

kyndryl™



# Kyndryl Resiliency Disaster Recovery as a Service

Mitigate business continuity risks in your hybrid multicloud journey

## Table of contents

1. Are you protected against unplanned outages?
2. Mitigate risks with Kyndryl Resiliency Services solutions
3. Kyndryl DRaaS as a difference-maker
4. The business benefits of Kyndryl DRaaS
5. Why Kyndryl?
6. Take the next steps

## Are you protected against unplanned outages?

The expansion of hybrid cloud adoption brings with it many business benefits, not the least of which includes superior customer experience (CX) and better business outcomes.

However, there's another side to the hybrid cloud coin: Organizations on the journey to cloud are dealing with considerable complexity and risk. Those issues prove particularly problematic in the face of unplanned outages—a reality that nearly all organizations must battle.

Resiliency has emerged as a critical business value enabler to assist clients in the evolution of their IT strategy. Everything from increased productivity and improved CX to identifying lost business opportunities and ensuring compliance is in play.

Of course, relying on traditional practices alone won't help meet today's recovery expectations of continuous business availability. Here's why:

- Business impact of outages in a hybrid multicloud world can be very high.
- Protection and recovery of assets/ production workloads caused by cyberattacks is insufficient.
- Multiple clouds and vendors create a challenge to manage.
- There is a need to protect enterprise and customer data while adhering to evolving regulations, but a lack of clarity in a shared responsibility model also exists.
- Diverse and unique workloads needs require choice in deployment models.
- Rapidly responding to disruptions, recovering and resuming operations within SLAs (RPO/RTO) and containing the business impacts of outages are top priorities.
- Rising costs of data and application protection and business continuity are at odds with shrinking budgets.

Traditional practices won't help meet today's recovery expectations of continuous business availability.

# Mitigate risks with Kyndryl Security & Resiliency Services solutions

Kyndryl offers a set of comprehensive solutions to address the day-to-day recovery challenges associated with ensuring the availability of critical workloads in hybrid cloud environments. Specifically, the Kyndryl Security & Resiliency Services portfolio of disaster recovery (DR) solutions cover a multitude of disciplines, including:

- Business continuity consulting services
- Data center services
- Cyber resilience services
- IT infrastructure recovery services

Together, these solutions encompass all aspects of recognized IT risk—conflicting process and governance structures, cyber risk such as threat and vulnerability management, and anomaly detection. The solutions also help assess clients' recent pandemic preparedness based on end user performance, data storage and data access risks.

Additionally, the practice offers fully managed disaster recovery as a service (DRaaS). Kyndryl DRaaS is a software-defined, highly secure, Kyndryl-managed IT infrastructure service.



## Key features

On demand recovery cloud for planned exercises and declarations

Server image and production data replication to the cloud

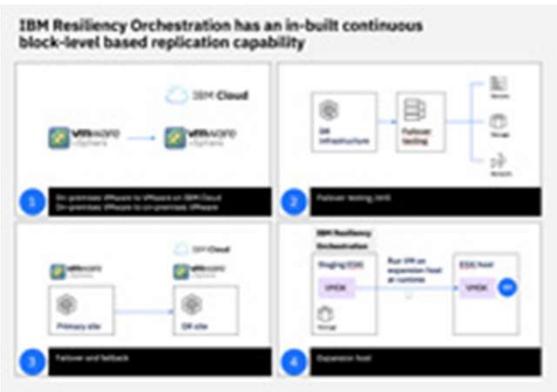
Automated failover and fall back between on-premises, hybrid and public clouds



# Kyndryl DRaaS as a differentiator

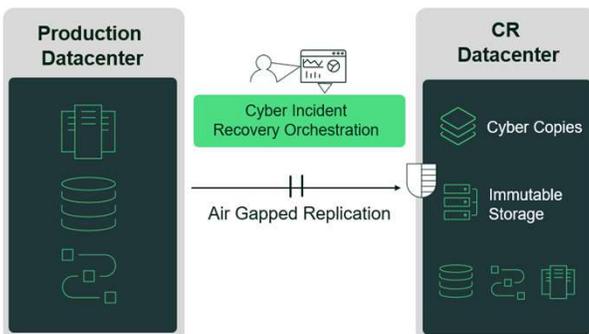
Powered by enterprise-class automation and orchestration, Kyndryl DRaaS protects enterprise applications running in hybrid environments. It provides continuous data protection for hypervisor-based, host/agent-based databases as well as storage replication, making it ideal for organizations with high expectations for rapid recovery in hybrid IT, multi-platform and multicloud environment.

Fully managed DRaaS contracts include one exercise per year by default, with the flexibility to purchase more as needed. Another option is to add on Kyndryl Resiliency Orchestration, which assists in the coordination of recovery across physical and virtual environments.



## Kyndryl Resiliency Orchestration for faster, cost-efficient recovery

Kyndryl Resiliency Orchestration has an in-built continuous block-level replication capability



## Kyndryl's Orchestrated Cyber Recovery as a Service capability

Kyndryl's solution for Cyber Incident Recovery enables quick recovery in the event of a cyber incident. With features like air-gapped protection, immutable storage, and anomaly detection, it is a purpose-built platform for cyber recovery. It helps clients mitigate cyber risks and avoid the high cost of a data breach. The solution is orchestrated using Kyndryl's Resiliency Orchestration software that also includes a new anomaly detection capability that uses rule-based heuristic identification augmented by artificial intelligence (AI).

# Key capabilities of Kyndryl DRaaS

- Multi-deployment model that supports DR for on-premises, hybrid and multicloud deployments
- Intelligent orchestration and automation that supports business process, and application, systems and database-level failover and recoveries as well as workflows to automate complex processes for dramatically improving speed of recovery
- Mitigate the impact of cyber disruption with an orchestrated resilience approach that helps identify risks, protect applications and data, and rapidly recover IT
- Fully managed and leverages industry leading data movers and replication software
- Comprehensive coverage that provide DR for physical, virtual and cloud-based workloads (x86, IBM System p, System i and System Z) as well as multiple hypervisors and operating systems (Windows, Linux, AIX, etc.)
- Data protection and quick recovery, recovery time objective (seconds to minutes) and recovery point objective (near-zero)
- Simplified visibility and around-the-clock monitoring, management and reporting capabilities

Kyndryl DRaaS enables simplified, rapid and reliable recovery of business-critical applications and data for hybrid cloud environments.

# The business benefits of Kyndryl DRaaS

Kyndryl DRaaS differentiates itself from competing solutions with its support of heterogeneous environments. Kyndryl microservices ensure greater flexibility for clients who want to avoid changing their existing infrastructure—and enables Kyndryl to automate and provide the protection required.

Another area of differentiation is that, compared to competitors, Kyndryl provides an end-to-end solution that supports:

- Client requirements for a predictable recovery outcome
- Increased levels of application and IT availability
- Continuity of service across hybrid multicloud environments

Be it public or private cloud, co-location or traditional client-owned on-premise environments, the benefits of Kyndryl DRaaS are consistent:

- **Speed:** DR automation that can reduce testing and recovery time from days or hours down to minutes—resulting in faster recovery time objectives (RTO) and recovery point objectives (RPO).
- **Scale:** A single management console to provision, monitor, validate, test and report, scale across multiple data centers, and support heterogeneous environments.
- **Simplicity:** An application-aware approach reduces the need for extensive expertise and makes it easier to deploy and manage multi-tier recovery.
- **High value:** Offers recovery for enterprise applications that span multiple technologies, helping to meet audit and compliance management requirements.
- **Reliability:** Backed by automation and Kyndryl Resiliency for 24x7 service and support.



## Kyndryl DRaaS by the numbers

507%  
three-year ROI

80%  
lower cost of business risk,  
lost productivity and revenue

80%  
less unplanned  
downtime

43%  
improvement in RPO

24%  
more efficient business  
continuity teams

Source: *The Business Value of IBM's DRaaS and Resilience Orchestration Services*, IDC, 2020

# Why Kyndryl

Kyndryl has been named as a leader in DRaaS by analysts. Kyndryl Security & 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
- RPO/RTO of near-zero/seconds, or as required by your business
- 950+ predefined patterns for faster, efficient implementation and scalability
- IBM Cloud® and Red Hat® for enterprise scalability

## Trusted

- Over 4000 customer agreements globally
- Kyndryl has more than 3.5 exabytes backed up annually and under management

## A global reach

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

# kyndryl.

© Copyright Kyndryl Inc. 2021

Kyndryl Corporation  
New Orchard Road  
Armonk, NY 10504

Produced in the United States of America  
November 2021

Kyndryl, the Kyndryl logo, Kyndryl.com, and Kyndryl Services are trademarks of Kyndryl Inc., registered in many jurisdictions worldwide. Other product and service names might be trademarks of Kyndryl or other companies. A current list of Kyndryl trademarks is available on the web at "Copyright and trademark information" at [www.Kyndryl.com/legal/copytrade.shtml](http://www.Kyndryl.com/legal/copytrade.shtml).

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

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. Kyndryl products are warranted according to the terms and conditions of the agreements under which they are provided.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. Kyndryl systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. Kyndryl DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.<sup>2</sup> Gartner press release.

