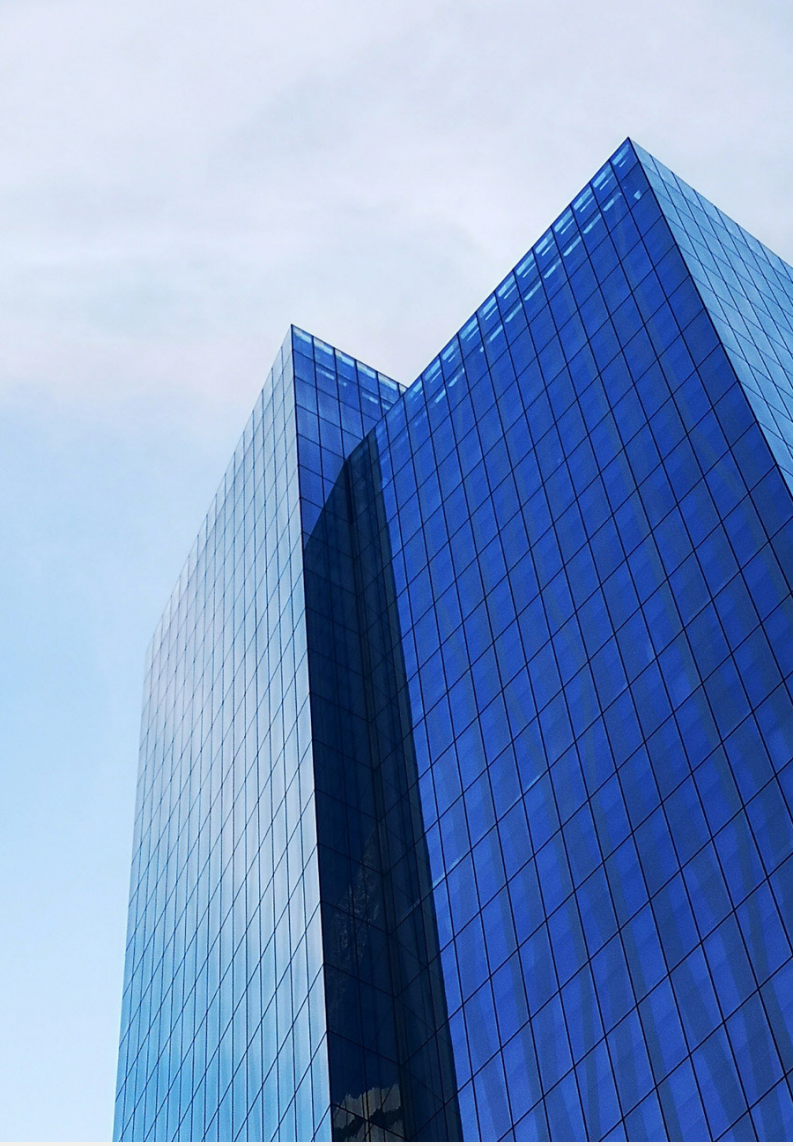

kyndryl

Data Protection Risk Assessment with Cohesity

With increasingly complex multi-cloud, multi-vendor, hybrid environments, customers face challenges identifying risk and protecting data. The Data Protection Risk Assessment analyses customer data environments and makes recommendations to increase cyber resilience for their organization.

Introduction

The Data Protection Risk Assessment allows customers to understand their data compliance against industry best practices for backup and restore, cyber incident response, and disaster recovery. It provides an in-depth review of data to understand areas of vulnerability and opportunities to strengthen security posture.

Increasingly, organizations are engaging with professional security services to address data needs as well as proactively address changing regulatory and compliance requirements. With a flexible scoping model, Kyndryl focuses on customer selected areas to assess, prioritize, and provide recommendations for improved data protection and recovery.

Kyndryl's Point of View

Data is more valuable than ever and so is the need to protect it. Organizations are facing new challenges with the increased use of disparate data environments (e.g., cloud, hybrid) and resource sprawl. The average data breach costs $4.35M and takes 277 days to identify and contain.[1] It is imperative that organizations have a clear view of data across multiple locations such as cloud, on-prem, and hybrid to protect against threats like user error, natural disasters, or cyber incidents.

Kyndryl uses ongoing assessments to address potential issues proactively. Customers benefit from combining Kyndryl's cyber resilience expertise with the comprehensive and unified Cohesity data management experience to collect, analyze, and transform these findings into actionable changes.

[1] Source: Cost of a data breach report 2022.

Highlights

Key Features

- Experts to guide one-time, periodic, or continuous assessments.
- Flexible scoping model for analysis focus and prioritization.
- Gain visibility and insight into data vulnerabilities to proactively detect and respond to threats.
- Prioritize budget and spending based on key findings.

Differentiators

- Automated data collection from customer environment.
- Data analyzed by Cohesity NetBackup IT Analytics to generate maturity using Kyndryl's proven cyber resilience framework.
- Portal to host data and assess progress overtime.

Data Protection Risk Assessment with Cohesity

Service Overview

Data Protection Risk Assessment creates a dynamic, flexible analysis that can be conducted at intervals for a point-in-time analysis or continuously to track progress. Guided by our global industry experts data is collected via a questionnaire and automated scans of the customer environment, leaving no element of data protection unexamined.

The Cohesity NetBackup IT Analytics tool collects metadata automatically for a minimum of 30 days. It is then analyzed across functional attributes such as process and compliance in accordance with the cyber resiliency lifecycle.

Customers are provided a risk assessment scorecard to help them understand their maturity level regarding their data protection risk for backup and restore, cyber incident response, and disaster recovery. It includes a prioritized list of recommendations to remediate the highest-impact risks, along with recommended actions that, when implemented, will improve the organization's maturity level.

For more information

To learn more about Data Protection Risk Assessment please contact your Kyndryl Representative or Kyndryl Business Partner, or visit www.kyndryl.com.

Why Kyndryl?

At Kyndryl, we understand the pros and cons of various cyber resilience strategy options and can help you navigate and select a strategy that is most capable of meeting your requirements and assumptions.

Experience

Execute faster by leveraging the extensive skills and resources across Kyndryl and our broad partner ecosystem.

Technology

More securely integrate emerging technologies across hybrid environments, benefiting from our decades of experience and patterns of success.

Support

Manage the rapidly evolving operational risks, effectively protect business-critical infrastructure, and mitigate the business impact of security and resiliency incidents.

kyndryl