CHAPTER 1

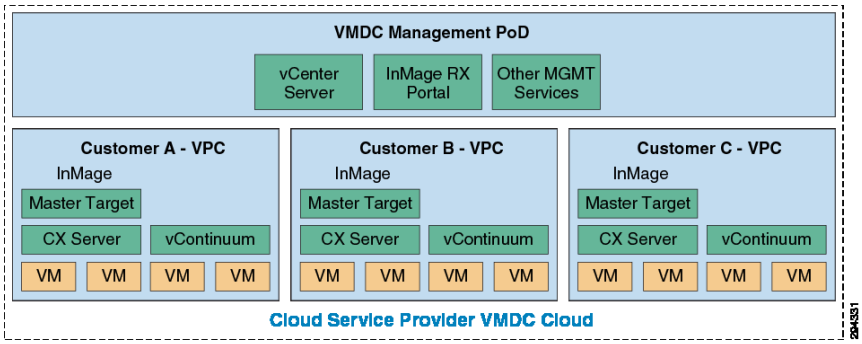
Overview

Cisco Disaster Recovery as a Service Solution (DRaaS) architecture described in this document is designed to provide a new set of related capabilities allowing Virtualized Multi-Tenant Data Center (VMDC)-based service providers (SP) to enhance their addressable market, financial performance, and differentiation vs. commodity cloud solutions. Many of Cisco VMDC-based SPs seek better monetization of their existing VMDC investments through layered services that are synergistic with the advanced networking capabilities delivered by VMDC. These SPs demand new, easily deployable services both to keep pace with the innovation of commodity/public cloud providers such as Amazon Web Services (AWS) and to address portions of the market that are not well served by commodity cloud solutions.

The key end user consumable services being enabled by this system architecture is to enable a SP to offer disaster recovery for both physical and virtual servers from a customer data center to a SP virtual private cloud (VPC). The DRaaS System primarily targets SMBs and enterprises. The global DRaaS and cloud-based business continuity is expected to grow from $640.84 million in 2013 to $5.77 billion by 2018, at a CAGR of 55.20%.

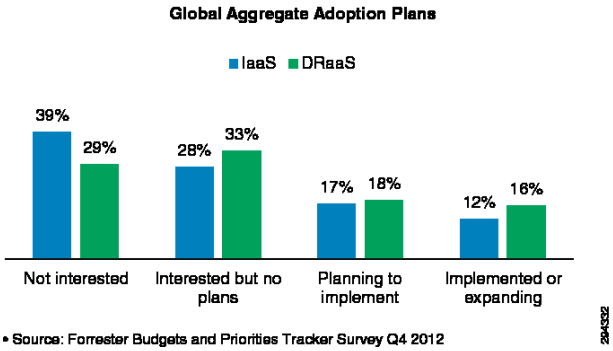
The traditional disaster recovery (DR) system constitutes a substantial portion of expenses annually. With the "pay as you go" model of the cloud-based DR system, the impact of downtime can be minimized through replication. DR can start up applications once the disaster is identified. In addition to recovery, cloud-based DR incorporates business continuity. Implementation of DRaaS with a virtualized cloud platform can be automated easily and is less expensive, since DR cost varies before and after a disaster occurs. The key requirements for DRaaS are Recovery Point Objective (RPO), Recovery Time Objective (RTO), performance, consistency, and geographic separation (Figure 1-1).

Figure 1-1 What is Disaster Recovery as a Service?



The market presents a strong opportunity for the SPs to take advantage of the demand for DRaaS services as illustrated by Figure 1-2.

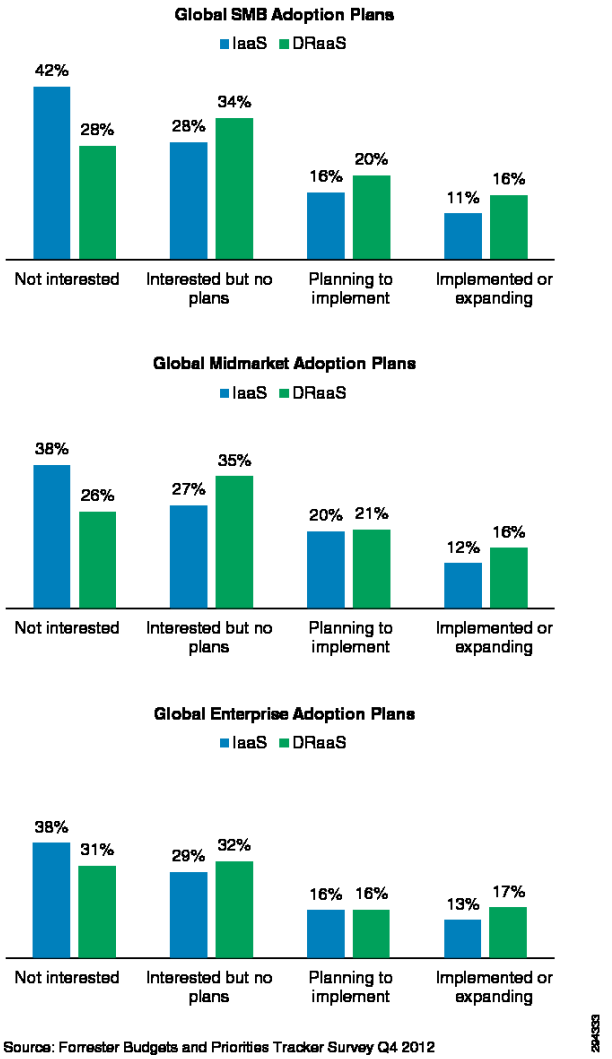
Figure 1-2 Strong Market Demand for DRaaS



• Source: Forrester Budgets and Priorities Tracker Survey Q4 2012

Further investigation of the global demand patterns for DRaaS indicates that the market opportunity and interest is equally spread across the enterprise, mid-market, and SMB segments as summarized in Figure 1-3.

Figure 1-3 Global DRaaS Demand by Segment



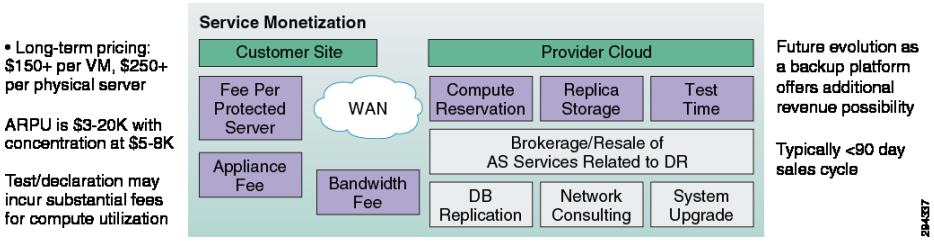
• Source: Forrester Budgets and Priorities Tracker Survey Q4 2012

This chapter includes the following major topics:

DRaaS: Business Drivers

Increased regulatory pressure drives the need for disaster recovery (DR) and business continuity plans and presents a hierarchy of requirements for the implementation of these solutions (geographic restrictions, regulatory compliance, etc.). Enterprises are constantly faced with budget constraints that prevent infrastructure duplication. Building DR infrastructure is a contextual business activity that requires a degree of specialization with IT skillsets or resources that are significantly harder to build without sufficient scale. Under these circumstances a growing desire exists to consume DR as a service, allowing incremental deployment and growth as budget becomes available.

Figure 1-4 Cisco's DRaaS Blueprint Solution



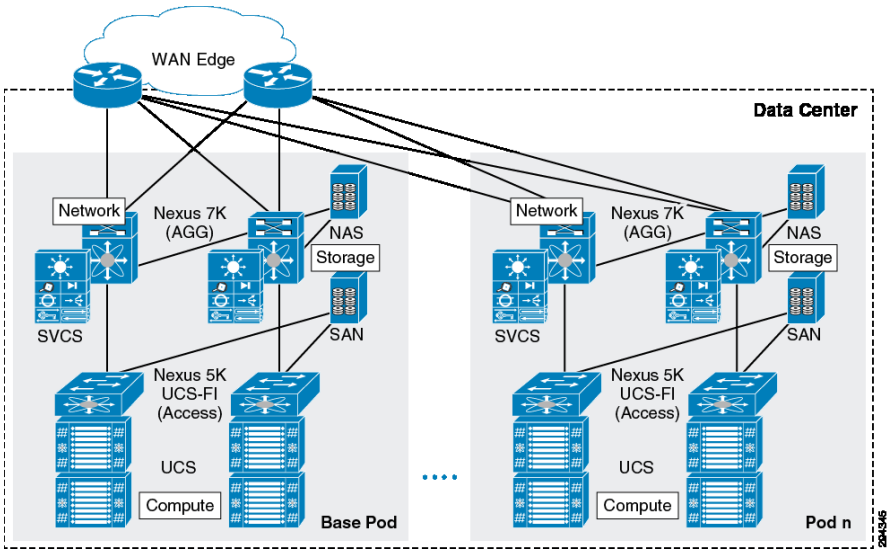
DRaaS: Technical Challenges

The selection of a specific technology and implementation for the DRaaS is a highly complex decision with technology challenges that need to be adequately explored and analyzed prior to choosing an appropriate technology. The following questions arise in the choice of the DRaaS implementation:

- How do we replicate data, databases, and virtual machines?
- What technology of replication do we use?
- What are our RTO/RPO requirements for the various applications requiring Disaster Recovery?
- How should we monitor what is being done during the testing and recovery events?
- How should we perform failover when needed either by a test or a disaster event?
- How should we virtual machines and databases be rebuilt?
- How can we ensure the consistency of databases and applications?
- How can we redirect traffic, reconfigure the Domain Name Services, etc.?
- How should we perform failback after a recovery event?
- How should our organization staff for Disaster Recovery and testing?

- How can our organization afford Disaster Recovery (which a cost and not a revenue generating activity)?

Figure 1-5 DRaaS Technical Challenges

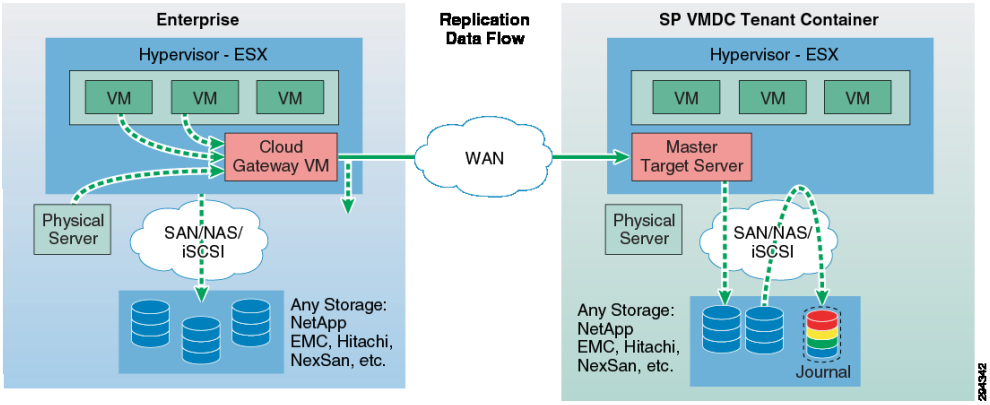


Challenges with Traditional Storage-based Replication

The use of traditional storage-based replication requires an identical storage unit on the DR site from the same vendor. The storage array-based replication software is not application aware and

needs additional intervention at the host level to achieve application consistency. Multiple points of management are required while performing DR and this introduces complexity in protecting and recovering workloads. The traditional storage-based replication approaches lack granularity and can replicate all virtual machines (VM) or none that are residing on a logical unit number (LUN). Replication of data happens between LUN pairs that need to be identical and this restricts the ability to failover a single VM residing on the LUN.

Figure 1-6 Any-to-Any Replication



Traditional storage replication approaches need additional functionality to take snapshots or clones of the target LUN to perform disaster recovery drills without interrupting data replication. Otherwise, replication has to be stopped for DR drills. Storage array-based replication does not support continuous data protection natively and data cannot be protected from logical failures.

VMware Site Recovery Manager (SRM) is an orchestration and runbook automation tool that streamlines the workflows for failovers and recovery of workloads. SRM leverages storage-based replication or vSphere replication to provide DR. Table 1-1 shows a comparison of the VMware approach to DR with the Cisco DRaaS approach.

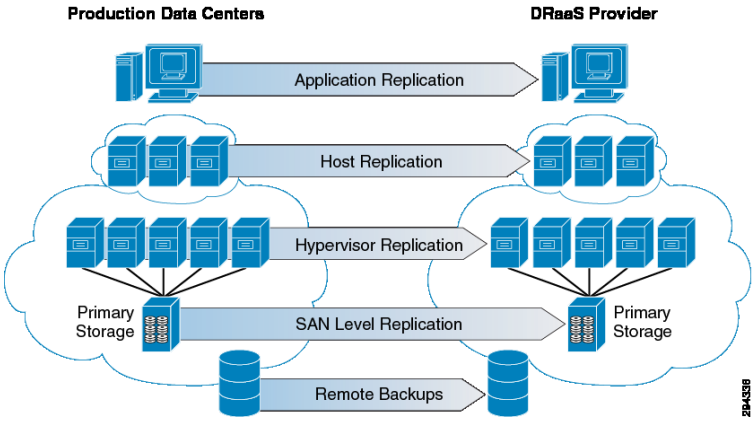
Table 1-1 VMware Disaster Recovery Solution Comparison

SRM with Storage Replication	SRM with vSphere Replication	Cisco Solution
• Supports only vSphereto-vSphere replication. • Needs to have similar storage arrays on customer and DR sites. • Involves a complex configuration to provide point-in-time copies for recovery. • Issues with incompatibility, as SRM coordinates with multiple components (Storage Array software, SRAs, Multipath software, vSphere versions). • Needs storage configuration or reorganization before RM is ready to use. • Limitation with N:1 replication and expensive to set up. • No multi-tenant portal	• Supports only vSphereto-vSphere replication. • Does not provide pointin-time copies for recovery. • Limited ESXi version support (only supports vCenter 5.1 and above and ESXi 5.x and above). • RPO cannot be less than 15 minutes. • Limitations with N:1 replication and scalability: – Simultaneous VM failover - between 10 - 80. – Site Pairing -10 Sites only per vCenter/ SRM pair. – Limited to 500 VMs. • Lack of cloning capability at DR site for performing DR drills. • No multi-tenant portal.	• Supports Any-to-vSphere replication. • Provides continuous data replication with multiple point in time copies for recovery. • Supports N:1 replication with any number of source sites. • Provides multi-tenant portal for customers. • Supports any-to-any replication with any storage type and vendor. • Supports near zero RPO and RTO.

DRaaS: Host-Based Replication As Preferred Choice

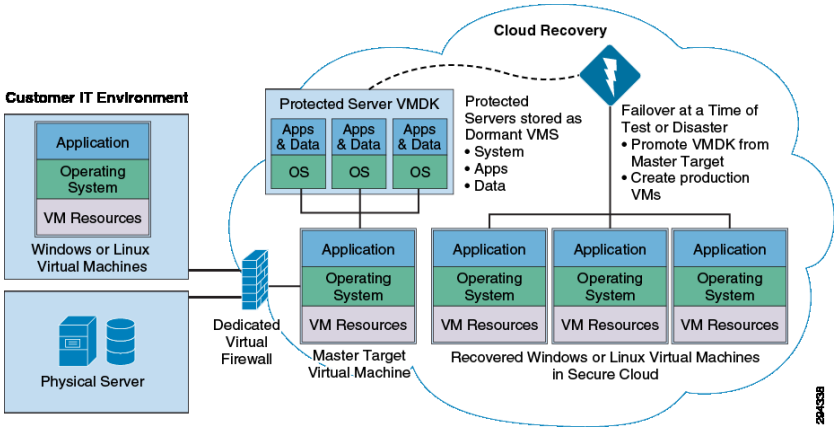
Several options exist in the choice of technology for the implementation of DRaaS, which is associated with varying levels of cost, complexity, and operational models. A summary of technology options for the implementation is presented in Figure 1-7.

Figure 1-7 Many Approaches to DRaaS



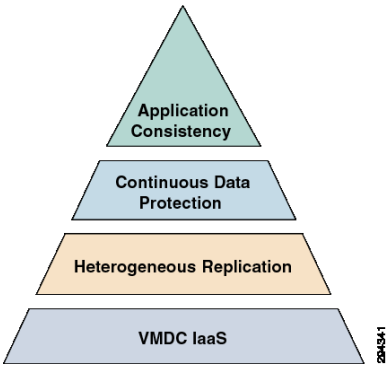
The host-based replication technology is the recommended implementation for Cisco's DRaaS System architecture. It is delivered in partnership with InMage ScoutCloud product offering because of the value and the differentiation it provides delivering DR services for physical-to-virtual (P2V) and virtual-to-virtual (V2V) workloads.

Figure 1-8 Host-Based Replication/Recovery Process



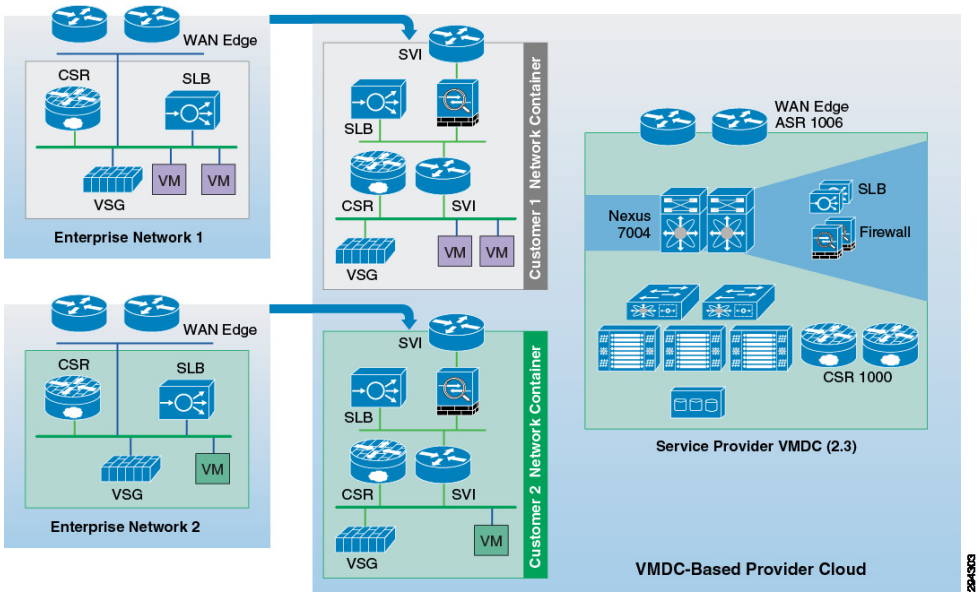
The Cisco DRaaS System, which offers architecture based on the VMDC 2.3 infrastructure architecture, provides P2V and V2V DR and business continuity capabilities. Cisco VMDC-based cloud provides secure multi-tenancy, services orchestration, high availability, and modularity.

Figure 1-9 DRaaS Offering



Layer 2 Extensions and IP mobility using Overlay Transport Virtualization (OTV) and Lisp to support partial failovers and active-active scenarios are targeted to be addressed as part of future capabilities of VMDC architecture. The solution presents heterogeneous, storage, and infrastructure-agnostic data replication capabilities for the creation and offer of DR solution offerings. The system offers continuous data protection (CDP)-based recovery with the ability to roll back to any point in time. The system provides guaranteed application consistency for most of the widely-used applications.

Figure 1-10 Host-based DRaaS on VMDC Architecture



Value of Cisco DRaaS Architecture for Service Providers

DRaaS offers the following value to SPs:

- **Increased Customer Relevance**: Not all of the customers requiring DR services want Infrastructure as a Service Offering (IaaS). Offering DRaaS provides better alignment with a typical IT buyer's focus. Leverage of DRaaS offerings by SPs provide them an opportunity to differentiate from commodity and over-the-top IaaS providers.
- **Bigger, More Profitable Deals**: DR instances command a premium and provide improved margins due to lack of commoditization. DR deals are typically larger compared to IaaS deals for SPs and generate higher margins. DRaaS offerings create reduced capital expenditures on compute resources and lower operating expenses on licensing due to oversubscription opportunities.
- **Strong Services Growth**: DRaaS offerings present a strong ability to attach additional services with the offerings and creates a pipeline of revenue from new and existing customers through new and improved monetization via services growth. Additional monetization opportunities present themselves through possibilities for hybrid services.

Cisco DRaaS Approach vs. Backup-based Disaster Recovery

One commonly encountered question is how do the backup-based disaster recovery approaches compared to Cisco's recommendation for DRaaS architecture for SPs. Table 1-2 shows the key considerations and a comparison of the approaches.

Table 1-2 Comparison of Cisco DRaaS vs. Backup-based DR

	Managed backup using Cloud Storage	Backup-based Cloud Recovery using Snapshots	Cisco Approach
Use Case	Backup to cloud: Cloud storage for backups	Disaster recovery: SP-managed disaster recovery	Disaster recovery: SP or customer self-managed disaster recovery
Pros	Customers have ability to store data offsite without shipping tapes or having a secondary site to host data	Makes use of existing backup and virtualization tools for recovery	SP managed or enterprise self managed Single solution for protecting both physical and virtual environments Automated recovery
Cons	• Does not ensure continuity of operations. Provides data availability only. • Impacts performance of application during backup window. • No automated recovery	• No P2V capability, protection for only virtual environments • Performance impact on production applications during snapshot creating • No automated recovery	
RPO/RTO	Very high	High	Near Zero
Continuous Data Protection (CDP)	N/A; works based on traditional backups	Near CDP, cannot achieve real CDP. Depends on the frequency of snapshots.	Real CDP, provides multiple point in time copies for an extended period of time.

Service Provider Tenant Operating Models

Cisco DRaaS presents a model that clearly delineates the responsibilities of the SPs providing the DRaaS services and the end customer guidance on the ownership and expectations in the system offering.

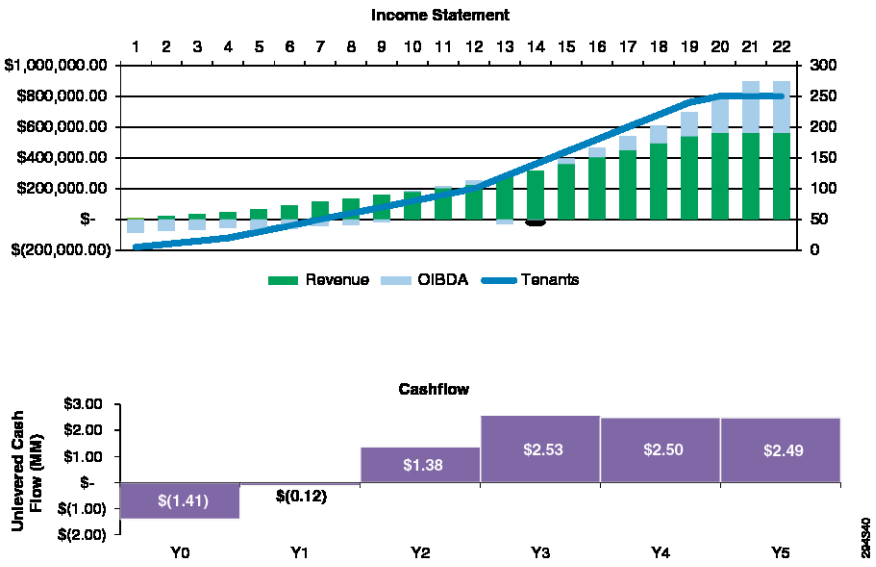
Table 1-3 Well-Defined Tenant/SP Operational Responsibilities Model

Responsibility	Service Provide	Tenant
Provide standby recovery environment (compute, network)	X	
Configure standby recovery environment with replication/ recovery plans for protected servers and network elements	X	
Recover/ boot protected servers to recovery environment with pre-defined VLAN/ IP address mapping and network topology	X	
Provide recovery to a specific point in time using CDP technology to create a bootable VMDK; boot associated VMs	X	
Ensure reachability of running VMs over pre-defined recovery network	X	
Validate application configuration and functionality		X
Provide notification of changes requiring recovery plan updates - VLANs, IPs, added/ removed volumes, new servers		X
Participate in annual recovery tests/ drills (no production impact)	X	X
Declare disaster		X

SP Monetization of Cisco DRaaS

Figure 1-11 is a financial model that presents the monetization opportunity for SPs associated with the deployment of the Cisco DRaaS System architecture.

Figure 1-11 Monetization Opportunity for SPs



Value of Cisco DRaaS for Enterprises

DRaaS provides the following value for Enterprises:

- **Recovery Time Is Key**: Enterprises frequently lack the knowledge to select and deploy the optimal DR tools for their needs. Current enterprise tools for low RPO/RTO tend to be cost prohibitive for widespread deployment.
- **Reduced Cost and Impact of Disaster Recovery Testing**: DR exercises present a significantly high cost and are a "distraction factor" to the normal business operation. The use of DRaaS allows enterprises to focus on application validation without being distracted by rack, stack, and recover activities with their infrastructure and IT services. It also presents a potential opportunity to better leverage the DR environment.
- **Accelerated Implementation**: The use of DRaaS presents an easier framework for implementation of business continuity plans and test execution and provides end customers with the ability to grow over time from a limited scope. An equivalent DRaaS solution to replace one that is provided and managed through a SP's robust offerings would be extremely time consuming to build for enterprises on their own as they include self-service, monitoring, and service assurance capabilities as a holistic offer from SPs.
- **Better Odds of Success**: The use of specialized SP offerings eliminate the need for a strong DR competency and addressed the difficulty associated with hiring and retaining talent for DR. The DRaaS is a niche technology that requires a significantly large scale to gain the required specialized experience. Globalization means many organizations cannot use traditional primary and secondary model of dedicated infrastructures for DR and business continuity operations.

Figure 1-12 Why Enterprises Choose DRaaS