IBM Global Technology Services
Data Sheet

IBM Resiliency Orchestration with Cyber Incident Recovery

Protecting data and configurations (applications, systems, devices) from cyber incidents with rapid recovery to minimize business impacts across hybrid environments

Highlights

- Heterogeneous support for hybrid, multiple-vendor environments
- Single dashboard for monitoring and management
- Improve RTO and RPO
- Intelligent workflows
- Software defined resiliency
- Complete lifecycle automation
- Build custom workflows using recovery automation library
- Standard and custom Compliance Reports

Key Features

- **Air-Gapped** access reduces risk of back-up corruption
- **Quick Recovery** reduces downtime and ensures best RPO
- Efficient **Point-In-Time** recovery with **Copy Data Management** technologies
- **Immutable Storage** for preventing corruption of back-up data

What is IBM Resiliency Orchestration?

IBM Resiliency Orchestration offers Disaster Recovery (DR) and Cyber Incident Recovery (CIR) monitoring, reporting, testing and workflow automation capabilities of complex hybrid IT environments in a scalable, easy-to-use solution built on industry standards. The offering combines automation and analytics for faster, more cost-effective DR and CIR to help keep daily business operations running. It can also help proactively avoid disruptions that can lead to lost revenue, brand damage and dissatisfied customers.

Why choose IBM Resiliency Orchestration?

Today's business environment has near-zero tolerance for service outages and disruptions. It can be a difficult balancing act to manage DR and CIR. This is complicated by a dispersed hybrid IT environment with cross-platform resource use and availability, scalability and performance requirements. The Resiliency Orchestration offering can simplify DR automation with real-time DR readiness validation that helps reduce DR test times and recovery time objectives (RTOs). The result: a more cost-effective DR experience that is smarter, more tailored and more agile than ever.

Solution advantages

With the Resiliency Orchestration solution, you can be more confident about your ability to recover from any outage, whether it's related to a disaster or an infrastructure failure. Implementing this solution helps your organization:

- Automate complex recovery for multiple-vendors physical and virtual environments
- Gain real-time insight into application data loss and recovery time
- Detect environment changes that cause recovery failure using dry-run capabilities
- Automate redundant, resource-intensive and costly DR processes
- Design recovery workflows to help meet service levels, recovery point objectives (RPOs) and RTOs
- Enables global recovery audit reporting and documentation

Solution highlights: IBM Resiliency Orchestration with Cyber Incident Recovery

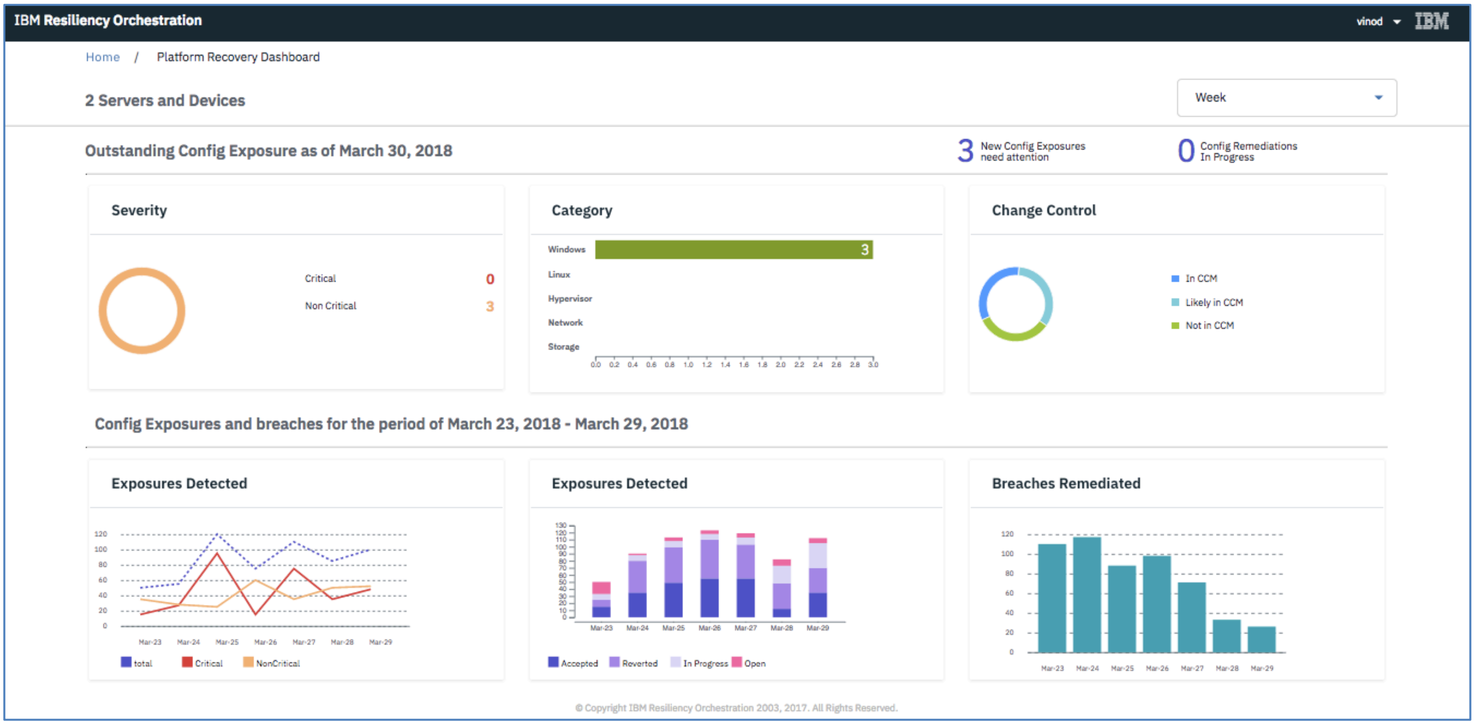
The number of cyberattacks and their business impact have grown significantly in recent years. Cyber breaches are no longer a question of "if" but "when".

The cost of a data breach is huge, breaches can result in financial loss, business disruptions, damage of reputation and can result in regulatory actions. Early detection of anomalies within the system can significantly reduce damages caused by breaches.

Addressing the quick recovery needs of applications and infrastructure to meet the always on requirement is challenging. Current DR/backup copies are vulnerable to corruption and are inadequate to handle a cyber outage. Continuous network exposure can cause corruption propagation to the DR sites, resulting in both primary and DR being unusable.

Cyber Incident Recovery

Cyber Incident Recovery, a capability of IBM Resiliency Orchestration, can enable quick recovery of platform configuration and data in the face of a cyber outage.



IBM Resiliency Orchestration

Home / Platform Recovery Dashboard

2 Servers and Devices

Week

Outstanding Config Exposure as of March 30, 2018

3 New Config Exposures need attention

0 Config Remediations In Progress

Severity

Critical	0
Non Critical	3

Config Exposures and breaches for the period of March 23, 2018 - March 29, 2018

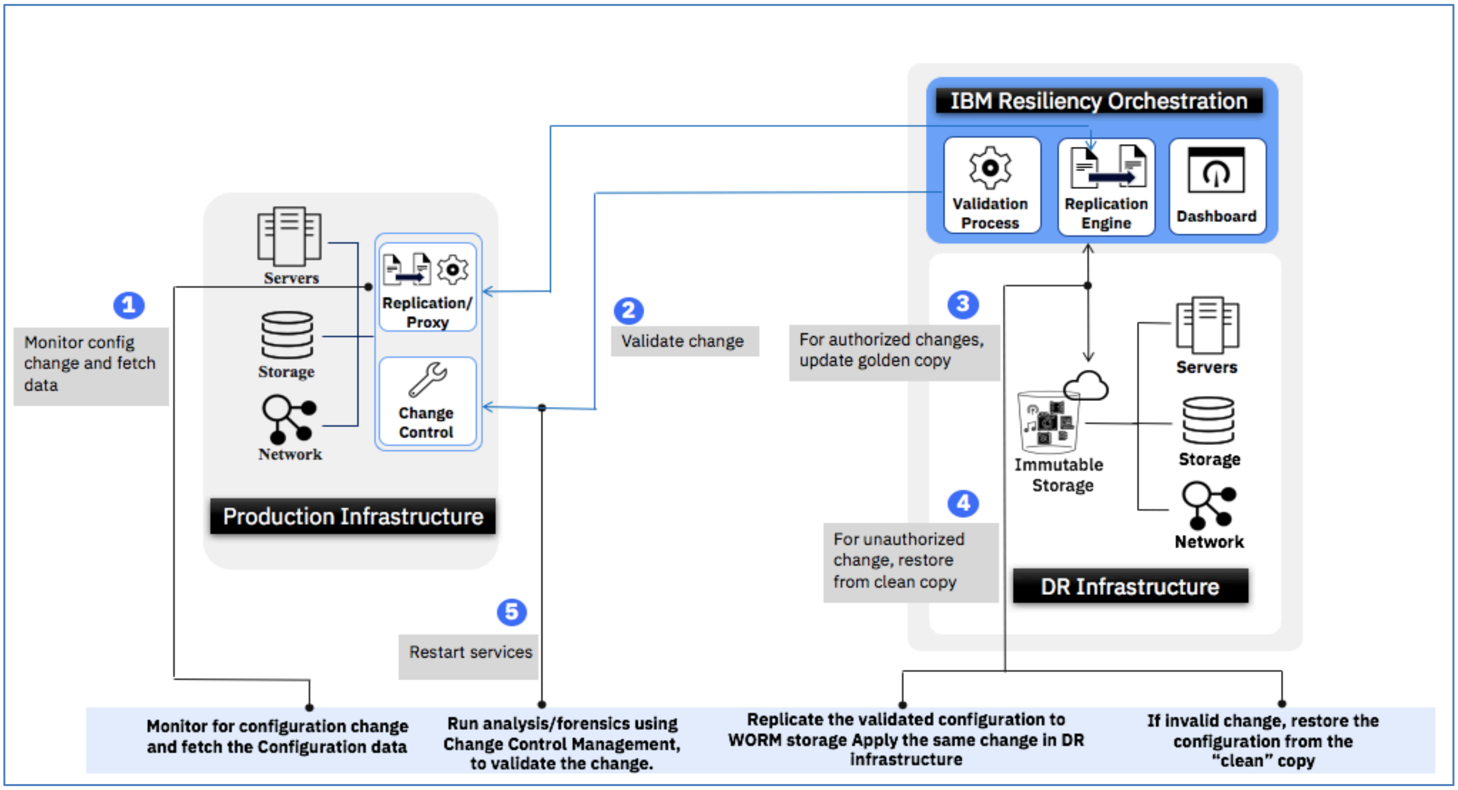
© Copyright IBM Resiliency Orchestration 2003, 2017. All Rights Reserved.

Cyber Incident Recovery Dashboard

Cyber Incident Recovery can recover critical production data and platform configurations rapidly in the aftermath of a cyber outage. Early detection of changes in the system enables faster recovery thereby reducing the business impact of cyber outage. Application aware recovery orchestration ensures that systems can be recovered rapidly. Immutable storage systems with "Write Once Read Many" (WORM) technologies help protect your data by not allowing changes once data is written, and by always writing a new version to reflect incremental changes. A validation framework enables verification that the data or configuration that is backed up is "clean" and recoverable. In addition, an audit trail proves veracity. Enabling air gaps ensures backed-up data is not accessible through the same network as production data, thus providing an additional layer of security. The solution also provides visibility and reporting into the process to help ensure compliance and audit readiness.

Cyber Incident Recovery for Platform Configuration

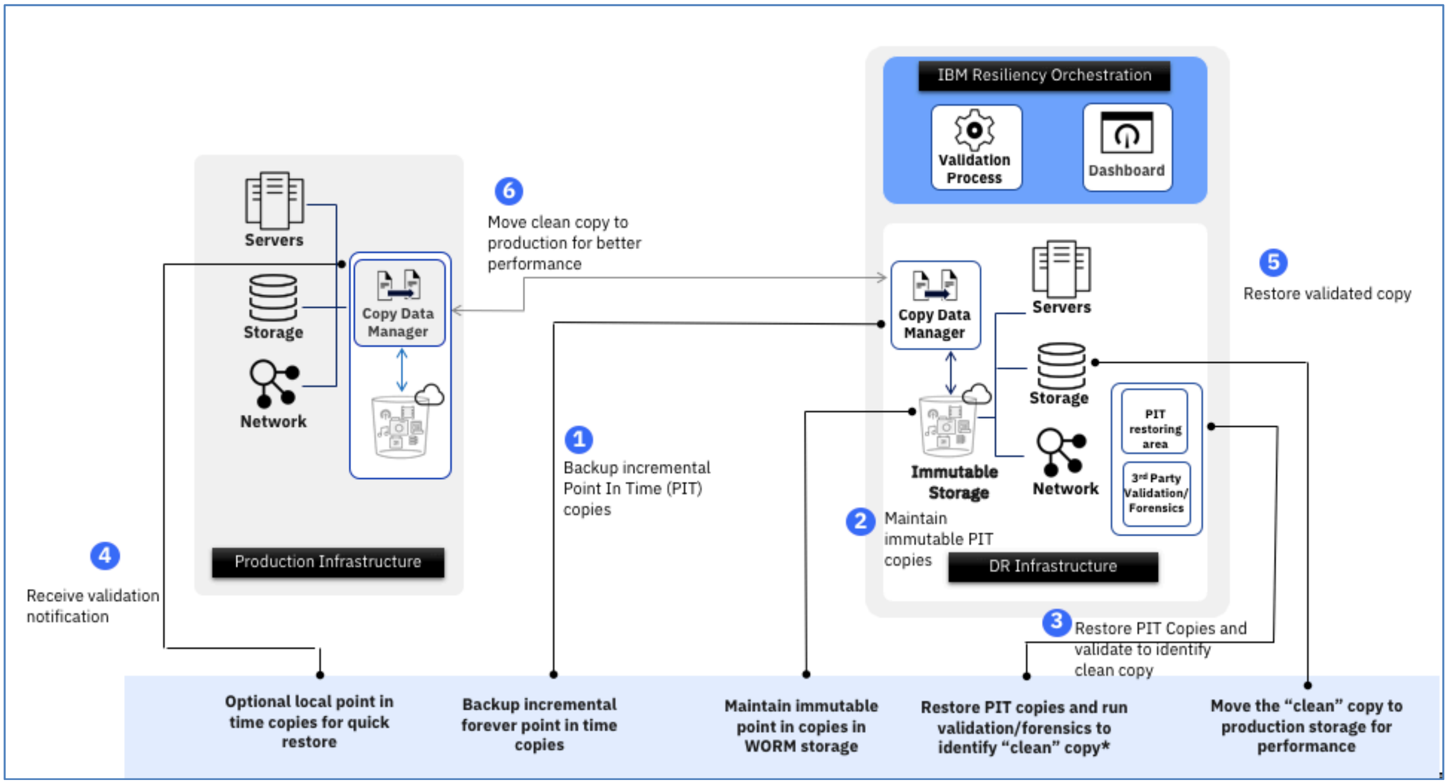
This feature enables recovery against cyberattacks that corrupt the configuration and alter the behaviour of data center platforms including network devices, storage devices and virtual or physical servers. It replicates the configuration data of these devices and servers with an air-gapped mechanism, into an immutable storage located in the DR site, and provides alerts when there is a suspicious change in configuration data and rapidly restores the original configuration to the impacted devices(s) or servers based on policies.


IBM Resiliency Orchestration
Validation Process
Replication Engine
Dashboard
Servers
Storage
Network
Replication/ Proxy
Change Control
Production Infrastructure
1
Monitor config change and fetch data
2
Validate change
3
For authorized changes, update golden copy
4
For unauthorized change, restore from clean copy
5
Restart services
Immutable Storage
Servers
Storage
Network
DR Infrastructure
Monitor for configuration change and fetch the Configuration data
Run analysis/forensics using Change Control Management, to validate the change.
Replicate the validated configuration to WORM storage Apply the same change in DR infrastructure
If invalid change, restore the configuration from the "clean" copy

Cyber Incident Recovery, Platform Recovery Solution

Cyber Incident Recovery for Data

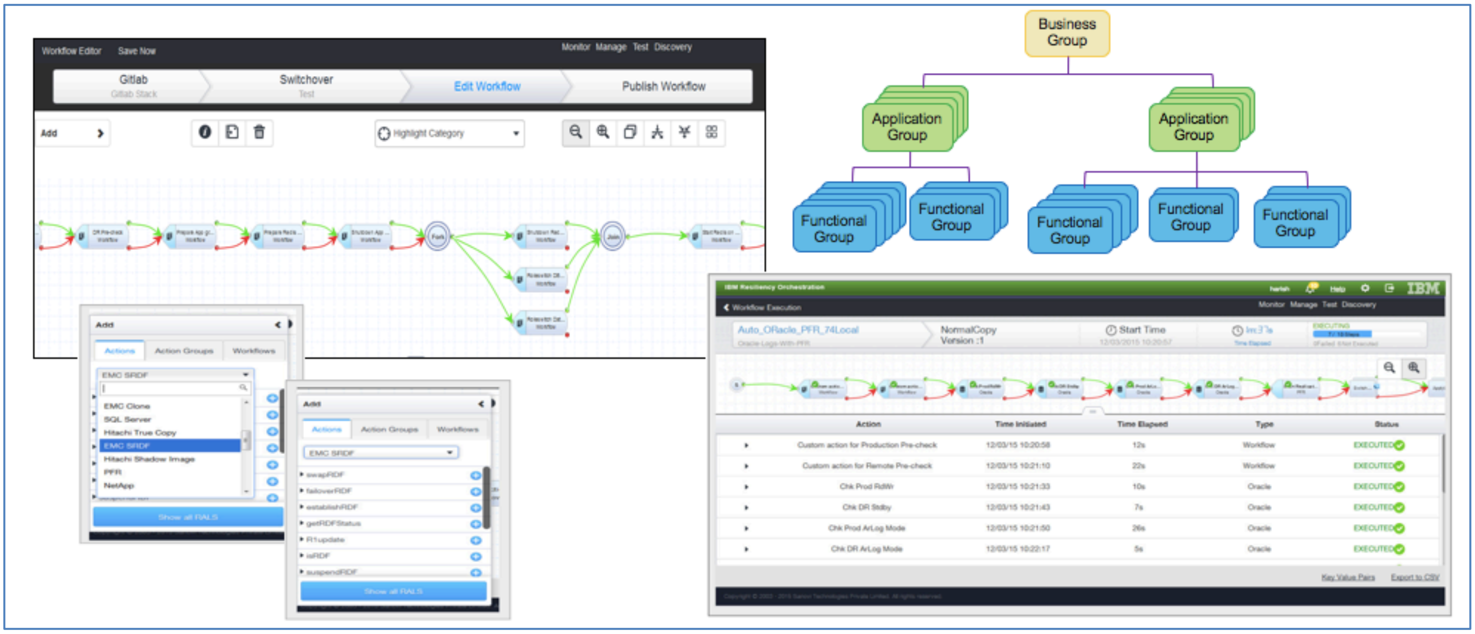
This feature enables recovery against cyberattacks that corrupt the data. It allows replication of the data from servers and storage using copy data management solutions, with an air-gapped mechanism, into an immutable storage located in the DR site of the customer and maintains multiple read-only PIT copies. When there is a cyber outage, it presents options to the user to select the appropriate copy to be restored and rapidly restores them on to DR compute infrastructure and DR storage infrastructure.


IBM Resiliency Orchestration
Validation Process
Dashboard
Servers
Storage
Network
Copy Data Manager
Production Infrastructure
6
Move clean copy to production for better performance
1
Backup incremental Point In Time (PIT) copies
Copy Data Manager
Servers
Storage
Immutable Storage
Network
PIT restoring area
3rd Party Validation/ Forensics
2
Maintain immutable PIT copies
DR Infrastructure
5
Restore validated copy
4
Receive validation notification
3
Restore PIT Copies and validate to identify clean copy
Optional local point in time copies for quick restore
Backup incremental forever point in time copies
Maintain immutable point in WORM storage
Restore PIT copies and run validation/forensics to identify "clean" copy*
Move the "clean" copy to production storage for performance

Cyber Incident Recovery, Data Recovery Solution

Enterprise solution built to support complete stack, heterogeneous technologies and hybrid environments

Across heterogonous systems for reliable, speedy and error-free recovery with powerful Recovery Workflow mechanism and 450+ pre-defined patterns



Action	Time Initiated	Time Elapsed	Type	Status
Custom action for Production Pre-check	12/03/15 10:20:58	12s	Workflow	EXECUTED ✓
Custom action for Remote Pre-check	12/03/15 10:21:10	22s	Workflow	EXECUTED ✓
Chk Prod RdWr	12/03/15 10:21:33	10s	Oracle	EXECUTED ✓
Chk DR Stdby	12/03/15 10:21:43	7s	Oracle	EXECUTED ✓
Chk Prod ArLog Mode	12/03/15 10:21:50	26s	Oracle	EXECUTED ✓
Chk DR ArLog Mode	12/03/15 10:22:17	5s	Oracle	EXECUTED ✓

Benefits of Cyber Incident Recovery

With Cyber Incident Recovery, you can be more confident about your ability to recover from cyberattacks and outages. Some of the key benefits include

- Significantly reduces impact of breach
- High reliability and scalability
- Ease of management through single console
- Air gap and Immutable storage for preventing data corruption
- Reduced operational expense (OPEX)

Why IBM?

- Nearly 60 years of experience helping clients worldwide with their backup and recovery needs
- Over 9,000 customers protected by our disaster recovery and data management services
- Leading data protection provider: 3.5+ Exabyte's of data backed up annually and under management
- More than 385 IBM Resiliency Centers in 68 countries around the globe providing managed disaster recovery and data protection
- Over 6,000 global professionals dedicated to Resiliency

For more information:
To learn more about IBM Cyber Incident Recovery, please contact your IBM representative or IBM Business Partner, or visit the following website: **ibm.com**/marketplace/disaster-recovery-orchestration

Additionally, IBM Global Financing provides numerous payment options to help you acquire the technology you need to grow your business. IBM provides full lifecycle management of IT products and services, from acquisition to disposition. For more information, visit: **ibm.com**/financing

3039 Cornwallis Rd., Bldg. 201 Research Triangle Park, NC 27709

Produced in the United States of America July 2018

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

The performance data discussed herein is presented as derived under specific operating conditions. Actual results may vary.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT.

IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client follows any law or regulation

Please Recycle