Solution Brief

Industry: Cloud and Security
Solution: Resilience Orchestration
Solution components: Cyber Recovery

Integration of IBM Resiliency Orchestration with Cyber Incident Recovery

Learn more at: ibm.com/services

IBM

Introduction

Today, organizations are increasingly vulnerable to cyber attacks that are designed to cripple businesses or permanently destroy IT systems. Such attacks can not only disrupt your business operations, but also dent your brand reputation and result in financial consequences.

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

Key Solution Highlights

- Air-gapped Protection - Network isolation separates the secured replicated storage
- Immutable Storage - Uses WORM technology to prevent corruption, overwrites and deletion of data
- Data Verification - Ensures that backed up configurations and data are clean and recoverable
- Automation and Orchestration - Enable rapid restoration of systems and data by replacing manual processes with predetermined workflows
- Regulatory Reporting and Assurances - Single dashboard and rich reporting for compliance requirements

Benefits of IBM RO with IBM CIR

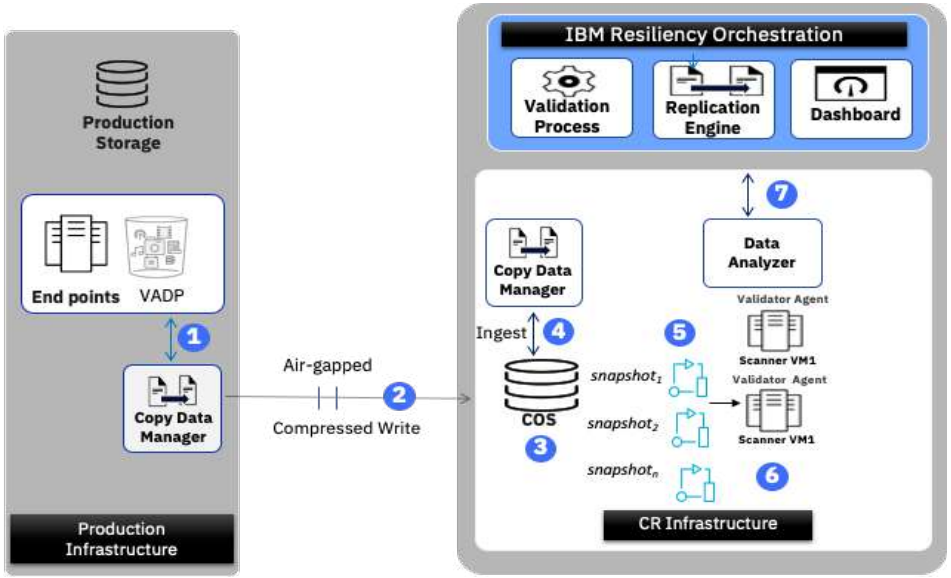
With Cyber Incident Recovery, you can be more confident about your ability to recover from cyberattacks and outages.

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)

CIR for Data Solution

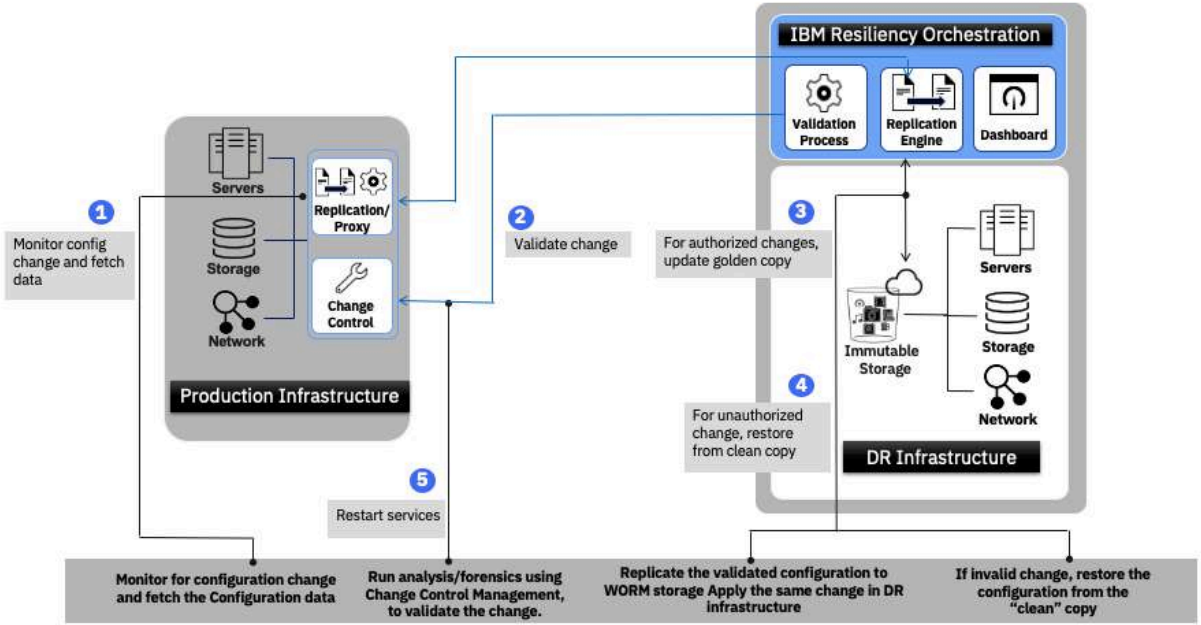
1. Copy Data manager captures discovery from endpoint
2. Backup point in time copies directly to immutable Storage
3. Maintain immutable point in time copies in WORM storage
4. MetaData Ingest from immutable storage by copy data manager for captured images
5. Mount snapshots into scanner VM into Clean Room
6. Perform anomaly scanning on mounted snapshots
7. Send scan results & raise alerts to notify user
8. Mark Snapshots as verified/verification failed



This CIR capability 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 Cyber site of the customer and maintains multiple read-only PIT copies.

The PIT copies are scanned periodically scanned for any anomaly. 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 CR compute infrastructure and CR storage infrastructure.

CIR for Platform Configuration Solution



This CIR capability enables recovery against cyber attacks 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 Cyber Recovery Solution functions

CIR for Data Solution

- Cyber protect the endpoints data through Copy Data Management (CDM) into an immutable storage and in an air-gapped environment
- Detection of anomalies in data through anomaly detection tool
- Clean Room provisioning for perform scanning, analytics, and testing of cyber data
- Rapid recovery of clean copies onto Cyber infrastructure
- Quick restore of clean copies onto production infrastructure optionally
- Ability to customize the validation workflow to enable user to add any 3rd party validation tool
- Highly customizable solution and flexible solution to support diverse environments
- Provide visibility and reporting into the process to ensure compliance and readiness

CIR for Platform Configuration Solution

- Cyber protect the configurations of network devices, storage, servers to avoid widespread
- Identify any anomaly in platform configuration by comparing the configuration against the golden copy
- Rapid restore of configurations onto production infrastructure incase the configuration change not authorized
- Protect configuration golden copies in air-gapped and immutable environment
- Easy testing capability to test the solution frequently without impacting production
- Provide visibility and reporting into the process to ensure compliance and readiness
- Shipped with default platform configuration files with the ability to add files on-demand

Cyber Vault integrated with orchestrated Cyber Incident Recovery solution

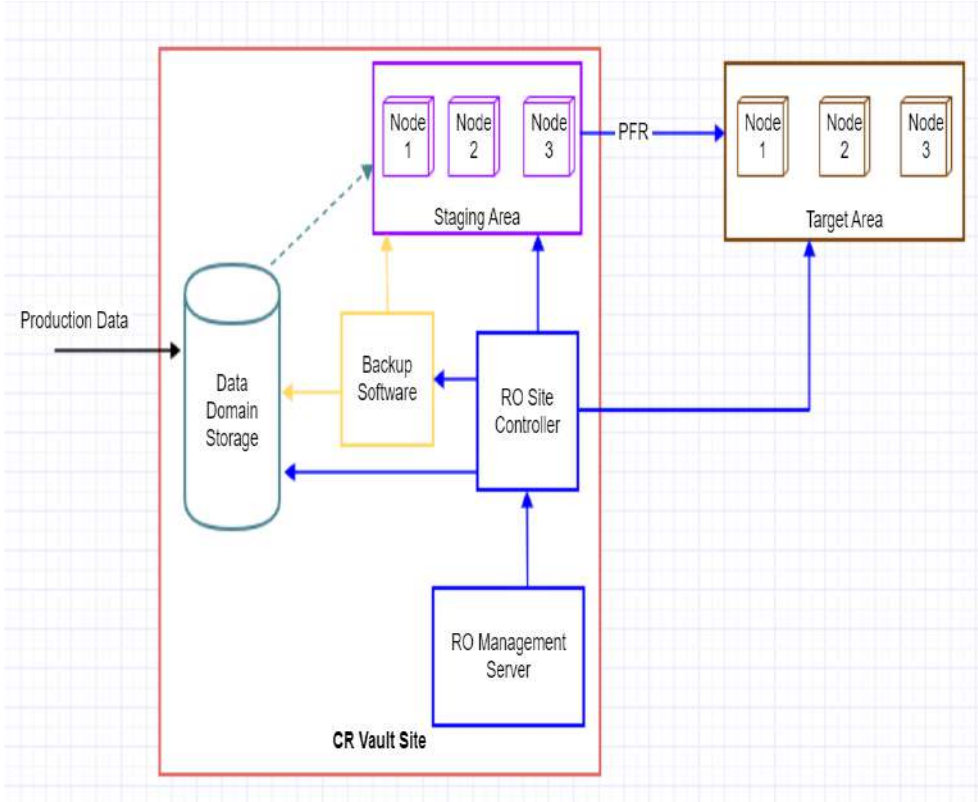
CIR using Cyber Vault:

The CRVault solutionenables enterprises to protect theirmission critical data by quickly recovering from cyber-attacks.

The CR Vault solution is provisioned on top of Data Domain (DD) storage. The Protected endpoints are periodically backed up by a traditional backup/recovery software into the production data domain which in-turn is replicated into the remote Data Domain located in Cyber Vault site. The replication between Production and Vault DD is disabled when replication is not in use hence giving an ability to airgap the vault from the production site.

Within the CR Vault, the backup software creates point-in-time (PIT) retention-locked copies that can be validated and then used for recovery of the production system. In case of disaster, recovery will be triggered by selecting the protected snapshots available in CR Vault.

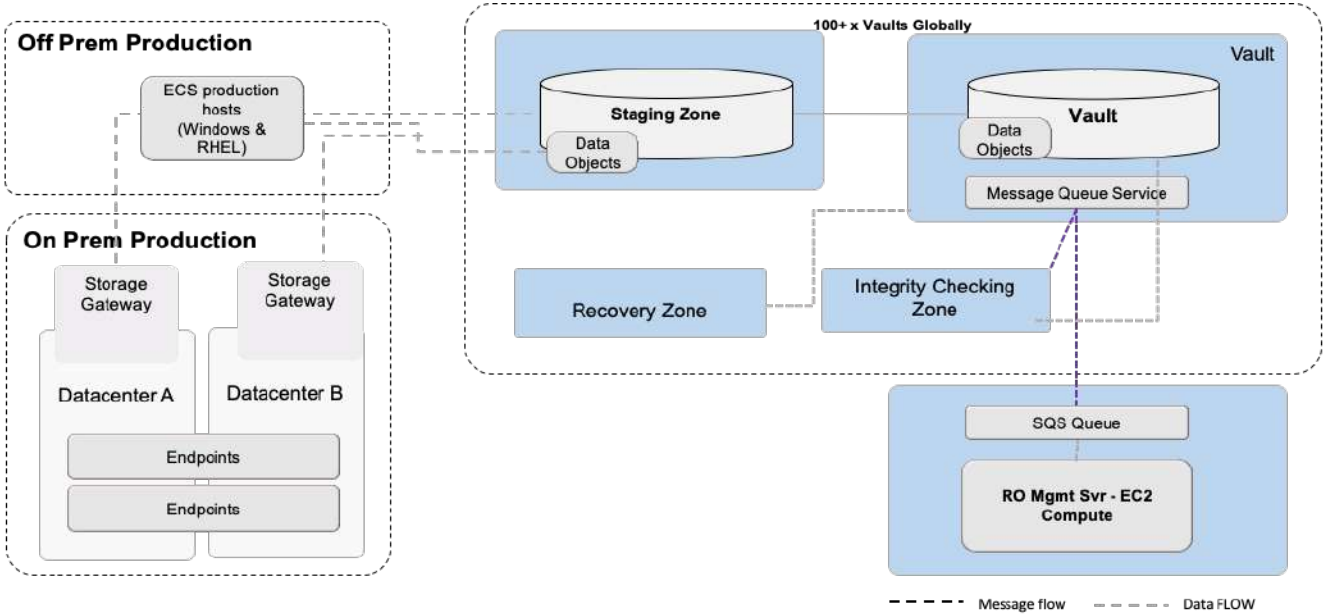
The solution entails the integration of IBM Resiliency Orchestration with CR Vault to enable user to perform file level recovery operation without having a direct interface with the protected endpoints. At the same time user can also monitor the on-going Data Domain replication health status.



Cyber Incident Recovery in AWS vault through AWS message Queues

CIR using AWS Vault:

IBM Resiliency Orchestration is integrated into the Cyber integrity solution by leveraging message queue service. There are inbound messages into Resiliency Orchestration to capture the details of snapshots of protected endpointsavailable in AWS vault. The SLAs are determined by monitoring the flow of inbound messages into IBM Resiliency Orchestration. In case of cyber outage, IBM Resiliency Orchestration provides user to select any of the monitored snapshots to trigger recovery. On execution of recovery process, IBM will send a message into message queue service to initiate recovery of selected snapshot from AWS vault into recovery zone.



Interoperability – CIR for Data

Cyber data Solution Signature	Supported Versions of the OS and Platforms	Supported Anomaly detection Tool	Supported Versions Protection Scheme (Replication)	Supported Modules						
				Cyber Recovery Monitor				Cyber DR Drill	Recovery Orchestration	Provisioning
				Cyber RPO	Cyber RTO	Data lag	Replication Monitoring			
Cyber Incident Recovery for Data with Actifio	VMware 6.0,6.5	Tripwire Enterprise Manager (8.7.2) for Linux Workloads Tripwire Enterprise Agent or Scanner VM RHEL 7.5, CentOS 7.5 Windows 2016/2012	Actifo version: 8.1.5 and above	☑	☑	☑	☑	☑	☑	☑
Oracle Full Database protection with Actifio	RHEL 7.5 (x86 64 bit), AIX 7.1/7.2 Oracle Full Database 11g [Note1] (64 bit) 12c (64 bit)	Tripwire Enterprise Manager (8.7.2) for Oracle on Linux only	Actifo version: 8.1.5 and above	☑	☑	☑	☑	☑	☑	☑
Cyber Recovery using AWS Vault	AWS message queue service AWS immutable vault	Not Applicable	Customer scripts will be used for the replication (Not part of RO solution)	☑	☑		☑		☑	☑
Cyber Recovery using Cyber Vault	Cyber Recovery v19.4, Avamar v18.2, Data Domain v6.2 Python 3	Windows/Linux files VMware VMDK backed up images	PFR 8.1				☑	☑	☑	

RO & Components supported Platforms			
Server and Components	O/S Platform	D/B Platform	Web Server
IBM Resiliency Orchestration Server	RHEL 7.5, 7.6, 7.7	MariaDB 10.2.27	TOMCAT 9.0.27
	RHEL 8.0	MariaDB 10.3.20 AWS RDS MariaDB 10.3.20	TOMCAT 9.0.27
Site Controller	RHEL 7.5,7.6, 7.7, 8.0 Windows 2012, Window 2016		

Interoperability – CIR for Platform

CR Platform Solution Signature	Supported Versions of the OS and Platforms	Supported Configurations	Supported Versions dependent components	Supported Modules					
				Cyber Recovery Monitor			Cyber DR Drill	Recovery Orchestration	Provisioning
				Config Monitoring	Change detection	Config Recovery			
Stateless Application with AWS (*For Cyber platform only)	Windows 2012 R2 Windows 2016	File in plain text and Registry Key	Windows 2012,2016 Staging Server	☑	☑	☑		☑	☑
Stateless Application with AWS (*For Cyber platform only)	SUSE Linux Enterprise server 11 SP4 RHEL 7.x CentOS 7.x	For Linux - Plain Text files	Linux : RHEL 7.x, CentOS 7.x Staging Server	☑	☑	☑		☑	☑
Stateless Application with AWS (*For Cyber platform only)	IBM AIX 7.x	For AIX - Plain Text files	Linux : RHEL 7.x, CentOS 7.x Staging Server	☑	☑	☑		☑	☑
Storage Device (*For Cyber platform only)	Storage: IBM DS8000 Series Version 8 Release 3 CLI	DS8K: IPSEC		☑	☑	☑		☑	☑
Network Device (*For Cyber platform only)	Virtual Switch : VMware VDS	Switch plain text config files	Linux : RHEL 7.x, CentOS 7.x Staging Server	☑	☑	☑		☑	☑
Network Device (*For Cyber platform only)	Ansible supported network devices Currently certified for Cisco catalyst switch and Juniper vSRX series	Running configuration	Ansible 2.9.6 with Python 3.6.8	☑	☑	☑		☑	☑

RO & Components supported Platforms			
Server and Components	O/S Platform	D/B Platform	Web Server
IBM Resiliency Orchestration Server	RHEL 7.5, 7.6, 7.7	MariaDB 10.2.27	TOMCAT 9.0.27
	RHEL 8.0	MariaDB 10.3.20 AWS RDS MariaDB 10.3.20	TOMCAT 9.0.27
Site Controller	RHEL 7.5,7.6, 7.7, 8.0 Windows 2012, Window 2016		

Learn more

Find out how IBM Resiliency Orchestration increases flexibility by providing built-in block replication capabilities to replicate virtual machines within any cloud that is based on VMware's virtualization technology.

For more information on Resiliency Block Replicator, go to: ibm.com/services

Financing Available: IBM Global Financing provides numerous payment options to help you acquire the technology you need to grow your business. For more information, visit: ibm.com/financing.

[Business Unit Name], New Orchard Road Armonk, NY 10504.
Produced in the United States of America, May 2020.