RecoverGuard software will find the critical configuration errors your last DR test missed.

And we can prove it.

Recently, one of the largest financial institutions in the United States conducted a DR Vulnerability Scan to test the effectiveness of Continuity Software's RecoverGuard. The software ran for 48 hours, automatically testing and monitoring the critical business services hosted in the firm's primary and DR data centers.

What RecoverGuard detected surprised the firm's IT staff and senior managers. But it didn't surprise us.

Results Inside. 

Customer Profile

This financial institution is one of the largest in the United States, with close to $200 billion in assets and a comprehensive line of financial services and products for consumers, businesses and institutions.

Situation Analysis

The firm was intrigued by Continuity Software's RecoverGuard™, the innovative software that automatically detects hidden configuration errors which could impact recoverability in the event of a disaster. To test RecoverGuard's capabilities, the firm conducted a DR Vulnerability Scan, during which the product analyzed the DR readiness of the critical business services hosted in institution's primary and DR data centers.

Results

Although the firm has an enviable DR infrastructure and a highly qualified IT team, RecoverGuard identified a number of previously undetected gaps that were created by the constant configuration changes required in this dynamic environment. As in any complex datacenter, it is impossible for an IT organization to eliminate gaps caused by human error, and impossible to perform a full DR test after each change is made within the datacenter. Without RecoverGuard, these gaps would have remained undetected, exposing the business to serious risk.

This firm has since implemented RecoverGuard in its datacenters and uses the software to automatically test and monitor its environment on a regular basis for configuration inconsistencies.

RecoverGuard discovered **over 20 hidden configuration gaps** for this large U.S. financial institution, some of which posed serious risks to the firm's ability to recover in the event of a disaster. These errors had either gone undetected in the last full DR test, or had occurred after the test was completed

The following pages are excerpted from the firm's full report to illustrate the detail and insight that RecoverGuard can provide.

All identifiable customer data has been removed.

Identified Risks to Business Services

Figure 1 outlines the Threat Landscape identified by RecoverGuard, and displays business services and their threat level weighted in terms of technical severity and business impact. Technical Severity is ranked in order of potential impact to Recovery Point Objectives, Recovery Time Objectives, and best practices. Business Impact is ranked in order of importance to the business service.

- **Trading System:** Significant risk of data and extended recovery should there be a DR event.
- **E-commerce System:** Significant risk of data not being replicated to the remote environment and therefore being unrecoverable
- **Billing System:** Subject to prolonged downtime in the event of a disaster event.

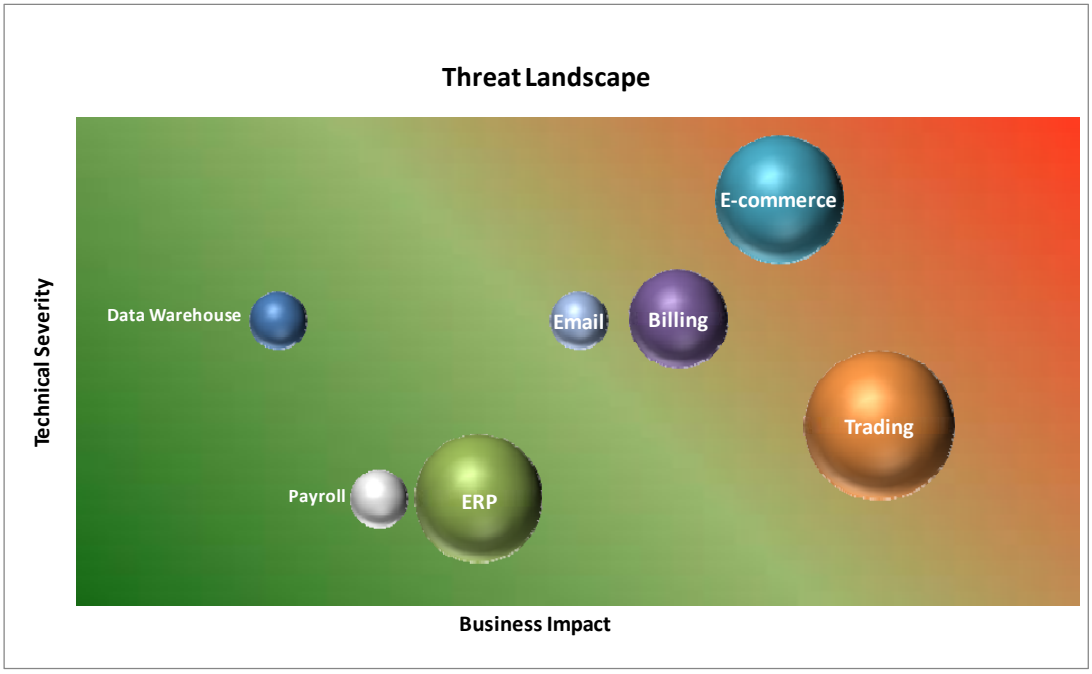


Figure 1

RecoverGuard ranks each identified gap from Informational to Critical. Figure 2 displays the percentage of all the protection gaps discovered in the firm's analysis, categorized by severity.

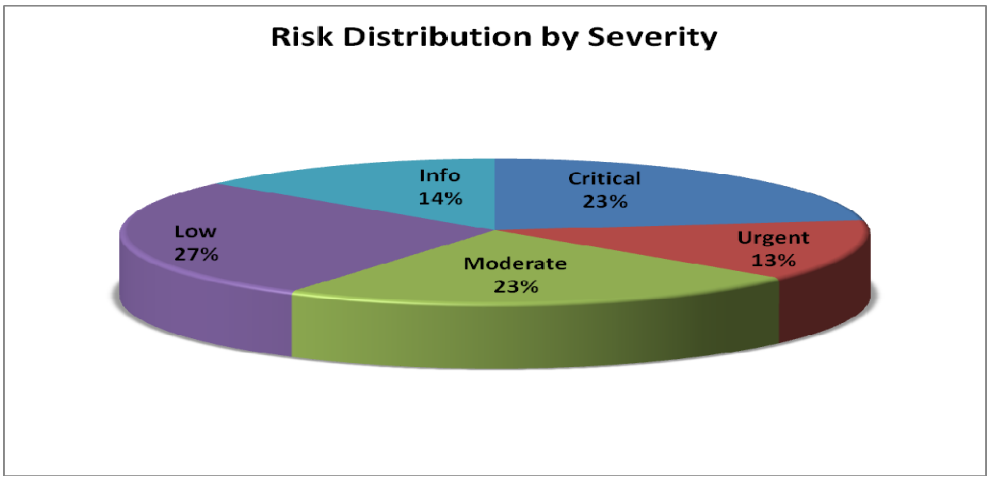


Figure 2

DR Readiness Gaps Identified

RecoverGuard isolated over 20 **separate protection gaps**, which were divided into 9 threat categories with associated technical impact and technical priority. The firm was able to evaluate the business impact of each gap and correct those that presented a business risk. The following table provides the technical priority risk ranking.

Category	Technical Impact	Technical Priority	Ticket Count	Ticket Ref. #	Business Service
Replica state inconsistency	• Data loss in a DR event	1	3	001-003	Email, E-commerce, Data Warehouse
RDF Group inconsistency	• Data loss in a DR event	2	1	004	E-Commerce
Replica Tree Structure	• Data loss in a DR event	3	1	005	Trading
Data incompleteness	• Data loss in a DR event	4	4	006-009	ERP, Trading
Missing mount export / share link	• Reduced availability • Data loss in a DR event • Not best practice	5	6	010-015	ERP, Payroll, E-commerce, Trading
Database not in archive mode	• Production data vulnerability • Data loss in a DR event	6	1	016	Billing
Inconsistent access to replicas	• Extended recovery time	7	3	017-019	E-commerce, Trading
Mixed Storage Type	• Reduced availability • Reduced performance • Bad practice	8	2	020-021	Trading
Mix of Databases	• Reduced performance • Limits possibility of deploying future point-in-time data copies • Not best practice	9	2	022-023	Billing

Gap Signature Details

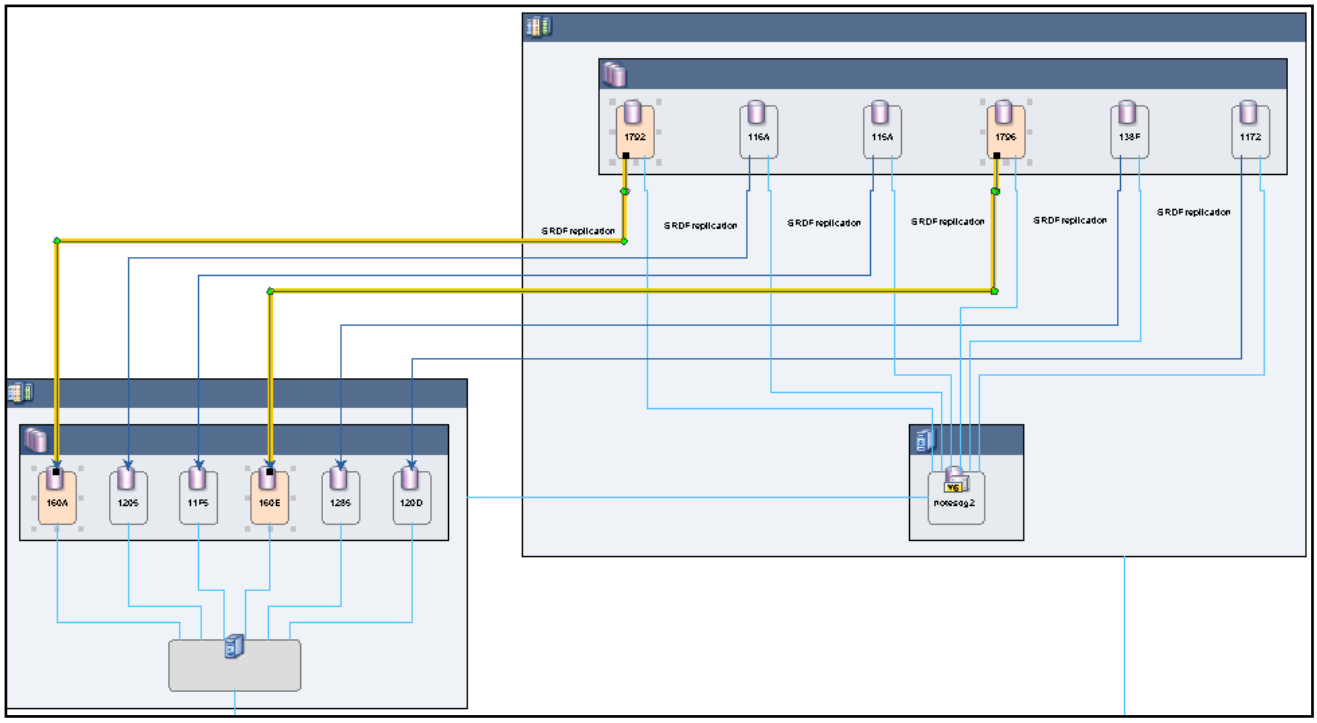
RecoverGuard automatically produces a detailed ticket for every vulnerability gap it detects. These tickets can be used on a daily basis to resolve issues before the business is impacted. The following pages contain three of the tickets produced for the firm during its RecoverGuard test.

Replica [State] Inconsistency Ticket

Ticket Count	3	Business Service(s)	(1)Email,(1)E-commerce, (1)Data Warehouse

RecoverGuard will automatically generate a ticket when the analysis encounters Meaningful Data Set (MDS) replicas for a host that are of different replication states, such as synchronized, suspended, or failed-over. All the replicas for a host MDS should be of the same state. If they are not it means the replicas are out-of-sync and will lead to data loss during a DR effort.

Ticket Topology



Ticket Summary

A Replica State Inconsistency gap was detected on volume group maildg2 on host A.

Technical Impact

Replicas for a volume group should have the same replication state and mode. If the volume group replicas are suspended for maintenance, then it is expected that all replicas in the volume group will have the state "Suspended". Otherwise, they should all be synchronized. If the replicas are inconsistent, meaning some are suspended while others are synchronized, then the entire replica would not be useful in the event of a disaster. This would result in data loss to the point of the latest successful backup.

Business Impact

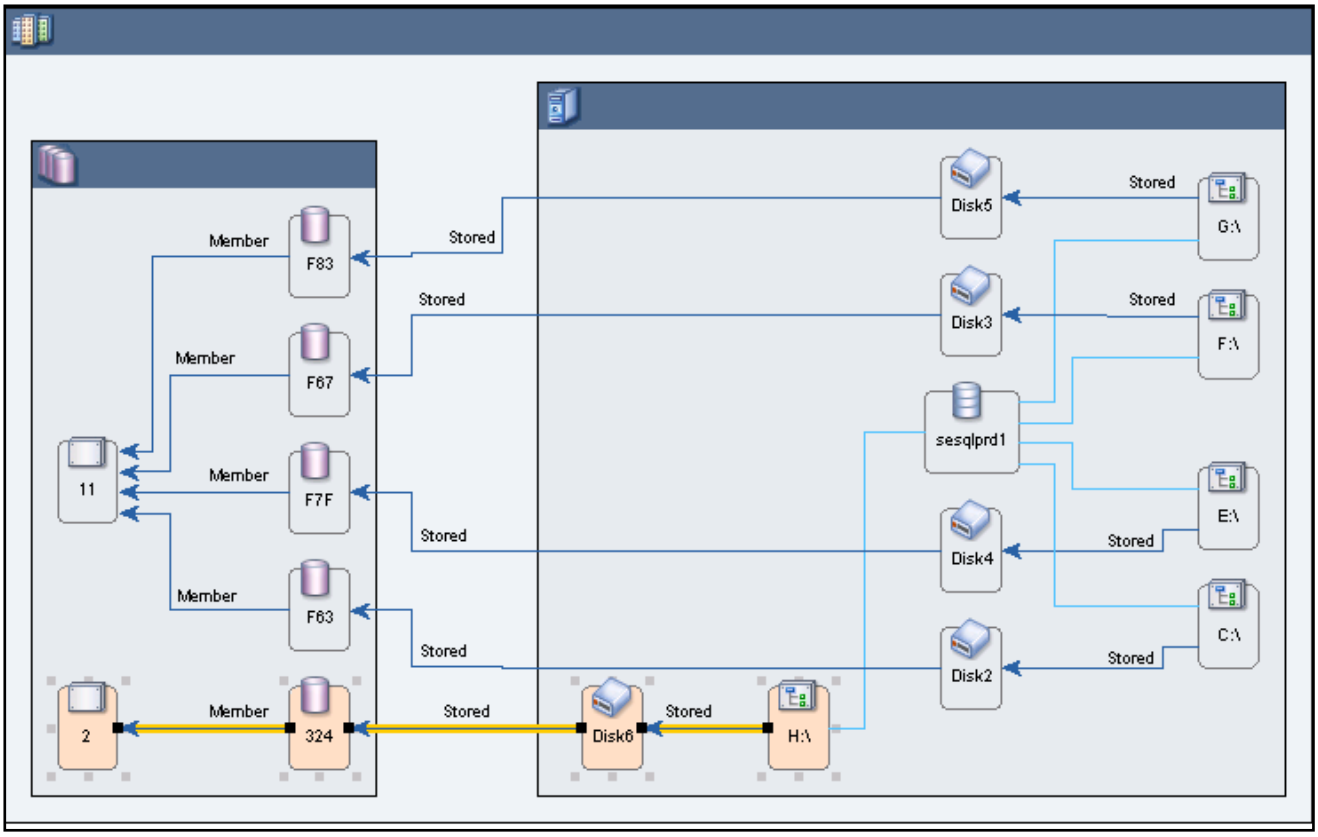
In the event of a disaster, large portions of corporate email would be lost and would require recovery from the latest backup. Recovery from backup would also extend the Recovery Time Objective.

Replica [RDF Group] Inconsistency Ticket

Ticket Count	1	Business Service(s)	E-commerce

RecoverGuard will generate a ticket when the analysis encounters a Meaningful Data Set (MDS) on a host in different Remote Data Facility (RDF) groups. A MDS on a host should be in the same RDF group. RDF groups share the same storage array communication resources. In the event of a disaster, different RDF groups can be disrupted at different intervals, which can lead to data loss if the same MDS is across multiple RDF groups.

Ticket Topology



Ticket Summary

An RDF Group Inconsistency gap was detected on MS-SQL server 2 for host B.

Technical Impact

In the event that communications between replicated storage arrays is disrupted as in a disaster, RDF groups can experience the disruption at different intervals. Database files that are across multiple RDF groups can become out-of-sync with each other resulting in data loss.

Business Impact

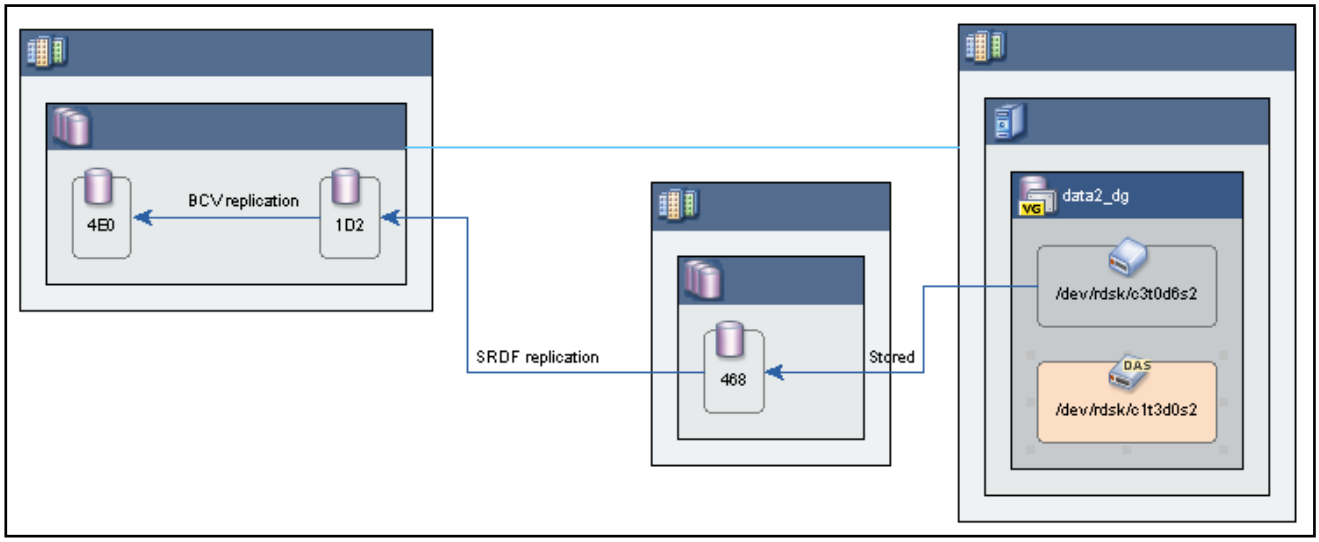
In the event of a disaster, a database for the E-commerce service would not be recoverable and would require recovery from the latest backup. Recovery from backup would also extend the Recovery Time Objective.

Replica [Tree Structure] Inconsistency Ticket

Ticket Count	1	Business Service(s)	Trading

RecoverGuard will generate a ticket when the analysis encounters a Meaningful Data Set (MDS) on a host that contains different or missing Data Storing Entity (DSE) replication structures. A MDS on a host should contain DSEs with the same replication structures. In the event of a disaster, different or missing DSE replication structures for a MDS can lead to data loss and extended recovery time.

Ticket Topology



Ticket Summary

Replication tree structure inconsistency was detected for volume group data2_dg on host C.

Technical Impact

Two gap signatures are detected for this ticket. The first is the replication tree structure gap. All the data storage elements for a volume group must have the same replication structure, meaning each storage device must all be replicated if one or more are. If the volume group is partially replicated it would render the entire volume group useless in the event of a disaster. The other gap is a Mixed Storage Type signature. The volume group contains a mix of both SAN and DAS data storing entities. A volume group should contain the same type of storage devices, whether SAN or DAS, RAID type, or from the same array, unless multi-array consistency technology is used. A variety of adverse affects can occur including data loss if a volume group contains different storage devices.

Business Impact

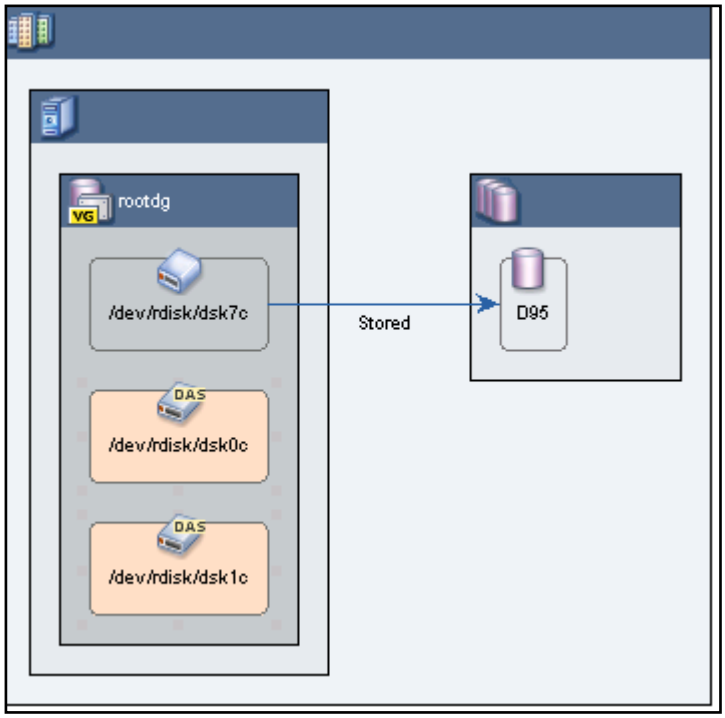
In the event of a disaster, data for Trading would be lost and would require recovery from the latest backup. Recovery from backup would also extend the Recovery Time Objective.

Mixed Storage Type Ticket

Ticket Count	2	Business Service(s)	(2)Trading,

RecoverGuard will generate a ticket when the analysis encounters a Meaningful Data Set (MDS) on a host that contains different Data Storage Entities (DSE). A MDS on a host should contain the same DSE. In the event of a disaster, different data storage elements for a MDS can lead to data loss and extended recovery time.

Ticket Topology



Ticket Summary

A Storage Volume type inconsistency gap was detected for volume group rootdg on host D.

Technical Impact

The volume group contains a mix of both SAN and DAS data storing entities. A volume group should contain the same type of storage devices, whether SAN or DAS, RAID type, or from the same array unless multi-array consistency technology is used. A variety of adverse affects can occur including data loss if a volume group contains different data storing entities.

Business Impact

In the event of a disaster, the configuration for the host D which is an application server for the Trading system may not be documented. The Recovery Time Objective may be extended.

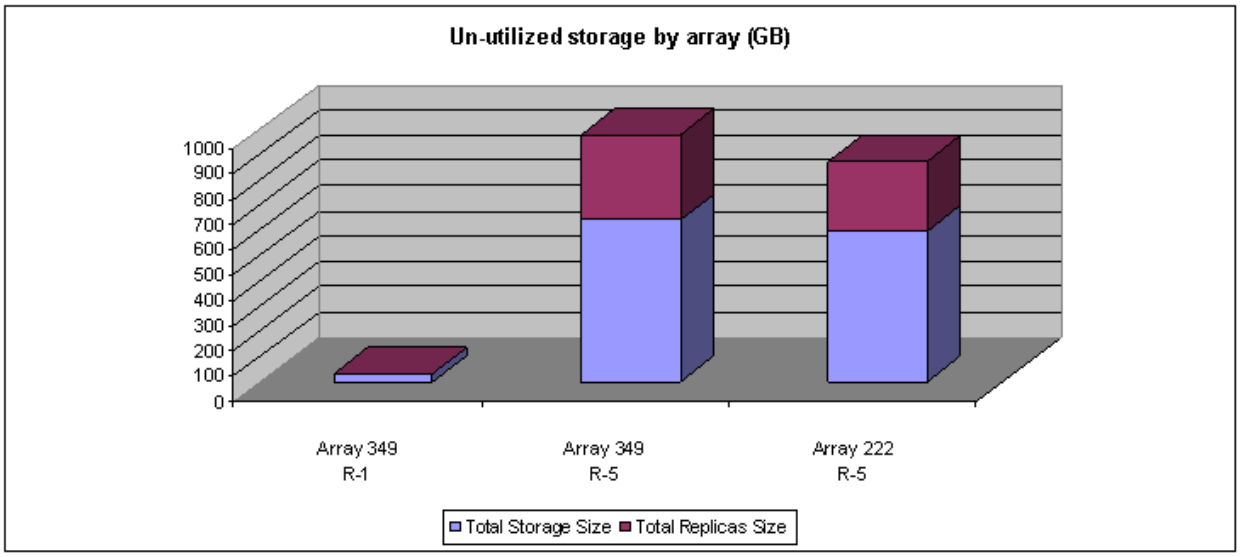
Storage Reclamation Opportunities

In addition to identifying data protection gaps, RecoverGuard also helped this financial institution uncover significant savings opportunities by identifying underutilized storage capacity in the following groups:

- Group 1 – storage volumes allocated to hosts or clusters, but not actually used by any host.
- Group 2 – configured replicas of storage volumes belonging to group 1.

Category	Total capacity
Storage devices connected to hosts but unused	1.24 TB
Replicas of the above	0.6 TB

The following chart summarized the distribution of unused storage resources between storage arrays.



The following table contains a more detailed view, grouping the found capacity by array, RAID type and size. In addition, it shows all the hosts using the disks associated with the different array, RAID type and size combinations.

Site	Storage Array	RAID Level	Size (GB)	Accessed by	Total Storage Size (GB)	Total including replicas (GB)
New York	187870349	RAID5	16.86	Host A	33.72	33.72
		RAID5	67.43	Host B, Host C , Host D, Host E, Host F	606.91	944.08
		2-Way Mirror	33.72	Host G	33.72	33.72
New Jersey	187880222	RAID5	71.41	Host H, Host F	142.82	214.23
		RAID5	16.86	Host I, Host J, Host Q	50.58	50.58
		RAID5	1.23	Host K, Host J	1.23	1.23
		RAID5	67.43	Host L, Host M, Host N, Host O, Host P, Host R	404.61	606.91
				Total	1273.59	1884.47

The following table lists storage volumes which are configured but unused according to the following criteria:

- The storage volumes are not replicas of other storage volumes
- The storage volumes are connected to one or more hosts
- The storage volumes are not used by hosts (e.g., no VG is using them)

The total amount of storage represented equals 1.24 TB.

Site	Storage Array	Storage Volume	Size (GB)	RAID Level	Connected to
New York	349	11D8	67.43	RAID5	Host D
		1090	67.43	RAID5	Host B
		F92	16.86	RAID5	Host B
		FCA	16.86	RAID5	Host B
		FF1	67.43	RAID5	Host S
		CC2	67.43	RAID5	Host C
		D02	67.43	RAID5	Host C
		D0A	67.43	RAID5	Host C
		D1A	67.43	RAID5	Host C
		D32	67.43	RAID5	Host C
		DCA	33.72	2-Way Mirror	Host G
		1224	67.43	RAID5	Host F
New Jersey	222	15CF	71.41	RAID5	Host T
		1580	16.86	RAID5	Host U
		A57	67.43	RAID5	Host U
		10BC	1.23	RAID5	Host K, Host V
		11D5	67.43	RAID5	Host K, Host J
		13D0	16.86	RAID5	Host W , Host X
		143E	16.86	RAID5	Host J , Host X
		15D3	71.41	RAID5	Host Y
		1302	67.43	RAID5	Host L
		131A	67.43	RAID5	Host L
		D50	67.43	RAID5	Host Z
		E25	67.43	RAID5	Host AA

Would you like to have this level of insight into your own environment?

You can take a closer look with our
DR Vulnerability Scan.
Let RecoverGuard monitor
your environment for 48 hours, and
find out what you've been missing.

www.continuitysoftware.com/closerlook

or email closerlook@continuitysoftware.com

CONTINUITY
SOFTWARE

5 Penn Plaza | 23rd Floor | New York, NY 10001 | ***T***: 646.216.8628 888.782.8170 | ***F***: 646.290.6706