Kyndryl Security & Resiliency

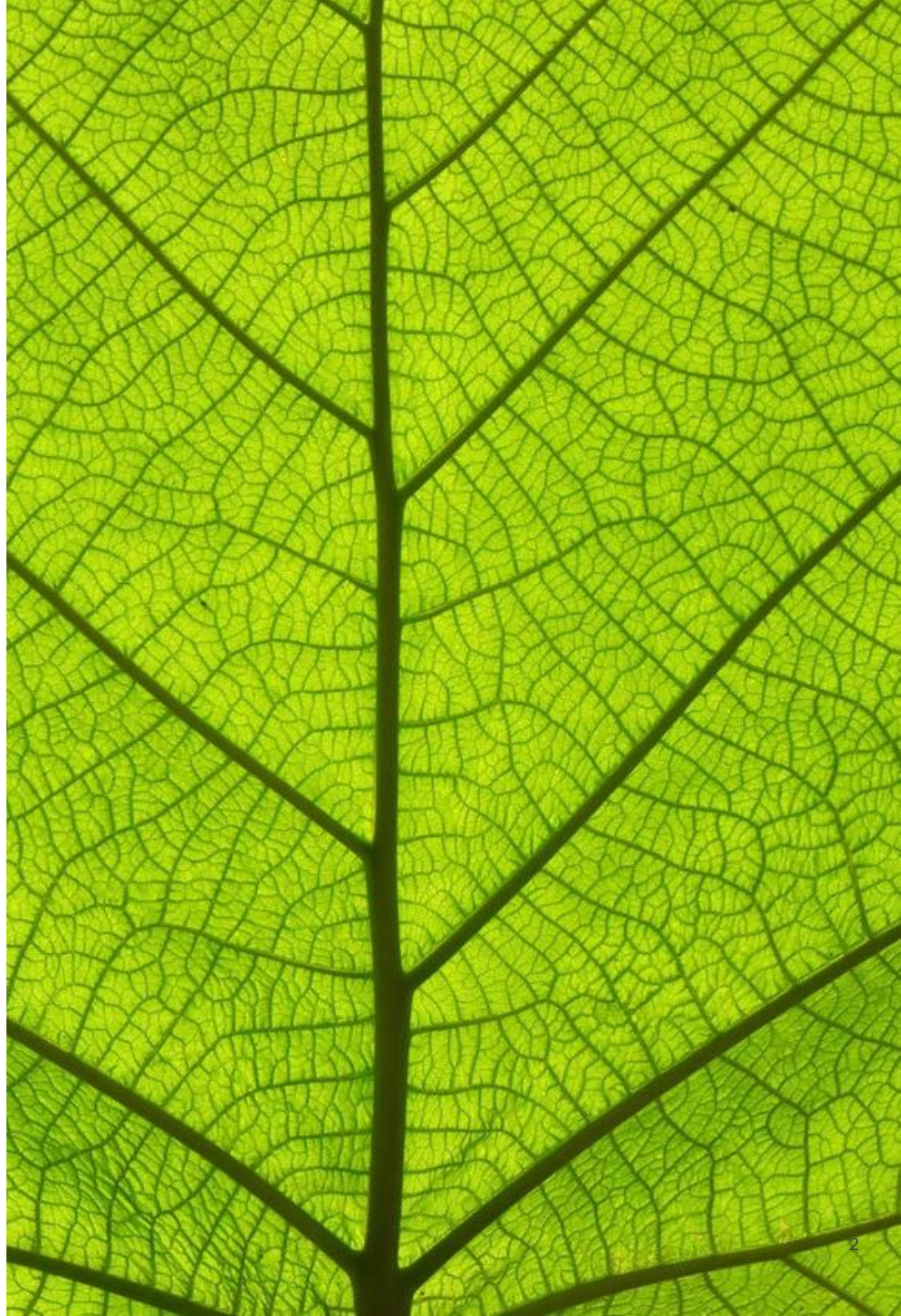
Kyndryl Data Security Posture Management

kyndryl

The Heart of Progress

Agenda |

- → Who is Kyndryl?
- → Market Data
- → Kyndryl Approach
- → Kyndryl's Value



kyndryl

A Client-Centric Approach to the World's Most Complex Business Problems

95%
customer retention and more than 10 years' avg relationship

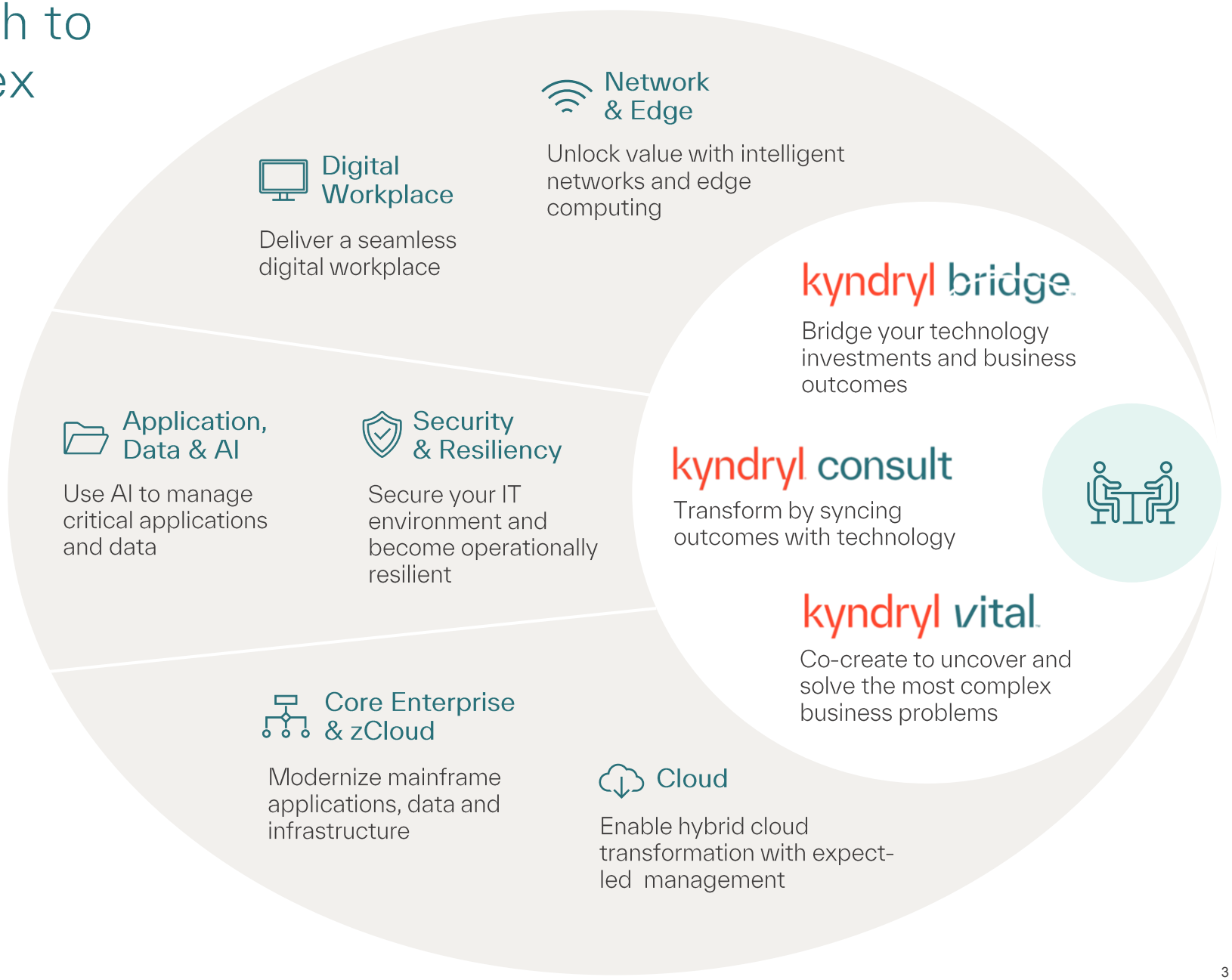
$3B
in annualized savings for customers via Bridge

Top 250
Fortune 1000 company

1,200+
customers deployed on AI-enabled Bridge

73k+
employees across 63 countries

77k+
technology certifications



kyndryl

Kyndryl's Security Journey from Legacy to Leading Edge:

Inherited:

1,800+	54	68
Business applications	On-prem datacenters	Data solutions/ information warehouses

Transformed:

<360	4	1	200-300M$
Business applications	Hyperscaler locations	Data platform	Savings

To better serve our clients, Kyndryl needed a lean, modern, and secure operating environment.

Safeguarded our business from cyber threats and improve continuity when we face any kind of disruption.

Embedded Zero Trust architecture and "secure by design" principles into all systems.

Moved to a cloud-centric infrastructure with SASE for a continuous security that protects data wherever employees work.

Launched a Security Intelligence Center and deployed SOAR tools for automated threat detection and response.

Our integrated Cyber Resilience framework helps businesses

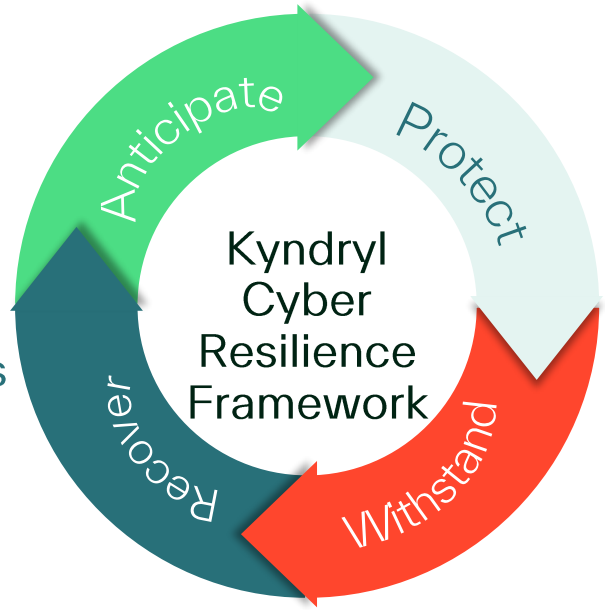
- Anticipate, assess, and mitigate rapidly evolving enterprise risks
- Protect brand and build trust
- Become operationally resilient
- Help maintain and achieve regulatory compliance

Governance, Risk, and Compliance Services

Provides understanding of risks by assessing security maturity, benchmarking controls across every lay of the enterprise

Incident Recovery Services

Minimizes the business impact of unplanned outages with enhanced, reliable, and scalable recovery across hybrid multi-cloud environments



Zero Trust Services

Mitigates risks and protects enterprise data by using zero trust principles to secure business outcomes

Security Operations and Response Services

Integrates the capabilities of offensive testing, managed security services, artificial intelligence and incident response to minimize business risk

Assess → Advise → Implement → Manage

Cloud

Core Enterprise & zCloud

Digital Workplace

Application, Data & AI

Network & Edge

kyndryl consult

kyndryl vital

kyndryl bridge

Kyndryl's Cyber Resilience Framework

Security + Resilience

	Anticipate	Protect	Withstand	Recover
	Governance, Risk and Compliance Services	Zero Trust Services	Security Operations and Response Services	Incident Recovery Services
Overview	GRC is the discipline that aligns the entire security program with business objectives. It moves cybersecurity from a technical conversation to a strategic dialogue about risk, enabling leaders to make confident, defensible decisions.	Zero Trust is the essential architecture for the borderless enterprise, operating on the principle of "never trust, always verify."	Security Operations is the front line of cyber defense, where threats are hunted, detected, and neutralized in real-time.	Cyber Resiliency is the ultimate backstop, ensuring a business can survive and rapidly recover from a destructive cyber-attack.
Subdomains	- Strategy, Risk & Regulation Advisory - Continuous Controls Monitoring and Management - Data Risk and Protection - Responsible AI - Third Party Risk Management - Security Assurance Management (SAMP) - Privacy	- Identity and Access Management - Cloud Security - Endpoint Security - Network Security	- Advanced Threat Detection, Monitoring and Response - Vulnerability and Risk Management - Security Operation Center Services	- Cyber Incident Recovery - Data Center Services
Differentiators	- Kyndryl is a highly regulated company operating in 60+ countries - Proven delivery model to meet global regulations - Strong partner ecosystem to leverage continuous advances - Kyndryl Bridge platform to rapidly scale up innovations for clients in a secure and resilient manner'	- 70M+ identities managed globally - Major relationships with hyperscalers to protect hybrid environments - Differentiated approach to Zero Trust vs. rest of the market - Strong integration with Network & Edge practice to optimize delivery	- 6 global SOCs and 4 local SOCs managing complex global orgs security - Platform to consolidate and optimize toolset - Differentiated Offensive Security approach to expand aperture - Continuous vulnerability management	- Market leading cyber recovery services - Pioneered 'Cyber Resilience' worldwide - Strong recovery expertise to help clients not only restore, but recover - Decades of experience managing datacenters

kyndryl

Governance, Risk, and Compliance Services

Yearly Assessments:

- **10,000+** Security & Privacy Tests
- **500+** 3rd Party Client Audits
- **160** SOC1/SOC2 Audits
- **150+** Internal Audit Assessments
- **100+** ISO PCI-DSS, HITRUST, Vendor Audits, etc.

451 Research

Top 5 Market Share Leader in Cyber Resilience Services Market 2024

Listed within the Top 10 for **Gartner®** Market Share: Security Services, Worldwide, 2024 View

MSSP Alert A CRA Resource

#1 in Top 250 MSSPs: Cybersecurity Company List and Research for 2024

NelsonHall TRANSFORM THROUGH INSIGHT

A Leader in 2024 NEAT™ Evaluation & Assessment Cyber Resiliency Services – Cyber Consulting & Strategy Construction

IDC

A Major Player in IDC MarketScape™ Worldwide Systems Integrators/ Consultancies for Cybersecurity Consulting Services 2024 Vendor Assessment

IDC

A Major Player in IDC MarketScape™ Worldwide Cybersecurity Risk Management Services, 2023

OMDIA

Leader in Omdia Universe, Global IT Security Service Providers 2024

Everest Group®

Leader in Cybersecurity Services PEAK Matrix® Assessment 2024 – North America

NelsonHall TRANSFORM THROUGH INSIGHT

A Leader in 2024 NEAT™ Evaluation & Assessment Cyber Resiliency Services – Overall Performance

Sources:
- 451 Research, part of S&P Global Market Intelligence Cyber Resiliency: Market Size & Market Position Study, June 2024
- NelsonHall NEAT™ Vendor Evaluation & Assessment for Cyber Resiliency Services 2024, Feb. 2024
- Omdia Universe, Global IT Security Services Providers 2024
- Everest Cybersecurity Services PEAK Matrix Assessment 2024 – North America, September 2024
- IDC MarketScape: Worldwide Cloud Security Services in the AI Era 2024–2025 Vendor Assessment, IDC Doc.#US52048124, Nov. 2024
- IDC MarketScape: Worldwide Systems Integrators/ Consultancies for Cybersecurity Consulting Services, 2024, IDC Doc. # US50463423, Jan. 2024
- MSSPAlert - Top 250 MSSPs: Cybersecurity Company List and Research for 2024 – Link
- Gartner - Market Share: Security Services, Worldwide, 2024, published 25 April 2025- ID G00827176

GARTNER is a registered trademark and service mark and IT Symposium/Xpo is a trademark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and are used herein with permission. All rights reserved.

Top Data Security Priorities tied to Business Outcomes:

	How Kyndryl's Data Security Services Help:
Building a Strong Data Security Team	**Augment scarce Responsible AI and data-security expertise** with consulting and co-managed services to stand up sustainable programs fast.
Managing Complex Regulations and Compliance	**Simplify compliance** by mapping requirements to recognized frameworks, turning policies into actionable processes, and **providing audit-ready documentation with ongoing compliance reports.**
Balancing Risk Management with Responsible AI	Secure the AI lifecycle, enabling **safe AI innovation without increasing data risk.**
Improving Data Quality, Bias, and Fairness	Unify data discovery, labeling/classification, and data lifecycle management to **reduce bias exposure and raise training-data integrity.**
Building Accountability, Governance and Controls	**Build responsible AI operating models and technical systems** that offer centralized visibility into AI activities - who is doing what and which data is being used where.

64%

Of data leaders and professionals face significant challenges providing timely, secure data access to authorized users.

kyndryl

Source: Immuta: 2025 State of Data Security Report

Top Factors Impacting Organizations Data Security Capabilities Today:

99%

of organizations have sensitive data dangerously exposed to AI tools

50%

of data leaders and professionals say compliance and privacy are their top data concerns in 2025

41%

say not having the right tools blocks efficient data access and management

88%

of organizations have exposed sensitive cloud data

kyndryl

Source: Immuta: 2025 State of Data Security Report

Common Challenges Kyndryl Sees in Data Security Today:

Scarcity of expertise and talent

A shortage of skilled staff that have strong expertise in responsible AI (e.g. governance, ethics, security, ...) and data security is one of the most widespread challenges our clients shared.

Regulatory complexity & compliance

The rapidly evolving regulations in the AI, data protection and cybersecurity space leave companies feeling overwhelmed. Many organizations are unsure which industry standards to follow, sometimes leading to inconsistent or incomplete controls.

Risk vs. Innovation pressure

Striking the right balance between managing risk and responsible AI adoption and the pressure to innovate and deploy solution is challenging for many of our clients. Data security and privacy programs aren't yet fully adapted for AI.

Data quality, bias & fairness issues

Ensuring AI models are trained on high-quality, representative data remains challenging. Data silos, bias in historical data, and inherent limitations of LLMs lead to AI that can inadvertently produce outputs not in line with enterprise guidelines and standards.

Accountability, governance and controls gaps

Defining clear accountability and establishing robust governance and sound (technical) controls is difficult and challenging for many organizations. Result: no central visibility into who is doing what with AI, or which data is being used where.

"In a world where data fuels innovation, Kyndryl's Data Security Posture Management helps organisations protect and ethically govern their data - enabling trusted, scalable AI and resilient digital transformation."

Anthonie De Bos
Vice President, Practice
General Management

kyndryl

Data Security Posture Management: Our Approach

Data Security Posture Management Pillars

Identify

- Automated data scanning and classification
- Unified data maps and catalogs
- Label-driven insights and reporting

Protect

- Protect data at scale with sensitivity labels
- Enforce data protection across Microsoft 365 and beyond

Prevent

- Policy-driven detection of risky activities
- Contextual alerts with user behavior analytics
- Automated workflows for investigation and response

Govern

- Retention policies and labels
- Archival and defensible deletion
- Comprehensive eDiscovery workflows

Data Consult Security Posture Management: Journey

Organization's Challenges

Lack of visibility to sensitive data

Unauthorized access to sensitive info

Protect data from insider and external threats

Compliance with applicable laws, regulations and policies

Detect, investigate and respond to unauthorized access

Data Discovery & Classification

- Structured &unstructured data
- Automated classification

Discover and classify data by type and sensitivity

Data Encryption

- Use KMS for encrypting with strong standards
- Persistent information protection

Encrypt data at rest and in-motion

Data Monitoring

- Define and implement Data monitoring policies to protect sensitive data, and on devices

Define and implement DLP policies across approved devices

Compliance & Governance

- Align data protection with regulations
- Ensure data retention, archival and deletion policies are followed

Enforce policies and compliance

Investigate & Auditing

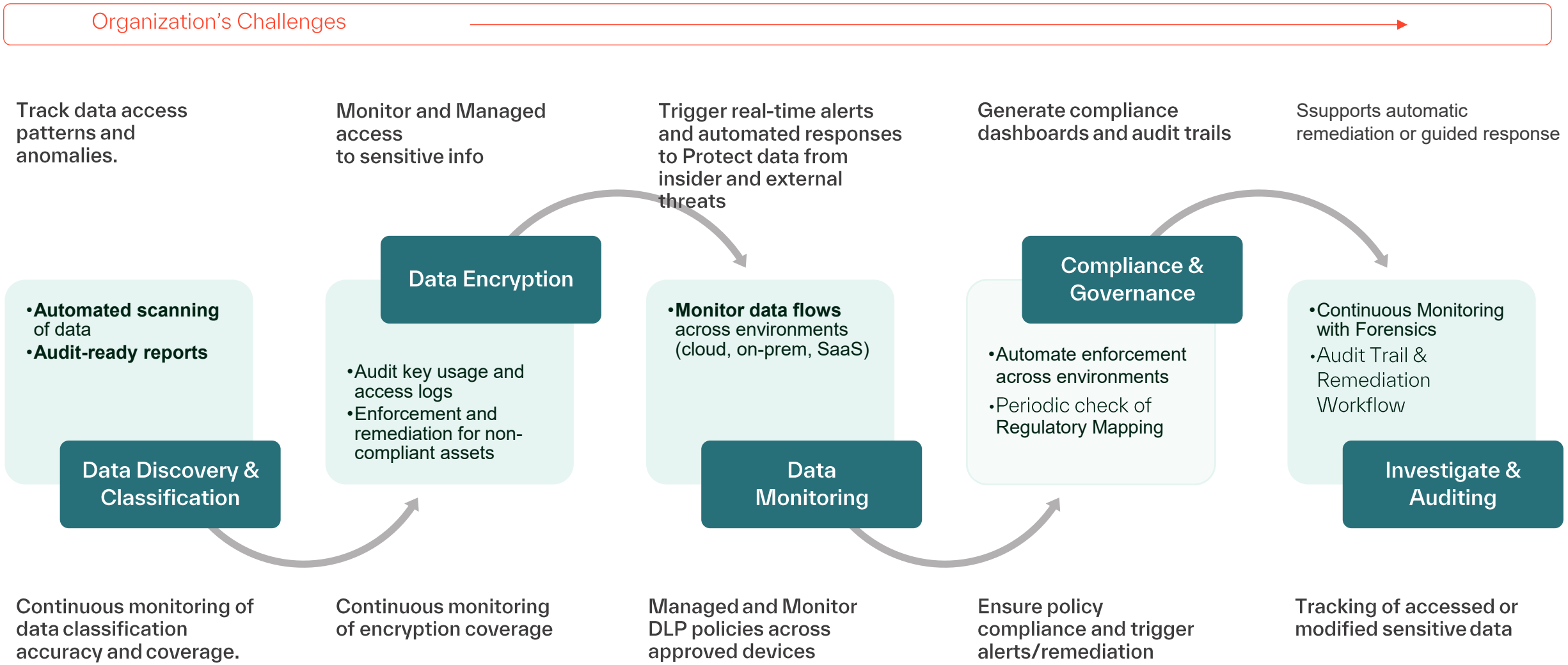
- Monitor alerts for data assets
- Assist with investigations

Plan and iterate on the data security measures

kyndryl

Data Security Posture Management Managed : Journey

Organization's Challenges



kyndryl

DSPM Best Practices

Data Discovery & Classification

Establish a data inventory baseline

Implement real-time discovery and classification to keep pace with data changes

Align with governance frameworks

Focus classification and protection efforts on data with the highest regulatory or business impact

Data Encryption

Apply consistent labeling and protection policies, across productivity tools (e.g., Word, Excel, SharePoint)

Evaluate exposure to quantum threats and prioritize systems for PQC migration

Adopt systems and solutions that can switch cryptographic algorithms without major reengineering

Data Monitoring

Use centralized dashboards to monitor DSPM recommendations

Continuously refine detection rules based on threat intelligence and incident learnings

Establish baselines for normal behavior and flag deviations

Compliance and Governance

Define roles, responsibilities, and escalation paths for data governance and compliance

Map controls to industry frameworks like NIST CSF, ISO 27001, and COBIT

Integrate compliance checks into DSPM workflows - especially for data discovery, classification, and protection

Data Consult Security Posture Management: Engagement Process

Assessment and Discovery

1. **Enterprise data scoping for assessment**
2. **Security, risk & privacy assessment** (for structured and unstructured data)
   - Review data security and risks for current governance, policies, and practices
3. **Recommendations, prioritization and roadmap**
   - Assist with prioritization of gaps
   - Present high-level recommendations to addresses maturity gaps
   - Assessment results

Pilot and POC

1. **Pilot planning**
   - Define pilot scope
   - Identify team and assign responsibilities
2. **Pilot solution provisioning**
3. **Data discovery and classification** (for limited scope)
   - Define data classification rules
   - Scan and classify data
4. **Configure and test data security policies** for DLP, access control, sensitivity labels and data retention for structured and unstructured data
5. **Configure and test insider risk management policies**
6. **Risk and policy compliance monitoring**
7. **Pilot review and evaluation**

Production and deployment

1. **Production planning**
   - Review pilot outcome and refine implementation plan
   - Define timelines for rollouts
   - Solution integration with existing tools
2. **Data governance all enterprise data assets**
   - Define/refine, test and implement classification rules and sensitivity labels
3. **Data Security configuration**
   - Sensitive information protection controls
   - DLP policies
4. **Insider risk management policies**
   - Define/refine, test and implement insider risk management rules and policies
5. **Policy compliance monitoring**
   - Update monitoring policy based on PoC outcomes
   - Enable automated reporting and audit trails
6. **Training and knowledge transfer**
   - Provide training to key stakeholders using the deployed solution
7. **Solution integration**

Consult Data Security Posture Management

- → Architectural documentation
- → Baseline of data scanning, discovery and classification
- → Data discovery and classification mapping
- → Metadata management and lineage
- → Create policies to access, move, and share data Limit the growth of real-time data by eliminating duplicates

Accelerate Customer Data Visibility

Rapidly scan, discover, and classify data across hybrid environments.

Integrate External Data Sources

Use connectors to bring in third-party data for comprehensive data security and compliance.

Protect Sensitive Information

Locate and secure high-risk data—even in unstructured formats like emails and documents.

Enable Secure Data Sharing

Implement policies that govern how data is accessed, moved, and shared—internally and externally.

Prevent Data Leakage

Deploy DLP policies that proactively block unauthorized data transfers.

Drive Compliance Outcomes

Automate policy enforcement and generate audit-ready reports to meet regulatory needs.

Mitigate Insider Threats

Detect risky user behavior and prevent data misuse before it escalates.

Reduce Data Sprawl

Identify and eliminate duplicate data to optimize storage and reduce risk.

Supported Vendor Products:

Microsoft Purview

Service Module:

Kyndryl Data Governance Implementation Service

kyndryl

Data Security Posture Management Managed

- Programmatic services for MS Purview:
- Kyndryl's DSPM Managed Services, delivered by certified Microsoft Purview experts, provide continuous oversight and refinement of your data governance strategy
- Data Security – DLP policies, Information Protection
- Risk and Compliance – Data lifecycle management through retention policies, support legal and compliance teams
- Data Governance – maintain data catalogs, data discovery and classification rules, maintain glossaries. Add/modify new data sources for discovery and cataloging.
- Operational services for platform management including health checking and break fix support 8*5

kyndryl

End-to-End Hybrid Visibility

Auto discovery and classification across all environments

Proactive Data Risk Management

Continuous posture monitoring & strategic shift

AI Readiness & Governance Alignment

AI-adaptive capabilities from the ground up

Simplified Governance Stack

Unified controls—encryption, DLP, compliance

Prevent Data Leakage

Managed and Monitor DLP policies across approved devices

Drive Compliance Outcomes

Generate compliance dashboards and audit trails

Consulting + Automation Synthesis

Expert-led implementation with managed refinement

Partnership with Microsoft

Built-in Purview integration and certified expertise

Supported Vendor Products:

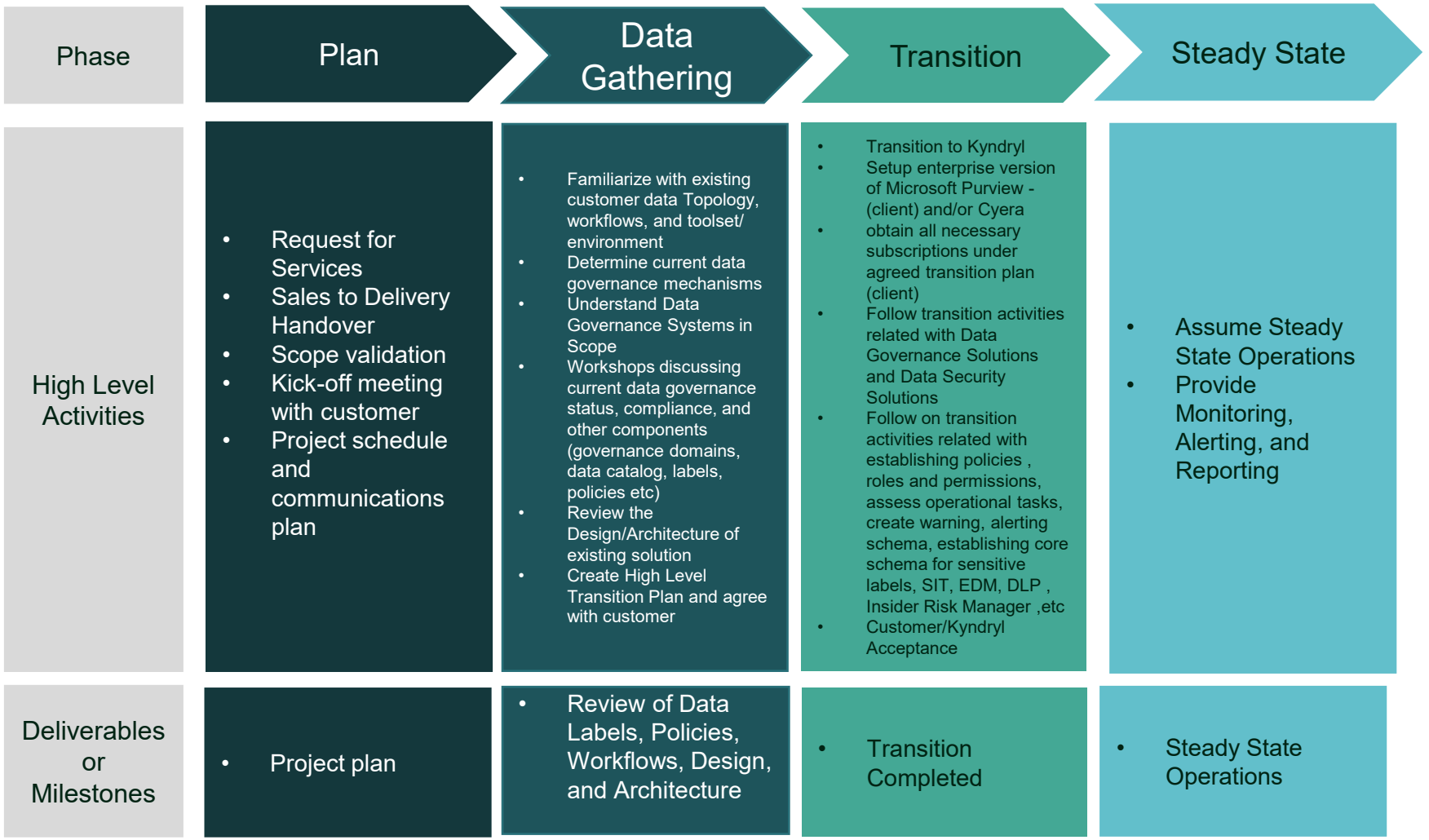
Microsoft Purview

Service Module:

Kyndryl Data Governance Implementation Service

Delivery Approach

The Delivery Approach for transitioning a clients Data Security Posture Management into Kyndryl Managed Services is shown below.



Key DSPM Capabilities

Data Discovery & Classification

Identifies and categorizes sensitive data across systems to apply appropriate protections.

Added Value:

- **Automated scanning tools** identify sensitive data across structured and unstructured sources.
- **Classification by sensitivity level** allows tailored protection strategies.
- Improved visibility into data assets **supports better governance.**
- **Foundation for compliance** with privacy laws and internal policies.

Data Encryption & Tokenization

Protects data at rest and in transit using cryptographic techniques.

Added Value:

- End-to-end encryption **protects data in transit and at rest** from unauthorized access.
- Tokenization **replaces sensitive data with non-sensitive** equivalents for safer processing.
- **Compliance with standards** like PCI-DSS and HIPAA is easier to achieve.
- **Reduced breach impact** by rendering stolen data unusable.

Insider Threat Detection

Monitors user behavior to identify and respond to potential data misuse.

Added Value:

- Behavioral analytics **detect anomalies** in user access and data usage.
- Real-time alerts help security teams **respond before damage occurs.**
- Audit trails and logging **support investigations and accountability.**
- **Protection** of intellectual property and sensitive business data.

Data Loss Prevention (DLP)

Prevents unauthorized sharing or leakage of sensitive data.

Added Value:

- Policy enforcement across endpoints, email, and cloud apps **prevents unauthorized sharing.**
- **Granular controls** allow for context-aware decisions (e.g., blocking, warning, logging).
- **Visibility into data movement** helps identify risky behaviors.
- **Reduced risk of accidental leaks** from employees or contractors.

Secure Data Sharing & Collaboration

Facilitates protected exchange of data between internal teams and external partners.

Added Value:

- Encrypted file sharing platforms **safeguard confidentiality during collaboration.**
- Role-based access controls **limit exposure** to only authorized users.
- Audit logs track **who accessed what and when.**
- Secure workflows enable **productivity without compromising data integrity.**

kyndryl

Biggest Data Access Challenges IT & Security Teams are Facing:

Q: What are the top business challenges impacting data access and management?

Source: Immuta: State of Data Security Report 2025

Kyndryl's Key Value:

1. Unique global partnership with Microsoft
2. Proven ability to align data objectives with business outcomes
3. World's largest infrastructure services provider proves ability to manage data
4. Cross-border data expertise
5. Cross-practice collaboration with Kyndryl's Apps, Data and AI practice
6. Regulatory and compliance experience

kyndryl

The Heart of Progress.™

Kyndryl help secure and strengthen resilience by protecting mission-critical systems to keep the world's technology safe and available.

© Copyright Kyndryl, Inc. 2025

Kyndryl is a trademark or registered trademark of Kyndryl, Inc. in the United States and/or other countries. Other product and service names may be trademarks of Kyndryl, Inc. or other companies.

This document is current as of the initial date of publication and may be changed by Kyndryl at any time without notice. Not all offerings are available in every country in which Kyndryl operates. Kyndryl products and services are warranted according to the terms and conditions of the agreements under which they are provided.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

GRC → Data Security and Privacy Management

Data Risk and Protection

Provide automated, AI-driven visibility and protection for sensitive data across hybrid environments—enabling proactive risk mitigation, regulatory compliance, and a secure foundation for responsible AI adoption.

Kyndryl's Data Risk and Protection offering delivers end-to-end services that help organizations protect sensitive information, ensure regulatory compliance, and unlock the full value of their data. Built on a foundation of data discovery, classification, and governance, the offering spans consulting, implementation, and managed services to support secure data usage across hybrid and multicloud environments. It integrates with platforms like Microsoft Purview to automate protection, enforce access policies, and enable responsible AI adoption. By combining deep security expertise with platform-agnostic delivery, Kyndryl empowers customers to reduce risk, simplify compliance, and build trust in their data-driven operations

Capabilities:

- → Architectural documentation
- → Baseline of data scanning, discovery and classification
- → Data discovery and classification mapping
- → Metadata management and lineage
- → Create policies to access, move, and share data Limit the growth of real-time data by eliminating duplicates

kyndryl

Change Management
Continuous communication to stakeholders informing them of policies, requirements and data changes.

Roles & Responsibilities
Identify the right people to steward, sponsor, socialize and deliver a positive return on data.

Metadata Management
Establishment of a business glossary to define and locate data, including information about business and technical processes, data rules, and logical and physical data structures.

Data Quality Management
Profile, measure and monitor data quality to increase its value and opportunities to use it throughout the organization.

Technology Alignment
Data governance helps streamline software development lifecycles and align IT with business goals.

Master Data Management
Deliver a single, consistent and accurate view of critical business data across systems, reduce the cost of data integration, and improve digital experiences for customers, products, employees, etc.

Our Preferred Partners:

Microsoft Purview

Key Use Cases:

Hybrid Data Discovery and Classification - *Automatically identifying and labeling sensitive data across cloud and on-prem environments*

- Improve visibility into data estates using machine learning classifiers
- Reduces manual effort through automated discovery and classification
- Supports regulatory compliance with built-in labeling and encryption
- Enables scalable governance across Microsoft and non-Microsoft endpoints

Continuous Monitoring of Third-Party Risk-
Ongoing surveillance of vendor activities and risk posture

- Detects emerging threats and changes in vendor risk profiles in real time
- Supports proactive risk mitigation and incident response
- Improve transparency through automated alerts and dashboards
- Strengthens resilience by identifying systemic or cascading risks

Regulatory Compliance and Audit Readiness -
Improving third-party relationships meet legal and industry standards

- Simplifies documentation and evidence collection for audits
- Reduces penalties and reputational damage from non-compliance
- Demonstrates due diligence to regulators and stakeholders

Contract Lifecycle Risk Management - *Embedding risk controls throughout the vendor contract lifecycle*

- Identifies and mitigates risk during contract negotiation and renewal
- Provides inclusion of key clauses like data protection and SLAs
- Tracks compliance with contractual obligations over time
- Reduces legal exposure and improves vendor accountability

Partner Specific Information

kyndryl

Microsoft Purview Overview

Microsoft Purview

Data Security

For information and cybersecurity teams

- Data Loss Prevention
- Insider Risk Management
- Information Protection

Data Governance

For data consumers, data engineers, data officers

- Data Map
- Data Catalog
- Data Estate Insights

Risk & Compliance

For risk, compliance, and legal teams

- Data Lifecycle Management
- eDiscovery & Audit
- Communication Compliance

On-prem and multi-cloud

Unstructured & structured data

Across IaaS, and SaaS

Govern and Secure Data with Microsoft Purview