerging to help IT organizations improve data protection, reduce data loss, and recover data more quickly is continuous data protection (CDP). CDP can reduce service levels – both RPO and RTO – from hours to minutes or even seconds. In fact, CDP is becoming a key means of driving toward near-zero RPO and near-zero RTO. Moreover, the highly granular nature of CDP recoveries can assist organizations in recovering to a point just prior to a ransomware/malware attack to ensure recovery with the least amount of data loss possible.

METHODOLOGY

The IDC survey, conducted in early 2021, involved 506 respondents from medium- to large-scale organizations. The demographics of the survey include:

- 59% of respondents were senior IT leaders with titles such as CIO, CTO, and VP.
- 31% of respondents were senior business leaders with titles such as CEO (MD), CFO, and general manager.
- 10% of respondents were from IT operations with titles such as virtual administrators and backup administrators.
- 73.3% of respondents were from North America, with the remainder from select Western European countries (United Kingdom, Germany, Belgium, the Netherlands, and Luxembourg).
- More than 18 vertical industries were represented, with no more than 15% of respondents from any single industry.
  - The most represented industries were manufacturing, information technology, and financial services.
- Results were weighted by GDP.

SITUATION OVERVIEW

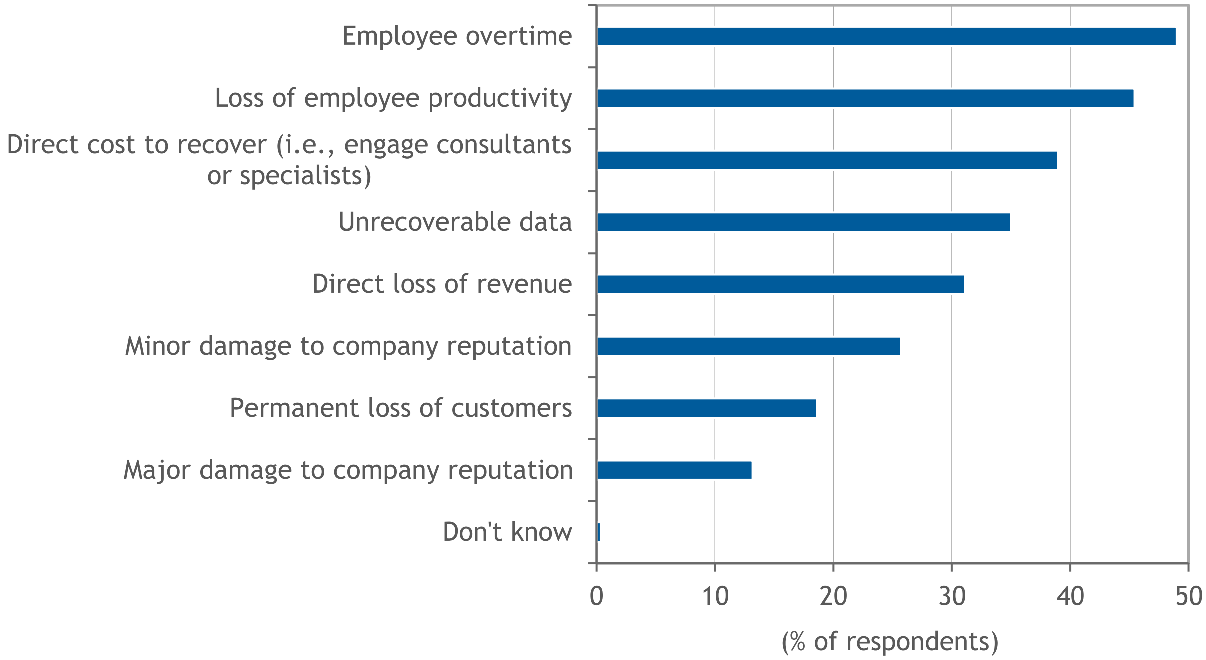
The threats to data are increasing and the consequences are becoming more serious. Attacks from bad actors have become nearly ubiquitous. In fact, from this survey, we learned that 95.1% of organizations have suffered a malicious attack within the past 12 months and 36.6% of respondents have suffered more than 25 attacks during that time. Unfortunately, with so many attacks, the chances of a successful attack become very high. Of the respondents that reported being attacked, 80.3% indicated that at least one attack resulted in data corruption. Of even greater concern, 43% of respondents have experienced unrecoverable data within the past 12 months.

These statistics concerning ransomware/malware attacks are stunning. Attacks are common, and the odds of being a victim seem to be a matter of when, not if. The impact on organizations from these attacks can be profound, as reported to us by those who had been victimized. The consequences of data corruption primarily affect people as respondents told us employee overtime, lost employee productivity, the direct cost of recovery, and unrecoverable data were the most significant issues. However, other significant consequences do occur, as shown in Figure 1.

From Figure 1, we can see that other consequences suffered include lost revenue, damaged company reputation, lost employee productivity, and permanent loss of customers. Put together, the consequences of disruption affect all aspects of the company, both internal and external.

FIGURE 1

Consequences of Data Disruptions



n = 323

Source: IDC's *Worldwide State of Data Protection and DR Survey,* January 2021

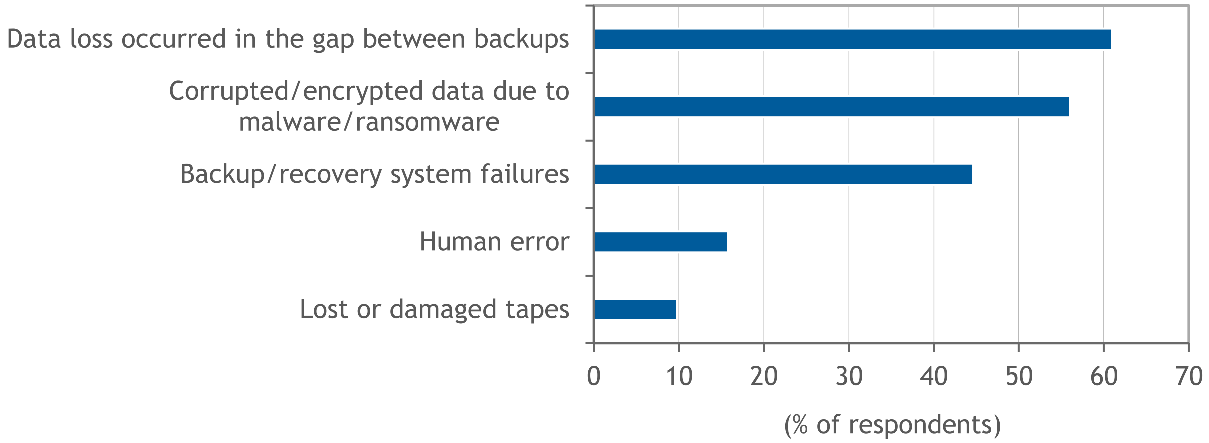
As we noted previously, data-driven companies simply cannot afford data loss, yet nearly half (43%) of the respondents reported having experienced unrecoverable data in the previous 12 months. For those organizations that had experienced unrecoverable data, we asked them to tell us the reasons behind those losses. Figure 2 shows the results.

It is noteworthy that two of the top 3 reasons in Figure 2 relate directly to the backup system itself and were experienced by large percentages of respondents. The number 1 reason, backup gap, can be attributed to the length of time between backups, which for most organizations remains at 24 hours. Moreover, there is a general assumption that backup/recovery systems are reliable. Unfortunately, this survey found that the backup/recovery system failed at a critical time for nearly 45% of respondents.

The number 2 reason, corruption or encryption due to malware/ransomware, was cited by more than half of the respondents (56%). Even this cause indirectly relates to the failure of backup systems. Clearly, the backup system for these respondents in these instances was not up to the challenge of recovering data from the ransomware attack. If organizations can deploy more reliable backup systems with more frequent and more granular backups, then it is entirely possible that they can eliminate the top 3 reasons for unrecoverable data. In this regard, CDP may offer the most promise as it nearly eliminates the gap between backups and does not rely on traditional backup windows for success.

FIGURE 2

Reasons for Unrecoverable Data



n = 218

Source: IDC's *Worldwide State of Data Protection and DR Survey,* January 2021

Given that the gap between backups is the leading cause of unrecoverable data, we can also deduce that the standard combined scheme of snapshots, replicas, and backups failed to prevent data loss. From this survey, we learned that the current most common RPO is 1-4 hours and the most common RTO is 4-8 hours. These SLAs have not changed from similar data in prior year surveys. While we cannot correlate specific SLAs to instance of data loss, we believe it is fair to conclude that the given SLA for respondents with data loss was not adequate to prevent the loss or at least ensure the recovery. Organizations must rethink availability SLAs based on new digital business models and market expectations. Reducing the RPO in particular can reduce the gap between backups from hours to seconds and thereby reduce the chance for data to be lost.

This survey took place when the COVID-19 pandemic had been in full swing for over a year during which organizations had been adjusting to the changing operating environment. In particular, the pandemic seems to have stimulated an increased urgency to adopt cloud computing, especially cloud-based data protection. In the survey:

- 88% of respondents indicated that public cloud would play at least some role in their future backup strategies.
- 91% of respondents said public cloud would play some role in their DR strategies.
- 64.5% of respondents believe public cloud will be "important" or "highly important" to backup plans, with 68.1% indicating "important" or "highly important" for DR plans.
- More than half (52.1%) of the respondents plan to invest more in both backup and DR improvements.
- 23.5% of respondents will invest more in backup improvements.
- 16.4% of respondents will invest more in DR improvements.

Pandemic-driven work-from-home changes were also shown to have a significant impact to data protection and DR plans. When respondents were asked how the COVID-19 pandemic had impacted their data protection (inclusive of disaster recovery) strategy for work-from-home workers, the results were stark: 94.7% of respondents said the pandemic had had an impact. Among the results were (multiple selections allowed):

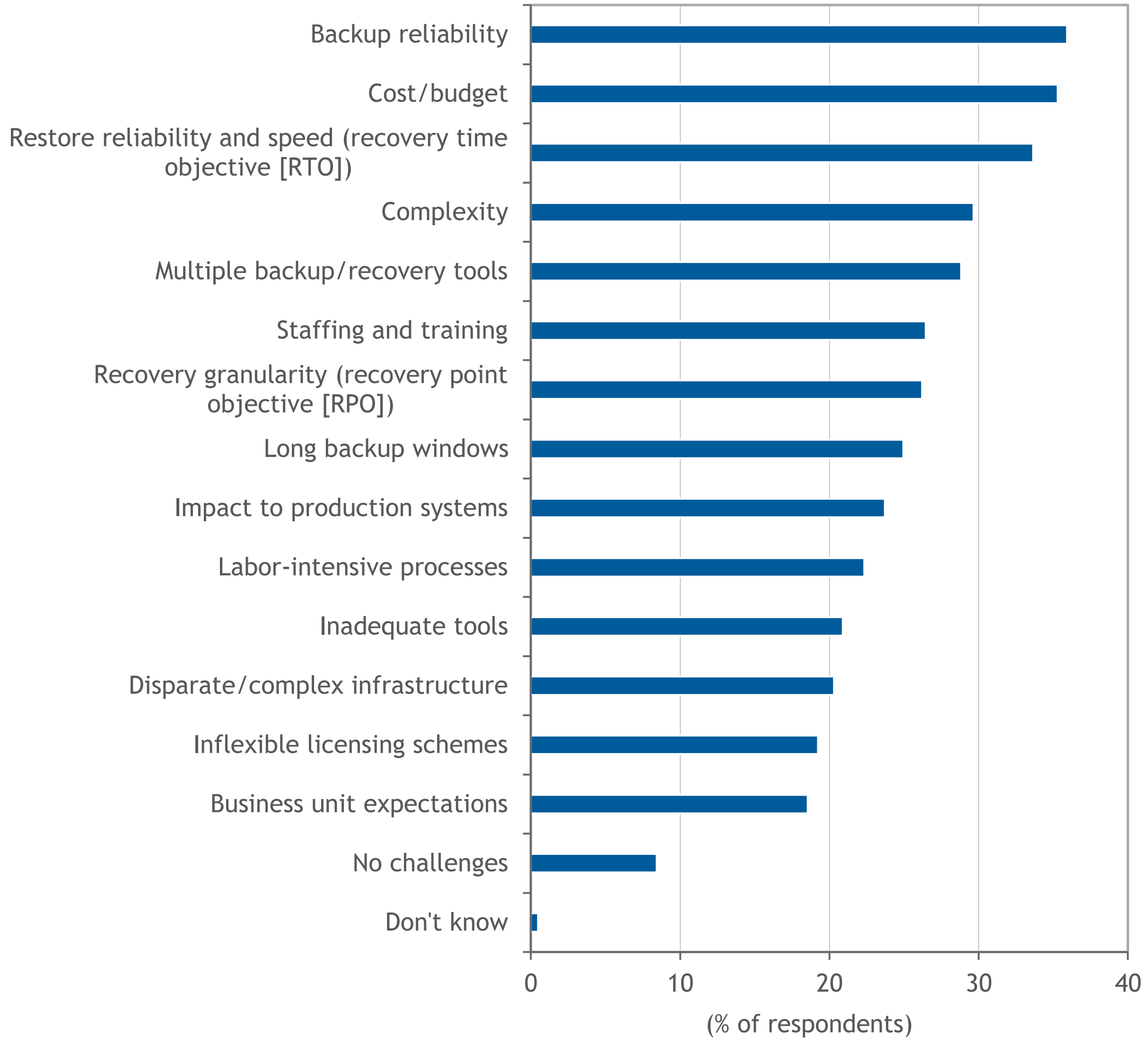
- 58% of respondents plan to invest more in cloud data protection solutions (including DR).
- 41.6% of respondents plan to invest more in in-house data protection solutions (including DR).
- 29.1% of respondents plan to invest more in cloud-based as-a-service data protection solutions (including DR).

Clearly, the preponderance of organizations has data protection and DR improvements as priorities and has some key areas to address. With respect to backup systems specifically, respondents identified backup reliability, cost/budget, and RTO as the top challenges to address. Full results are shown in Figure 3.

The top concern — backup reliability — certainly correlates to data highlighted previously regarding the causes of data loss and was expressed by 35.9% respondents. Having at least one-third of respondents or more indicating a problem with backup reliability as well as restore reliability (number 3) points to a very broad industry challenge. With cost/budget as the number 2 challenge, respondents clearly have concern over the expense of solutions, even as they expect to invest more as described previously. Reliable backup products are required, but organizations can also leverage the cloud (as they clearly plan to do) to help with infrastructure reliability and pay-as-you-go storage for better cost control.

FIGURE 3

Biggest Challenges Regarding Backup and Recovery



n = 506

Source: IDC's *Worldwide State of Data Protection and DR Survey,* January 2021

When we investigated DR challenges that respondents were experiencing, we found both similarities and differences when compared with backup challenges. As with backup, recovery time was the number 3 concern for DR. The top 2 DR-related challenges – IT staff knowledge/skills and IT personnel time/availability – indicate that people-related concerns are much greater for DR than backup. However, when considering the people, process, and technology relationships to DR, greater automation at the technology level can automate processes and reduce the impact to personnel time and knowledge.

Respondents indicated an average of 29.3 hours of unplanned downtime. This average is across all industries and organizational size; the amount of unplanned downtime will vary based on an organization's specific situation. With other IDC research showing that the cost of downtime ranges from thousands of dollars per hour to hundreds of thousands of dollars per hour (varying by industry and organizational size), reductions in downtime can have a significant impact on the ROI of new solutions or solution improvements. Thus organizations that implement steps or technology to improve RTO and thereby reduce downtime can achieve a very rapid payback.

FUTURE OUTLOOK

The research detailed in this study can be summarized by four key imperatives: a need for reliable backup; fast data recovery regardless of whether it is a normal recovery or a DR scenario; assured recovery from ransomware/malware; and simplified backup and DR operations to reduce staff time and effort. Organizations are clearly both willing and planning to make investments in these areas.

The fact is that common data protection technologies in use today are not able to reduce RPO and RTO to levels needed by data-driven organizations. Snapshots, the most granular recovery technology deployed by most organizations, may be executed no more often than hourly even for mission-critical applications and may be executed as little as every 4 or 8 hours. To be sure, some organizations will deploy snapshots every 15 minutes for their most sensitive applications. However, few will use snapshots at their highest frequency of every 5 minutes because of the necessary storage overhead and impact to applications such a schedule would entail. Moreover, snapshots rarely factor into DR execution. Standard practice DR relies on backup copies or replication to move data. Because of the cost of synchronous replication in both bandwidth and infrastructure, this practice is reserved for only the most sensitive applications. Consequently, most applications recovered through DR processes have a 24-hour RPO.

IDC has identified an emerging trend toward the convergence of backup and DR enabled by automated recovery workflows. As organizations leverage the cloud for data protection, adding workload migration and recovery orchestration can yield very low RTO and RPO. Using the cloud for these recoveries makes DR economical and rapid recovery of applications practical. We believe as CDP, workload migration, and recovery orchestration merge in a hybrid cloud environment, organizations will no longer need to treat backup and DR as separate efforts.

Container backup is another important requirement emerging for data protection. According to this survey, 47.6% of organizations have already deployed container-based workloads in production. We expect the majority of new applications to be cloud-native applications utilizing containers. Container backup differs in important ways from traditional backup. Traditional backup captures the data and the virtual machine image (if applicable) only. With containers, where Kubernetes is the dominant orchestrator, backup capabilities must include the data, the system image, and the Kubernetes state to perform a restore. Moreover, the backup application must be able to capture persistent data and images and ignore transient data and images.

This survey also found that most organizations lack confidence in their current backup and DR solutions. Only 15.3% of respondents expressed 100% confidence in their backup system's ability to recover data, and 20.4% have 100% confidence in their DR solution to recover data. Other results include:

- 45.8% of respondents were "somewhat confident," "not very confident," or "not confident at all" in their backup system; 45.6% gave the same responses with respect to confidence in their DR systems.

The general concern regarding respondents' backup and DR systems was further illustrated in their willingness to update or change solutions. From the survey, nearly half (48.7%) of the respondents plan to supplement or replace their backup and DR systems within the next three years. Certainly, IT organizations are challenged to protect ever-growing data volumes with more certainty and faster recovery. Among those organizations planning to change or supplement their backup or DR systems, the highest priorities were for speed of recovery (65%), cloud backup (62%), and simplicity/ease of use (45%).

CDP is a technology that is gaining traction in the industry. This technology, which is a part of backup solutions and not a standalone product, can significantly reduce the potential for data loss, regardless of cause, while reducing the time to recovery and simplifying recovery. CDP captures data changes as they are written so that the effective RPO is reduced to seconds and virtually eliminates the "backup gap" that was identified as the top cause for data loss.

Because of the granularity of CDP, it also helps recover from ransomware attacks with minimal data loss and rapid recovery. Administrators can select a restore point just prior to the attack, thereby eliminating the trial and error of picking backup sets or snapshot versions to restore. In addition, CDP solutions enable backup and DR with minimal data loss, especially when combined with recovery orchestration and workload migration.

As noted previously, IT transformation and cloud-based DR implementations are among the top 3 priorities for IT organizations. Most organizations will use these opportunities to modernize their data protection and DR infrastructure, which could include the opportunity to implement CDP. From the survey, 53.7% of respondents indicate that data protection modernization is "very important" or "critical" to their digital transformation (DX) and ITX projects. An additional 37.1% of respondents consider it "somewhat important." Only 8.6% of respondents indicated that data protection modernization was "not very important" or "not important at all."

Considering Zerto

The Zerto Platform is architected to provide backup, disaster recovery, data mobility, long-term retention, security, and compliance in a single integrated software-only scale-out solution. The platform is designed to protect virtual infrastructures, whether on-premises, cloud, hybrid, native, or multicloud.

The core of the Zerto Platform is a continuous data protection engine that can reduce RPO to seconds with:

- Thousands of restore and recovery points, seconds apart, to recover enterprise applications without using snapshot copies or relying on backup copies that may be up to 24 hours out of date.
- Application-consistent recovery for accelerated RTOs with quick and consistent recovery even with complex multi-VM applications.
- Instant journal-based recovery for a simple, granular recovery experience that doesn't impact production systems. This journaling technology can be used locally and remote on premises across other sites and the cloud, thus enabling the fulfilment of the data protection 3-2-1 rule.
- Long-term retention for cost-effective storage on premises and in the public cloud. Data may be retained from months to years to assist with meeting compliance and data retention regulations.

Combining backup, disaster recovery, and data mobility based on a foundation of CDP with near-synchronous replication, the Zerto solution is designed to provide a single software-only platform experience across all data recovery scenarios with the same mission-critical RPOs and RTOs for any workload. IT teams do not need to classify different workloads and treat them with different SLAs.

The Zerto Platform does not rely on snapshot technology, either array based or its own, so that RPO is not limited by snapshot intervals, thus minimizing the risk of data loss and performance impact. The platform also includes backup and disaster recovery orchestration to automate and simplify operations and reduce human error, with a single, simple recovery experience. Users can leverage the same Zerto implementation for backup and then extend it to disaster recovery, migrations, and other use cases. Full recovery with built-in orchestration and automation removes many manual processes to simplify complex disaster recovery, backup, cloud migration, and data protection modernization projects. With a single user interface, administrators have centralized management and a common experience, whether on premises or in the cloud. The platform has flexible REST APIs to fully automate deployment and VM protection using ready-made examples. Nondisruptive DR and backup testing can validate recoverability, perform a migration dry run, or test against production replicas, with no production impact or disruption in protection.

Also included in the platform is an analytics engine with:

- Built-in dashboards and reporting and access from desktop, tablet, or mobile device for monitoring SLAs from any device.
- Capabilities for forecasting future infrastructure needs with Zerto Resource Planner for accurate infrastructure planning using the organization's own actual application data; ability to forecast required capacity and size protection needs for both protected and unprotected VMs.
- Backup and DR reporting across all resources to ensure having timely, accurate data, whether for compliance and auditing or performance analysis.

CHALLENGES/OPPORTUNITIES

The data protection market is highly dynamic and becoming more challenging due to the increasing application deployment schemes for core, cloud, and edge. Data is becoming more siloed, making the protection and recovery of it more challenging. Because of the number of types of applications, deployment platforms, data, geographies, and more, it simply is not possible for any single product or platform to address all possible scenarios. Most IT organizations will be faced with the need to adopt multiple products, even when consolidation is desirable.

As a solution developer, Zerto is also faced with the task of choosing which scenarios it will address in its products. The company must focus on its core value proposition to stay ahead of its competition in these core areas. Zerto competes in a marketplace where IDC recognizes more than 44 vendor participants, many of which are multibillion-dollar firms with much larger R&D budgets. Zerto must ensure that it gets maximum "bang for the buck" when it invests in product development.

Containers will also emerge as a key growth market for data protection and DR products. Zerto, which recently introduced support for containers with Zerto for Kubernetes, must move quickly and aggressively to meet the emerging needs as many competitors are now scrambling to address containers in what will become a highly competitive segment.

Growth and market share gains for data protection software vendors are heavily dependent upon those vendors both participating in cloud ecosystems (e.g., AWS, Azure, GCP, and IBM) and developing their own ecosystem of cloud service providers and managed service providers. Zerto has been one of the more successful companies in this regard, adapting to the changing landscape, which requires constant attention and product development.

CONCLUSION

Modernizing data protection, including backup and DR, is a high priority for many IT organizations. Nearly every organization faces increased competition and challenges and must respond with data-driven decisions, digital business models, and operational efficiency. This means not only driving new business but also ensuring a better experience, without downtime and data loss for customers, partners, and employees. To that extent, it is an arms race among organizations constantly seeking an edge through greater data availability, usability, and reliability.

The complexity of application deployments, data types, governance requirements, and data dispersed across the core, cloud, and edge makes data management and availability a serious challenge for IT organizations to provide. The industry is responding to these needs with multicloud data management solutions that provide integrated backup, DR, recovery orchestration, policy management, and SLA tracking. CDP is among the latest introductions in delivering the capabilities needed to drive shorter recoveries with much less data loss. While CDP can help in common types of data recoveries across backup and disaster recovery, it can also play an instrumental role in combating cyberattacks such as ransomware. By using CDP to return to a point just seconds or minutes prior to an attack, recoveries can be made quickly and with minimal data loss. We expect CDP to play a key role as organizations drive closer and closer to SLAs requiring zero downtime with zero data loss.

MESSAGE FROM THE SPONSOR

Zerto helps customers accelerate IT transformation through a single, scalable platform for cloud data management and protection. Built for enterprise scale, Zerto's software-only platform uses continuous data protection to converge disaster recovery, backup, and data mobility and eliminate the risks and complexity of modernization and cloud adoption. Zerto enables an always-on customer experience by simplifying the protection, recovery, and mobility of applications and data across private, public, and hybrid clouds.

For more information on how continuous data protection sets a new standard to minimize data loss and ensure rapid recovery, read Continuous Data Protection: A New Era of Backup and Recovery.

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. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

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