SOLUTION SHOWCASE

Veritas Resiliency Platform: A Holistic Approach to Protecting Business Services for 2017

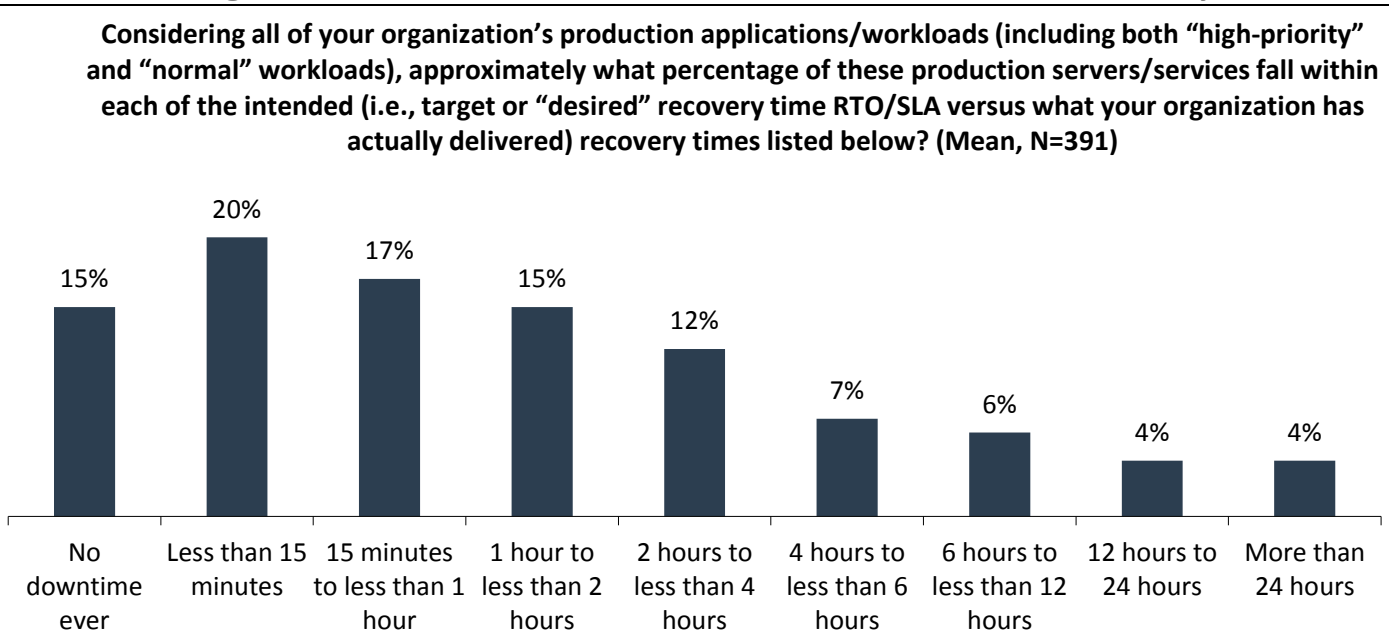
Date: August 2017 **Authors:** Jason Buffington, Principal Analyst; and Monya Keane, Senior Research Analyst

Abstract: We are more dependent on data and IT services than ever before. With that fact in mind, it is safe to say that backup alone, while extremely important, isn't enough. Organizations must proactively deploy a resiliency and availability technology that will work in complement with the restoration and preservation capabilities of their other data protection solutions—and simultaneously cater to current and future technologies in and out of the data center.

Overview

At their core, all IT teams have the same mission: to deliver data and data-related services to end-users who depend on them. Regardless of the size of the entity being supported or the heterogeneity of its hardware platforms and software frameworks, *availability is imperative*. In fact, people have never been more in need of data and IT service availability than they are today, as evidenced by the fact that the average organization reports that more than half of their production platforms have a recovery time of less than an hour (see Figure 1).[1]

FIGURE 1. Percentage of Production Servers/Services that Fall Within Each Intended Recovery Time



Source: Enterprise Strategy Group, 2017

[1] Source: ESG Research Report, *The Evolving Business Continuity and Disaster Recovery Landscape*, February 2016.

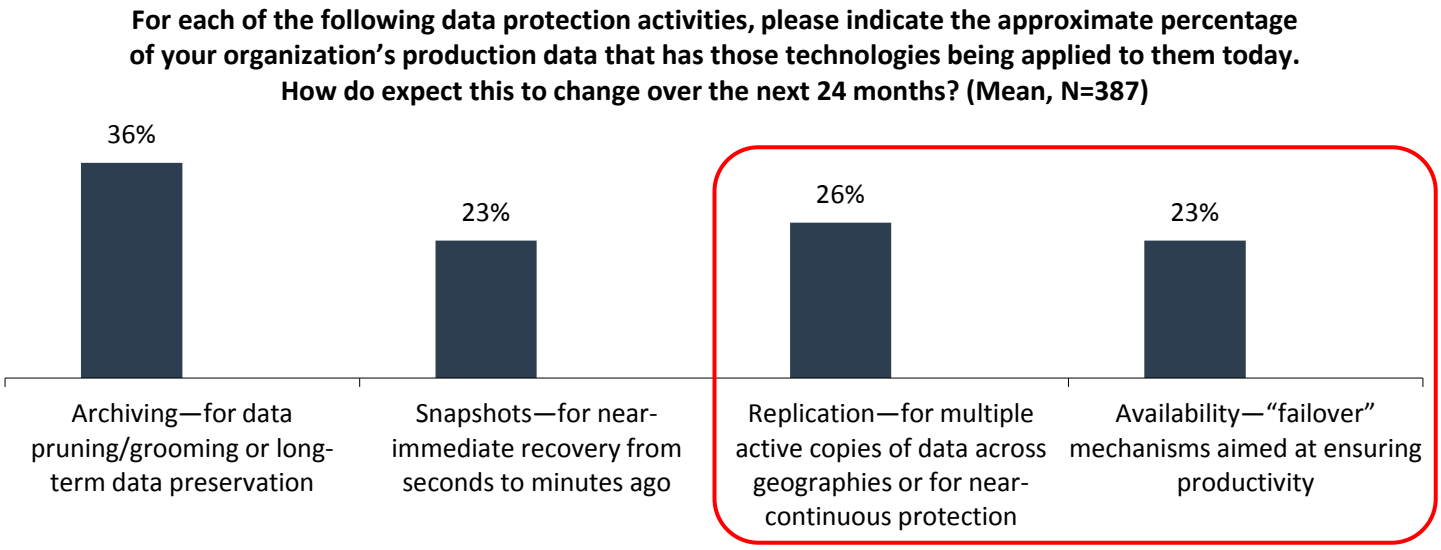
It used to be that most organizations had only a few "critical" servers. Now, downtime for any IT resource is unpalatable—with more than half of servers having a targeted RTO/SLA of less than an hour (see Figure 1). In fact, 35% of servers have SLAs of 15 minutes or less, which is unattainable via backup alone.[2]

That's why organizations need to combine their traditional data protection mechanisms with modern data availability technologies such as the Veritas Resiliency Platform.

The Accidental Architecture of Availability Today

Many organizations that ESG surveys say they deploy multiple disparate data protection and availability technologies across workloads (e.g., for each database platform, hypervisor, etc.) as different resiliency mechanisms may be chosen by platform owners or administrators across environments or geographies. As Figure 2 shows, on average, 26% of production data has replication technologies being applied today, while 23% of production data has some level of a failover mechanism for ensured availability and continued productivity. [3]

FIGURE 2. Percent of Production Data with Data Protection Technologies Being Applied



Source: Enterprise Strategy Group, 2017

So, numerous mechanisms are already in use. And it seems likely that the use of "better than backup" methods for ensuring rapid recovery or availability will continue to increase as organizations rely more on their IT systems. Notably, although Figure 2 reflects the treatment of all kinds of data, it is especially common to see mission-critical applications such as databases and virtualization hosts having a high percentage of supplemental availability technologies applied to them.

Be advised, however, that even though separate solutions and approaches can make great sense, they also might:

- Cause inefficiencies and drive up costs—Each method makes sense from a per-platform/per-dataset perspective. But multiple availability mechanisms can cause inefficiencies. Those inefficiencies then increase infrastructure CapEx, management OpEx, and the overall complexity of the environment.
- Create challenges in monitoring and ensuring coverage—Many stakeholders are invested in IT resiliency. It can be difficult to satisfy everyone and monitor every platform when several point technologies are achieving IT resiliency in

[2] Often, in the case of recovery strategies that rely solely on backup, an IT group will need more than two hours to (a) discover an availability problem has occurred, (b) diagnose the issue, (c) restore the data, and (d) resume service.

[3] Source: ESG Research Report, *Data Protection Modernization in 2017*, to be published.

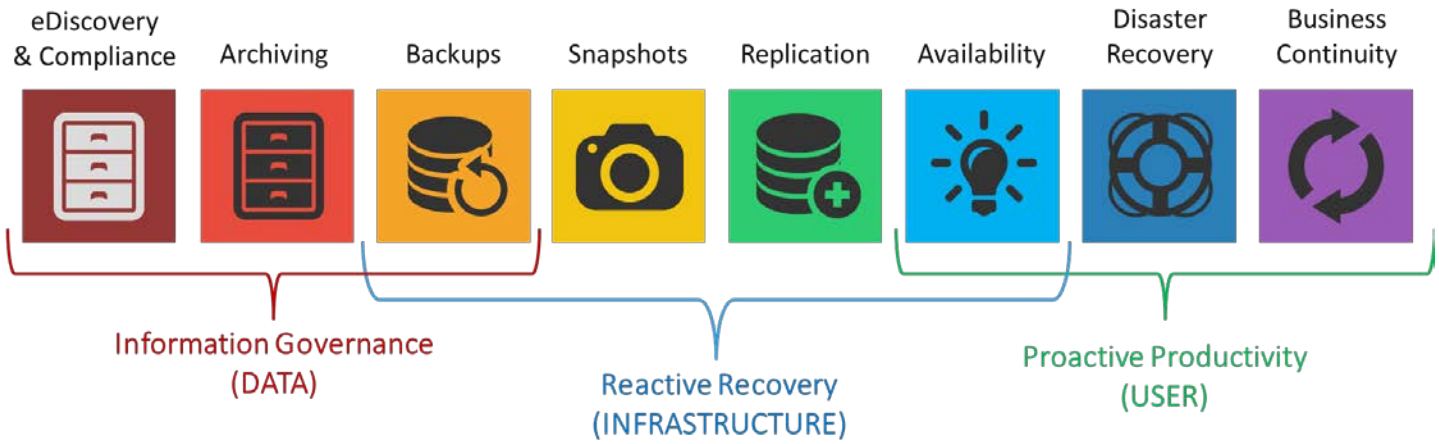
their own separate ways. This situation is particularly problematic in virtualized environments—ESG research shows that five of the top six challenges in protecting a virtual server environment are visibility related.[4] Data recoverability may be the biggest unique challenge for a highly virtualized environment, but achieving virtualization "savviness" associated with the visibility and manageability of the broader ecosystem is challenging as well.

ESG's Recommendations for Heterogeneous Data Protection and Availability

Recommendation 1: Plan for a Hybrid Architecture

Different IT organizations have varying degrees of heterogeneity in their production platforms (both the physical servers and the VMs running under different hypervisors). So, it's a smart idea to use a full spectrum of data protection and availability approaches (see Figure 3).

FIGURE 3. The Spectrum of Data Protection



Source: Enterprise Strategy Group, 2017

Data protection and availability methods vary based not only on platform, but also on the workload's nature and its business value to different locations and users. This is another reason organizations should strive for a broad data protection/recovery strategy that encompasses as many spectrum activities as possible in a unified way—for example, managing backup, snapshots, and replication through a single framework.

Data protection does not have to happen exclusively through on-prem management, either. IT professionals supporting midsized organizations or remote locations within large enterprises will likely find hybrid architectures, which include on-prem servers plus publicly hosted VMs, as appealing for resiliency purposes. That approach entails leveraging third-party cloud services to augment the internal IT infrastructure.

Recommendation 2: Embrace a Single IT Resiliency Strategy (Even if Using Multiple Methods)

At many organizations, the use of multiple methods across multiple platforms and locations is inevitable. That's because IT must partner with a variety of platform administrators and business unit owners, yet still achieve the overall availability level(s) the entire organization demands.

However, that requirement shouldn't equate to following disparate strategies or maintaining different mindsets regarding how resiliency, protection, and availability are to be achieved.

[4] Source: ESG Research Report, *Trends in Protecting Virtualized Environments*, August 2015.

Instead, the IT organization should seek to establish a comprehensive strategy for achieving resiliency, regardless of the myriad tactical methods it may actually deploy to deliver it. As IT tries to achieve the protection behaviors depicted in Figure 3, it should leverage unifying mechanisms where possible—but use separate mechanisms when warranted.

Recommendation 3: Over-communicate Through Monitoring and Collaboration

As mentioned, data-resiliency stakeholders and beneficiaries include platform owners, business unit leaders and their teams, senior executives, and of course, every IT staff member whose job involves delivering durable IT.

Considering how many technical and non-technical people are affected by resiliency goals and the availability-delivery strategy, communication (even over-communication) is crucial—communicate with everyone about the strategy, its implementation, and the success levels of the various IT tools/toolsets being used.

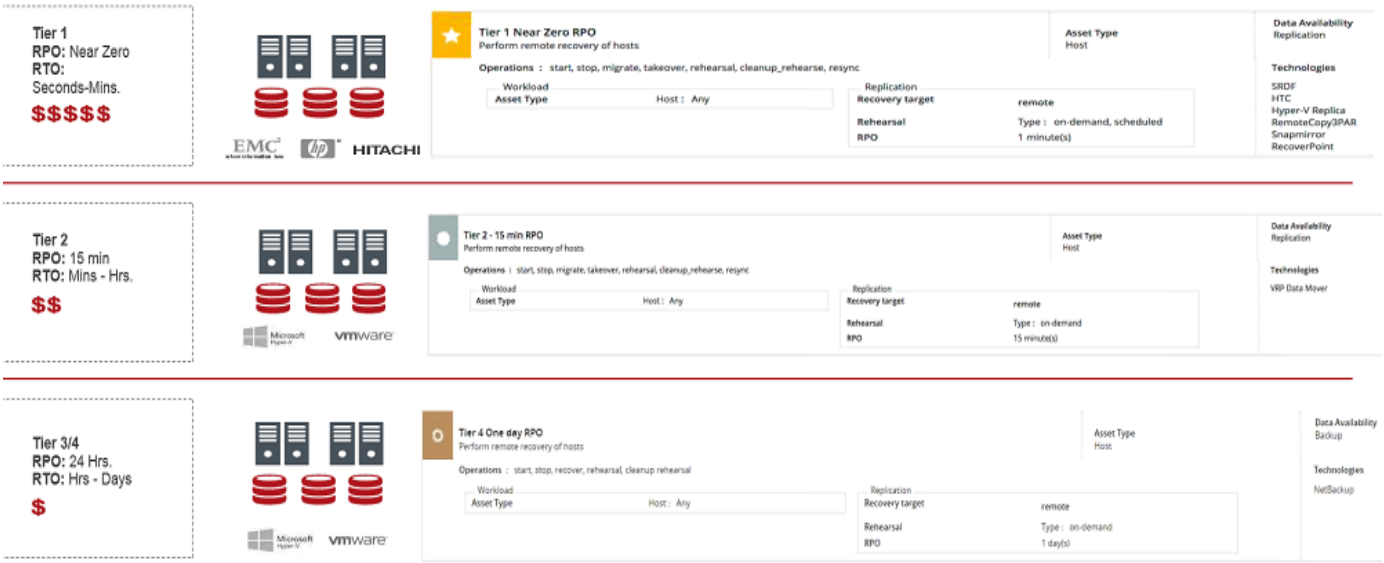
Without effective dashboard-based monitoring and frequent communication and notification, the confidence of the virtualization administrators, IT operations teams, data protection specialists, and all the stakeholders and end-users can deteriorate.

One Solution to Consider: Veritas Resiliency Platform

The availability pedigree of the Veritas Resiliency Platform (see Figure 4) is formidable. For more than two decades, Veritas (as a standalone company or as the data protection arm of Symantec) has been producing availability technologies that overlay existing IT infrastructures and are well designed to enhance data availability and increase IT agility.

Veritas calls Resiliency Platform a one-stop-shop for supporting the resiliency needs of a business, as it provides integrated resiliency across all required service level objectives.

FIGURE 4. A Better Approach: Integrating Resiliency Across All Service Level Objectives



Source: Veritas, 2017

A Unified Approach to Ensuring the Availability of IT Services Across Many Physical and Virtual Servers

Imbued into the Resiliency Platform architecture is Veritas's knowledge that its technologies and expertise are being overlaid across existing heterogeneous infrastructures. Veritas designed Resiliency Platform to work not only with the existing resiliency mechanisms found on physical servers, but also with the two most common hypervisor technologies shipping today—VMware and Microsoft Hyper-V. Resiliency Platform also works with important line-of-business applications that often contain their own resiliency technologies (e.g., SQL Server database mirroring).

A Unified Architecture for Availability Across Data Centers and Clouds

IT organizations are embracing the cloud for protection and availability, including data backup and BC/DR. The Resiliency Platform architecture is able to support multi-site self-managed IT and leverage multiple cloud-based solutions as migration or failover targets.

What's New in 2017: Integrated Data Protection, Proactive Resiliency, and Public Cloud Support

Integrated Data Protection and Proactive Resiliency

One of the most exciting recent enhancements to the Veritas portfolio is the integration of Resiliency Platform with the flagship Veritas NetBackup backup and recovery solutions (see Figure 5).

This integration aligns directly with ESG's recommendation that organizations seek out unified, well-integrated data protection portfolios that allow multiple stakeholders to use the same pane(s) of glass to manage tactical backup/restore and strategic replication/availability and BC/DR initiatives. This capability is important for complex, tiered business workloads that rely on different technologies for different tiers.

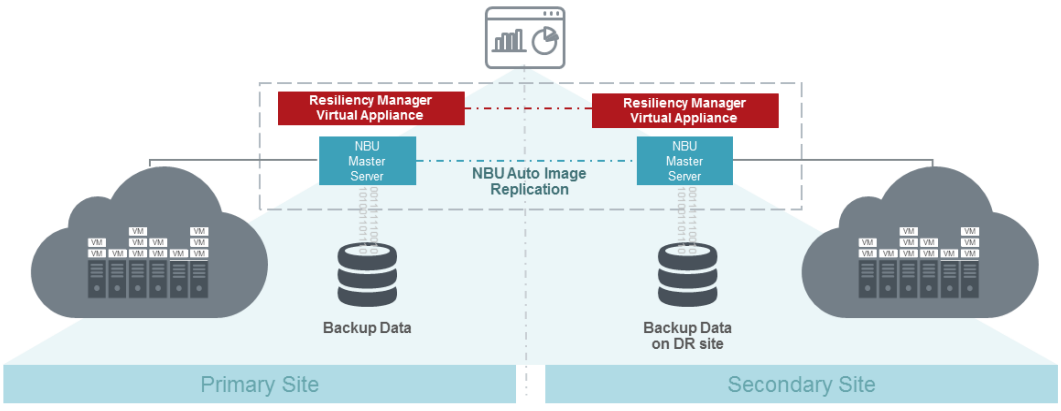
For example, a tiered application could be relying on replicated data for a database tier, but restoring a middleware tier from backup data. The integration of Resiliency Platform and NetBackup ensures seamless recovery of complex tiered applications with varied service level components.

Also this year, Resiliency Platform customers can perform single-click bulk restores/recoveries of virtual machines. When operations are automated, recovering 500 VMs can happen really fast—and more reliably.

Predictable, Integrated Resiliency

This year, the Veritas Resiliency Platform features a new value proposition—direct integration with Veritas NetBackup software and NetBackup appliances. It is an appealing enhancement for supporting applications that have short RTOs/RPOs. With it, one can orchestrate recoveries of complex applications where those applications rely on either replication or NetBackup as a data transport layer.

FIGURE 5. Veritas Resiliency Platform Solution Architecture, Better Together with NetBackup



Source: Veritas, 2017

In regard to unified instrumentation for monitoring and availability, it is notable that Resiliency Platform not only delivers higher IT resiliency via automated recovery processes, but also monitors and communicates the status of individual platforms and associated SLAs as they are being achieved.

Integrations with Amazon Web Services and Microsoft Azure Public Clouds

Another Resiliency Platform innovation centers on enabling organizations to incorporate Amazon Web Services and Microsoft Azure into their IT architectures and gain the benefits of the multi-cloud. Businesses can either adopt these clouds as a permanent migration target for their business applications or as a disaster recovery target in place of a secondary data center.

A major strength is that Resiliency Platform will enable organizations to migrate or recover applications to AWS and Azure quickly because of the direct integration into AWS Elastic Block Storage and Azure Managed Disk. According to Veritas, because Resiliency Platform replicates directly to EBS volumes and Managed Disk volumes that can be directly attached to compute instances, Resiliency Platform ensures lower RTOs for migration and recovery, and makes recovery seamless for applications with higher IOPS.

Figure 6 illustrates the vision for the Veritas Resiliency Platform Solution Architecture.

FIGURE 6. Veritas Intends to Solve Uptime Concerns with Unified Resiliency Management Across Hybrid Clouds

Source: Veritas, 2017

The Bigger Truth

Businesses are demanding more from their IT teams than ever before in terms of availability. To achieve that availability, however, the IT teams often had to cobble together myriad data protection approaches—because different approaches made sense for different workloads. Unfortunately, myriad availability approaches eventually result in resiliency-related inefficiencies and a general level of complexity that is unacceptable.

The good news today is that organizations can formulate availability strategies that leverage hybrid protection and are suited to physical and virtual solutions alike—yet still take application- or workload-specific requirements into

consideration. A hybrid resiliency architecture in 2017 can encompass secondary sites and take advantage of cloud services to achieve the high level of data availability that businesses require today.

But with so much depending on the durability of such an infrastructure, whom should the IT organization partner with to achieve it? Veritas is one company that has been an availability innovator for more than 20 years. And with its newly enhanced Resiliency Platform offering, the vendor has again raised the bar for heterogeneous, hardware-agnostic data availability solutions matched to the modern enterprise, promising to ensure resiliency across both legacy onsite and new cloud architectures with a single solution.