kyndryl

Resiliency Orchestration with Cyber Incident Recovery

Purpose-built cyber resilience for fast, reliable and scalable recovery in hybrid multicloud environments

Contents

You might be overdue for a change

The more your data and applications traverse an increasingly interconnected infrastructure of on-premises, public cloud and multicloud environments, the more ways cyberattackers can disrupt the continuity of your business. The complex nature of hybrid multicloud environments exposes your critical data and system configurations to higher levels of risk than ever before, so much so that the likelihood of a successful cyberattack has become an absolute certainty. No matter how vigilant your IT security team may be, a cyberattack will eventually lead to a business disruption in the form of an outage, data theft or data corruption—causing reputational damage and financial fallout.

In the not-too-distant past, traditional disaster recovery solutions could be counted on to help mitigate the damage of most conventional cyberattacks. But that was long before hybrid multicloud environments were a reality. While IT infrastructures have grown in complexity, cyberattackers have grown more sophisticated, too. Data encryption and malware attacks are now being designed to target data backups in ways that were once unimaginable. As a result, these attacks are gaining access to backup and disaster recovery locations, leaving both primary and backup data unusable and significantly delaying the ability to restore production-level operations.

Kyndryl Resiliency Orchestration with Cyber Incident Recovery minimizes the business impact of cyberattacks with its fast, reliable and scalable recovery across hybrid multicloud environments.

Purpose-built cyber recovery for a hybrid multicloud world
Kyndryl™ Resiliency Orchestration with Cyber Incident Recovery can recover your data and platform configurations at rapid speed in the event of a cyber outage. It provides intelligent automation of data protection and disaster recovery workflows, and enables recovery testing, data immutability, anomaly detection, monitoring, management and reporting across hybrid multicloud environments. The solution delivers automated, reliable and fast recovery of physical and virtual workloads, including business processes, applications, systems and databases from cyberattacks.

Cyber Incident Recovery provides:

- 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 optimizes recovery point objectives (RPOs)
- Scalability to handle large, site-level detection and recovery in minutes
- Simplified visibility and reporting to help address regulatory requirements

Kyndryl Resiliency Orchestration with Cyber Incident Recovery delivers automated, reliable and fast recovery of physical and digital workloads from cyberattacks.

An architecture that enables an agile approach to cyber resilience

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 disaster recovery environments. This enables an agile approach to recovery across your virtual and physical workloads.

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 your 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 disaster recovery (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.

Anomaly detection
Kyndryl Resiliency Orchestration includes an anomaly detection capability that uses rule-based heuristic identification, augmented by artificial intelligence (AI). It is trained on different change patterns of known malware, captures and compares the change patterns in backed up data to predict the data anomalies with high accuracy. This anomaly detection capability at the DR site will help identify anomalous backed up snapshots and restore from clean copies.

Configuration data verification
This component uses the in-built, AI-based anomaly detection capability to help ensure the configuration or data being protected is clean and recoverable. The process, built into Resiliency Orchestration, will automatically detect when your system configurations have been modified. 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 recovery process for data and applications, 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 to recover an entire business process, application, database or discrete system with the click of a button. 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 800 predefined patterns that can be combined to build workflows.

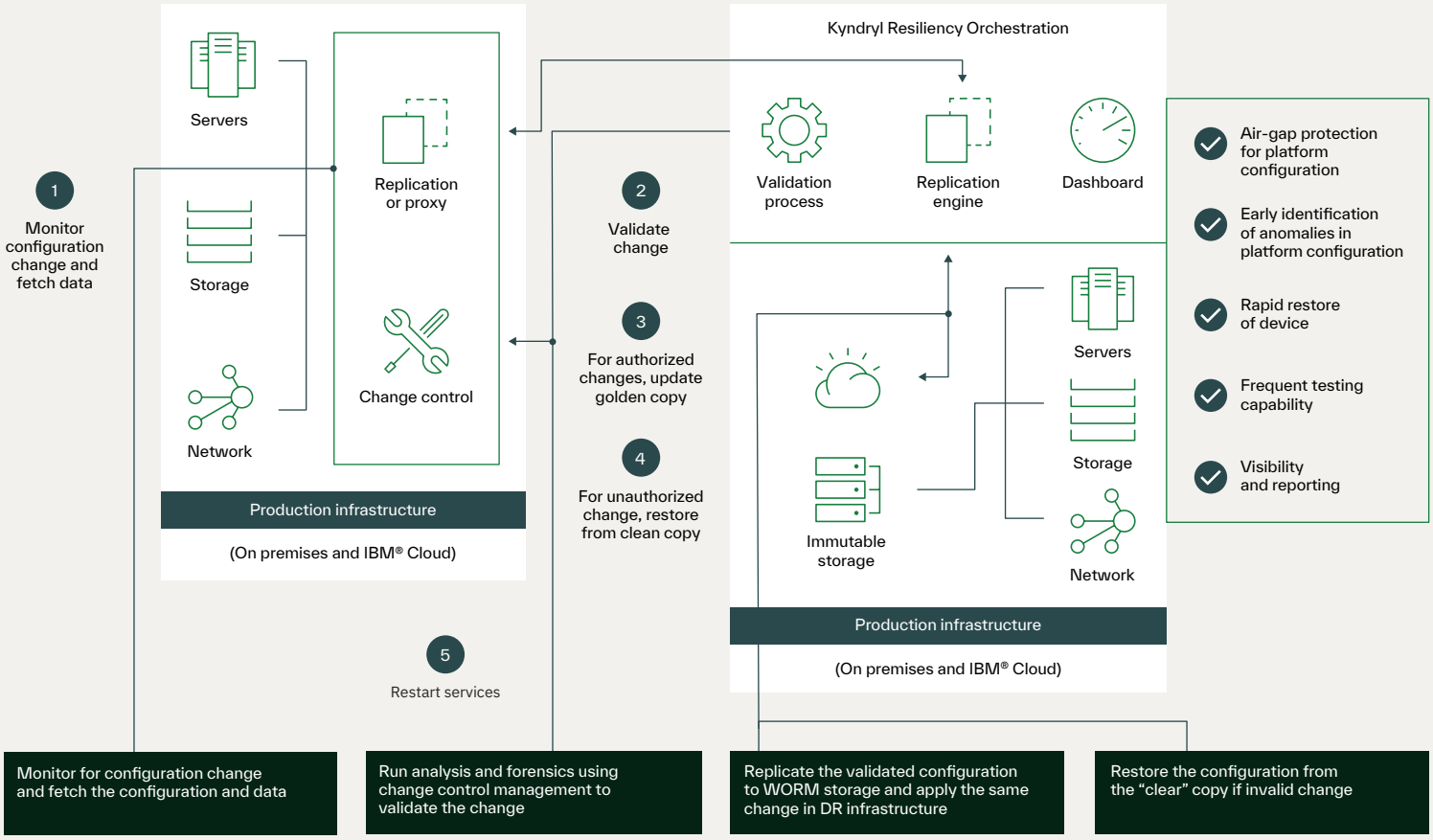
Cyber Incident Recovery for platform configuration

Malware often alter the configurations before corrupting the data itself, so it is critical to detect any configuration changes before the actual data becomes infected. The platform configuration feature of Cyber Incident Recovery protects configuration data of virtual and physical workloads, applications, storage systems and network devices across on-premises, public cloud, hybrid cloud and multicloud environments.

Keeping business going with a "golden copy"
This component uses the built-in technologies to identify any change in production endpoint configurations and alerts the user for any authorized and unauthorized change. The alerts can also provide relevant tickets from change control management software. To enable fast restoration of services, Cyber Incident Recovery replicates a "golden copy" of server and device configuration data to air-gap protected immutable storage.

Responding to invalid and valid configuration changes
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. In case of valid changes, a new "golden copy" is created in an immutable storage.

Kyndryl Cyber Recovery as a Service
Cyber Incident Recovery for Platform Configuration



*Air-gap not supported for immutable storage hosted on cloud

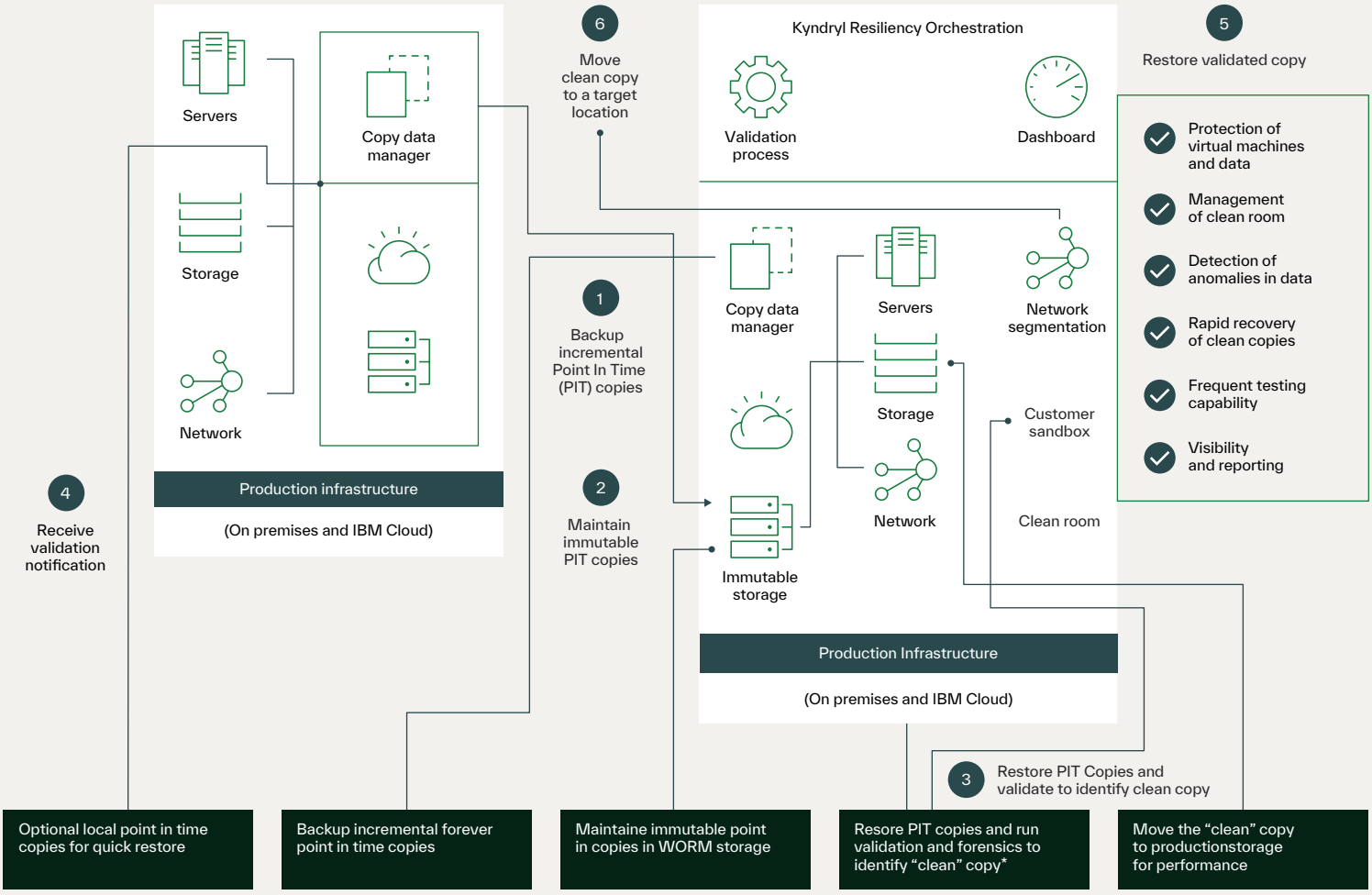
Cyber Incident Recovery for data

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 disaster recovery site.

Protecting large volumes of data across every environment
Cyber Incident Recovery is designed to handle large volumes of application data, no matter where that data lives. 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're "forever" copies that cannot be changed. Copy data management software replicates data to a disaster recovery or alternate site, creating the PIT copies. PIT copies can also be made and stored at the production site for quick restore capability.

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

Kyndryl Cyber Recovery as a Service
Cyber Incident Recovery for Data



Dashboards and reporting that simplify management

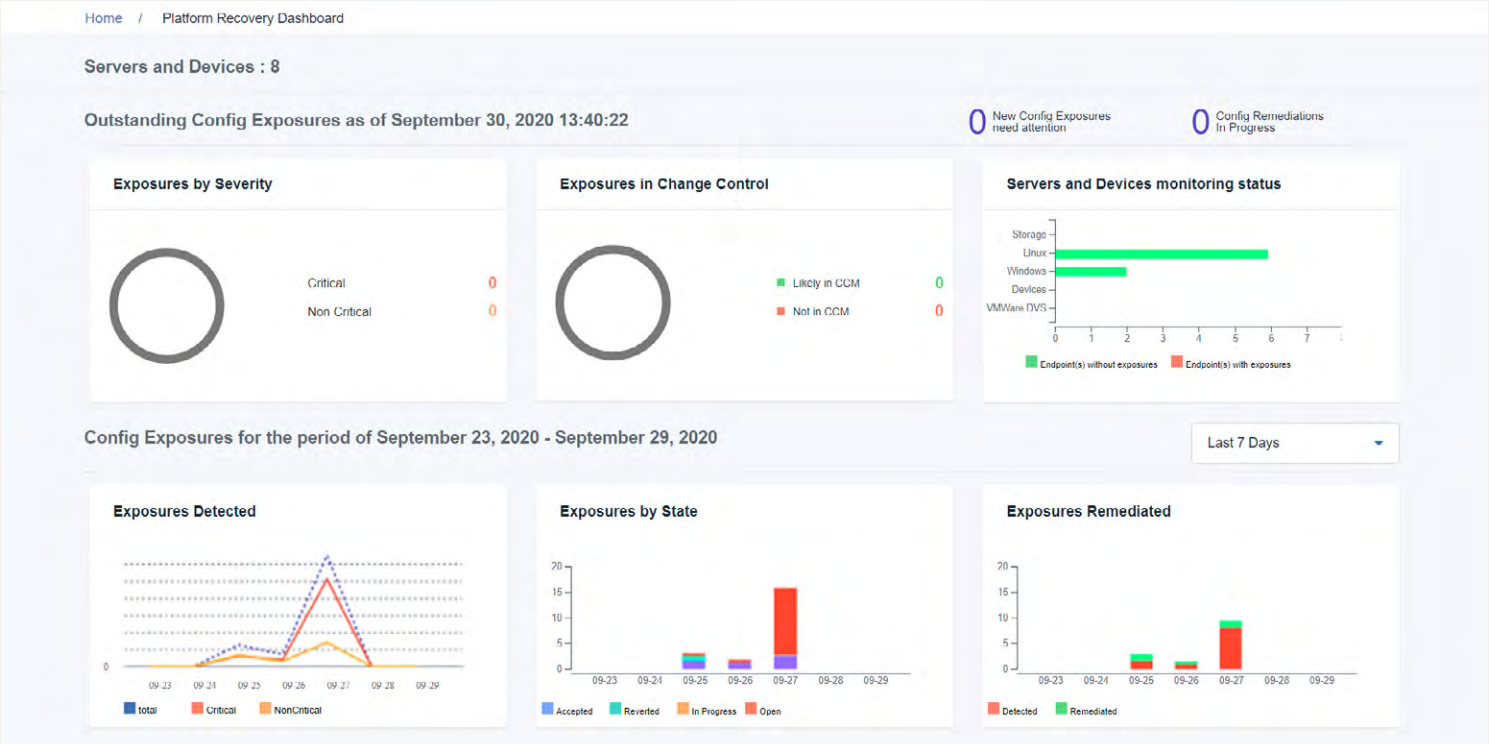
Cyber Incident Recovery includes a dashboard that simplifies cyber recovery management and the monitoring of platform configuration changes and data changes. It provides real-time visibility into RPO and recovery time objective (RTO) deviations, snapshot validation status and critical cyber recovery updates.

Meanwhile, senior management or the board of directors can receive real-time critical cyber recovery updates for faster, more informed decision making.

Better tracking of vulnerabilities and increased visibility
The Cyber Incident Recovery dashboard tells you the number of vulnerabilities across your environments, along with the severity level of each. You can track open vulnerabilities and make decisions informed by visibility into cyber RPO deviation, cyber RTO deviation, snapshot validation status and current cyber readiness.

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

Cyber Incident Recovery provides real-time visibility into RPO and RTO deviations, snapshot validation status and critical updates



Kyndryl Business Resiliency Services has decades of experience helping clients worldwide with their backup and recovery needs.

Kyndryl advantage
- Expertise across the resiliency lifecycle
- Automated recovery of physical, virtual and cloud workloads
- 800+ predefined patterns for faster, efficient implementation and scalability
- Choice of clouds, including AWS, Azure and IBM Cloud, for enterprise scalability

Trusted
- Over 9,000 customers are protected with Kyndryl disaster recovery and data management services
- Kyndryl has more than 3.5 exabytes backed up annually and under management

A global reach
- There are more than 300 IBM Resiliency Centers in more than 50 countries around the world
- IBM dedicates over 6,000 professionals worldwide to resiliency

Why Kyndryl?

Kyndryl has deep expertise in designing, running and managing the most modern, efficient and reliable technology infrastructure that the world depends on every day. We are deeply committed to advancing the critical infrastructure that powers human progress. We're building on our foundation of excellence by creating systems in new ways: bringing in the right partners, investing in our business, and working side-by-side with our customers to unlock potential.

Ready to learn more?

To learn more about what Kyndryl Resiliency Orchestration with Cyber Incident Recovery can do for you, please contact your Kyndryl representative or visit www.kyndryl.com

kyndryl

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America

July 2021