IBM Resiliency Orchestration with Cyber Incident Recovery

Protect data and platform configurations with a purpose-built capability for fast, reliable and scalable recovery from cyberattacks

Highlights

- Air-gapped immutable storage for data and platform configuration files
- Quick detection of anomalies within the Windows or Linux system configurations, including Windows registry, application configurations and device configurations
- Fast, orchestrated restoration of data and platform configurations helps to reduce the impact of disruption caused by a cyberattack or any other outage
- Automated testing and verification platform enables frequent testing without impacting business systems
- Visibility into the process and reporting help address compliance requirements.

Cyberattacks continue to plague organisations of all sizes. While IT security teams are getting better at preventing cyberattacks from happening, attacks remain a matter of 'when' one will occur (if it hasn't already) rather than 'if' it will happen. A business disruption caused by cyberattacks corrupting your critical data and configurations of your systems can be as damaging to an organisation's financial well-being and reputation as data theft or a complete IT outage.

This can be especially true when cyberattacks involve data encryption or malware specifically targeting data backups. Continuous network exposure to backup and disaster recovery (DR) locations can allow malware the opportunity to corrupt or encrypt this data, leaving both primary and backup data unusable, significantly delaying the ability to regain production-level operations.

Often the damage occurs because existing DR solutions are not designed to recover from cyber events or are plagued by persistent problems facing DR capabilities: over-reliance on manual processes, outdated runbooks and inadequate testing. The result is that recovery takes too long, the data recovery points are too old, or the recovery itself fails.

A capability purpose-built for cyber resilience

Cyber Incident Recovery, powered by IBM® Resiliency Orchestration, is designed to recover data and platform configurations very quickly in the event of a cyber outage. Purpose-built for cyber recovery, Cyber Incident Recovery offers:

- Easy testing capability that does not impact production environments
- Faster detection of data corruption and quick response to reduce downtime
- Efficient point-in-time recovery that optimises recovery point objectives (RPO)
- Scalability to handle large, site-level detection and recovery in minutes
- Simplified visibility and reporting to help address regulatory requirements.

The technology building blocks that make up the Cyber Incident Recovery capability provide a platform that spans compute and data layers of both production and DR environments to enable an agile approach to recovery from a cyber disaster. This architecture includes:

Immutable storage. Using unalterable storage technology for configuration data or write-once-read-many (WORM) storage for application data helps prevent corruption and ensure recoverability by not allowing changes to be made to backups once they are saved. For application data, this approach also helps reduce storage costs by only writing new copies of point-in-time incremental changes.

Air-gapped protection. Network isolation separates production environments from the WORM storage that contains the protected, backed-up data at a remote or DR site. Access to the WORM storage is also restricted to only those times when data is available to backup. This approach, combined with immutable storage, helps prevent protected data from being corrupted by malware that can traverse networks or that is designed specifically to target backup data.

Configuration data verification. This component helps ensure the configuration or data being protected is clean and recoverable. This process, built into Resiliency Orchestration, will automatically detect when your system configurations have been modified and do not match the 'golden' versions. Resiliency Orchestration will also integrate with client-provided application validity scripts to provide application- and data-level testing.

Automation and orchestration. By automating the end-to-end (E2E) recovery process for data, applications, switches and compute infrastructure, Resiliency Orchestration enables quick restoration of your IT environment. Resiliency Orchestration replaces the traditional manual processes with pre-determined workflows that have been tested and validated, allowing you with the click of a button to recover an entire business process, application, database or discrete system. These workflows orchestrate the multiple steps required to recover interconnected systems and data, limiting human error. Resiliency Orchestration helps speed solution implementation by leveraging an extensive library of more than 450 predefined patterns that can be combined to build workflows.

Cyber Incident Recovery for platform configuration

Doing business around the clock requires continuous availability of the IT infrastructure underlying business-critical applications: physical servers, VM instances, storage systems and network devices. Cyber attackers can bring business to a standstill by corrupting the configuration data of these platforms.

The platform configuration feature of Cyber Incident Recovery (see Figure 1) enables fast restoration of services by replicating a 'golden copy' of server and device configuration data to air-gap protected immutable storage in a cloud object storage or IBM data centre. Production devices are examined to detect changes in the configuration data. The system analyses the change to determine whether it is valid and provides alerts when it detects a suspicious change in the configuration data. The alerts can also provide relevant tickets from change control management software.

IBM Global Technology Services
Solution brief

IBM Business Resiliency Services

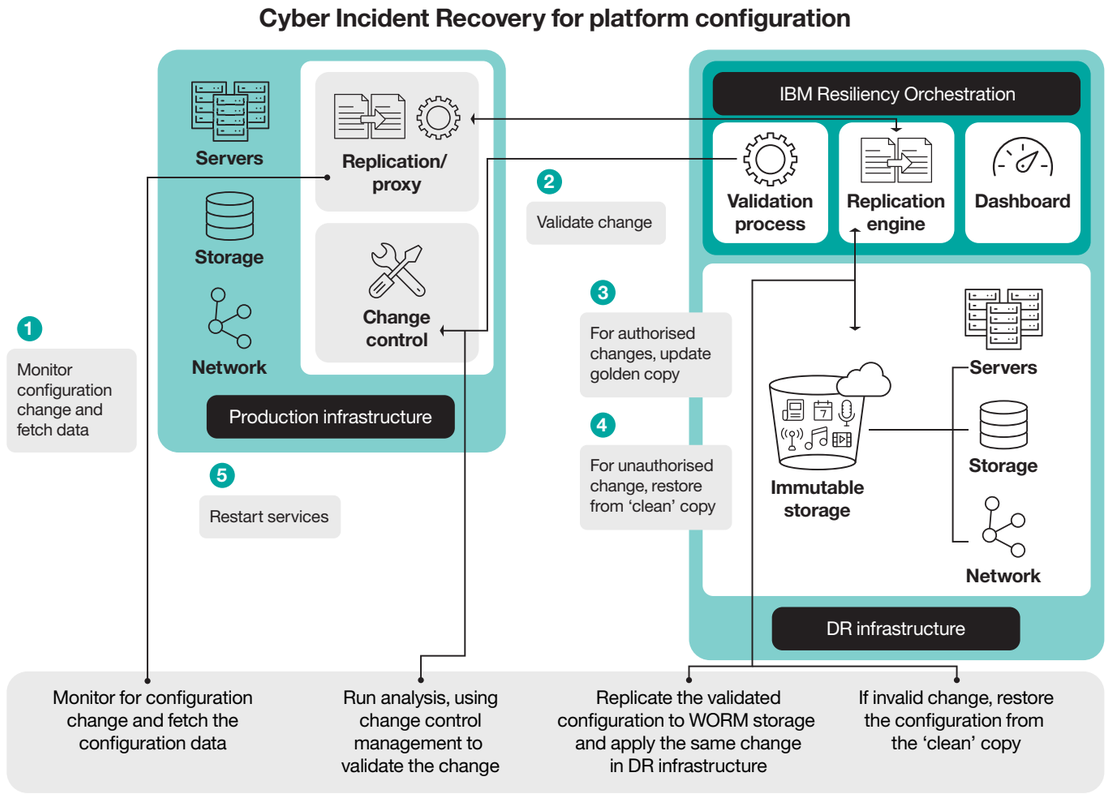

Figure 1. Cyber Incident Recovery for platform configuration helps protect configuration data of physical and virtual servers as well as storage and network devices.

In the case of a valid change, configuration data is protected by replication of a new 'golden copy' to immutable storage. If an invalid change is identified, the latest clean copy of device configurations is quickly restored to the production infrastructure by Resiliency Orchestration, based on pre-established policies and with the appropriate management consent. Dedicated and virtual machine configurations are restored onto a clean production infrastructure.

Cyber Incident Recovery for data

The data feature of Cyber Incident Recovery enables highly reliable, fast recovery against cyberattacks that corrupt the data itself. It protects data through the use of air-gapped protection and immutable storage while orchestrating fast recovery at the client's DR site.

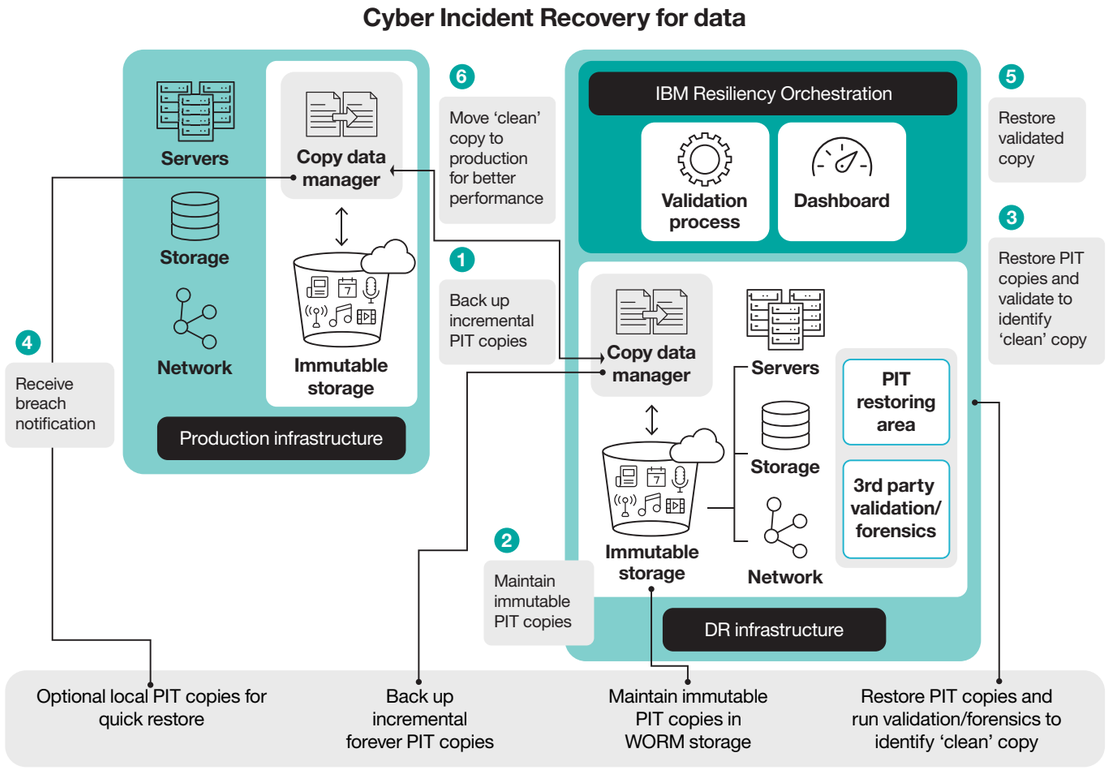

Figure 2. Cyber Incident Recovery for data provides efficient backup of large volumes of data with non-disruptive testing and quick restoration.

Cyber Incident Recovery is designed to handle large volumes of application data. It employs copy data management technology to create and maintain incremental point-in-time (PIT) copies of data. Because these copies are kept on immutable storage like cloud object storage or storage with WORM capability, they are 'forever' copies that cannot be changed. As shown in Figure 2, copy data management software replicates data to a DR or alternate site, creating the PIT copies. Optionally, PIT copies can also be made and stored at the production site for quick restore capability.

When a DR manager receives notification that a data breach or an encryption malware infection has been discovered, automated testing of PIT copies is performed at the DR site to verify the recoverability of the data. The latest 'clean' copy identified by the testing and verification process is then recovered on the DR infrastructure by the copy data manager software's fast recovery process. Testing can also be conducted frequently at the DR site, helping to ensure recoverability of data without impacting business operations. Resiliency Orchestration helps ensure that platforms can be recovered quickly, in parallel.

IBM Global Technology Services
Solution brief

IBM Business Resiliency Services

Dashboards and reporting simplify management

Cyber Incident Recovery includes a dashboard feature (see Figure 3) that helps in monitoring platform configuration changes and data changes. It can also provide real-time critical cyber recovery updates to senior management or the board of directors, enabling them to make informed decisions quickly.

Figure 3. Central dashboard

A cyber incident dashboard provides details such as the number of vulnerabilities and severity level and enables tracking of open vulnerabilities. A cyber data dashboard provides visibility into cyber RPO deviation, cyber RTO deviation, snapshot validation status and current cyber readiness.

The built-in reporting module offers a rich set of reports, including cyber resilience or DR posture, which can be exported and shared with regulators for compliance purposes, along with charts captured during normal business operations.

Why IBM?

IBM Business Resiliency Services has nearly 60 years of experience helping clients worldwide with their backup and recovery needs. Today, over 9,000 customers are protected by our DR and data management services, and we have more than 3.5 exabytes of data backed up annually and under our management. More than 300 IBM Resiliency Centres in more than 60 countries around the globe provide managed DR and data protection, and over 6,000 global IBM professionals are dedicated to resiliency.

For more information

To learn more about Cyber Incident Recovery, please contact your IBM representative, or visit the following website:
ibm.com/services/business-continuity/cyber-resilience

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

IBM United Kingdom Limited
PO Box 41, North Harbour
Portsmouth, Hampshire PO6 3AU
United Kingdom

IBM Ireland Limited
Oldbrook House
24-32 Pembroke Road
Dublin 4

IBM Ireland registered in Ireland under company number 16226

Please Recycle

89017289GBEN-02