kyndryl

Kyndryl Cyber Resilience for Enterprise Workloads including SAP on Microsoft Azure

Customer Presentation

February 2023

Your enterprise data is at risk

Enterprise data is growing at an exponential rate—driven by new technologies. It's a key source of business insights and competitive value.

However, the world is riskier than it used to be, and as the amount of data increases, so does the risk of data loss.

Managing and safeguarding your enterprise data can be especially challenging as your organization is faced with:

- Increased risk of data loss due to disruption, outage, or disaster
- Rising costs of data and application protection, backup, and continuity
- Need to comply with changing government and industry regulatory requirements

kyndryl

The business problem

The risks landscape is constantly changing, and preventing and mitigating risk is a top board-level mandate.

Cyber security risks rank among the top 10 global risks in terms of severity in the short term (2 years) and long term (10 years).

Source: World Economic Forum, The Global Risks Report 2023

Global risks ranked by severity over the short and long term

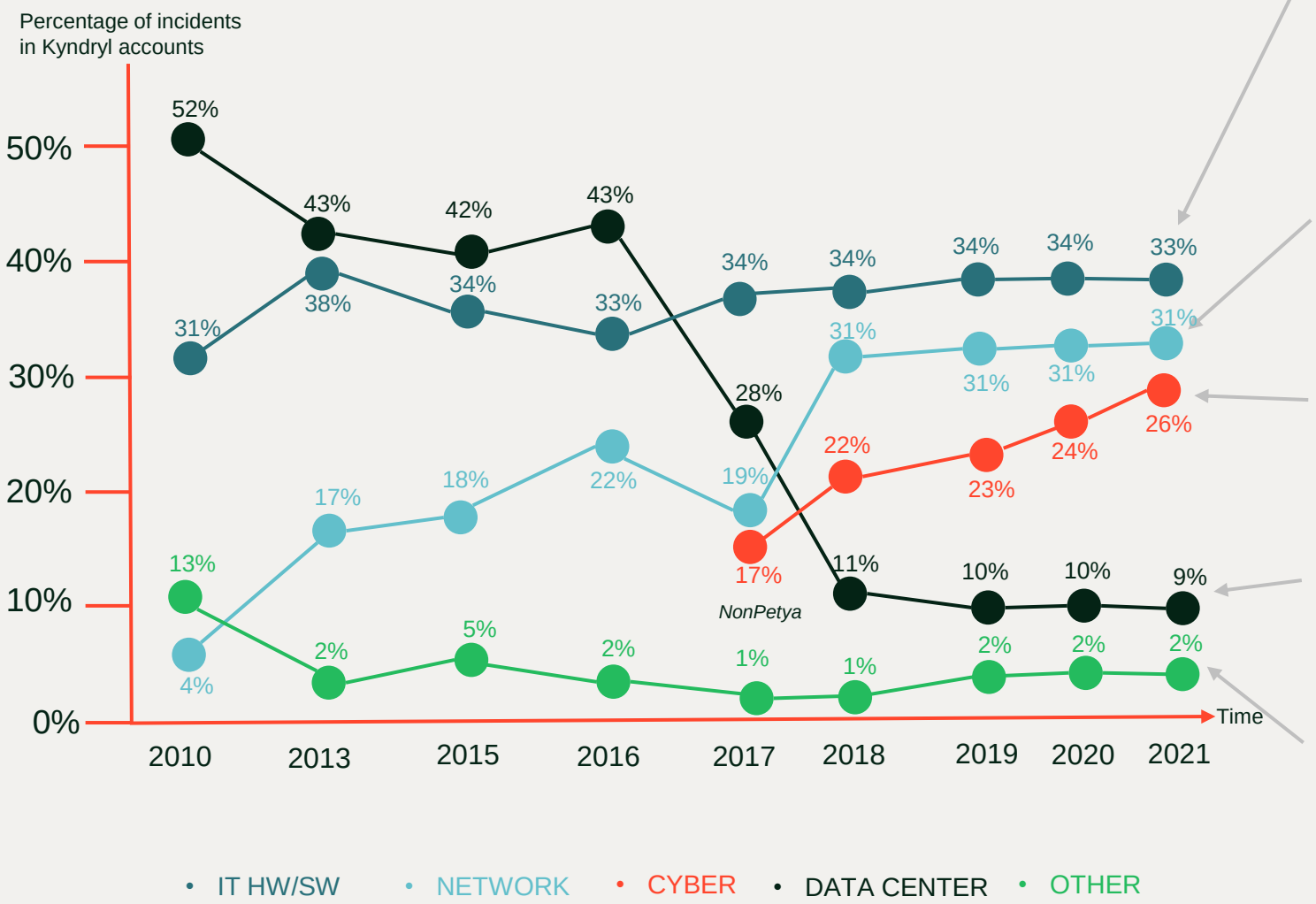
kyndryl

Kyndryl's Incident Analysis

Analyzing severity 1 incidents:

- 130+ customers
- Timeframe 2010-2021
- Large scale enterprise outages
- Greater than 4 hours duration
- Customers and Kyndryl

Kyndryl's Major IT Outage Analysis 2010-2021



Technical debt is pervasive and is a key factor in many outages

Trying to link legacy networks into Cloud networks is proving complex

Since NotPetya (2017), Cyber as a cause of outage is a new category and steeply trending upwards

The move out of aging Data Centers to Co-Lo and Cloud is lowering building failures

Change management and process failures still dominates this category

kyndryl

Kyndryl Cyber Incident Recovery with Microsoft Azure

Cyber resilience challenges

1

Increase of attack surface due to digital transformation and cloud adoption

2

Corruption propagation into disaster recovery (DR) and backup copies that affects recoverability

3

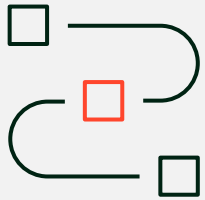
Insufficient and highly manual response and recovery plans

4

Rapidly evolving and increasingly complex regulatory environment

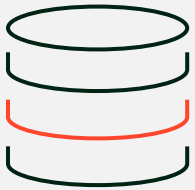
Kyndryl Cyber Incident Recovery with Microsoft Azure

Current disaster recovery/backup copies are vulnerable for corruption and are not adequate for cyber resilience!



Continuous Network Exposure

Continuous network exposure can cause corruption propagation to the DR sites, causing both primary and DR unusable



Traditional DR/Backups being Targeted by Cyberattacks

Attacks corrupting traditional DR and backup copies directly

Inefficient Point in Time Copies

Point in time copies provided by traditional backup has high recovery point objectives (RPO) and recovery time objectives (RTO)

Let a trusted set of partners help protect your business-critical data and recover in the event of a cyber incident

To more efficiently protect your data against cyber threats, reduce costs and manage compliance requirements in a hybrid IT or cloud environment, you need a highly secure, fully managed and cost-effective cyber resilience solution that can help ensure your business is “always on.”

kyndryl

Kyndryl Cyber Incident Recovery with Microsoft Azure

- Fully managed Cyber Incident Recovery service on Azure to protect critical business data in a security-rich, isolated environment.
- The solution provides logical air gap. The Blob immutable containers owned and managed by Kyndryl are accessed only by the Veritas servers in Cyber Incident Recovery (CIR) tenant and immutable storage to protect critical data.
- The snapshot taken by Veritas is submitted for anomaly scanning and analyzed to identify potential cyber infections.
- The data can be restored through Resiliency Orchestration providing the capability to pick up a backup copy from Blob within the retention period and orchestrate the restore to the clean room. This clean room is in an isolated vNET within client subscription.

kyndryl

kyndryl / Microsoft

Why partner with Kyndryl and Microsoft?

The partnership

Together, our strategic partnership with Microsoft supercharges our customer-first focus, empowering enterprises with the best technical expertise, service excellence and ability to innovate in the market to help you solve your biggest challenges.

We offer deep operational knowledge, born out of our experience in managing the most complex workflows in the world. We understand the technologies that power the work you need to do, and how to optimize those technologies as your business needs change.

Kyndryl's advanced specializations:

- Kubernetes on Microsoft Azure
- SAP on Microsoft Azure
- Analytics on Microsoft Azure

Benefits

Expertise:

- Kyndryl has deep experience across all major industries in integrating enterprise services with the Microsoft Cloud. We rank in Microsoft's Top 5 partners with the most certifications, globally.
- Our Microsoft University for Kyndryl enables us to continue to expand our skills.

Innovation:

- Kyndryl/Microsoft Joint Innovation Lab showcases cloud-based solutions in experiential demo environments, enabling agile experimentation and new products/services development.

Speed:

- Co-creation of joint solutions helps you get to market faster and deliver cloud experiences from the edge to application.

Trust

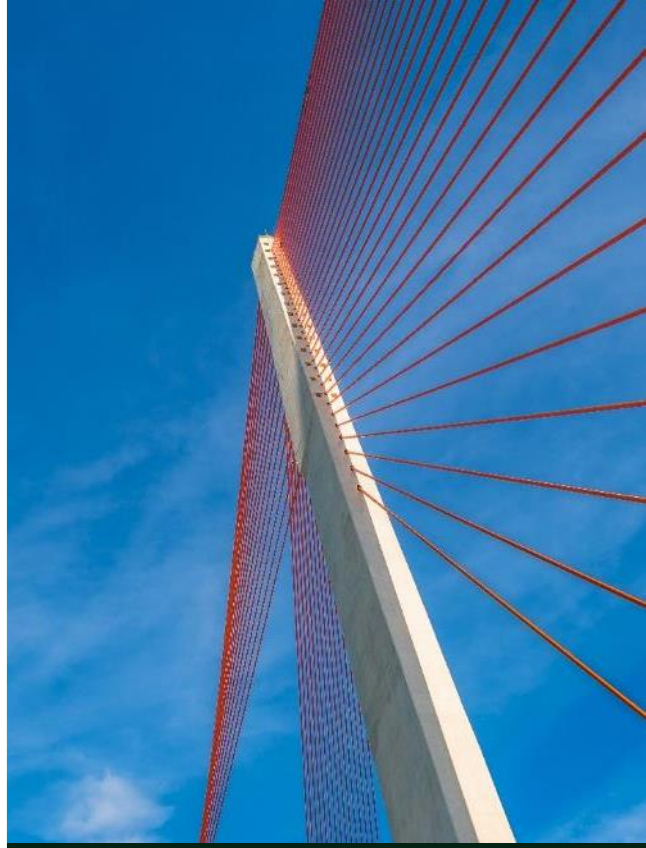
- Our joint partner network empowers our ability to continually solve your biggest challenges. The right partners, for the right use case, at the right time.

Joint Solutions

- Migration, Modernization and Deployment Services for Azure enhanced with data management and AI
- Managed cyber-resiliency for SAP and enterprise application workloads on Azure
- Modern Work for the digital workforce
- Mission-critical infrastructure management with IBM zCloud and Azure

Business Outcomes

- Empower flexible, modern work environments
- Leverage Microsoft Cloud to automate for increased productivity
- Unlock maximum business value from technology investments



Gold
Microsoft Partner
Azure Expert MSP
Microsoft

Learn more about the partnership.

kyndryl

Why are other approaches not enough?

Data encryption does not protect you against destructive or ransomware attacks

Traditional data recovery leaves backups open to attack, risking further infection

Tape backups take weeks to recover and require backup infrastructure

Added security can't succeed every time because of human error and insider threats

Cyber insurance does not protect your customers or your reputation

Self-managed solutions won't prevent internal attacks

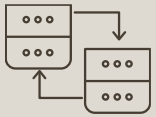
kyndryl

Kyndryl Cyber Incident Recovery with Microsoft Azure Use Case

1. Unified solution for cloud native workloads – protection for Azure native VMs and SAP workloads deployed on Azure VMs
2. Manages and monitors immutable backups on Azure Blob
3. Automated validation of snapshots through Resiliency Orchestration Anomaly Detection (ROAD) tool
4. Crash consistent and application consistent recovery through automated workflow
5. Cyber SLAs monitoring RPO, RTO and snapshot copies
6. Cyber recovery workflow to ensure seamless recovery during the cyber incident

Key Components for Cyber Incident Recovery

Orchestration/ Automation



NetBackup Data Mover

Reporting

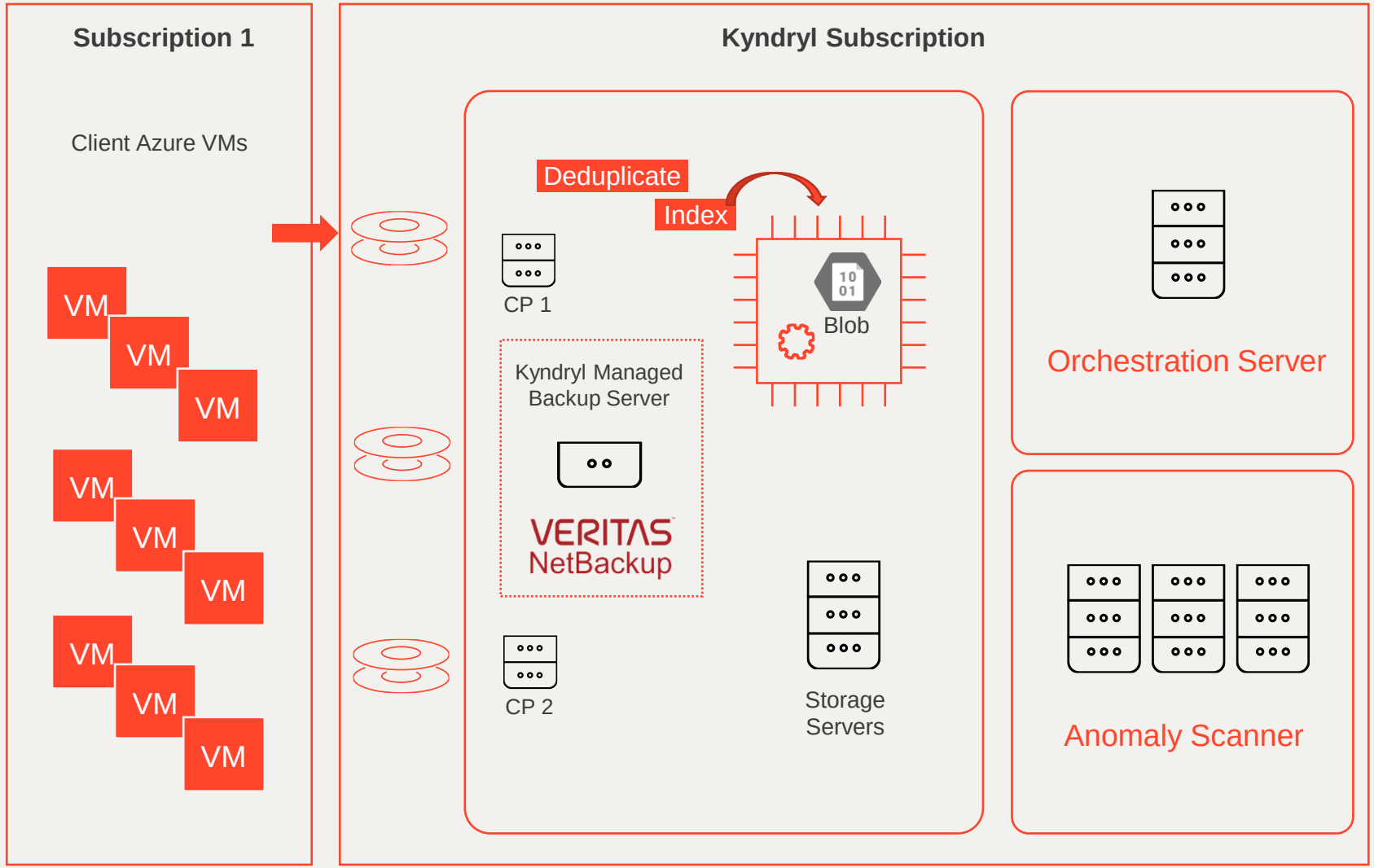
Immutable Storage (WORM)

Data Verification

kyndryl

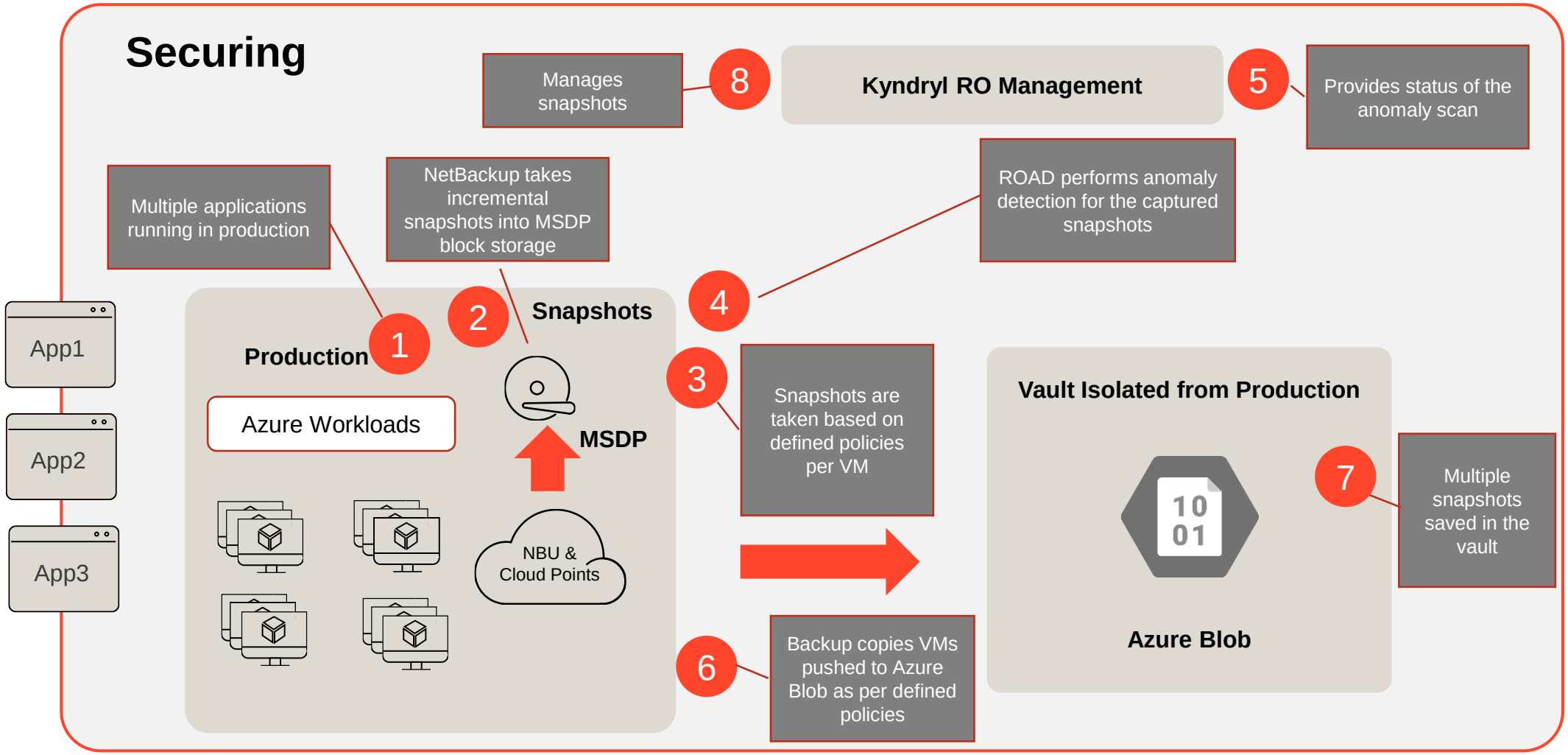
Solution Overview

- Solution leverages Veritas NetBackup as the standard data mover for protecting Azure workloads
- NetBackup takes incremental snapshots of Azure native VMs
- The snapshots are de-duplicated, compressed and encrypted backed up into immutable Azure Blob
- Resiliency Orchestration monitors the availability of new snapshots and performs mounts into Resiliency Orchestration Anomaly Detection (ROAD) tool for anomaly scanning
- ROAD tool scans the snapshots and analysis is published in Resiliency Orchestration dashboard
- Resiliency Orchestration presents the snapshots with its property and anomaly scan output
- In anomaly disaster, customer's user can select the point in time validated copy and perform recovery

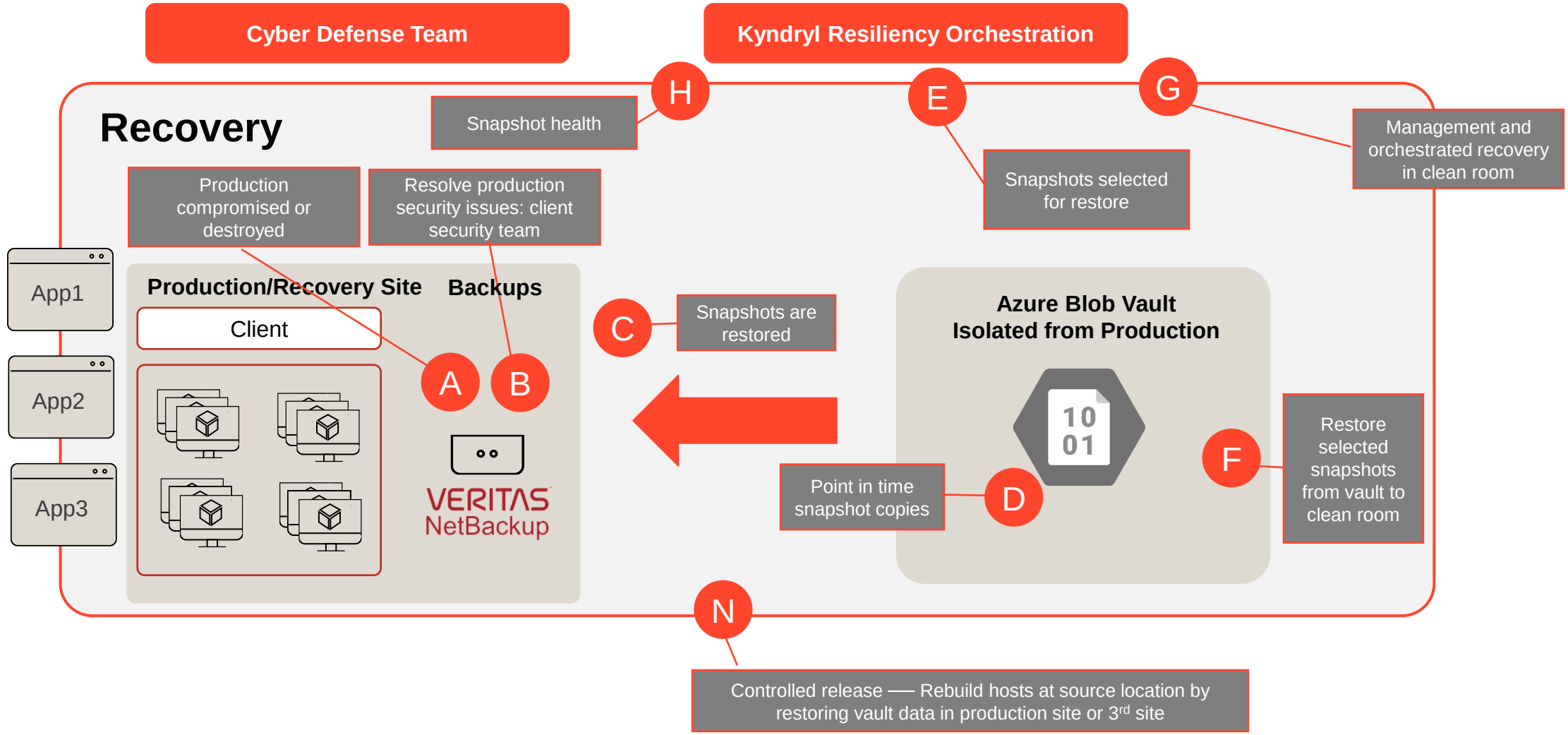


kyndryl

Kyndryl Cyber Incident Recovery Securing Key Processes: Workflows

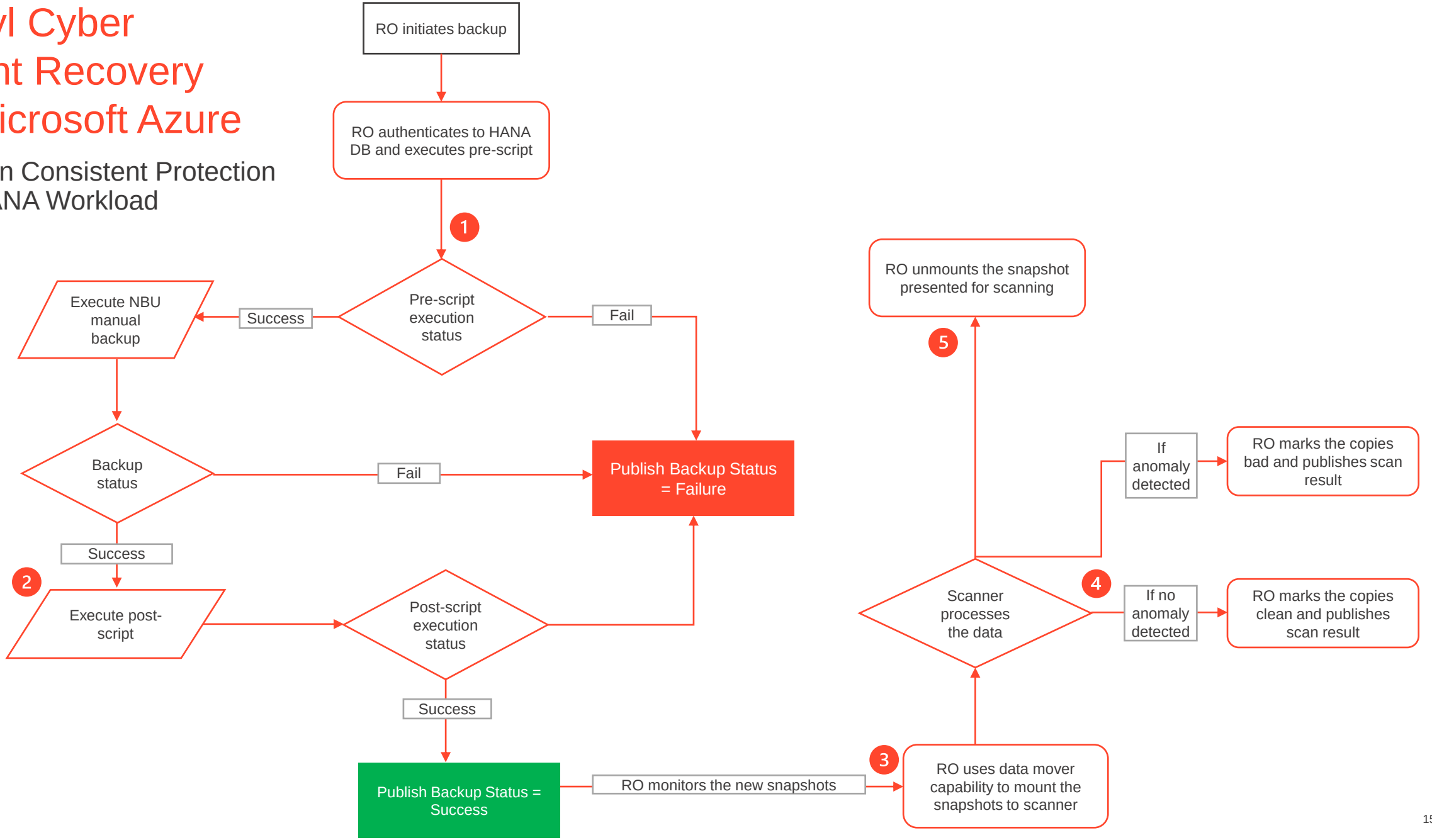


Kyndryl Cyber Incident Recovery Securing Key Processes: Workflows



Kyndryl Cyber Incident Recovery with Microsoft Azure

Application Consistent Protection – SAP HANA Workload

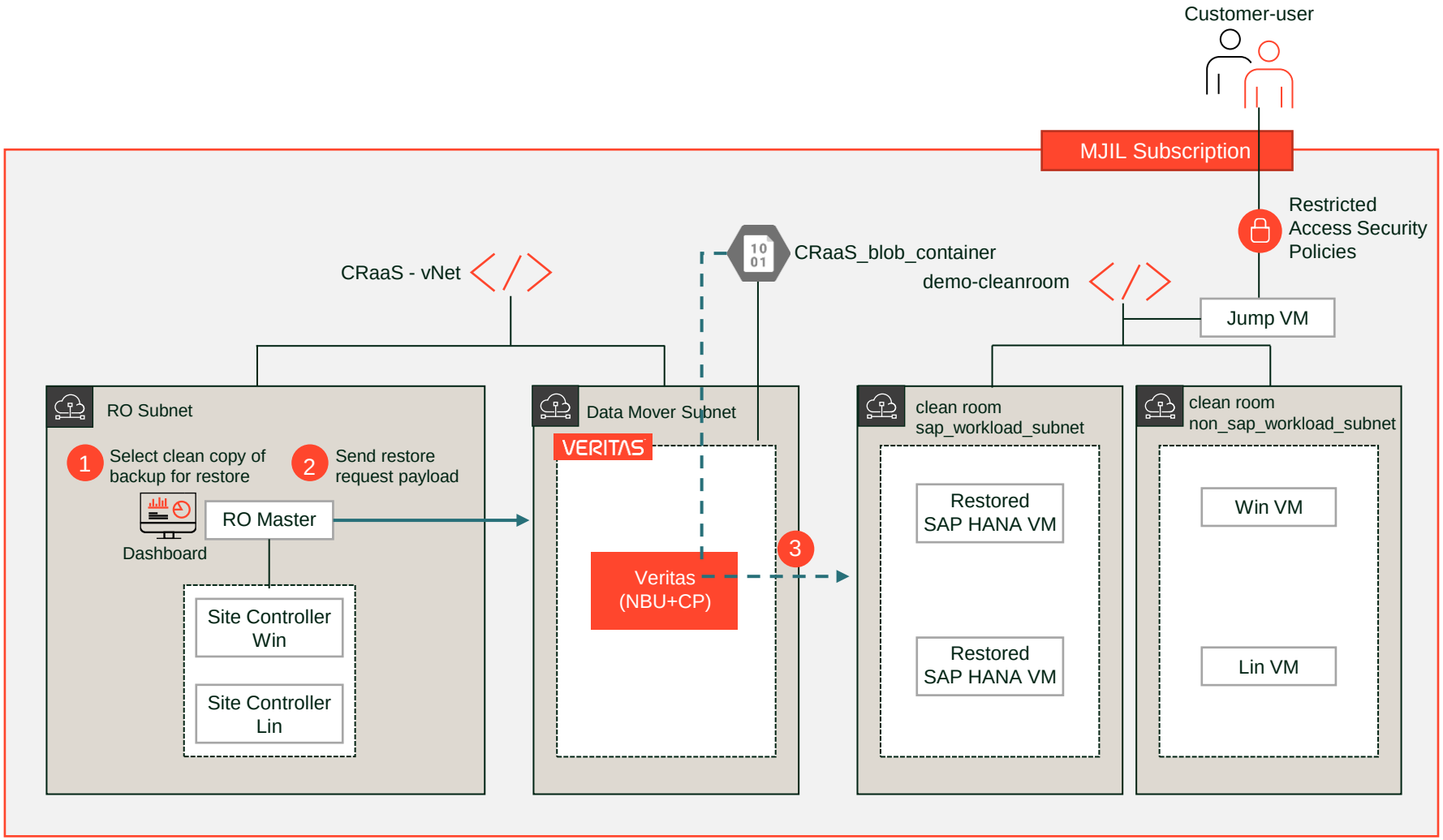


Kyndryl Cyber Incident Recovery with Microsoft Azure for SAP Workload

Restore to Clean Room

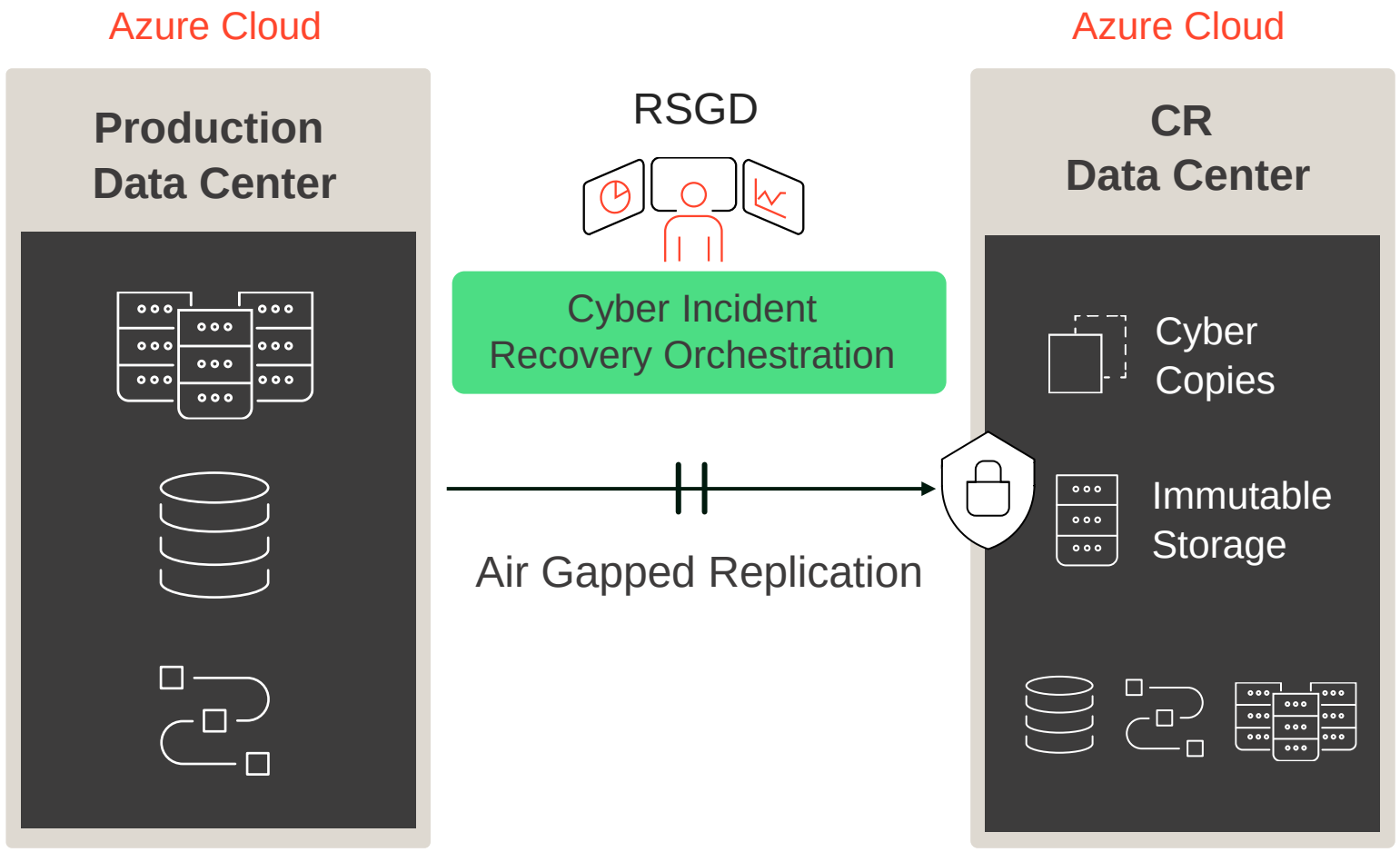
Clean room is an isolated environment provided for out of place restores for clients to validate the data before moving them back to production

1. Pick the clean copy of data listed in RO
2. RO sends the restore payload to the data mover based on:
   - Anomaly scanning status
   - Date and time of backup from which restore is requested
   - Full VM restore
   - Optional FLR
   - Target network for restore
3. Data mover initiates the restore to clean room
4. Customer's user has restricted access to clean room to validate the restores
5. RO monitors and publishes the restore state and status



Kyndryl Cyber Incident Recovery with Microsoft Azure

End-to-end services for Cyber Incident Recovery



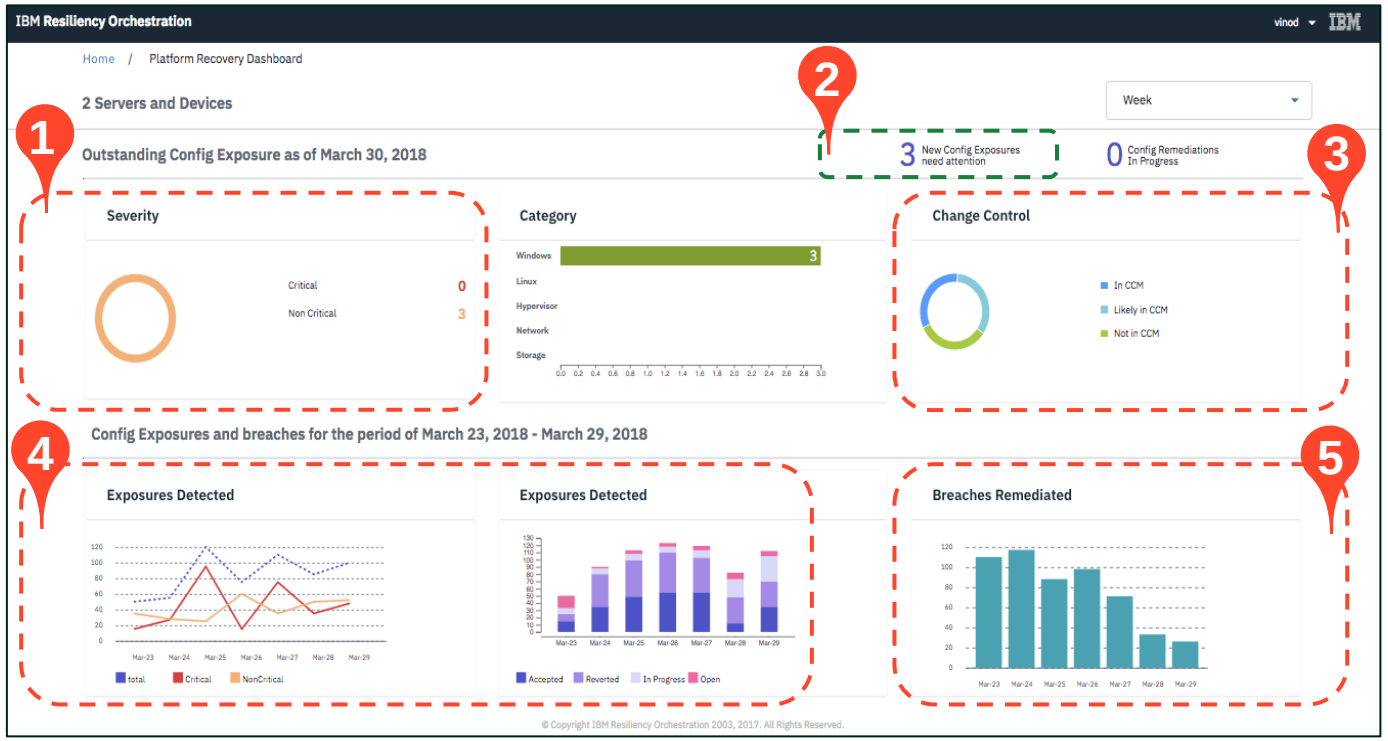
Key Deliverables of Managed Services

- Orchestration servers, site controller servers, immutable storage, and data mover
- Resiliency Service Global Delivery (RGSD) provides monitoring and management
- Local subject matter experts and project management services for implementation and regular coordination

Kyndryl Cyber Incident Recovery with Microsoft Azure

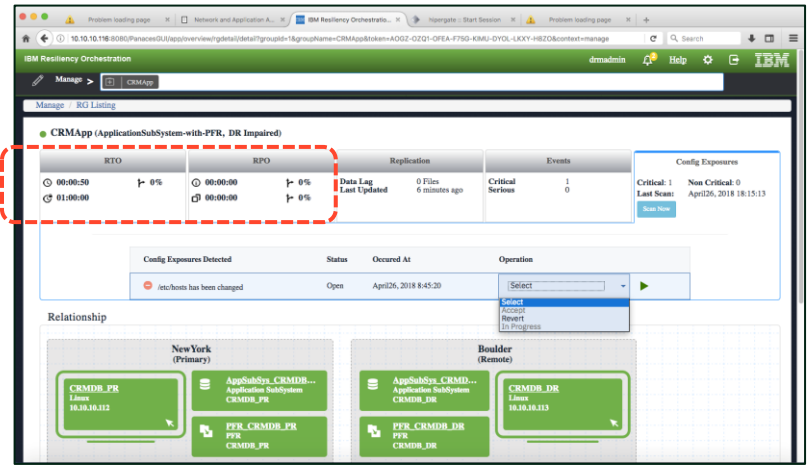
Resiliency Orchestration with CIR with Microsoft Azure provides a dashboard for visibility and governance

Comprehensive Dashboard

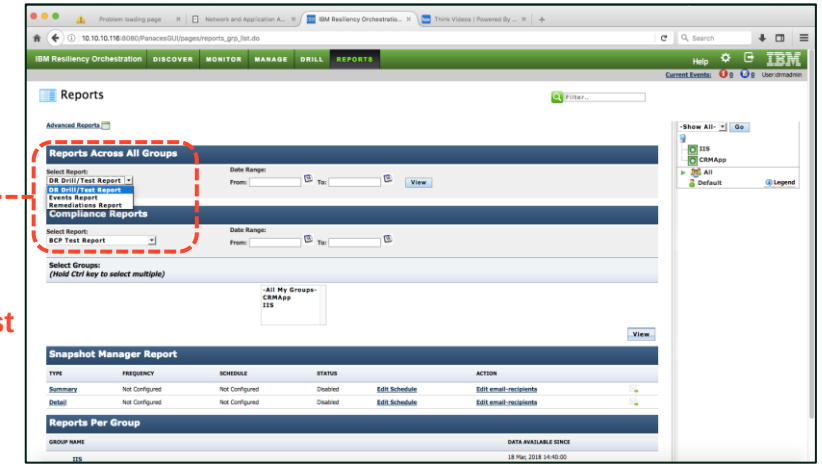


1. **Severity of Exposure**
2. **Vulnerability**
3. **Change Management System**
4. **Anomaly Detection**
5. **Efficiency**

Integrated Response and Recovery Reports



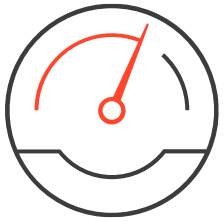
SLAs



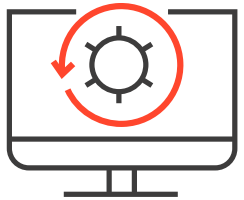
Drill/Test Reports

Kyndryl Cyber Incident Recovery with Microsoft Azure

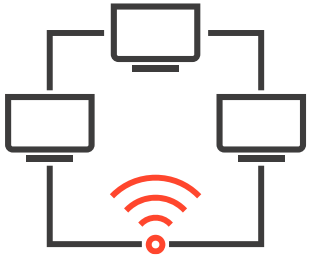
Kyndryl has end-to-end responsibility for monitoring and managing the performance of the Cyber Recovery Site as well as retrieval of the data and delivery to the client for restoration based on SLAs.



Performance and Capacity Management



Cyber Incident Recovery Management



Connectivity Management

Security Management

kyndryl

Features

Limits exposure by securing data in an Azure Cloud isolated from production and backup environments

Prevents changes to data copies by using immutable storage

The snapshot taken by Veritas is submitted for anomaly scanning and analyzed to identify potential cyber infections

Maintains a known good copy that can be restored quickly in the event of a cyber attack

Benefits

Significantly reduced impact of cyber attacks
Faster recovery helps companies get back to business quickly

Highly reliable and scalable
Ability to handle large enterprise data protection

Ease of management through single console
Centralized visibility and control

Reduced OPEX
Flexible consumption-based pricing model

kyndryl

30+ years of designing, building and managing mission-critical IT environments for our customers

Our people:

90,000
Skilled professionals

247,000
Skills badges earned, including:

- 61,000 in cloud
- 43,000 in agile
- 43,000 in analytics
- 42,000 in AI
- 38,000 in Design Thinking

31,000
Vendor-recognized certifications in Microsoft Azure, VMware, Cisco, Red Hat, AWS and more

2.9M
Hours of training in first half 2021

Powering mission-critical technology systems across essential industries

5/5 top airlines by revenue passenger miles (RPM)

45% of passenger cars made by our customers

61% of assets under management by the top 50 banks managed by our customers

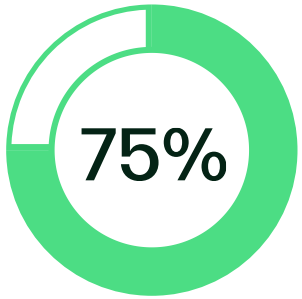
4/5 largest retailers

49% of mobile connections managed by our customers

*2019 numbers

Empowering thousands of customers

4,000
Global customers, including:



…of the Fortune 100 and more than half of the Fortune 500

Providing undisputed leadership

6.1M mainframe installed MIPS

300K network devices managed

5,200+ WAN devices managed

3.5M LAN ports managed

67K+ VMware systems managed

14K+ SAP instances managed

3.5+ exabytes of customer data backed up annually

kyndryl

kyndryl

Thank You

Date