kyndryl

BANCHE& SICUREZZA

Come le soluzioni per la resilienza si possano aggiornare per gestire il rischio cyber

Mauro Proserpio, Kyndryl Distinguished Engineer

May 20, 2022 - Milan

EVOLVERE IN SICUREZZA: NUOVI STRUMENTI PER LA RESILIENZA OPERATIVA

Agenda

01 Kyndryl Italy at glance – professional view

02 The shifting cybersecurity paradigm

03 Kyndryl’s cyber resilience solution approach

Agenda

01 Kyndryl Italy at glance – professional view

02 The shifting cybersecurity paradigm

03 Kyndryl’s cyber resilience solution approach

Kyndryl in Italy

A leading player across legacy and cloud IT environments

1800 employees with deep technical skills

- 130 IT Architects
- 900 Technical Specialists
- 490 Project & Service Managers
- 50 Consultants & Industry SMEs

1200+ certifications o/w 480 on cloud

500 new hiring by the end of 2022

400+ partners within local ecosystem

4 owned/managed data centers (ANSI/TIA level IV)

5 client owned/managed data centers

2 help desks – multi-language

Company certifications:

- ISO27001 - Information Security
- ISO27018 - Information technology - Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
- ISO27017 - Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services
- ISO22301 - Business Continuity
- ISO20000 - IT Service Management
- ISO9001 – Quality
- ISO14001 – Environmental Management
- ANSI/TIA (for owned data centers

Agenda

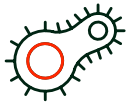
01 Kyndryl Italy at glance – professional view

02 The shifting cybersecurity paradigm

03 Kyndryl’s cyber resilience solution approach

Cyber risk is increasingly a top executive priority

Rising cases of unplanned outages driven by sophistication of cyberattacks and widening skills gap



COVID-19

69% of board of directors accelerated their digital business initiatives following COVID-19 disruption[1]

Ransomware

73% of organizations are increasing spending for data protection as a result of ransomware threats[2]

Regulations

50% of businesses are pressure testing supplier business continuity plans as a result of COVID-19[3]

C-Suite / Board Oversight

40% of board of directors will have a dedicated cybersecurity committee overseen by a qualified board member by 2025[4]

Security Skills Gap

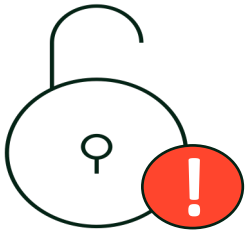
52% of businesses report a security skills gap in their organization[5]

Gartner® predicts, "By 2025, 70% of CEOs will mandate a culture of resilience to survive coinciding threats including cybercrime from COVID-19, cybercrime, severe weather events, civil unrest and political instabilities." [6]

Source:
[1] Gartner, 4 Major Sourcing Trends for a 'New Normal' World: Change, Outcomes, Risk and Agility | Published 23 November 2020 - ID G00733227| By Claudio Da Rold, Fabio Di Capua, Katie Gove, Andy Rowsell-Jones
[2] 451 Research, part of S&P Global Market Intelligence; Source: Voice of the Enterprise: Storage, Data Management and Disaster Recovery 2021
[3] Gartner, Assess Supplier Business Continuity Plans for Risk Mitigation and Operational Resilience, Gartner, March 2021 - ID: G00730918 | By Geraint John , Sam New , Roberta Witty , Sarah Watt
[4] Gartner, Predicts 2021: Cybersecurity Program Management and IT Risk Management Published 8 January 2021 - ID G00735901 | Analyst(s): Sam Olyaei, Katell Thielemann, Richard Addiscott, Khushbu Pratap
[5] IDC, Security ServicesView 2020: Worldwide and Regional Survey Findings, Doc # US47092420, December 2020
[6] Gartner, Resilience: Inconsistent Scope Could Drive Overconfidence and Risk Not Meeting Business Objectives | Published 24 September 2021 - ID G00754811 | Roberta Witty

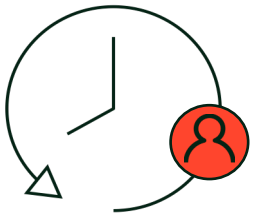
Cyber resilience challenges

Traditional practices are unable to meet today's recovery needs.



Increased attack surface due to multi-cloud adoption and business digitization

Propagation of corrupted data to backup copies and DR affects recoverability



Insufficient and highly manual response and recovery plans

Rapidly evolving and increasingly complex regulatory environment

Agenda

01 Kyndryl at glance

02 The shifting cybersecurity paradigm

03 Kyndryl’s cyber resilience solution approach

Coping with the dynamic nature of risks

Build cyber resilience characteristics into broader IT strategy

SHIFT LEFT

Build cyber resilience into digital initiatives, underpinned by cloud and zero trust principles

SHIFT RIGHT

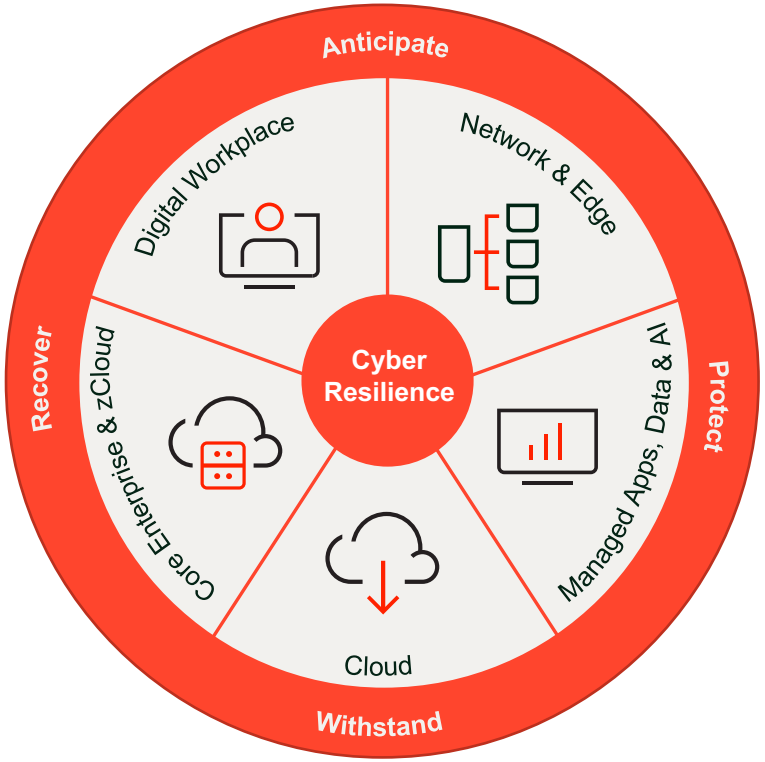
Since protection is not enough, establish and improve linkage between security and resiliency

STREAMLINE APPROACH

Radically streamline approach to security and resiliency as foundational cyber-risk model

Kyndryl CyberResilience Framework to help anticipate and mitigate adverse cyber events

Simplify cyber risk management across cloud and legacy environments



Cyber Resilience Framework

Security Assurance | **Zero Trust** | **Security Operations & Response** | **Incident Recovery**

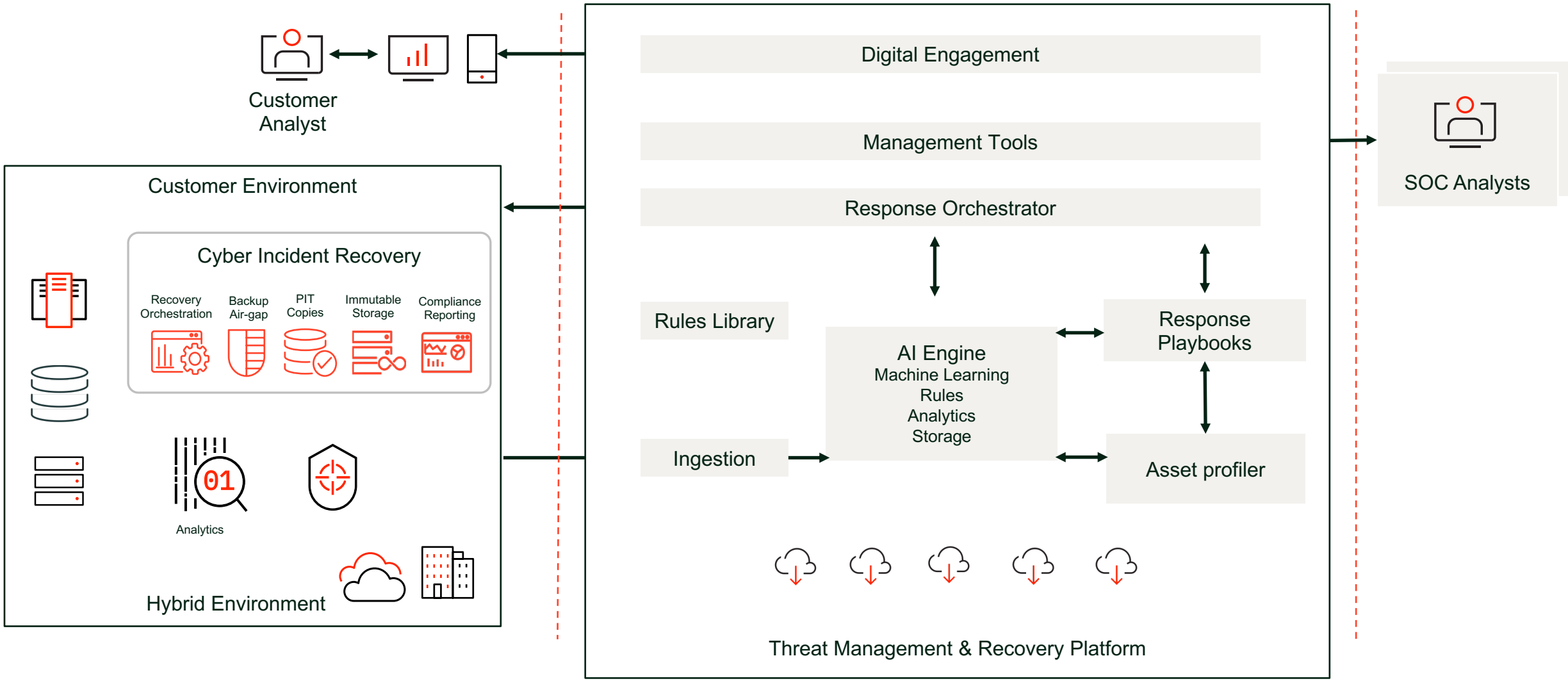
Anticipate → **Protect** → **Withstand** → **Recover**

Cybersecurity + **Recovery**

Focus on Digital Innovation & Cloud Adoption

Adaptive cyber resilience delivery platform

Open architecture, highly configurable toolset, and choice of target clouds



Kyndryl Cyber Recovery as a Service

Overview of key components

I. Backup to Air-gapped Vault Storage

II. Anomaly Detection & Data Integrity Validation

III. Clean Room Recovery

IV. Orchestration and Automation

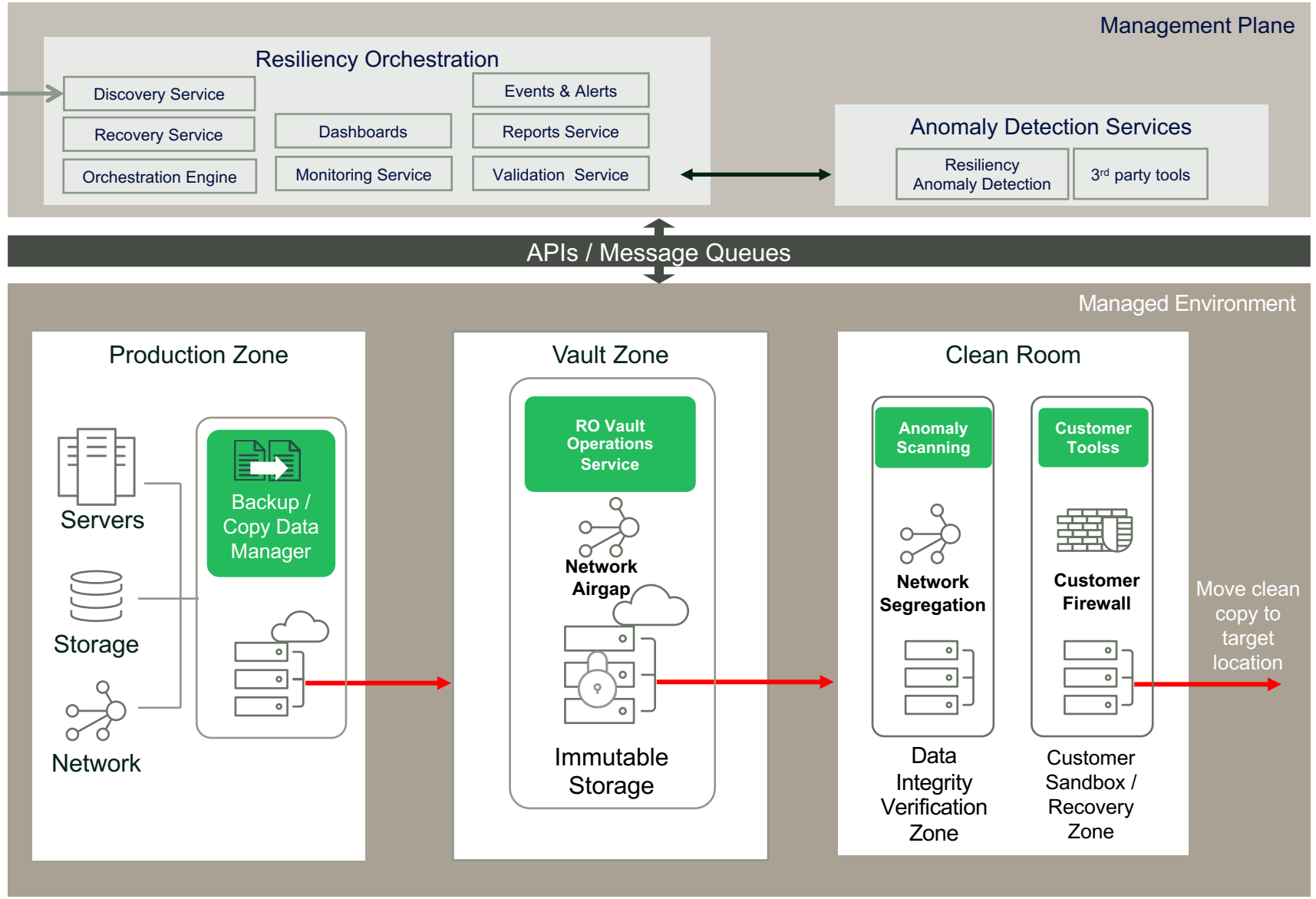
Technology/ Platforms

- Cloud IaaS/PaaS
- Virtualization
- Storage
- Network
- Database
- Application

Platform Provider Tools

Data Discovery Services

Client/Service Provider CMDB



www.kyndryl.com/it/it