

# Will Your Disaster Recovery Solution Work?

## *Continuity Software Validates & Monitors End-to-end DR*

**Date:** June, 2007

**Authors:** Bob Laliberte, Analyst

**Abstract** Continuity Software enables enterprises to validate that their disaster recovery solutions have been deployed correctly and will work when required. The software uncovers any potential vulnerabilities and helps to optimize the disaster recovery environment.

The events of September 11, 2001, the hurricane season of 2005 and the rise of compliance and corporate governance initiatives have caused companies of all sizes to assess the risk of business-critical application downtime in recent years. Virtually any amount of downtime can mean lost productivity, lost revenue, lost customers and lost opportunities.

Companies have responded by creating secondary and tertiary data centers to satisfy disaster recovery requirements. Typically, these are either provided by 3<sup>rd</sup> party hosted services (IBM, BCRS or SunGard, for example) or they have been developed in-house (collocation or secondary data centers). The investment in these solutions can be quite large with enterprises spending hundreds of millions of dollars to ensure adequate disaster recovery capabilities. In theory, these enterprises are now protected. However, in reality, they may not be. It's not from a lack of planning or technology, but rather the fact that these alternate locations, combined with ever increasing dependencies, create a tremendous amount of complexity. Companies struggle to maintain two or more fully functional sites with all of the moves, adds and changes inherent in daily operations. Ensuring that a disaster recovery site is always ready to resume all operations can be a daunting—if not impossible—task.

Typically, in order to verify that they are protected, companies will run a Disaster Recovery (DR) test once or twice a year. Also typical is that some part, if not all, of that test will fail. The problems can usually be corrected, but by the time the company runs their next DR test, another set of problems will have surfaced that will cause the test to fail again. Basically, the company is exposed for some portion of those six months. Clearly, this could be potentially very damaging to a business. However, it is not feasible to run manual disaster recovery tests in large environments on a weekly or monthly basis, let alone daily. What is needed is a way to proactively assess and validate that mission-critical applications are being replicated and that, in the event of a disaster, they will recover as designed and originally implemented.

Continuity Software is focused on solving that very problem. Founded in Israel in 2005, the company has developed a software solution that automatically validates that a company's disaster recovery environment will execute as expected. Although they have just launched their US operations, they already have real world deployments here to augment their growing customer base in Israel.

### Analysis

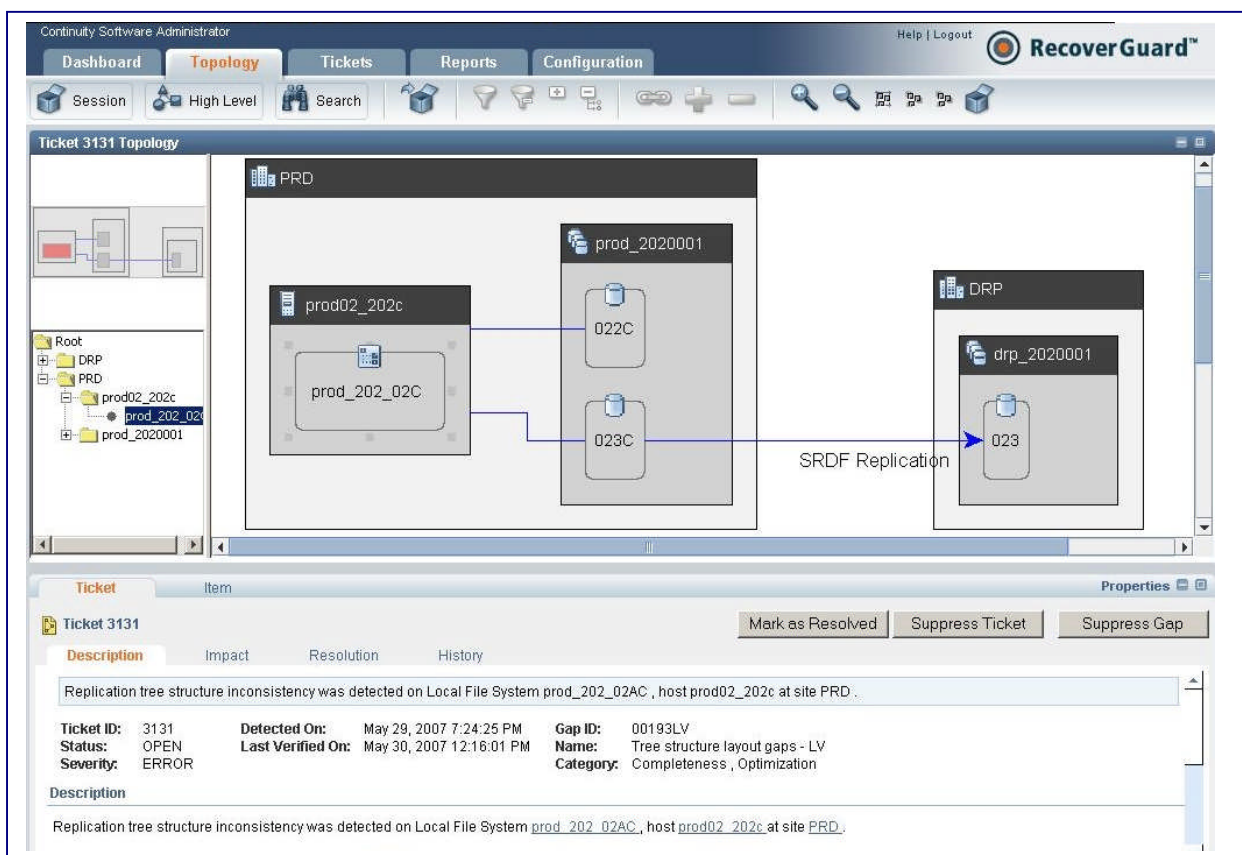
Continuity Software's flagship product, RecoverGuard, is a scalable, agentless enterprise software solution for monitoring production and recovery environments to ensure that mission-critical applications are protected and recoverable in the event of a disaster. In addition, RecoverGuard provides optimization recommendations to reduce waste, improve performance, and optimize existing data protection investments. The solution installs quickly and scans the IT infrastructure, including storage, database, servers and replication configurations, looking for potential risks and vulnerabilities. The software can be broken down into three sections:

**Document:** RecoverGuard Data Collection Engine leverages an agentless, automated process to scan infrastructure and collect configuration data from key technology elements. Typically, the data collection engine will pull information from storage management frameworks, servers and databases. Think of this periodic scan as an interrogation of the production and DR sites, in which the questions asked are: Where is the storage? Is it being replicated? How (SnapShot, Mirror)? What servers are feeding this data? What databases are leveraging these

servers? Basically, the collection engine replaces several days of manual work trying to track down and correlate the applications to the underlying infrastructure, only to have it become obsolete shortly after completion. This can be particularly difficult in larger environments, when the information collection spans multiple different siloed domains (apps, servers, storage).

**Detect:** Once all the data has been collected, RecoverGuard builds out a detailed topology map of your disaster recovery environment. This topology illustrates the dependencies of the applications through the infrastructure, including multiple sites. This master topology and dependency information forms the foundation for analysis. The analytical work takes place in the RecoverGuard Gap Detection Engine. This engine leverages a Gap Signature Knowledgebase populated with over a thousand potential data protection environments and best practices signatures. These signatures have been developed and maintained by a team of experts at Continuity Software's Lab and continue to expand through practical field experience. Your environment is compared against this knowledgebase and potential gaps or best practice violations are identified. Figure One shows an example of a DR environment with an open ticket highlighting a violation that would prevent a successful recovery.

Figure One: RecoverGuard Topology Map



The upper half of Figure One illustrates RecoverGuard's ability to map the DR environment and create a topology based on discovered items and their dependencies. The lower half demonstrates the power of the Gap Detection Engine. In this case, the software has detected some replicated storage volumes that are not consistent and could cause a problem in the case of a failover.

**Optimize:** Based on the documented environment, RecoverGuard implements an optimization engine to help fine tune the infrastructure. Specifically, it can identify underutilized storage assets, mis-configured replication environments and orphaned databases and storage volumes.

This information can all be accessed and visualized through easy to understand dashboards and prepackaged reports. The software also has the capability to generate custom reports.

**Risk Free Assessment:** To make it easier to understand the value of this software, Continuity Software offers a 48 hour Data Protection Risk Assessment (DPR/A) in an environment of 30 servers or less (fee-based). If they do not find any problems, they will not charge for the assessment. To date, every environment they have tested has exhibited multiple faults. In fact, one customer tested had more than 33 faults, with 6 critical, on just 8 servers. The customer was able to correct these faults within two weeks and then purchased RecoverGuard for on-going monitoring.

### The Bottom Line

In today's 24 x7 business environments, Continuity Software's RecoverGuard is well positioned to validate a company's ability to successfully recover from a disaster. Clearly, this functionality is a must-have for any company that can't tolerate downtime. Continually monitoring and verifying the DR environment is essential for finding and fixing the inevitable problems that will arise in a complex multi-site environment. All they ask for is 48 hours to monitor up to 30 servers to demonstrate their value. If there are no problems detected, you don't even pay them for their time.

Currently, Continuity provides support for EMC and NetApp storage environments. As they continue to expand their product offering, they will need to provide support for not only the large storage vendors, but for host-based and database replication environments, as well. In order to rapidly expand their business they will need to secure some large go-to-market partners and resellers. Most importantly, they will need to make their presence known and secure some name brand accounts to build momentum.

The starting price for this software is based on an annual fee of \$2,000 per server. The pricing puts them in the affordable category, particularly when compared to the cost of the overall DR environment. This could be especially true for those companies that are leveraging 3<sup>rd</sup> party DR services and would like to have verification that their SLAs are being met. RecoverGuard could probably get you a very quick return on investment in just missed SLA penalties alone. At the very least, it would give you some insight into your environment being hosted at a third party providers' site.

The ability to recover from a disaster is something you always hope you don't need to do, but it would be nice to know you always can. Even \$15,000 automobiles have continuous monitoring systems that let you know if the airbags or ABS brakes in your car have a problem. When the light comes on, you quickly get these items fixed, just in case you need them for an emergency situation. Why wouldn't you invest in a system to monitor the multi-million dollar disaster recovery environment that your business depends on?