Introduction

Digital transformation (DX) is well underway throughout the industry. IDC estimates that 55% of organizations will have executed on some element of their DX strategy by 2020. This movement means that DX efforts are in earnest for the near term with the purpose of delivering competitive advantage through faster, more insightful use of data in business decision making. Clearly, data availability is foundational to DX and resilience is a cornerstone of data availability.

Many IT organizations are dealing with the legacy of complex interrelationships of backup/recovery software, snapshots, local and remote replication, and more to ensure data survival. This mix has evolved over the years in response to different data threats and business requirements because no single product can meet all requirements. However, the result is a complex, labor-intensive environment that is a challenge to manage.

Business resilience has emerged from this traditional disparate collection of point products to offer a cohesive set of capabilities for data availability delivering the desired service-level requirements. It represents a new class of products, called resiliency platforms, to help IT organizations simplify and improve data availability whether on-premise, in the cloud, or in a disaster recovery (DR) scenario. These platforms automate data protection processes, making them simpler and more reliable.

As this concept gains currency with the business, IDC suggests that IT managers take the following actions:

» Rethink data protection processes, moving from reactive data restore to proactive data and application availability based on concepts of business resilience

» Simplify and automate data protection processes wherever possible

» Consider business resiliency platforms to unify data availability operations
**Definitions**

» **Business resilience** is a holistic approach to business operational readiness that includes IT capabilities supporting business units in avoiding or rectifying business disruptions to minimize the impact on customers and stakeholders.

» **Recovery point objective (RPO)** is the maximum allowable data loss as measured by the time between data protection events and the most recent point at which data is at a known consistent state.

» **Recovery time objective (RTO)** is the maximum acceptable amount of time to recover an application to a business-ready state.

**Benefits**

The IT application landscape is constantly changing and becoming only more complex. Organizations must contend with a mix of operating platforms including Windows, Linux, and proprietary and legacy operating systems as well as distributed operations including on-premise, cloud native, hybrid, software as a service (SaaS), Internet of Things (IoT), and endpoints. There are also many data types such as NoSQL, containers, and objects in addition to traditional database and file systems. The possible permutations and support matrices are daunting, and no single data protection product addresses them all.

IDC research, however, shows that 80% of x86 workloads are virtualized. Further, 90% of IT organizations expect to use some element of public cloud as part of the data protection strategy within 12 months. In most cases, this will involve a hybrid cloud architecture where the solution includes on-premise and cloud data repositories and/or compute infrastructure. Thus, virtualized workloads in a hybrid cloud environment represent the "sweet spot" for resiliency operations and platform automation. Legacy platforms often have established products and processes for application resiliency. Whether products for these platforms are ideal or not, few new entrants are challenging incumbent vendors. In contrast, the virtual infrastructure and cloud environments are highly dynamic with new capabilities routinely introduced to the market, offering IT organizations a rich environment.

Business resiliency platforms can offer multiple benefits such as:

» **Consolidating data protection operation for virtualized environments:** Although consolidation across the infrastructure is not possible, key data protection product groupings with virtual infrastructure are both possible and highly impactful. This consolidation can eliminate the need for IT teams to stitch together various point products to achieve complete protection. It also facilitates an automation of processes that may not be possible across disparate products from unrelated vendors. Consolidation reduces the potential for human error, offers better data governance, and frees up staff time to address other projects.

» **Orchestrating disaster recovery:** Effective disaster recovery is a classic combination of people, process, and technology. Traditional DR efforts involve runbooks, which guide people through the process of recovering infrastructure and applications. These runbooks are prone to rapid obsolescence unless IT organizations diligently and frequently update them. Recovery orchestration tools automate these processes and can reduce or eliminate the need for runbooks, at least with respect to the recovery of systems. To the extent that these tools automate processes, they also reduce human effort, which is an important consideration in recovering from a disaster when staff availability may be limited.

» **Facilitating recovery across diverse infrastructure:** Cloud computing is essentially an anywhere-to-anywhere deployment scheme. Whereas applications may migrate on-premise to cloud, cloud to cloud, or cloud to on-premise, recovery orchestrators help reduce the complexity and tasks associated with recoveries in disparate environments.
Trends
Disaster recovery is one of the hottest segments of the data protection marketplace. Although IT managers know they should have a DR plan, many organizations chose to forgo the costly duplicate infrastructure and accept the risk of a disaster even if the results could be catastrophic to the organization. Fortunately, cloud economics have fundamentally changed this equation, and organizations find that effective DR contingencies need not blow up the IT budget. IDC estimates that more than 2,000 cloud service providers offer some type of DR-as-a-service plan. Offerings from these cloud service providers range from do-it-yourself on-demand infrastructure to "white glove" services that include threat analysis, architectural planning, failover planning, and testing. These providers may be regional, national, or global and give IT a wide breadth of options.

IDC is also witnessing an ongoing shift from a system-centric perspective (i.e., servers, arrays, and virtual machines [VMs]) to an application-centric focus. IDC forecasts that as many applications will be deployed in the next five years as have been deployed in the previous 40 years. Many will be cloud-native applications that are owned and managed by a vendor with their own data protection requirements yet are an essential part of the organizational application ecosystem. Given the volume of applications and the diverse platform deployments, IT organizations should start now in laying the foundation for application resiliency.

Considering Veritas
The Veritas Resiliency Platform (VRP) is a single solution designed to recover applications, VMs, and data across the range of application deployment models including virtual, physical, and cloud. It is designed especially for the virtual and cloud environments but also addresses physical x86 workloads.

The platform addresses three primary use cases:

» Virtual machine recovery: VRP functions as a gateway appliance utilizing the VMware VAIO API to intercept data and replicate it to a DR site. This capability yields several benefits: Data is immediately protected offsite, along with any changes to the virtual infrastructure, which facilitates rapid failover and failback of virtualized workloads.

» Application recovery: Using VRP, administrators can establish resiliency groups based either on the logical affiliation of those applications or on applications with similar service-level specifications. Establishing a resiliency group is as simple as dragging and dropping applications into the group. With a resiliency group, administrators can set recovery policies and priorities. Initiating the recovery of one of these groups requires simply clicking on the group name. The recovery will be accomplished based on the defined workflow and the location and infrastructure specified.

» Multicloud recovery: VRP not only facilitates recovery of on-premise applications to or from the cloud now but also will facilitate public cloud to public cloud in the near future. In this case, workloads may be moved to AWS using EBS volumes. Or, using a data gateway, workloads may be moved to any S3-compatible repository with no format conversion. The platform includes site-to-site communication to ensure data consistency.
Challenges
The concept of business resilience is rapidly gaining currency in business, and demand for this more holistic approach is rising. As a result, the market for business resilience solutions is quickly drawing new entrants and seeing competition increase. However, because business resilience is a hot area, there are also misperceptions about what it is and what it should do. As a relatively early entrant in this market, Veritas has both the challenge and the opportunity to educate IT leaders regarding business resilience and what it can do, the components of business resilience, and how Veritas fits into the market. Because business resilience is so broad, IDC expects a wide array of functionality among products. Thus, product differentiation and staying in front of, or at least abreast of, the technology evolution will be challenges for any vendor, including Veritas.

In addition, the rapid evolution of application deployment models, containers, and data types will multiply the possible market segments to address. Veritas need not cover all of them, but the company must closely follow the requirements of its customer constituency and avoid spreading itself too thin.

Conclusion
Business resilience is a critical success factor for digital transformation and the competitiveness of organizations. Organizations that are able to maximize application availability will have a comparative competitive advantage over competitors that do not. As application and IT environments become even more complex, existing manual efforts around application and data recovery will simply be insufficient.

Business resilience is about much more than disaster recovery, which is one of its key components. It is a holistic effort and partnership between business units and IT to ensure that customer systems are always available and that the organization has the information needed to make the best possible decision. IT organizations should begin now in establishing the foundational technologies across critical platform stacks to deliver on the promise of business resilience.
MESSAGE FROM THE SPONSOR

Resiliency Platform is designed for large enterprise, public sector companies and service providers to recover data centers, applications, and virtual machines across different hypervisors, operating systems, storage, and cloud platforms without intervention from IT teams. Companies will achieve business benefits from the following:

» Built-in orchestration designed to automate resilience, migration, and takeover plans
» Automated rehearsals that test links and processes at every functional level without disrupting production uptime
» Optimized, bi-directional data movement between sites with built-in compression and deduplication
» Encrypted connectivity between sites
» Single-click sequential shut down, migration, and start-up of business services that get applications back on line sooner

Learn more with technical briefs, video tutorials, and download a trial at: www.veritas.com/resiliency

About the analyst:

Phil Goodwin, Research Director, Infrastructure Systems, Platforms, and Technologies Group

Phil Goodwin is a Research Director within IDC’s Enterprise Infrastructure Practice, covering research on data management. Mr. Goodwin provides detailed insight and analysis on evolving industry trends, vendor performance, and the impact of new technology adoption. He is responsible for producing and delivering timely, in-depth market research with a specific focus on cloud-based and on-premises Data Protection, Business Continuity and Disaster Recovery, and Data Availability.

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2019 IDC. Reproduction without written permission is completely forbidden.