

How to Avoid Data Breaches — Why Proactive Data Security Is a Must-Do



CEO Infotechtion, Microsoft MVP

Atle Skjekkeland

Atle Skjekkeland is an information management innovator and educator specializing in how to best secure and govern unstructured data with Microsoft Purview. Atle is the CEO of Infotechtion, a consulting and solution firm specializing in data governance and security for Microsoft 365 and beyond with offices and staff in the US, EU, UK, and India.



CEO Infotechtion, Microsoft MVP

Vivek Bhatt

Vivek is a leading expert in Microsoft cloud, recognized as an early influencer together with Microsoft led information governance and records management journey. He has led several strategic Microsoft 365 and Azure cloud transitions for global enterprises across energy and utilities, financial services and UK public sector.



Principal Group Product Manager @ Microsoft | Data Security and AI

Danika Loadholt

Danika Loadholt is a Principal Group Product Manager at Microsoft, specializing in Data Security and AI. In this role, she leads strategic product initiatives to infuse advanced security and AI capabilities into Microsoft's data platforms.

Know your data to protect your data



Data at risk of misuse if organization has no visibility into their data estate

1

User falls prey to phishing attack, compromises user credentials



Data compromise by external threat



2

User copies file to a USB, then uploads to a personal Dropbox



Data theft by malicious insider



3

User inadvertently shares the file copy with a few colleagues



Data exposure by negligent insider



4

Artificial Intelligence use sensitive data to generate content

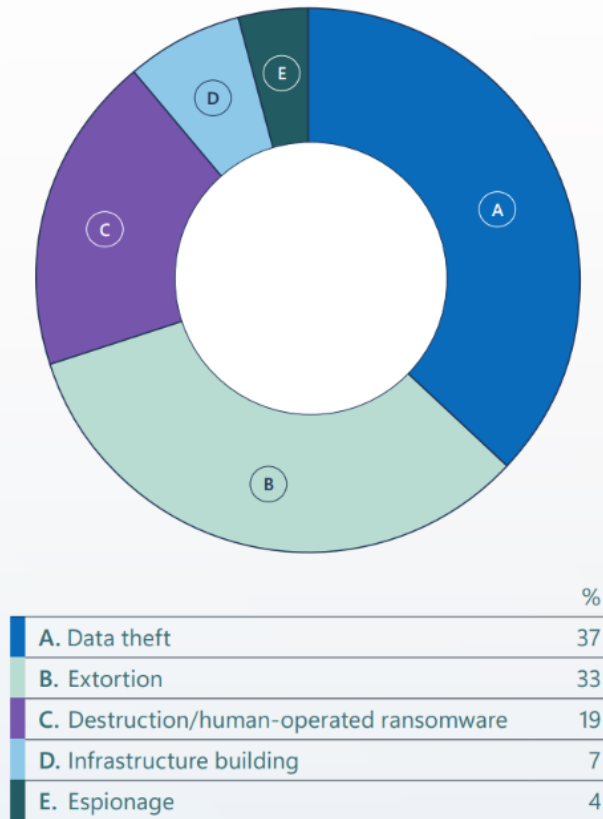


Data exposure by artificial intelligence



The External Threats

Identified motivations in incident response engagements



From the Microsoft Digital Defense Report 2025:

The risk of a data breach has never been higher, driven by five converging forces:

- Identity under constant attack
- Data theft as the primary attacker objective
- AI dramatically scaling attacker capability
- Cloud/SaaS misconfigurations creating easy entry points
- Supply-chain and third-party weaknesses expanding the attack surface

The Insiders Threats

From Forrester:

- 22% of data breaches are caused by internal incidents (insider threats).

Of these internal incidents:

- 40% are accidental (e.g., policy violations, negligence).
- 47% are malicious (intentional acts like data theft or sabotage).
- 13% involve a mix of both inadvertent misuse and malicious intent.

The real challenge is that many more risky behaviors never escalate to a breach and remain invisible (the hidden risk surface).



The AI Threats

Data leak and oversharing

- **80%** of leaders cite sensitive data leakage as their **top concern** when adopting AI
- **78%** of AI users bring **unmanaged AI apps** (e.g., ChatGPT, Claude) into work environments

Vulnerabilities and emerging threats

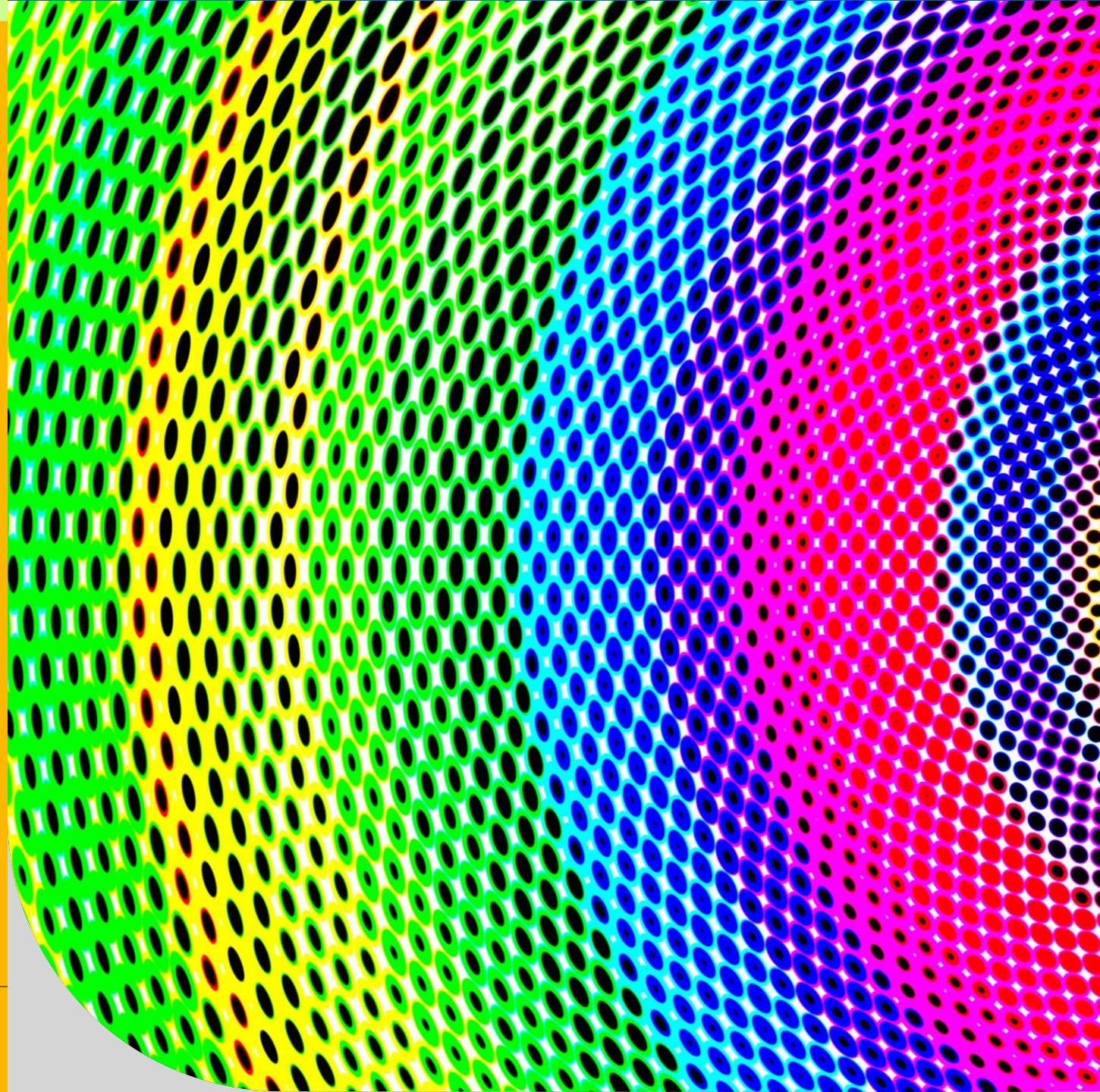
- **66%** of organizations are building/testing AI apps, leading to **new security gaps**
- **77%** are concerned about threats like **indirect prompt injection attacks**

Non-Compliance

- New regulations like **EU AI Act** and **NIST AI RMF** are emerging
- **55%** of leaders lack a clear understanding of **AI regulatory requirements**

MICROSOFT SECURITY

Danika A. Loadholt
Principal Group Product
Manager Microsoft Purview
Microsoft



Securing data is complex and multi-faceted



Different types
of data, users,
and objectives



Regulations
continue to
evolve



Fragmented
solutions increase
risks



New risks
with the use
of GenAI

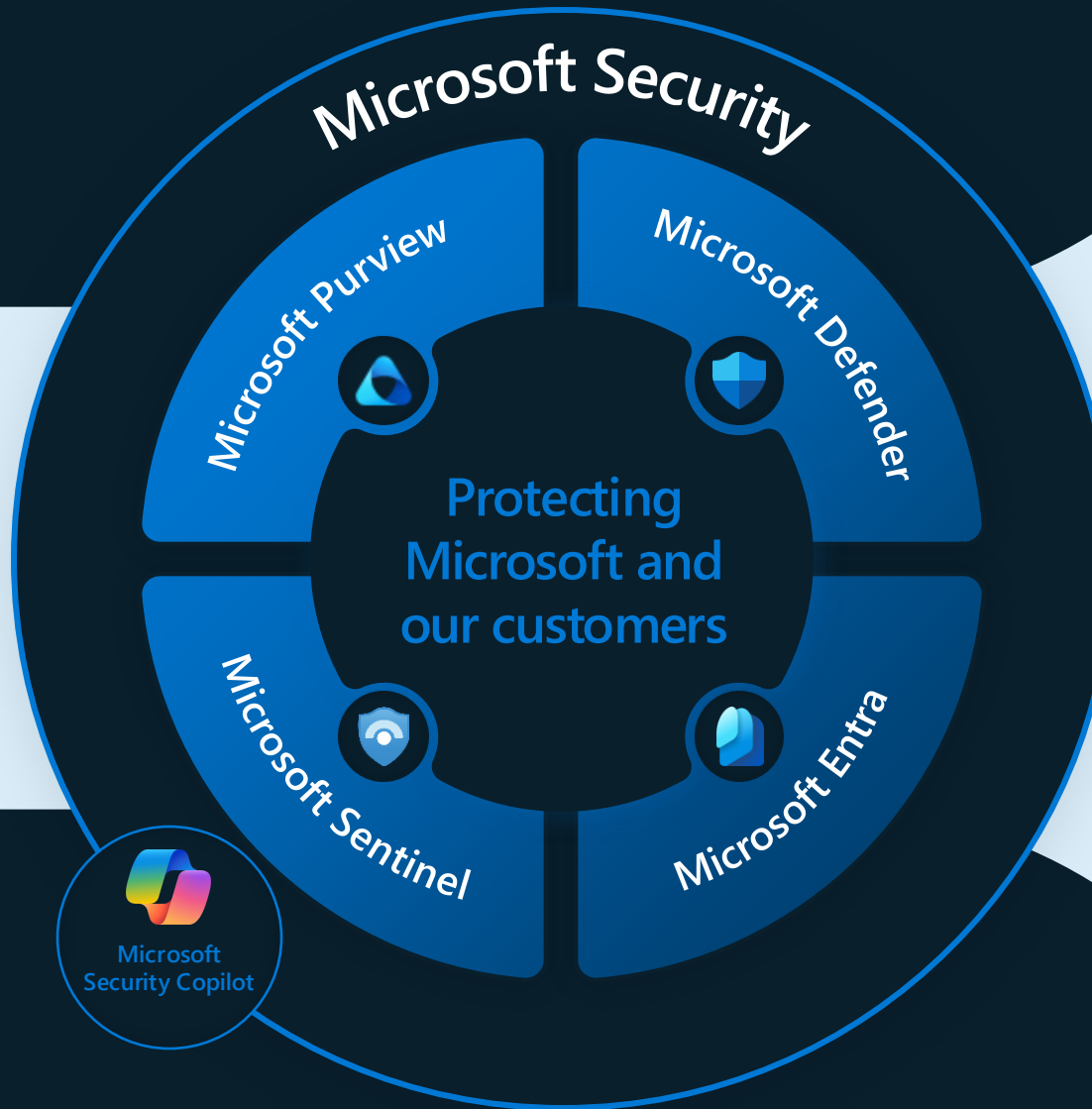
Securing customers with a Zero Trust approach

Verify explicitly | Use least-privileged access | Assume breach



Zero Trust is a proactive mindset that assumes all activity—even by known users—could be an attempt to breach systems.

Enabling
end-to-end
security



8.4M

Identities Protected

1.5M

Endpoints Protected

720K

Share Point
Site Protected

225TB

Ingested Weekly

200

Additional detections
Against TTPs

Threat Intelligence
Powered by 84 Trillion Signals

Microsoft Entra



Secure access

Identity and access management across your digital landscape

- Risk-based adaptive policies
- Seamless experience for any user
- Unified identity management and access to any app
- Simpler identity and access lifecycle



Visibility and control

Govern any identity and any resource with permissions across multi-cloud

- See all identities and resources
- Detect and right-size unused or excessive permissions
- Automate least privilege everywhere



Identity verification

Verify credentials based on decentralized identity standards

- Create trust with verifiable credentials
- Onboard and recover accounts faster
- Secure access to apps
- Gives individuals control of their data

Microsoft Defender + Microsoft Sentinel



Threat protection

Stop threats across your entire organization

- Secure all clouds, all platforms
- Get leading integrated protection
- Deliver rapid, intelligent response



Cloud security

Get integrated protection for your multi-cloud resources, apps and data

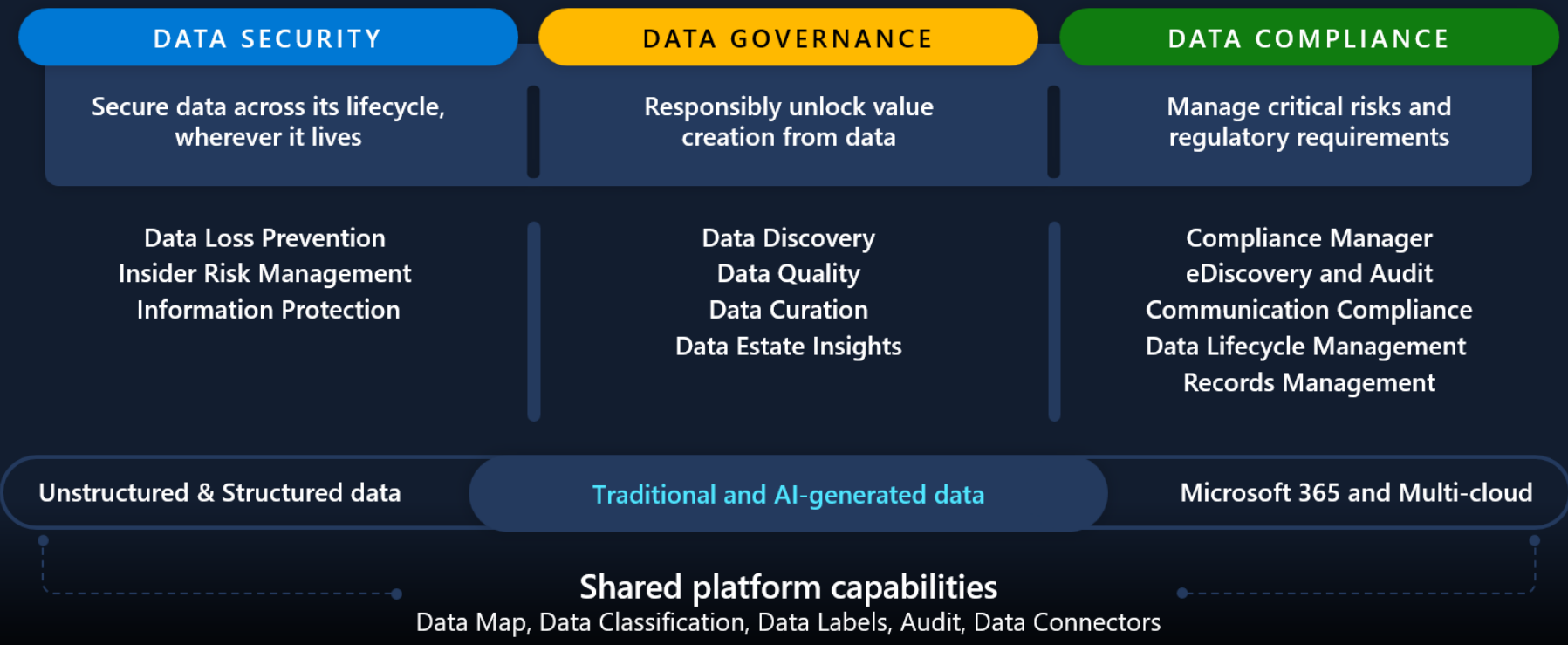
- Strengthen your security posture
- Defend against evolving threats
- Control access to critical apps and resources
- Build secure apps from the start



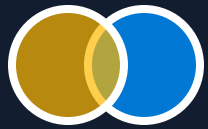
Microsoft Purview



Integrated solutions to secure & govern your entire data estate



Microsoft Purview: Data Security with an integrated approach



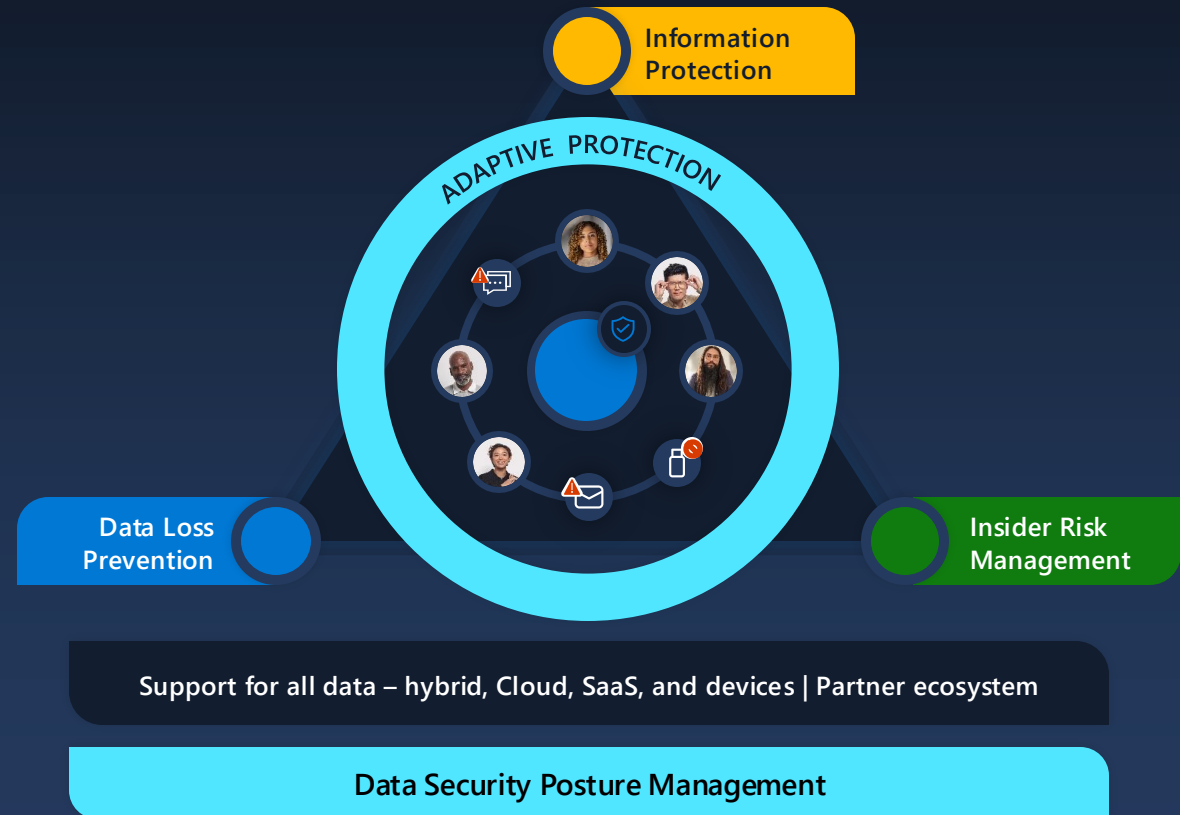
Automatically **discover, classify and label sensitive** data, and **prevent its unauthorized use** across apps, services, and devices.



Understand the **user intent and context around the use of sensitive data** to identify the most critical risks



Enable **Adaptive Protection** to assign high-risk users to appropriate DLP, Data Lifecycle Management, and Entra Conditional Access policies



Managing data security posture

Pain Points

Need of comprehensive view
for managing data security
posture

Lack of integrated processes
and shared understanding
across data and user context

Vast data volume and
quantity of alerts



Microsoft Purview Data Security Posture Management

Provides a consolidated view of the effectiveness of your data security posture and enables the discovery of opportunities to strengthen your data security program

Strengthen data security posture
across your data estate with
built-in and seamless integration

Analyze and improve actions to
protect your data in a centralized
solution

Leverage the power of GenAI to
uncover hidden data risks in
natural language

Data Security Posture Management (preview)

Get insights and recommendations for protecting sensitive data, improving security posture, and identifying top risks using Security Copilot. [Learn more about Data Security Po...](#)

Get started with Copilot

- Prioritize alerts**
Which alerts were triggered in the last 30 days for users leaving the org?
- Detect sensitive data leaks**
Which sensitive files were shared outside the org from SharePoint in th...
- Find devices at risk**
Which devices were involved in exfiltration activities?
- Find risky activity**
Show any suspicious activity sequences involving sensitive data.

Top data security risk recommendations

[View all recommendations](#)

Mitigate potential risks with adaptive protection

Set up adaptive protection to help detect potentially risky activity and dynamically enforce protection actions based on users' insider risk levels.

[View recommendation](#)

Prevent sequential activities that might leak sensitive data

Potentially disgruntled users downgraded sensitivity labels, downloaded, then exfiltrated sensitive files. Prevent future activity by setting up Insider Risk Management and Data Loss Prevention (DLP) policies.

[View recommendation](#) [Show users involved](#)

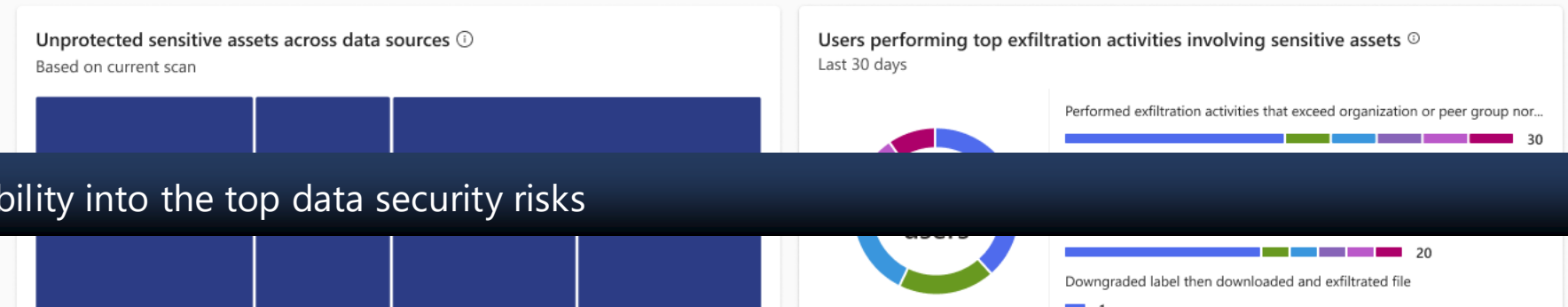
Activities
5

Sensitive info type detected
Project Obsidian

Potentially disgruntled users involved
1

Analytics reports

[View all reports](#)



Copilot Preview

Let's get started

Start with one of our suggested prompts or type your own prompt to ask Copilot for help in summarizing a topic, finding related information, and more.

Find risky activity
What are the top methods being used for exfiltrating unprotected sensitive data?

Review data at risk
What kind of sensitive data is involved in the exfiltration activities?

Identify risky users
Display the top 5 users with the most exfiltration activities in the last 30 days.

Nov 11, 2024 1:30 PM

Which sensitive files were shared outside the org from SharePoint in the last week?

Nov 11, 2024 1:31 PM

In the last week, the following sensitive files were shared outside the org from SharePoint:

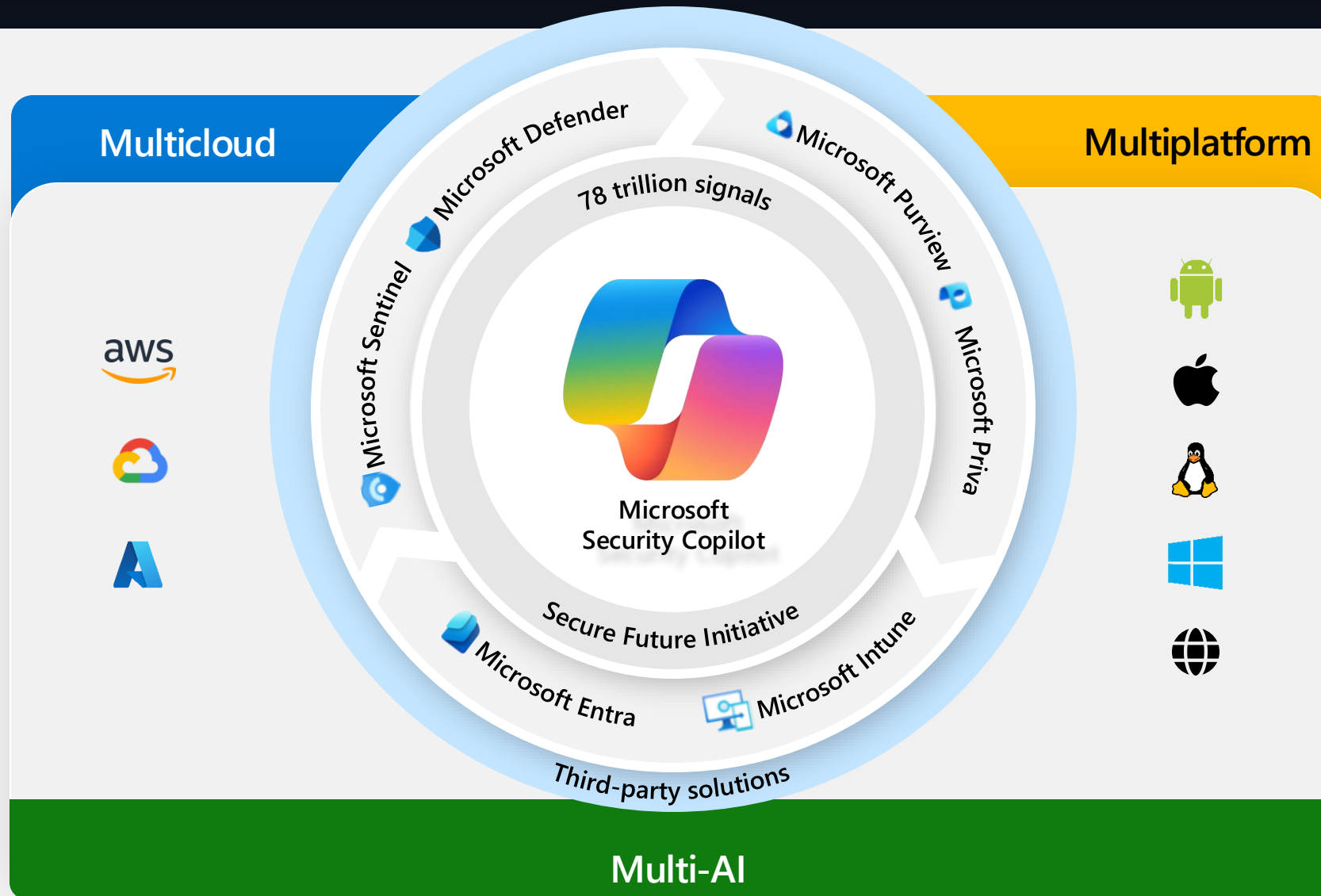
Timestamp: 10/11/2024 15:40:14
File: ProjectObsidian.docx
Sensitive info type: Project Obsidian, Acquisition

Timestamp: 10/11/2024 15:30:12
File: ObsidianAcquisition.pdf
Sensitive info type: Project Obsidian, Acquisition

Timestamp: 10/10/2024 10:40:14
File: MyResume.docx
Sensitive info type: All Full Names

[Check it for accuracy.](#)

Microsoft Security can help you achieve more



Protect comprehensively with unmatched threat intelligence, best-in-breed protection, and generative AI

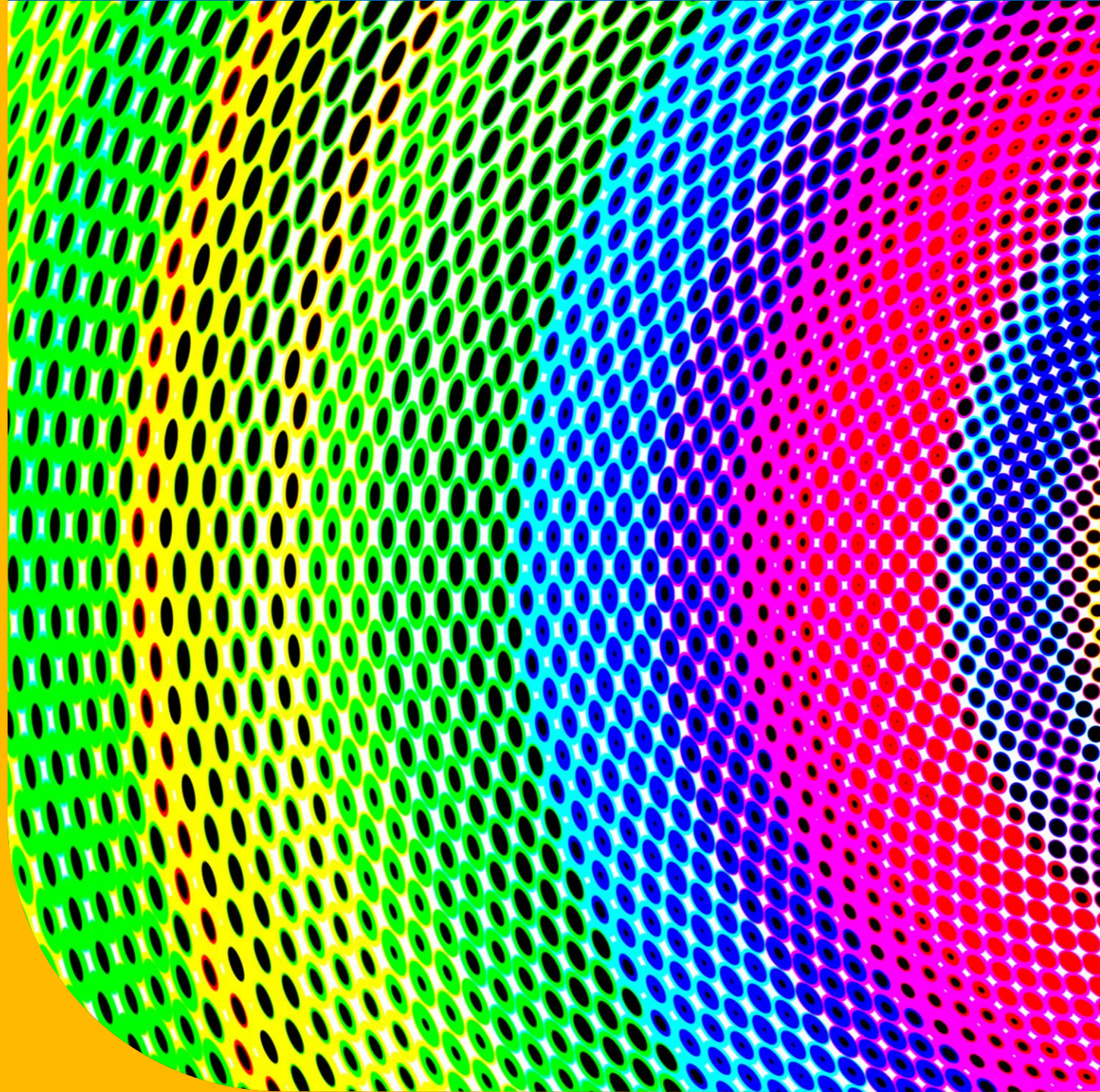
Lower TCO by integrating 50+ categories and delivering up to 60% cost savings

Supercharge your talent by using GenAI to help you defend at machine speed

Safeguard your AI future by securing the development and adoption of AI solutions

ESTABLISH DATA SECURITY AS A SERVICE

VIVEK BHATT - CTO



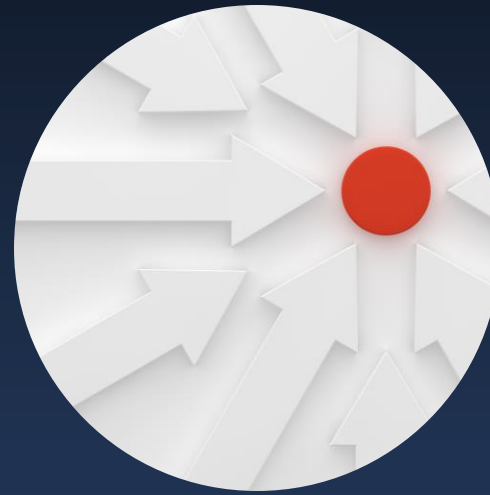
DATA SECURITY AS A SERVICE IS THE EXECUTIVE THEME FOR 2026



75% of organizations plan to implement Data Security Posture Management (DSPM) in the next 12 months.



83% of security leaders say lack of visibility into data weakens their overall security posture.



87% find their current data discovery & classification solutions need continuous refinement.



93% CISOs now list AI, automation, and data-centric security among their top priorities.

What is an Operating Model?





An operating model depicts the ways in which an enterprise orchestrates its I&T* capabilities to achieve its objectives.



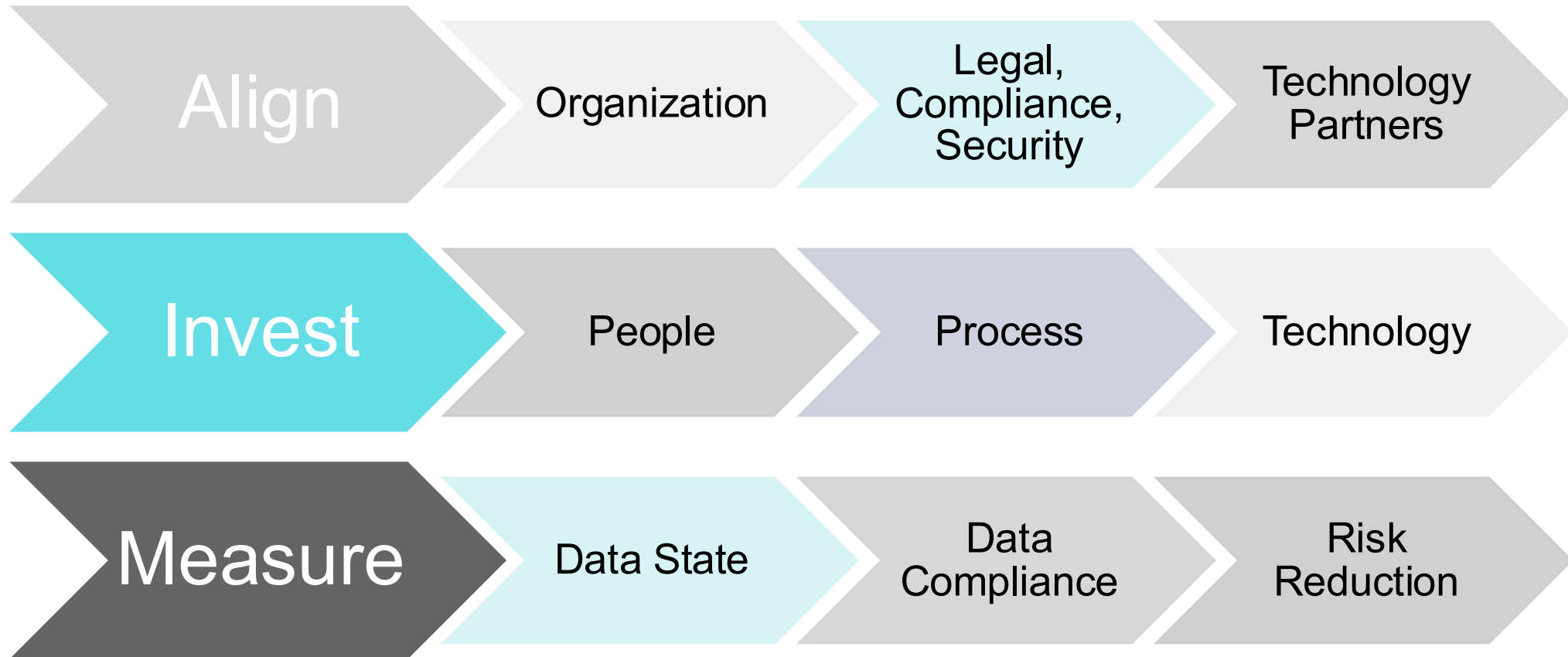
More simply, it shows "how things get done."

Every enterprise has an I&T* operating model, regardless of whether the model is explicitly or implicitly defined.

Key benefits of a Data Security Target Operating Model

| 01 | 02 | 03 | 04 |
|---|--|--|---|
|  |  |  |  |
| Consistency | Integration | Improvements | Data Centric |
| Ensures consistent application of best practices and standards across all data types, improving the quality, accuracy and reliability of data classification. | Ensures solution is strategically integrated with the wider operations, enhancing overall efficiency, issue resolution, and incident management. | Drives continuous improvement and innovation, ensuring that the data classification solution remains effective and relevant as the technology, regulations and organisation 'ways of working' evolves. | Shift to a Data centric security informed by Data driven insights is safeguarding digital information from risks including unauthorized access, disclosure, modification or noncompliance both. |

Data Security TOM Framework



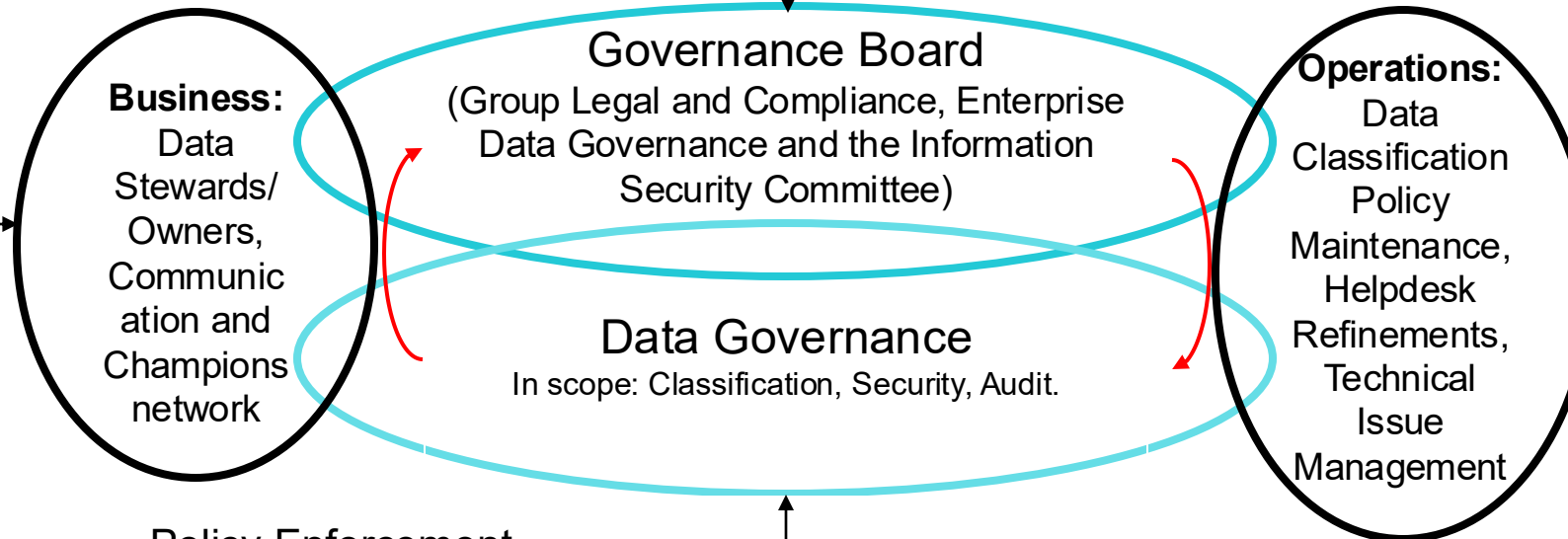
Align: Governance Structure

Policy Setting

- Monitor operating model effectiveness.
- Sets Target for Program (Metrics for Outcomes).
- Sets/Approve Data Compliance Policies , compliance issue management (Workflow, Processes, Lifecycle, Classification, Rules).
- Data Retention and disposition strategy and directive to reduce risk / threat attack surface.
- The governance board also defines the requirements (the classification and protection criteria)

Data Ownership

- Responsible
- Accountable
- Final Arbiter
- Classification / Policy outcome decision
- Report issues
- Identify new Data compliance / security risk scenarios



Business:
Data
Stewards/
Owners,
Communica-
tion and
Champions
network

Governance Board
(Group Legal and Compliance, Enterprise
Data Governance and the Information
Security Committee)

Operations:
Data
Classification
Policy
Maintenance,
Helpdesk
Refinements,
Technical
Issue
Management

Data Governance
In scope: Classification, Security, Audit.

Policy Enforcement

- Policy Architecture and Design authority.
- Reviews Reporting against KPIs and Metrics.
- Creates value case for investment, improvements and technology roadmap.

Operations

- Knowledge base for service desk
- Policy maintenance, review, refinement.
- Data Security Analytics and Automation
- Skills development

Lessons Learned from Customers



Securing Sensitive Data with Microsoft Security solutions

Implementing a zero-trust security solutions on-prem and cloud to prevent data breaches from outside and inside of the organization, aligned with industry standard and frameworks.



AI and Agentic AI Governance

'AI ready Data' and controls governing AI access to your data ensuring alignment with EU AI Act



Legal and Regulatory Compliance

Automated policy enforcement to manage data lifecycle, aligned with legal retention requirements, and organizations information sharing standards.



Operationalization of Purview as a Service

Operationalisation of Purview capabilities enabling long term management of security posture, new skills required to manage the emerging AI and data centric threats.



Infotechtion

DATA SECURITY AS A SERVICE

Security Scenarios as a Service

Offering security-focused scenarios as a service helps organizations stay ahead of emerging threats and adapt quickly to changes.

Target Operating Model

Defining a clear operating model for data security improves governance, clarifies responsibilities, and supports agile decision-making.

Scalable and Adaptive Protection

Scalable, adaptable data protection ensures organizations meet evolving business needs and regulatory requirements efficiently.



Infotechtion