Infotechtion

Replacing Legacy Document and Records Management systems with Microsoft 365

Thursday, 20 June 2024

7:00am PDT
9:00am CDT
10:00am EDT

15:00 GMT
16:00 CEST

Speakers

Atle Skjekkeland
Chief Executive Officer

Infotechtion

Vivek Bhatt
Chief Technology Officer

Infotechtion

Rakesh Chenchery
Chief Technology Officer

Proventeq

Charles Tostain
EMEA Manager, Global Black Belt Team, Data Risk

Microsoft

Agenda

- Introduction
- Why Microsoft 365
- What to do
- How to migrate
- Q&A

Member of
Microsoft Intelligent
Security Association

Microsoft Security

Microsoft
Solutions Partner

Security

Specialist
Information Protection and
Governance

Microsoft

Preferred

Content AI

Microsoft
Solutions Partner

Modern Work

Specialist
Adoption and Change
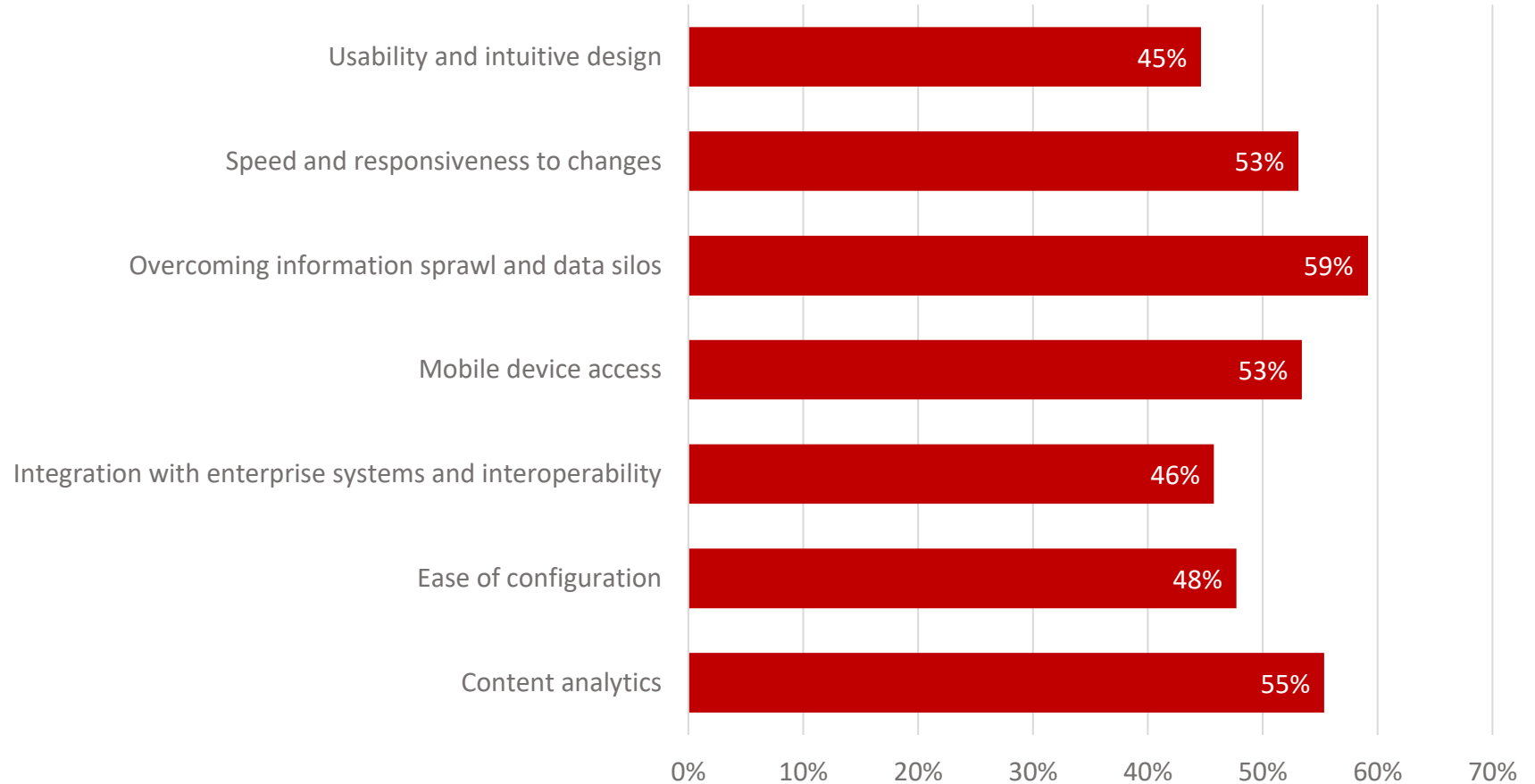Management

Microsoft

proventeq

Infotechtion

Enterprise Content Management

Case management
Document management
Document centric
collaboration
Records management
Email management
Archiving
Imaging
Workflow
Templates
Version control
Audit trail

Archived content

Collaborative content

Transactional content
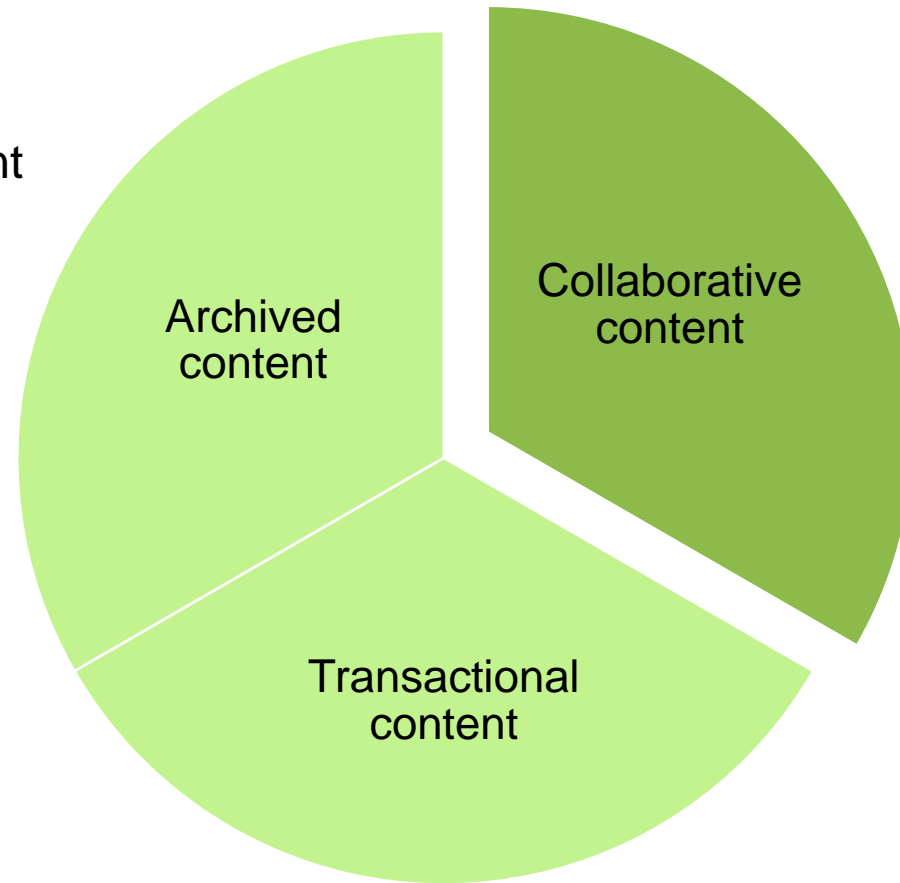
Immutability
Retention
Disposition review
Search
Metadata
Taxonomies
Links
Access control
Redaction
Notifications
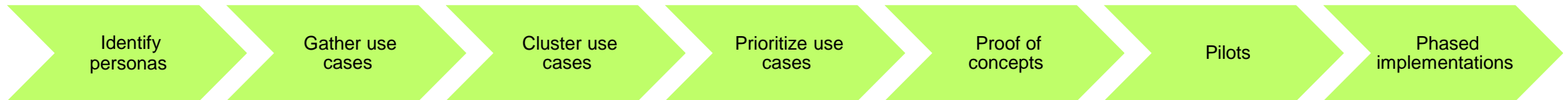Numbering
OCR/ICR

Microsoft

proventeq

Infotechtion

ECM: Expensive, Complex, and Minimal

How well do your existing IM/DM/RM systems meet your needs in the following core areas? -- % saying "**fails**" or "**struggles**"

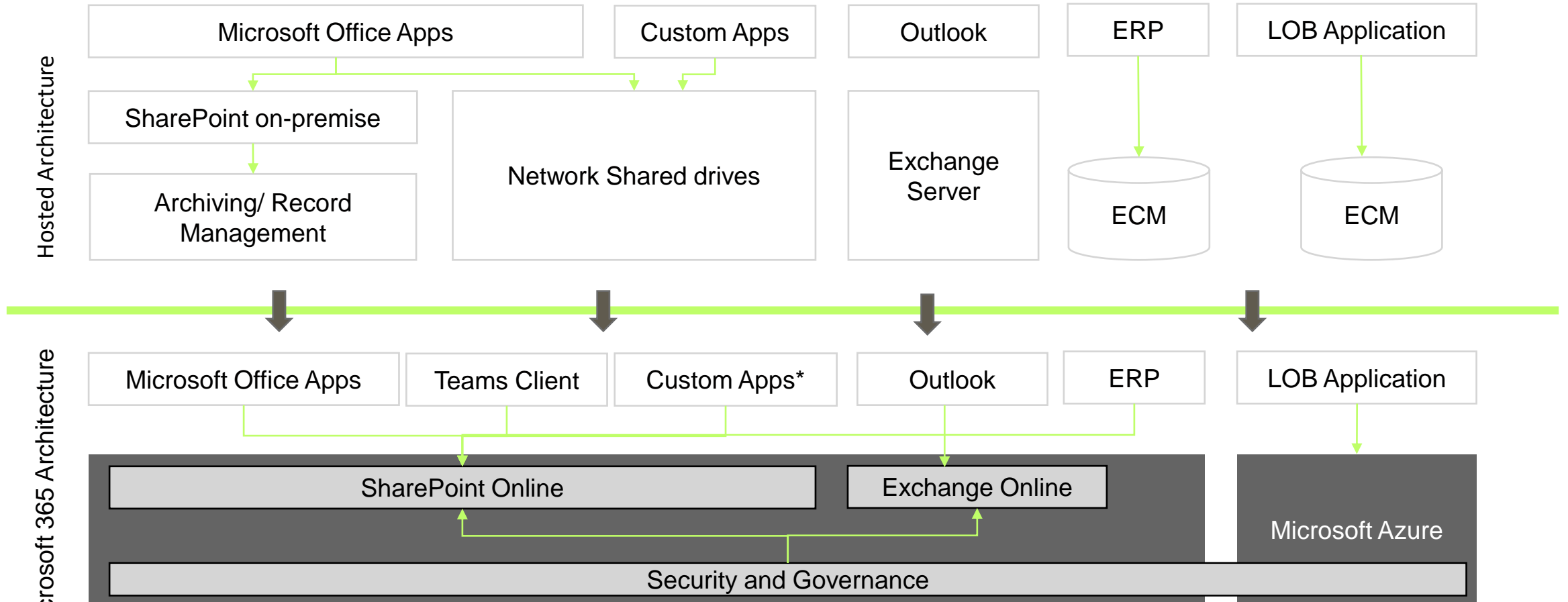| Category	Percentage
Usability and intuitive design	45%
Speed and responsiveness to changes	53%
Overcoming information sprawl and data silos	59%
Mobile device access	53%
Integration with enterprise systems and interoperability	46%
Ease of configuration	48%
Content analytics	55%

Microsoft   proventeq   Infotechtion

Replace legacy ECM with M365

- Define use cases, not features
- Plan for continuous improvements, not install and forget
- Try to make it simple, smart, safe, secure, scalable, and sexy

| Identify personas | Gather use cases | Cluster use cases | Prioritize use cases | Proof of concepts | Pilots | Phased implementations |

Microsoft   proventeq   Infotechtion

Transform content management

Hosted Architecture

| Microsoft Office Apps | Custom Apps | Outlook | ERP | LOB Application |

| SharePoint on-premise | Network Shared drives | Exchange Server | ECM | ECM |
| Archiving/ Record Management | | | | |

Microsoft 365 Architecture

| Microsoft Office Apps | Teams Client | Custom Apps* | Outlook | ERP | LOB Application |

SharePoint Online   Exchange Online

Microsoft Azure

Security and Governance

*Examples include Digital Signatures app, Meeting Decisions app, Unique Number Generator app, Authority Relations SharePoint site, Physical Records Management SharePoint site

Microsoft   proventeq   Infotechtion

Why M365

Top security challenges with Data

Insufficient visibility and controls
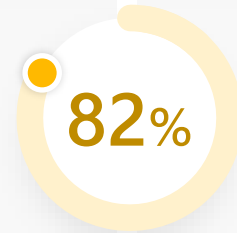
82% of leaders cited leakage of sensitive data as their main concern.
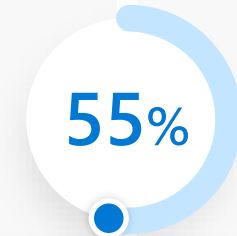
Overreliance and ethical concerns on AI outputs
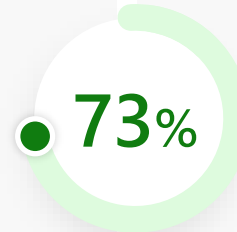
73% of leaders worried about ingress of inaccurate data and hallucinations; 57% concerned about harmful, biased, or distressing output.

Increased regulatory liability and uncertainty

55% of leaders lack understanding of how AI is and will be regulated, amongst different industries.

48% of leaders expect to continue banning all use of AI in workplace.

* % of CISOs and Security Decision Makers (ISMG First Annual Generative AI Study: Business rewards vs. Security Risks)
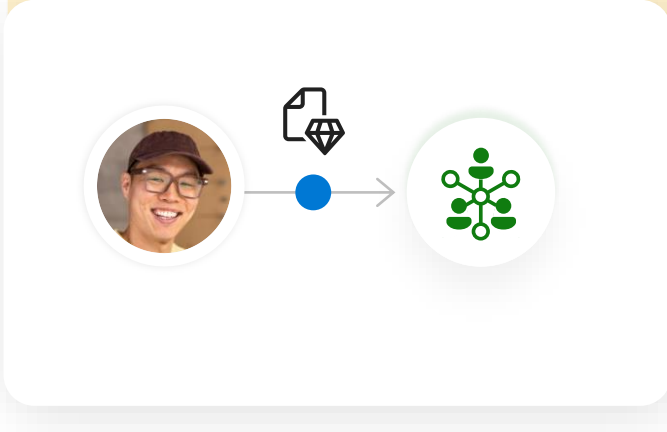
Security concerns associated with Data usage

🚫⚠️ Insufficient visibility into the usage of Data can result in security and compliance challenges.
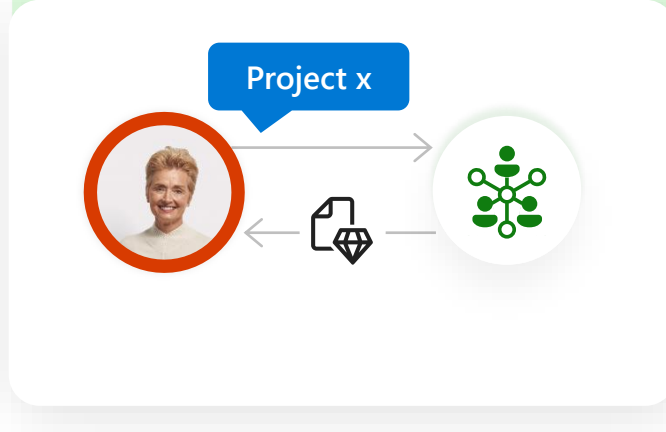
1

Data leak:
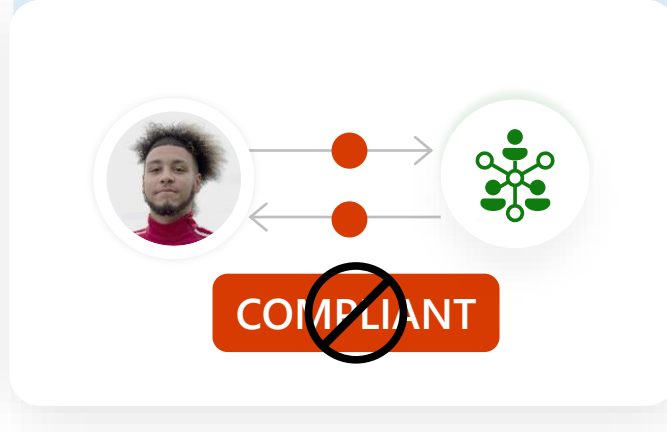Users may inadvertently leak sensitive data to external party

2

Data oversharing:
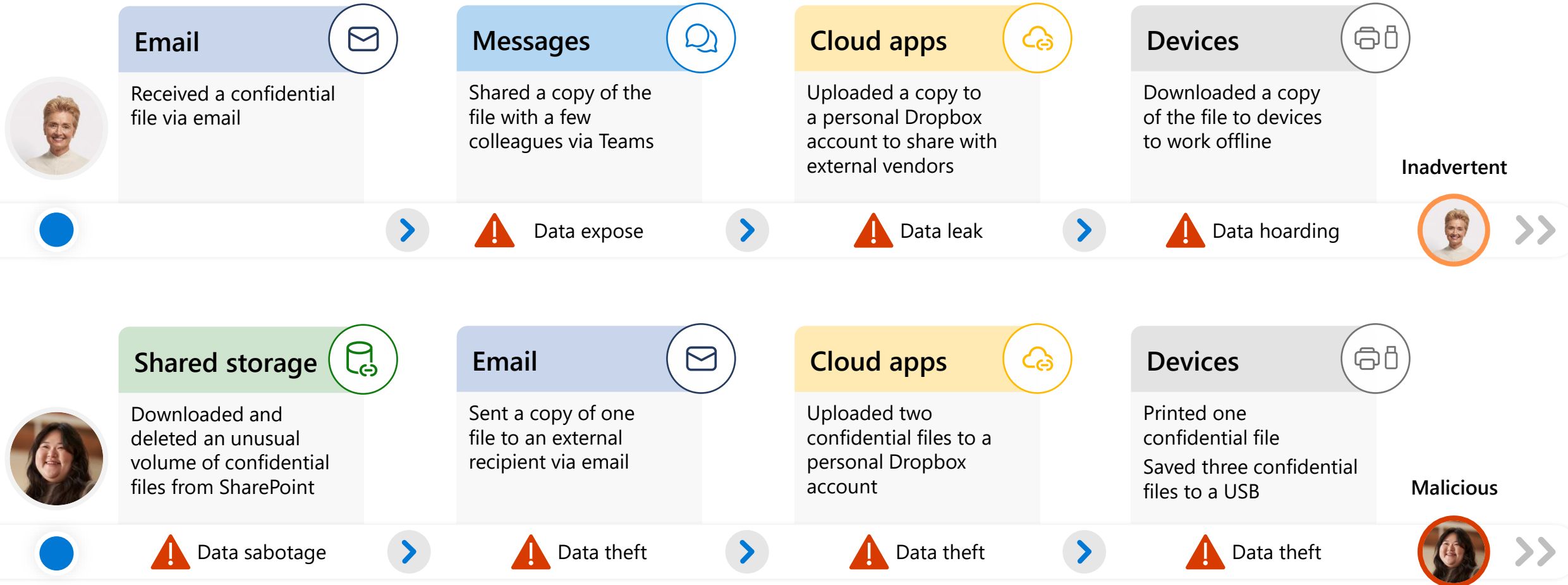Users may access sensitive datas they are not authorized to view or edit

Project x

3

Non-compliance usage:
Users use AI apps to generate unethical or other high-risk content

COMPLIANT

Data security incidents can happen anytime anywhere

Data doesn't move itself; people move data

Email	Messages	Cloud apps	Devices
Received a confidential file via email	Shared a copy of the file with a few colleagues via Teams	Uploaded a copy to a personal Dropbox account to share with external vendors	Downloaded a copy of the file to devices to work offline

Inadvert

⚠️ Data expose   ⚠️ Data leak   ⚠️ Data hoarding

Shared storage	Email	Cloud apps	Devices
Downloaded and deleted an unusual volume of confidential files from SharePoint	Sent a copy of one file to an external recipient via email	Uploaded two confidential files to a personal Dropbox account	Printed one confidential file Saved three confidential files to a USB

Malicious

⚠️ Data sabotage   ⚠️ Data theft   ⚠️ Data theft   ⚠️ Data theft

The most urgent data security challenges

- **Discover** sensitive data, whether structured or unstructured, on-premises or in the clouds

- **Secure configuration** to prevent sophisticated attacks

- Detect how users are **interacting with data** and identify **insider risks**

- Ensure your data remains **secure** from **data leakage** and **data exfiltration** activities

Microsoft   proventeq   Infotechtion
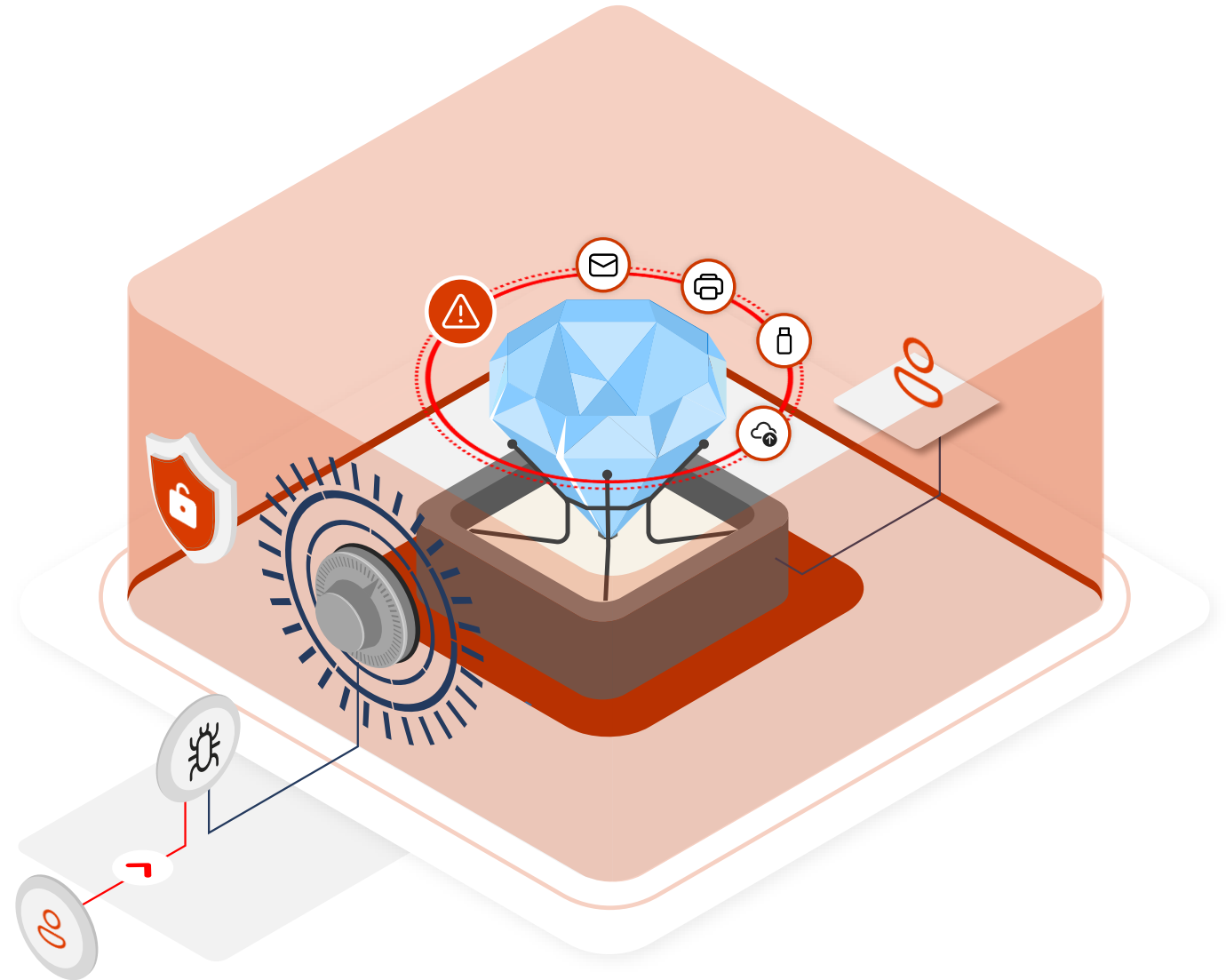
Why Microsoft 365 is Safe : Purview

Secure and govern your data

Comprehensive data security
Secure data across its lifecycle, wherever it lives

Data Loss Prevention
Insider Risk Management
Information Protection

Modern data governance
Govern data seamlessly to empower your organization

Business & Data Glossary
Data Catalog
Data Quality Management
Master Data Management
Data Estate Health Insights

Risk and compliance posture
Manage critical risks and regulatory requirements

---

eDiscovery
Data Lifecycle Management
Communication Compliance
Records Management
Compliance Manager

Unified Platform: Data Map, Data Classification, Data Labels, Audit, & Data Connectors

Copilot for Microsoft 365 is transforming work

60%
of leaders say a lack of innovation or breakthrough ideas is a concern

64%
of people have struggled with finding time and energy to get their work done

70%
of people indicated they would delegate as much as possible to AI to lessen their workloads

68%
said Copilot improved the quality of their work

70%
said Copilot made them more productive

77%
said they didn't want to give Copilot up

Discover AI risks associated with data, users, and AI apps

Identify sensitive data in AI interactions with 300+ pre-built classifiers

- Sensitive info types
- Credential SITs
- Named entities
- Context-based classification
- Exact data match
- OCR
- Trainable classifiers
- Fingerprint SITs

Understand user activities and detect risky access with curated and correlated detections

Users who visited AI apps

7.1K

- ■ High Risk
- ■ Medium Risk
- ■ Low Risk
- ■ None

Discover risky and unmanaged apps in use with a catalog of hundreds of AI apps

Risk score

47 MB

Total
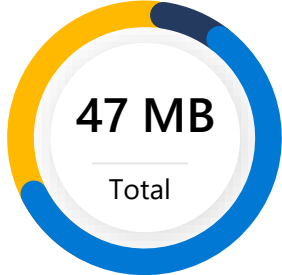
- ■ Traffic from high risk apps
- ■ Traffic from medium risk apps
- ■ Traffic from low risk apps

Protect AI apps and sensitive data in prompts and responses

Protect sensitive data in AI interactions automatically with persistent labeling policies and DLP

Confidential
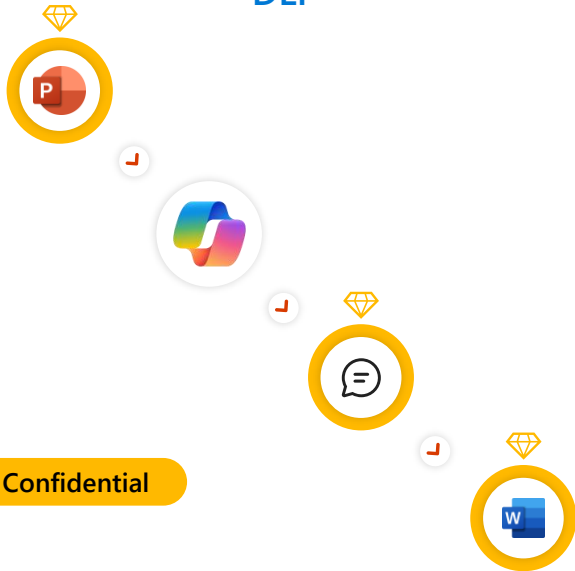
Approve, restrict, or block access to AI apps based on identity risks and the risk posture of AI apps
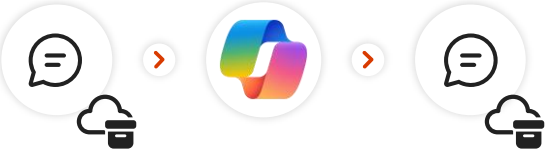
9

5

2
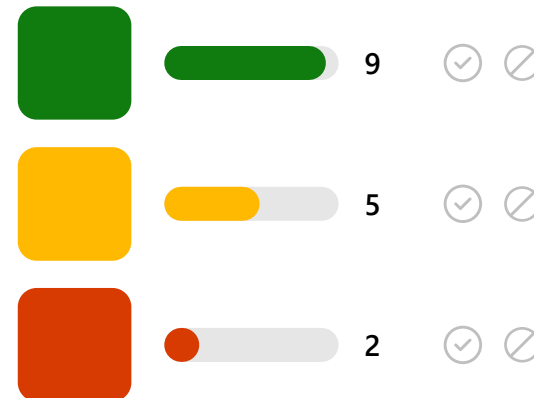
Detect and respond to threats in Copilot with out-of-the-box threat protection
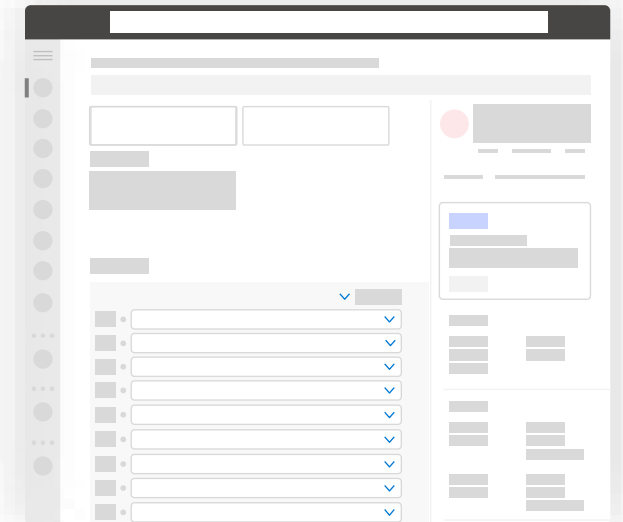
Govern Copilot usage to comply with regulatory and code-of-conduct policies

Manage data lifecycle, including data that can be processed by Copilot, prompts, and responses, with retention policies

Detect regulatory or code of conduct violations in Copilot with ML-powered communication compliance

⚠️ Confidential projects

⚠️ Corporate sabotage

⚠️ Regulatory collusion

Investigate potential incidents and respond to litigations with audit logs and eDiscovery

John Doe project obsidian

Secure future initiative (sfi)

| Secure by design | Secure by default | Secure operations |

Security culture and governance

Protect identities and secrets

Protect tenants and isolate production systems

Protect networks

Protect engineering systems

Monitor and detect threats
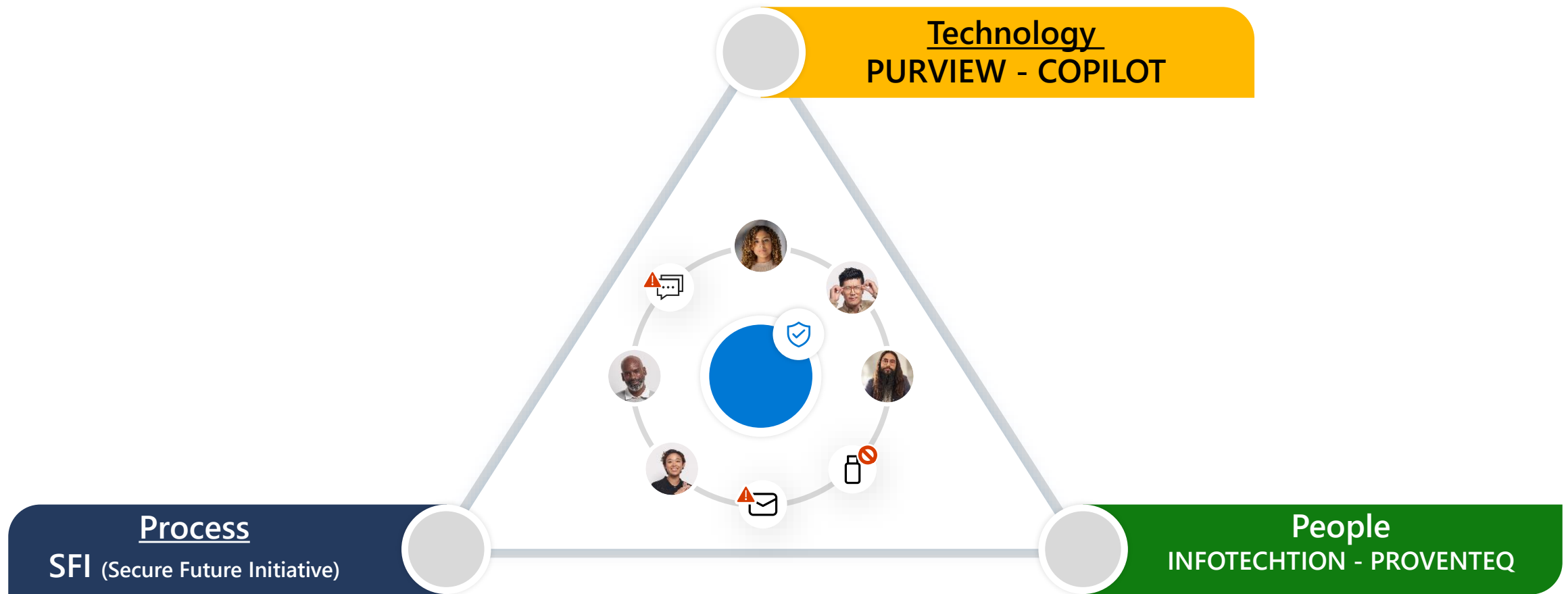
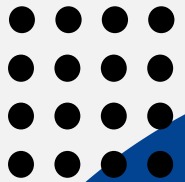**Accelerate response and remediation**

Continuous improvement

Paved path

Standards

Microsoft   proventeq   Infotechtion

Microsoft's approach to data security

Technology
PURVIEW - COPILOT

Process
SFI (Secure Future Initiative)

People
INFOTECHTION - PROVENTEQ

Microsoft   proventeq   Infotechtion

What to do

Common Migration Scenarios

User Home Directories

Team/Project Collaboration spaces

Departmental Fileshare

Large File Stores

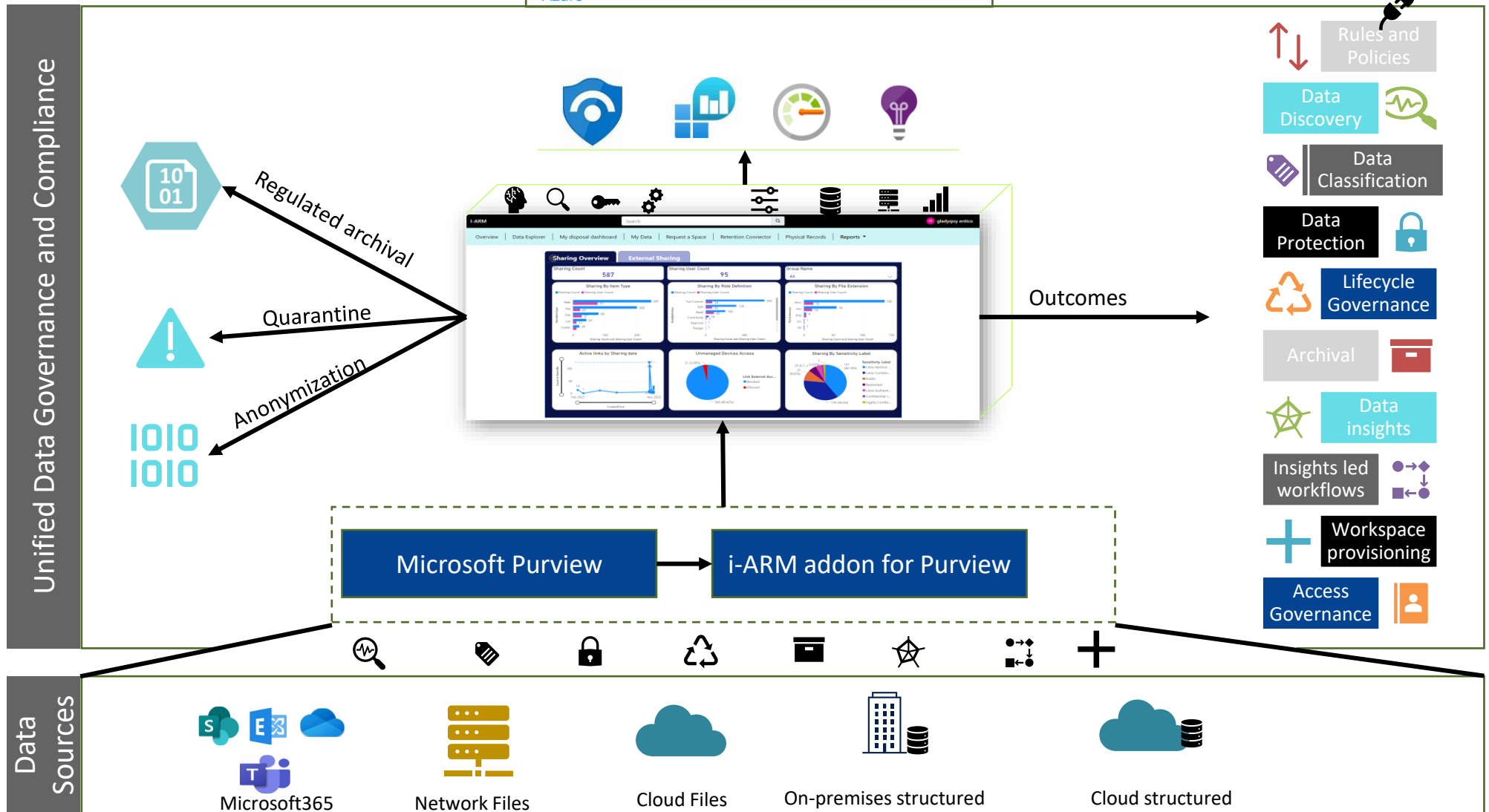Application-Focused Data / Backups

Archival Storage

Microsoft

proventeq

Infotechtion

A Reference Architecture
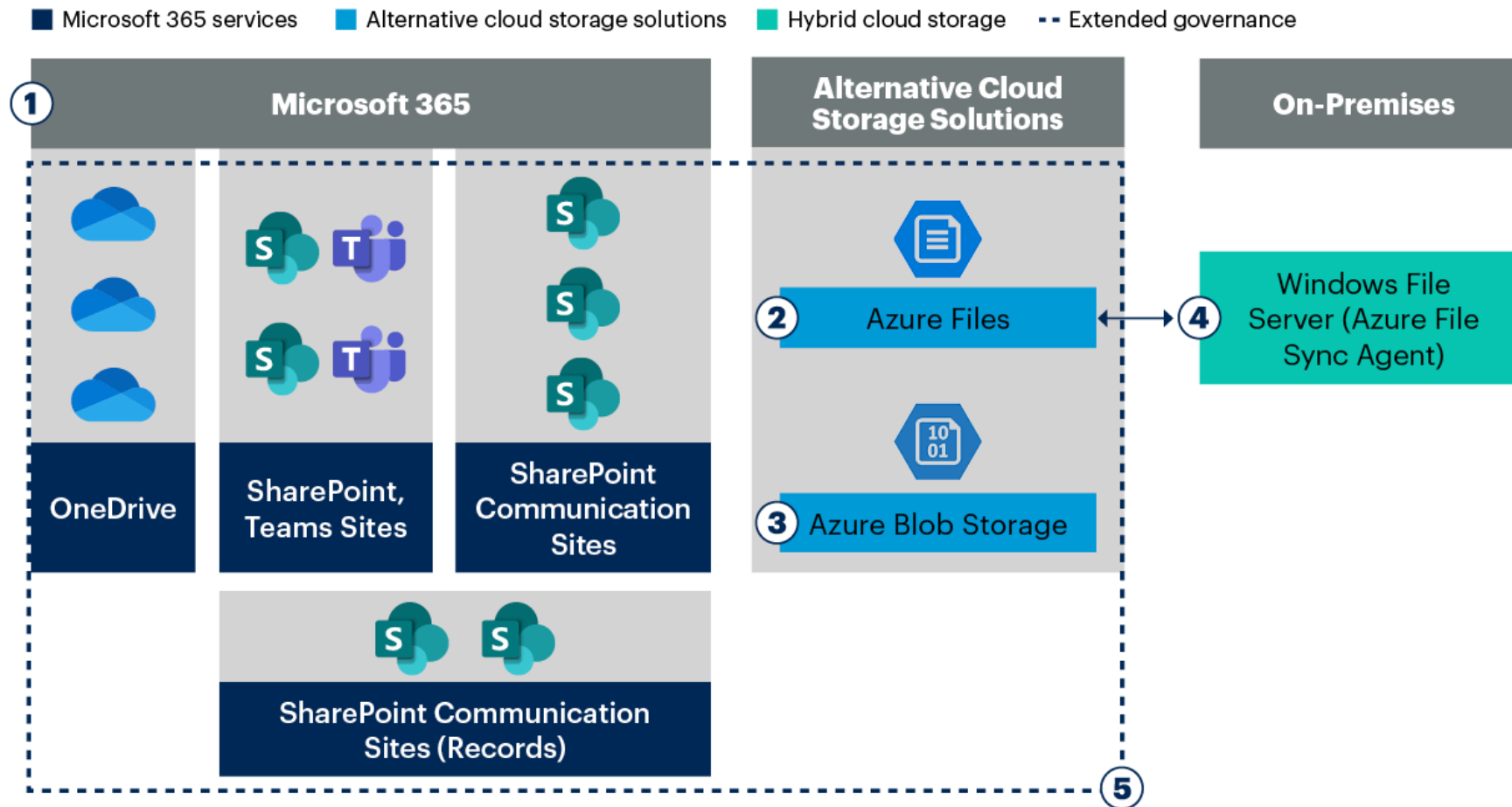
Leverage Microsoft Purview Extensions to Discover and Classify Data

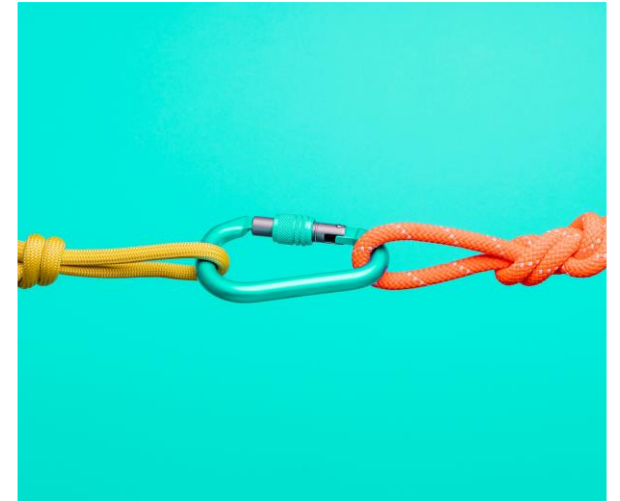# Recommendations

Resist

Lift and Shift to M365
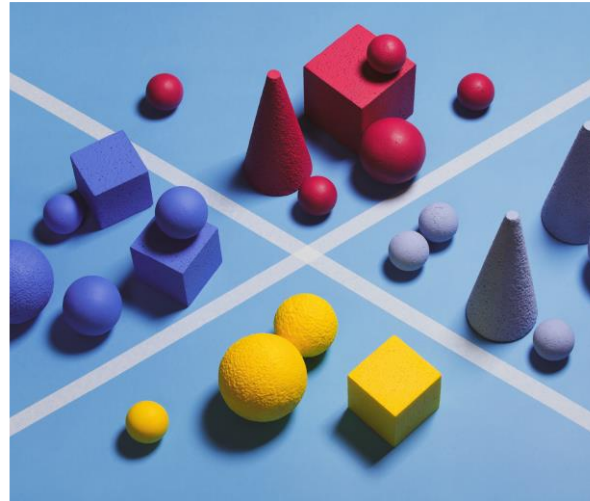
Discover

The data quality, file types, usage, sensitivity.

Protect and Govern

The data and migrate to cloud services that best support the use cases

Microsoft   proventeq   Infotechtion

Case Study – HPE TRIM:M365 migration

Record Mapping

- All records migrated from TRIM are mapped to '**Document Libraries**' in SharePoint Online

- A minimum set of metadata is proposed to ensure record retention and referential integrity is maintained.

- Where a Workgroup contains items more than SharePoint limit for a library, then additional libraries are automatically created

- Access Control Lists (ACLs) are different between TRIM and SharePoint Online.

Governance

- **Access Controls are added as a group,** at the **site** and / or **Document Library level**

- Hyperlinks are re-directed to avoid broken links.

- Managing retention integrity is a key aspect of migration to ensure all record retentions and disposition dates remain unchanged during migration

- Data clean-up with AI Purview AI models to identify data of long-term value and apply a short-term retention to the rest of the data.

Disposition

- SharePoint tenant cannot have automatic disposition switched off

- Records set for disposition in TRIM will be **automatically deleted in SharePoint** on the exact date

- **Expiration status date** = Created date (day & month) + 'Date Due for Destruction' (year)

	Disposition *Type*	Disposition *Date*
hp	Manual	End of Year
S	Automatic	Exact Date

Information Architecture

- Records can be migrated to new SharePoint Sites or an existing Site.

- Legacy Centre site owners can submit a **ServiceNow request to move records** from Legacy Centres to existing SharePoint sites

Mapping records: HPE - Sharepoint

EXAMPLE TRIM Workgroup

EXAMPLE SharePoint Site Structure
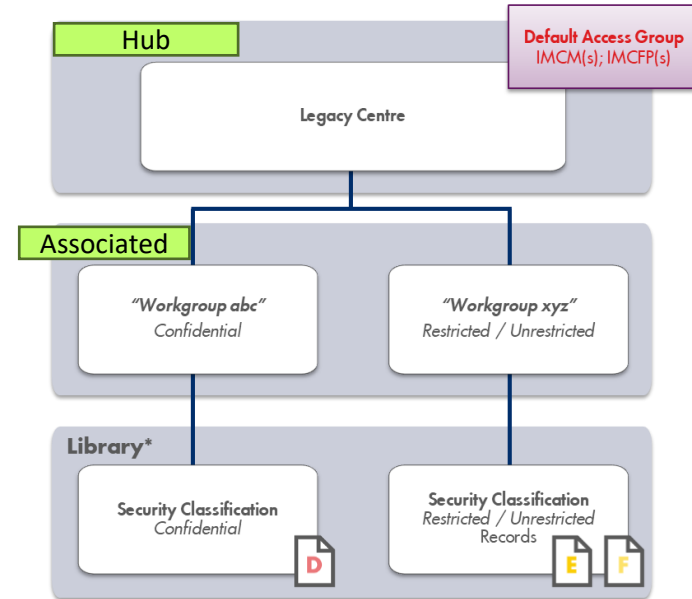
- TRIM adopts the concept of a **container hierarchy**
- **Electronic Records** or information (metadata) about **Physical Records** are stored in Record containers known as Workgroups
- **Workgroups** may / may not have been attributed to a known Line of Business, Business or Function in TRIM

- **Hub Sites** – top level collection of SharePoint sites, enabling navigation to associated sites
- **Library** – a collection of records defined by Workgroup and / or security classification(s) as per selected site structure
- **Folders** / document sets providing further structure to support related records.

Key Outcomes

75 TB of data migrated to Microsoft Cloud

Microsoft Purview based automated data security and retention classifications

Records searchable from Microsoft search with other data

A single platform for integrating Physical records lifecycle with Digital records.

Microsoft

proventeq

Infotechtion

Published Microsoft Success Stories

Teaming up with a committed Microsoft partner—Infotechtion

The global lockdown necessitated the need for a virtual office. Fortunately, FSA had recently replaced its Skype deployment with Microsoft Teams. "When we had to work from home, people realized that they could do everything they needed to do with Microsoft Teams," recounts Young. "We've been working from home and collaborating securely, functioning well as one organization."

That positive experience was the boost Young needed to embark on a replacement records management system. She was concerned about one crucial gap. "I've wanted to launch a modern records management rollout for a long time," she says. "But we realized that although we had great expertise in house, we didn't have the capacity we needed. And while I know records management, I didn't have any experience with the full depth of records management capability in Microsoft Purview."

Customer
Equinor

Partner
Infotechtion

Products and Services
Microsoft 365 E3
Microsoft Purview Data Lifecycle Management
Microsoft Teams
SharePoint Online

Industry
Energy

Organization Size
Corporate (10,000+ employees)

"Equinor tested many of the leading solutions in the records management space against several use cases. We felt that Microsoft Information Governance was the best approach, and verified our decision with several POCs."

—Atle Skjekkeland: Chief Executive Officer
Infotechtion

https://customers.microsoft.com/en-us/story/1511233412897677008-food-standards-agency-government-microsoft-purview

https://customers.microsoft.com/en-us/story/856258-equinor-energy-microsoft-365-security-compliance

How to do it

Preparing for migration

Content Category

Object Types

Activity

Data to be migrated

Collaborative Content

Created and improved by multiple individuals working together

Archived Content

Content that is not needed immediately

Transactional Content

Content pertaining to business process

Record in RMS

Managed as evidence of an activity or transaction performed by the organization in pursuit of legal obligations/ regulatory requirement

Document in DMS

Organise (structure, category), Secure (ACL), Control (versions, renditions) documents

- **Logical Storage :** File plan, Category
- **Lifecycle:** Create/Declare, Review, Dispose
- **Security:** ACL, Protective Marking

- **Logical Storage :** Folder structure, Content categorization, Metadata, Rendition
- **Lifecycle:** Create, Review, Publish
- **Security:** ACL

Microsoft proventeq Infotechtion

Key challenges while migrating from non-Microsoft ECM & file shares to M365

Platform differences

- Single monolithic repositories vs distributed teams/Sites/OneDrive

- Many ECM allow to file the same document in multiple locations, which can cause duplication when migrating to M365

- Transitioning to an environment with a modern way of working

Content incompatibilities

- Different filenames for different versions

- Different extensions for different versions

- Deep nested hierarchy not compatible with M365

- Invalid characters in file & folder names

Content security & integrity

- Different security model, requiring security re-modelling.

- Proprietary hyperlink format within documents, that will be rendered invalid post migration.

- Retain/transform metadata and taxonomy.

- Retain state of mid-workflow objects.

Microsoft   proventeq   Infotechtion

Readiness for SharePoint Premium (SPP), Purview & Copilot for M365
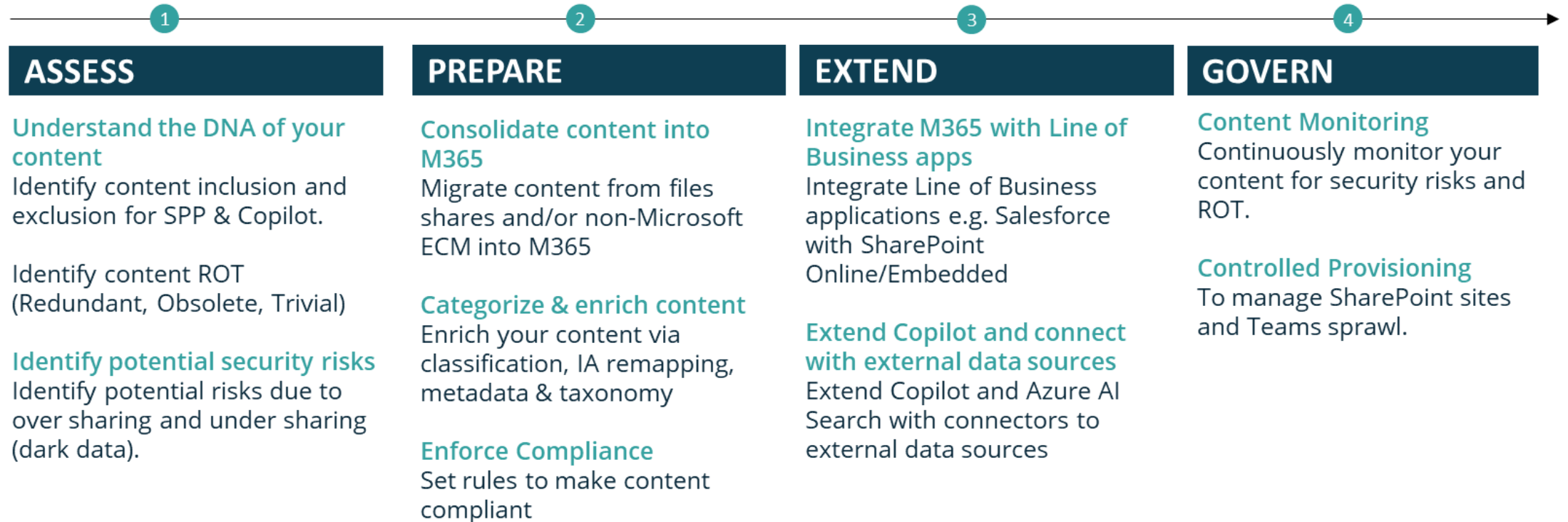
1 — ASSESS

Understand the DNA of your content
Identify content inclusion and exclusion for SPP & Copilot.

Identify content ROT
(Redundant, Obsolete, Trivial)

Identify potential security risks
Identify potential risks due to over sharing and under sharing (dark data).

2 — PREPARE

Consolidate content into M365
Migrate content from files shares and/or non-Microsoft ECM into M365

Categorize & enrich content
Enrich your content via classification, IA remapping, metadata & taxonomy

Enforce Compliance
Set rules to make content compliant

3 — EXTEND

Integrate M365 with Line of Business apps
Integrate Line of Business applications e.g. Salesforce with SharePoint Online/Embedded

Extend Copilot and connect with external data sources
Extend Copilot and Azure AI Search with connectors to external data sources

4 — GOVERN

Content Monitoring
Continuously monitor your content for security risks and ROT.

Controlled Provisioning
To manage SharePoint sites and Teams sprawl.

Microsoft   proventeq   Infotechtion
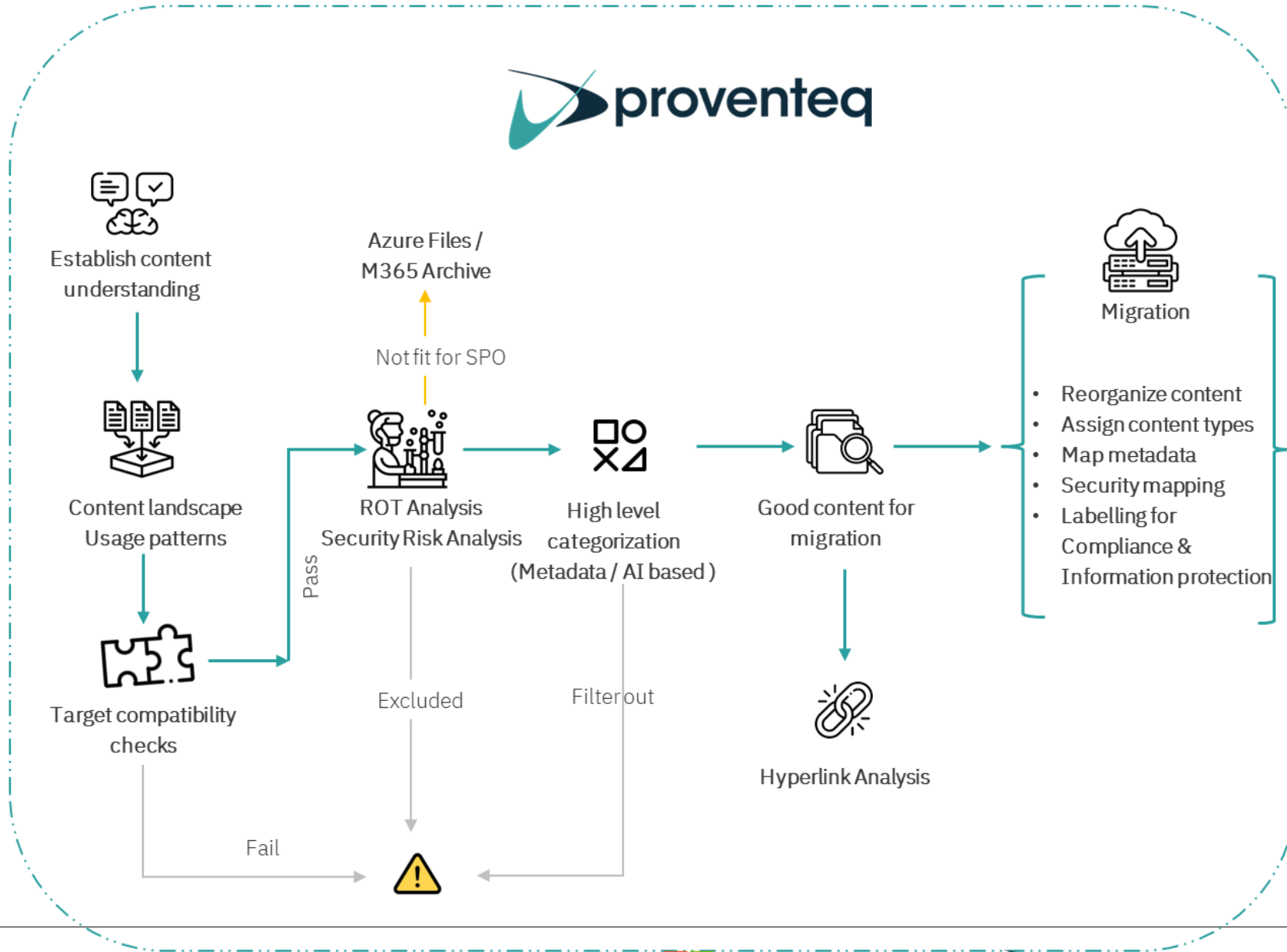
Questions & Answers

Call to action

- Schedule a call to discuss your requirements
  - In North America: contact Mike Alsup at Mike.A@infotechtion.com
  - In Europe: contact Per Sivertsen at Per.S@infotechtion.com
  - In United Kingdom: contact Maria Lim at Maria.L@infotechtion.com
  - In Nordic: contact Torgeir Thorsteinsson at Torgeir.T@infotechtion.com

Microsoft   proventeq   Infotechtion