

Is business data safe?

Can Business Continuity plans actually bring business back to life when disaster strikes?

Identifying the Business Continuity Gap

With Data Replication increasingly being used to ensure that corporate data and information is immediately available in the event of disaster why do so many IT executives feel business applications are vulnerable? Because the opportunity to perform holistic, application specific testing is limited to annual, or bi-annual Disaster Recovery tests which are expensive and time consuming to setup, and ineffective in proving that every critical business application and process will respond following a disaster.

The underlying storage infrastructure supporting Data Replication is complex and constantly changing. Business drives competitive advantage with enhancements to existing products and services which directly impact the storage configurations supporting the applications. The implementation of these technical definitions and configuration changes is usually manual and must be maintained in both the production and replicated backup and DR environments. Validation is manual, frequently using maker/checker methodologies and errors creep-in, leading to unavailability of critical business applications following a disaster or data corruption.

Compliance to SARBOX and other regulatory requirements are mandatory and current processes to assure data availability to the business applications are mostly manual and flawed. Continuous, automated compliance and validation is required to meet today's stringent regulatory requirements.

Continuous Compliance

Continuous Compliance ensures corporate regulatory requirements are met, and that application specific data policies are adhered to. Onaro's SANscreen Business Continuity delivers Continuous Compliance.

In the event of a disaster, U.S. Business Executives have a high expectation that their critical information is safe. But their IT executive counterparts are nearly four times more likely to feel that their companies are very vulnerable to losing access to data.

Source: RoperASW/EMC

ASSURE COMPLIANCE	Assure compliance of Business Continuity data policies, automate compliance reports, and keep a permanent audit record of all changes
CONTINUOUS POLICY VALIDATION	Continuously validate that business data is available to the application in the event of disaster. Real-time monitoring alerts IT and the business to data policy violations and immediately identifies the Root Cause of the problem
EFFECTIVE COMMUNICATION	Communicate effectively and consistently across the organization from CFO, CIO and CRO to Business Units, and across the IT teams
IT PROCESS AUTOMATION	Automate Business Continuity testing of data policies, and enable SOPs in the Change Management process
ASSET MANAGEMENT	Gain visibility across the replicated data environment, maintaining a central repository(CMDB) of application specific data policies, inter-relationships, and dependencies. Past, present and future reservation of assets

The Solution

SANscreen Business Continuity (BC) ensures infrastructure readiness of the Replicated Data for Disaster Recovery (DR). It validates that replications are configured correctly to support the DR objectives for every application. SANscreen BC continuously monitors and reports on the state of data availability for DR, highlighting policy violation, and compliance status ensuring that data is available for applications in case of a disaster. In addition SANscreen BC reports on the deployment of replications for each application and each DR class, providing the information required for effective financial decisions.

Assure Compliance

Generate compliance and audit reports for NASD, OCC, Sarbanes Oxley and the CRO to assure and prove that application data is available in case of a disaster.

Continuous Policy Validation

Eliminate downtime and the risk of data loss by assuring data is always available and avoid mis-configuration of replications that may lead to data loss, corruption and downtime. Root Cause Analysis minimizes correction time and risk.

Communicate Effectively

Solve organizational coordination problems. Generate reports that keep the organization informed, from the CRO to Business Units as well as storage engineering and operations. Share policies, the status of the change cycle, violations and compliance level that enable team work to solve outstanding issues quickly.

IT Process Automation

Leverage Onaro's Standard Operating Procedures (SOPs) knowledge base to customize and enable SOPs around DR decision making to automate the Change Management and policy validation process.

Asset Management

Gain visibility into the replicated environment, and achieve financial effectiveness. Quantify the cost of DR, discover unused capacity, over replication and too many copies that could be reclaimed.

The Technology

SANscreen BC leverages Onaro's patent-pending Predictive Change Management engine to provide:

Automatic Discovery

Automatic discovery utilizes device APIs and management consoles to continuously gather array, fabric and DR configurations (e.g. EMC SRDF) and dependencies. The agent-less architecture supports highly scalable environments and deploys in hours.

Accurate CMDB

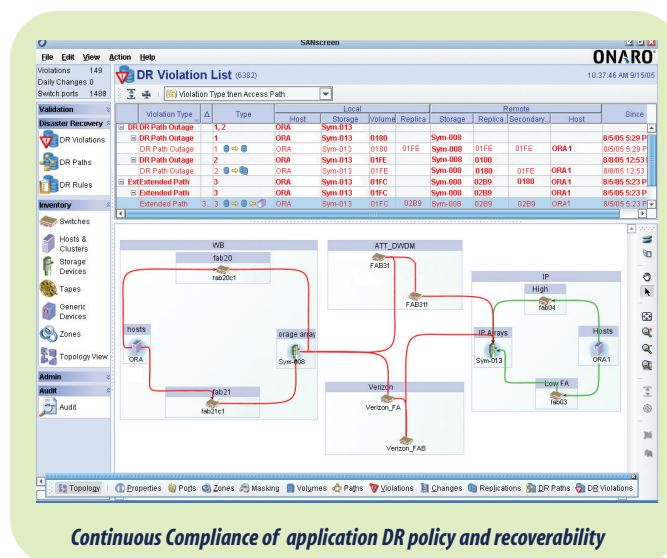
All discovered Configuration Items (CI) are stored in the CMDB as well as every change to any CI parameters or dependencies. SANscreen BC analyzes end-to-end DR paths from a production server through production and remote storage arrays to DR servers and stores the real-time DR path list and changes into the CMDB.

DR Policies

A centralized repository of DR policies for each application, including capacity, number of local and remote copies, remote servers etc. A policy wizard accelerates implementation.

Continuous Compliance Reports

Generates on-demand reports for DR policy compliance, Risk assessment, DR cost, DR tests etc.



Real-time Monitoring and Troubleshooting

Continuously reports on DR policy violations using email and SNMP alerts. Each violation indicates the affected server and the specific DR policy violation.

Troubleshooting Using Root-Cause Analysis

Root-Cause Analysis indicates the specific change that caused the violation and the optimal resolution to follow.

Change Audit

Records every array, volume, replication or fabric change and automatically analyzes its impact on DR path and policies.