Cool Vendors in Business Continuity Management and IT Disaster Recovery Management, 2014

Published: 24 April 2014

Analyst(s): Roberta J. Witty, John P Morency, Robert Naegle

Improved crisis communications and making the transition from IT disaster recovery management to IT service continuity management are and will be top-of-mind for many organizations in the next few years. Five new Cool Vendors provide these services, which can mature organizational resilience.

Key Findings

- IT disaster recovery (DR) solutions are evolving to become more sophisticated IT service continuity management solutions for IT disaster recovery management.
- Cloud computing and virtualization present IT disaster recovery professionals with many benefits as well as challenges that must be managed in order to ensure full server restoration according to recovery objectives.
- Crisis communications is fast becoming a two-way street with savvy mobile device constituents wanting personal safety coverage and to become a participant with emergency management and business continuity management (BCM) professionals in event dialogue.

Recommendations

- Investigate hybrid cloud computing to support selective application failover and data-center-wide disaster recovery without incurring unnecessary fixed monthly service costs.
- Investigate IT DR management products, which can provide the flexibility to leverage cloud and on-premises capabilities to optimally meet business recovery SLAs.
- Consider conducting full server restoration in a time, effort and cost-effective manner that meets continually shrinking recovery time objectives (RTOs).
- Leverage mobile devices and the growing interest in citizen populations to assist in disaster management to provide best-of-breed personal safety solutions.
Recovery as a service (RaaS) providers must provide a strong delivery platform as well as customer service. The interface of cloud computing services and virtualization technologies brings many benefits to RaaS providers.

Table of Contents

Analysis..................................................................................................................................................2
What You Need to Know..................................................................................................................2
CloudVelocity................................................................................................................................... 2
Geminare..........................................................................................................................................4
Sanovi.............................................................................................................................................. 5
TapShield......................................................................................................................................... 7
Zerto................................................................................................................................................ 8
Where Are They Now?......................................................................................................................9
   Unitrends (previously VirtualSharp)..............................................................................................9
Gartner Recommended Reading..........................................................................................................10

Analysis

This research does not constitute an exhaustive list of vendors in any given technology area, but rather is designed to highlight interesting, new and innovative vendors, products and services. Gartner disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

What You Need to Know

Moving from traditional IT disaster recovery to IT service continuity management shifts the focus from recovery to resilience. Technologies such as recovery as a service, cloud management platform, data replication for virtual machines and recovery assurance tools can assist in the transition. Also, the growing adoption of mobile devices and personal participation in a disaster through crowdsourcing enhance crisis management and communications strategies.

The five new companies in this year’s Cool Vendors for BCM provide all this capability in order to help organizations move from recovery to resilience.

Included in "Cool Vendors in Business Continuity Management and IT Disaster Recovery Management, 2012," VirtualSharp, now Unitrends, and its ReliableDR offering have been negatively impacted by the arrival of new entrants that are offering similar functionality.

CloudVelocity

Santa Clara, California (www.cloudvelocity.com)
Why Cool: A current limitation of many RaaS providers is their fixed monthly pricing policies for both virtual machines and storage resources. These policies limit a customer organization’s ability to control its service costs by only using these cloud resources when needed, either to support recurring recovery exercising or to facilitate recovery operations. In addition, many RaaS providers also limit the number of recovery tests that can be conducted by a customer without incurring additional per-test charges.

This limits the extent to which failovers can be initiated between the premises and the cloud in order to more rapidly facilitate application problem bypass. CloudVelocity enables organizations to overcome these limitations. Its One Hybrid Cloud software supports flexible transition between the premises and the cloud of IT services that can be as simple as one service supported by a single virtual machine all the way to a set of multitier applications that is supported by a more complex collection of both physical and virtual machines.

Both VM and supporting storage resources are more dynamically allocated inside an IaaS cloud (supported by providers such as Amazon Web Services [AWS] Elastic Compute Cloud [EC2]) by leveraging the provider’s on-demand resource allocation and capacity elasticity management technologies. The result is the realization of hybrid cloud computing that can be equally effective in supporting both selective application failover as well as data-center-wide disaster recovery without incurring unnecessary fixed monthly service costs.

The cloud resources required to support individual IT services are defined by One Hybrid Cloud via blueprints that are typically the byproduct of an on-premises autodiscovery of relevant server, storage, network and database resources that are required to run a specific application service. Blueprints not only define the required infrastructure resources, but also define the resource conversions needed to run the on-premises application in the specific cloud service.

For example, on-premises enterprise applications may be supported by a mix of virtual machines that run on VMware’s ESX Server, or other hypervisors, and physical systems. However, the ESX guest virtual machines and the physical systems may not have the necessary software, and configuration to allow them to run in Amazon’s EC2. One Hybrid Cloud would transparently handle the process of preparing and reconfiguring all of the systems-related on-premises applications to enable them to run in Amazon’s cloud. This process involves steps such as driver injection, device reconfiguration, physical- and virtual-to-cloud conversion, and other steps to make the systems ready to transparently run in the cloud. When the systems are run in the cloud, One Hybrid Cloud also securely extends the data center network to the cloud for services still in the data center.

Challenges: CloudVelocity will inevitably be competitively challenged over the next few years by the growth of hybrid cloud management systems, both from external IaaS providers targeting a greater foothold in the enterprise as well as base system and management software vendors planning to extend their reach into a variety of public cloud services and increase the number of their strategic provider partners.
Who Should Care: IT operations managers who are responsible for supporting IT service continuity (that is, the combination of both IT disaster recovery and IT service availability) will find One Hybrid Cloud an intriguing alternative to the use of more mainstream cloud-based recovery services. In addition, use of One Hybrid Cloud is not restricted to just service continuity management applications. A policy for managing more flexible compute and storage capacity for development and test systems or lower priority production workloads could also be managed.

Geminare
Los Altos, California (www.geminare.com)

Analysis by Robert Naegle and John P. Morency

Why Cool: Geminare is a cloud management platform (CMP) vendor whose Cloud OnRamp Enablement (CORE) software provides a robust management infrastructure for the delivery of cloud-based RaaS via provider partners. Cloud CORE, a patented technology that is one of the earliest CMP offerings, now includes 18 management capabilities in two products: Cloud Recovery and Virtual Server Rapid Recovery.

Geminare equips its service provider partners with one of the market’s most complete management platforms for setting up, administering and managing recovery service instances. One of its differentiated technologies is its Virtual Network Operations Center (VNOC). VNOC provides a complete remote management and monitoring (RMM) platform that facilitates proactive provider responses to events that either occur inside the managed cloud infrastructure or at the customer premises.

The primary offering from Geminare, Cloud Recovery (CR), is a host-based replication solution that allows end users to replicate server data, applications and system information from either cloud-hosted or on-premises servers into a cloud platform. Cloud Recovery enables a hybrid recovery model with the ability to protect physical and virtual servers at both production and recovery service (or colocation provider) sites. Additionally, Cloud Recovery simplifies the failback of both virtual and physical systems via block-level changes without requiring a bare-metal restore.

Given that many RaaS providers are evolving their offerings to combine VM spin-up with managed data backup, replication and archival services, support for these more integrated service offerings is critical. Addressing this evolution is a unique VNOC feature called Virtual Server Rapid Recovery (VSRR). VSRR deploys a standby restore-ready server in the partner’s cloud that is in constant communication with the on-premises production server via an encrypted tunnel. The cloud-based standby server keeps current with the most recent production system state information and data changes by leveraging standard online backup tools and provides the customer with a preconfigured, restore-ready standby server. When a complete server recovery is needed, using a preconfigured restore-ready server ensures significantly better recovery time objectives (RTOs) and dramatically reduces the time, effort and costs required to complete full restorations of production servers and data.

Typical service provider implementations, primarily driven by Geminare partners, reportedly range between 100 and 250 virtual machines (VMs) with an associated production storage footprint of
roughly 10 terabytes (TB) to 20TB. As the RaaS market has grown significantly over the past couple of years, larger implementations (that is, 500-plus VMs and hundreds of terabytes) are currently being rolled out.

Current Geminare partners include NTT Communications, HP, CA Technologies, Iron Mountain, Microsoft, Hosting, Cosentry, Allstream, Bell Canada, CenturyLink/Qwest, Columbus Networks and many others.

**Challenges:** Given increasing CMP competition from players such as Cisco, Citrix, Eucalyptus Systems, VMware and others, Geminare will be increasingly challenged to grow its business in a market where at least 90% of existing RaaS production instances are primarily VMware-based, resulting in potentially growing partner preference for an all-VMware solution. Given the phased industry evolution to hybrid cloud services from Amazon, Microsoft, IBM and Google, among others, increasing deployment of managed workload availability and portability across private and public cloud infrastructure will begin to reduce the need for traditional disaster recovery, regardless of whether it is supported by cloud-based services or not.

In addition, increased CMP competition will inevitably result from both the open-source community (especially for OpenStack-compliant public cloud infrastructure) as well as vendors supporting private cloud management (including the big four management vendors — BMC, CA, HP and IBM — as well as a growing number of much smaller vendors).

**Who Should Care:** IT operations managers who are considering implementing RaaS but require a service that needs flexibility in both VM format and physical deployment, which can be storage- and cloud-platform-agnostic as well as guarantee data protection and consistency between the premises and the cloud, should strongly consider one or more Geminare partner providers ([Geminare partner list](#)).

Sanovi
Bangalore, India ([www.sanovi.com](http://www.sanovi.com))

*Analysis by John P. Morency*

**Why Cool:** Sanovi is a recovery and availability management software vendor that supports a range of recovery assurance capabilities through its Enterprise Disaster Recovery Management (DRM) and Cloud Continuity product families. The company was founded in 2003 and currently has over 100 customers.

The focus of recovery assurance, a relatively new technology, is twofold. The first is the reduction of the time, cost and logistics associated with traditional disaster recovery exercising through the use of orchestration workflow automation that improves exercise and managed failover consistency, manageability and sustainability.

The second is the combination of DRM Recovery Monitor and DRM Validation that actively tracks the likelihood of reliably and effectively recovering application operations. Its proprietary technology supports active monitoring of current states of production and backup data as well as tracking the
execution of key activities of the storage management system that have directly impacted the recoverability and integrity of production data as well as applications. Monitoring data roll-up is reflected in a management recoverability dashboard that summarizes the current likelihood of successful recovery for a set of user-designated applications.

For many Gartner clients, recovery plan exercise management that is largely based on completely manual or semimanual procedures is not sustainable over the longer term, especially as the number of in-scope production applications and the amount of in-scope data continues to increase. Exercise automation is essential for reducing exercising time while also freeing up valuable support resources for testing those lower-tier applications that are far less frequently tested, if at all.

Sanovi was one of the first vendors to address this need by delivering both a general-purpose workflow automation engine via its Drill Manager offering and supplementing it with an out-of-the-box recovery automation library, which is a repository of recovery actions that can be used for testing mainstream mission-critical applications based on Microsoft SQL Server, Oracle databases and SAP ERP systems, among others. Today, there are other orchestration automation products that can be utilized, such as BMC Atrium Orchestrator and HP Operations Orchestration, but none of these products is natively IT DRM aware, and none currently supports functionality similar to Sanovi’s active nerve center and management dashboard reporting.

Recently, Enterprise DRM functionality has been extended to public and hybrid clouds through the introduction of Sanovi Cloud Continuity, which extends its recovery assurance to managed multitenant RaaS. A key enabler is Sanovi’s Application Defined Continuity technology, which facilitates both the porting to and operation of premises-based applications within either public or hybrid clouds. An initial partnership has been established with Netmagic Solutions (an NTT Communications cloud service provider based in Mumbai, India), and more partnerships with similarly sized service providers are planned over the course of 2014.

Challenges: Unlike many other management software markets, recovery orchestration and assurance is relatively small both in the size of the overall market and in the number of players. This is likely to remain the case for the foreseeable future. The major challenge that Sanovi and competing vendors will face is not just the growth of RaaS, but the longer-term industry transition to the use of hybrid clouds as vehicles for the execution of increasingly mobile workloads. Once the production data center boundary becomes virtual instead of physical, the need for traditional disaster recovery management all but vanishes. This is not likely to happen in the immediate future for many organizations, but is much more likely over the next three to five years.

Who Should Care: IT disaster recovery managers tasked with the management and evolution of production applications recovery and management will likely find the functionality of Enterprise DRM very appealing. It not only has the potential to reduce the amount of manual exercising effort, but also can reduce the in-house dependencies on both the development and maintenance of custom run books and scripts. In addition, the combination of DRM Recovery Monitor, DRM Validation and DRM Service Reporter provide a much more turnkey basis for more formalized recovery and continuity service-level management.
TapShield
Orlando, Florida (www.tapshield.com)

Analysis by Roberta Witty

Why Cool: TapShield technology turns mobile devices into personal safety systems that can leverage crowdsourcing in order to instantly send relevant information to emergency responders, potentially averting dangerous situations and sending for help more quickly. Examples of dangerous situations include:

- A student is attacked on campus and needs the ability to quickly summon help from anywhere and at any time.
- A lockdown or threat occurs at a facility, and the organization needs to account for all individuals.
- Traveling employees, students and others under the due care of the organization need to be located and communicated with during crisis activity overseas.
- Students or employees walking home or through company parking lots late at night need to get to their end destination safely (or issue an immediate alert if threatened).
- Students or traveling employees want to understand real-time crime information in their immediate vicinity so that they can make safer decisions.
- A student takes a late night run through campus and desires an extra layer of personal safety.

By leveraging mobile devices and crowdsourcing, TapShield’s Shield Command, a Web-based incident management system, quickly, securely and privately gives dispatch centers and physical security officers real-time GPS location and relevant caller identification (for example, allergies, age and photo ID) so that first responders can react faster and make better-informed decisions.

TapShield offers a unique combination of features that set it apart from the competition:

- Silent Alarm sends a covert emergency alert without the user having to touch his/her smartphone. TapShield Yank uses advanced smartphone technology to issue an alert once the headphone or a Smart Dongle is pulled out of the device, instantly sending real-time GPS and caller info to the authorities.
- Instant Mass Notification can alert up to one million users within a specified area using geofencing technology.
- Always Connected enables discrete, two-way communication between users and authorities through secure voice over IP (VoIP) during and after a crisis.
- Never Alone/Entourage allows users to alert their contacts when they depart one location for another location to ensure that they arrive safely at their end destination. If the user does not arrive at his/her scheduled destination within the allotted time, authorities are alerted to the users' precise location, enabling them to respond effectively.
The community-based security app, SafeCircle, allows organizations to crowdsource emergency reporting and response, essentially expanding physical security forces into a pervasive, campuswide network of potential responders. SafeCircle alerts other relevant responders in the surrounding area as to whether their help is needed or whether they should evacuate the area.

**Challenges:** A key success factor in growing TapShield is end-user adoption of the client-side app. While TapShield offers on-site consulting and engagement tools to the customer, they need to evolve their process to help customer download efforts. Another challenge will be from the emergency/mass notification services (EMNS) vendors that are currently entrenched in higher education and private enterprise — many already have mobile device apps with some level of personal safety features. They could easily be a partner or acquisition target of the EMNS vendor market, providing the needed capital and resources to this small organization to expand into additional industries and geographies.

**Who Should Care:** Physical security, emergency management and business continuity managers in organizations who need to provide personal safety for the people in their charge should be interested in this vendor. Industries with such a profile include higher education (including both urban and remote high schools), private enterprises with a significant traveling population, organizations interested in executive personal safety and healthcare organizations that perform senior care.

Zerto

Boston, Massachusetts; Tel-Aviv, Israel ([www.zerto.com](http://www.zerto.com))

*Analysis by Robert Naegle and John P. Morency*

**Why Cool:** Zerto has elevated the replication and recovery of VMware-based virtual environments with its innovative replication mechanism that captures and streams VM changes in real time while supporting very low RTO and recovery point objective (RPO) targets. It also supports the definition of virtual protection groups and enables full read/write testing without impacting the currency of production systems.

Zerto’s replication mechanism captures data at the hypervisor level and continuously streams block-level changes to the data store at the target site. The focus on delta change information reduces system and network resources required to support recovery efforts. Reference customers report minimal impact to operations or bandwidth in implementations that support up to 500 servers. Zerto does not use the VM snapshot approach that commonly leads to larger payload transmissions and disrupts the operating environment. A continuous change-streaming approach supports more aggressive SLAs or "near real time" RPOs and RTOs.

Virtual protection groups, another interesting Zerto capability, provide the ability to maintain the interdependencies between member virtual machines. VMs can be identified, associated, moved and replicated as a group. This method ensures a "Group Level" SLA, protecting and ensuring proper startup ordering and write order fidelity across volume sets and hosts, thereby enabling more consistent application recovery. The challenge for IT leaders will be that applications or...
service-based groupings of VMs are defined based on IT’s knowledge of critical service/application dependencies.

Additionally, full read/write testing can be executed without affecting replication and production. Recovery groups can be stood up and tested without disrupting production systems or the continuous streaming of production change content to the recovery environment. This means that recovery testing does not need to be scheduled after hours or in low production usage windows.

Zerto is a privately held, venture-funded company that is growing rapidly and has recently completed a $13 million round of Series C financing. It supports VM recovery solutions directly to the enterprise and as a service via its two partner programs, Zerto Alliance Program and Zerto Cloud Ecosystem (ZCE). Zerto Virtual Replication Manager provides migration orchestration, automation and replication of production workloads with support for automated failover and failback to enterprise clients. Cloud service provider partners (CSPPs) that are interested in providing DRaaS can add Zerto Cloud Manager for additional capabilities like centralized management and automated reporting in a single view of all customer and CSPP resources.

**Challenges:** The expanding capabilities and competitive pressures from vendors like VMware could significantly impact the competitive differentiation of the Zerto solutions. Moreover, the limited focus on recovery of VMware systems only limits Zerto’s reach. Also, it does not currently have a solution for physical-to-virtual or physical-to-physical recovery requirements.

**Who Should Care:** IT operations managers or those responsible for disaster recovery in environments with a high percentage of VM servers who are looking for a more efficient way to manage their own disaster recovery to a private or public cloud should consider Zerto Virtual Replication. Similarly, cloud providers looking to offer RaaS should evaluate the use of the Zerto software as a viable alternative to a VMware-only solution.

**Where Are They Now?**

This year, Gartner looks back at a Cool Vendor profiled in 2012 and provides an update on where software vendor VirtualSharp is today.

**Unitrends (previously VirtualSharp)**
Burlington, Massachusetts (www.unitrends.com)

*Analysis by John P. Morency*

Profiled in "Cool Vendors in Business Continuity Management and IT Disaster Recovery Management, 2012"

**Why Cool Then:** VirtualSharp Software’s ReliableDR supported IT disaster recovery orchestration, which consisted of the mapping, automated testing and assurance reporting of a set of application services supported by sets of Windows VMware- or Linux-based virtual machines. ReliableDR used the core characteristics of virtualization to generate virtual test sandboxes, which were virtual data center instances that had their own sets of virtual storage and network infrastructure and could be
activated at a recovery location (which may be a secondary facility or a VMware-based public cloud service) for testing or recovery operations.

Snapshots of VMs were loaded into the test sandboxes, and an orchestrator verified that the IT service had been recovered according to user-defined policies, including RTO-based and RPO-based service levels. The software allowed IT administrators to simulate failover scenarios to the recovery site as often as required, and it supported the means to automate application recovery test scripts.

ReliableDR could run either as a stand-alone application or as a VM in the secondary site. In addition, ReliableDR was independent of the data replication mechanism, which meant it could utilize data that is replicated on a storage area network or via host-based replication software.

**Where Are They Now:** On 2 April 2013, PHD Virtual, a Philadelphia-based vendor of virtual machine backup and recovery software, acquired VirtualSharp. Details of the acquisition were not disclosed. Today, ReliableDR is the member of the PHD Virtual product family that supports recovery assurance functionality for VMware similar to that originally developed by VirtualSharp.

In turn, on 13 December 2013, PHD Virtual itself was acquired by Unitrends, a vendor of enterprise backup software based in Burlington, Mass. Today, the combined company supports backup and replication software products for VMware, Hyper-V and Citrix Xen virtual machines, as well as physical and virtual appliances that support consolidated data backup for both physical and virtual environments and data archival.

**Who Should Care:** Although it is a member of a much larger software product family today, ReliableDR still provides the same recovery testing flexibility and automation benefits. However, it does not appear that any interface, command or data integration with other Unitrends products, including VMware Backup and Replication, Citrix Backup and Replication, Hyper-V backup, Unitrends Backup or CloudHook Cloud Backup exists at this time. In addition, comparable software products from competitors such as Zerto, as well as the capabilities of a large number of cloud-based recovery providers, have negatively impacted VirtualSharp’s ReliableDR competitive differentiation.

**Gartner Recommended Reading**

*Some documents may not be available as part of your current Gartner subscription.*

"How Gartner Defines Crisis/Incident Management"

"Magic Quadrant for U.S. Emergency/Mass Notification Services"

"ITScore for Business Continuity Management"

"Survey Analysis: BCM Program Posture, 2013"

"Hype Cycle for Business Continuity Management and IT Disaster Recovery Management, 2013"
GARTNER HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

Regional Headquarters
AUSTRALIA
BRAZIL
JAPAN
UNITED KINGDOM

For a complete list of worldwide locations,
visit http://www.gartner.com/technology/about.jsp