Data#3 Microsoft

I Have Had 1000 Discussions Around Microsoft Security

Insights from countless discussions on Microsoft Security challenges and solutions

Mark Hindson – Security Solution Architect

JuiceIT2025

SIMPLIFY
CONNECT
PROTECT

Insights Derived From

Assessments and Workshops

Insights Derived From : Workshops / Assessment

Analyse customer's requirements and priorities for risk mitigation

Deploy selected Microsoft security solutions in production environment.

Discover threats to that exist within customers environment

Discover and prioritise vulnerabilities and misconfigurations across the customers environment

Plan next steps

Insights Derived From

Assessments
and Workshops

Microsoft Peers
Globally

Customers
nationally

Common Pain Points

Common Discussion Points

Insider Risk Management and Data Security

Identity and Access Management

Threat Protection & Detection

Incident Response & Security Automation

Insider Threats and Data Security

Insider Threats / Data Security

Data Breaches are growing 9% up from previous period

Inadequate Data Protection and Monitoring

Rising Insider Threats

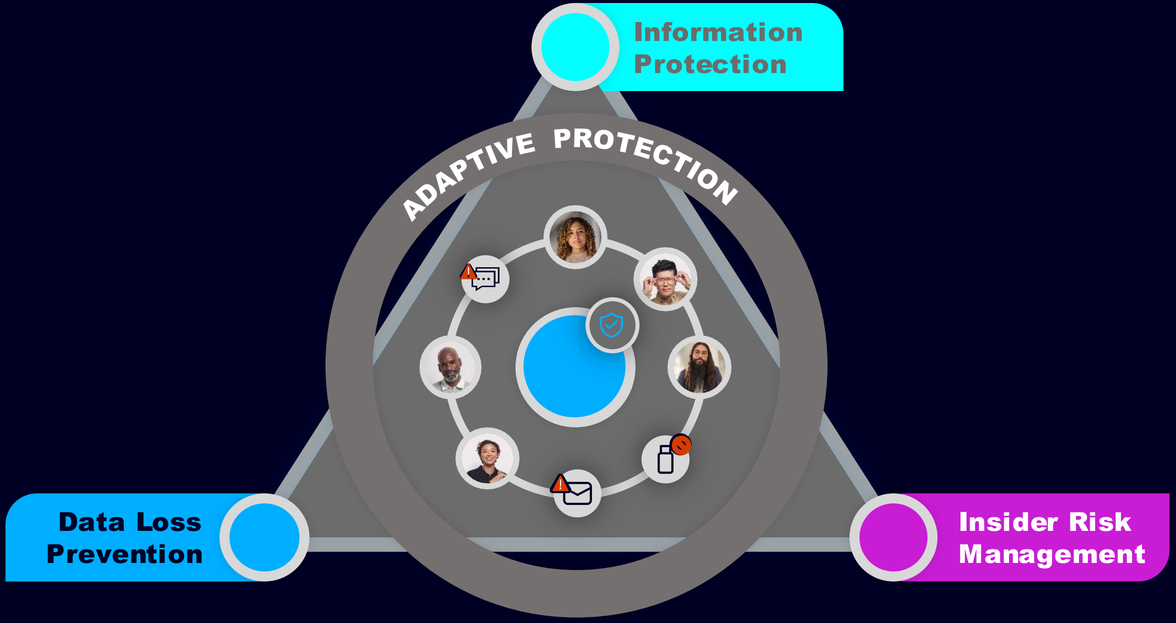
Compliance and Financial Impact Risks

Fortify data security with an integrated approach using Purview

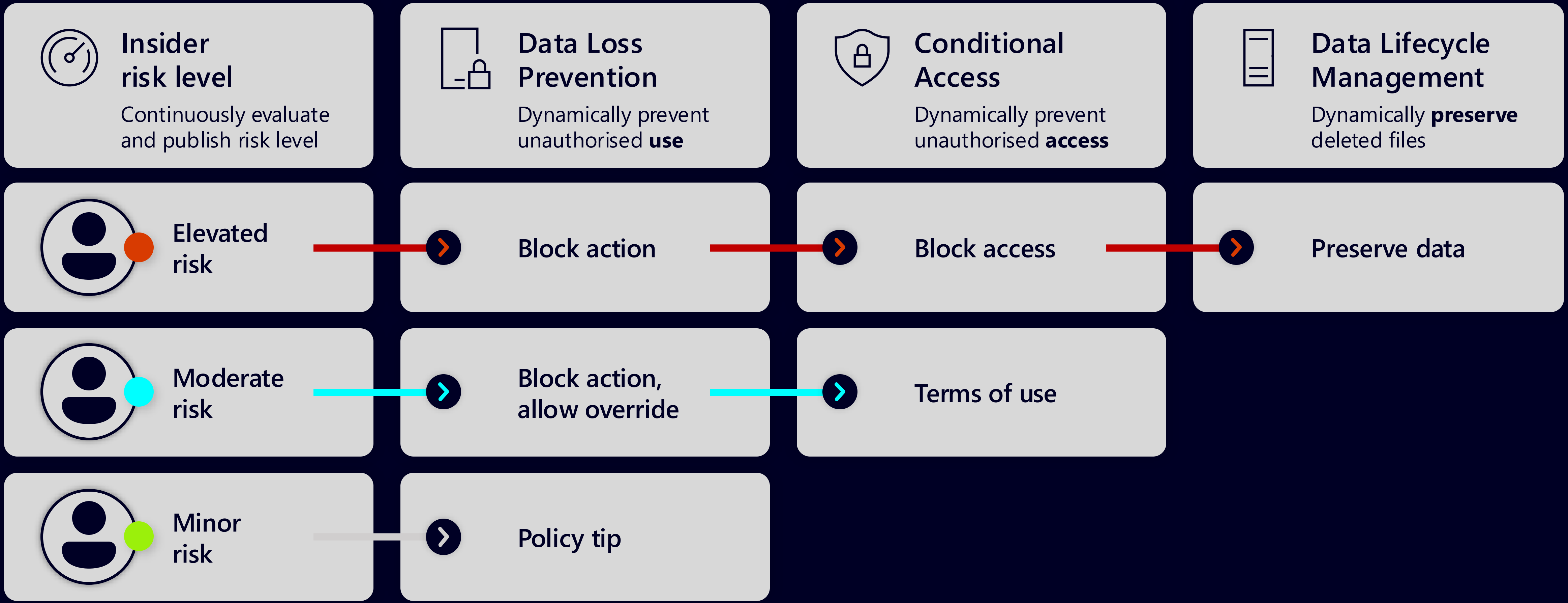
Automatically **discover, classify and label sensitive** data, and **prevent its unauthorised use** across apps, services, and devices.

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, and Entra Conditional Access policies



Adaptive Protection in Microsoft Purview



Insider risk level Continuously evaluate and publish risk level	Data Loss Prevention Dynamically prevent unauthorised **use**	Conditional Access Dynamically prevent unauthorised **access**	Data Lifecycle Management Dynamically **preserve** deleted files
Elevated risk	Block action	Block access	Preserve data
Moderate risk	Block action, allow override	Terms of use	
Minor risk	Policy tip		

Identity and Access Management

Insights – Identity and Access Management

- Weak Access Controls & Overprivileged Accounts
- Poor Multi-Factor Authentication (MFA) Adoption
- Orphaned & Dormant Accounts
- Lack of Identity Monitoring & Threat Detection

Threat Protection and Detection

Insights – Threat Protection and Detection

Cyber Threats Are Becoming More Sophisticated

GenAI is being employed by threat actors

Malware generation

Automated vulnerability discovery

Customising exploits

Password cracking

Phishing and social engineering

Disguising malicious code

Command and control communication

Deepfakes: data, email, voice

Insights – Threat Protection and Detection

Cyber Threats Are Becoming More Sophisticated

Too Many Disconnected Security Tools

Security Teams Are Overwhelmed & Understaffed

Slow Threat Detection & Response Times

Insights – Threat Protection and Detection

Defender XDR + Microsoft Sentinel

Incident Response & Security Automation

Insights – Incident Response and Automation

High Volume of Cyberattacks

Budget Constraints

Lack of Knowledgeable Personnel

Complex IT Environments

Insights – Incident Response and Automation

High Volume of Cyberattacks

Budget Constraints

Lack of Knowledgeable Personnel

Complex IT Environments

Consolidate tools
Microsoft XDR + Sentinel integrate security across all platforms
Security CoPilot
Single Pain of Glass

Security Evolution – What Jurassic Park Teaches Us About Managed Security

Proactive Insider Risk and Data Protection monitoring

Zero Trust and Identity & Access Management

Threat Detection & Response (24/7)

Automated Incident Response

Data#3 Microsoft Managed Extended Detection and Response

Bundled Options

Highly Automated

Defined Outcomes & Scopes

Standardised

XDR Foundation Layer

End Point

Cloud App

M365

Entra ID

Global Team

480+
Certified Security Analysts & Support Staff

Managed Detection & Response (SOC)

L1 – Security Engineer
L2 – Security Analyst
L3 – Security Consultant
L4 – IR Specialist
Manager

SOC Application, Infra & NOC

L1 – Security Engineer
L2 – Security Analyst
L3 – Security Consultant
L4 – Lead

Threat Intel & Advisory

L1 – Security Engineer
L2 – Security Analyst
L3 – Security Consultant
L4 – Lead

Managed Network & Security Device Management

L1 – Security Engineer
L2 – Security Analyst
L3 – Security Consultant
L4 – Lead

Content Management

L2 – Security Analyst
L3 – Security Consultant
L4 – Lead

Staff Certifications

- GCIH
- CISSP
- OSCP
- PCNSE
- CCIE
- IBM
- ITIL
- GPEN
- GWPAT
- CCSE, CCSM
- JNCIS, JNCIP
- FCNSP
- AWS, Azure
- ECIH

Service Management, Onboarding & Governance

Cyber Security Manager
Service Governance Lead
Onboarding Team

↔

Professional Services & Advisory

Professional Services
Advisory
Customer Experience Manager

Certified. With Access to Global View, Data Stored In Australia

Alpha Beta Charlie Delta Echo

How can Data#3 further help?

- Assessments/Workshops
  - Threat Protection
  - Data Security
  - Modern SecOps

Professional Services

Managed SOC / MXDR

Questions?

Feel free to come to the Microsoft Security booth and have a chat.