
SPARTANS
SECURITY


MACSeye

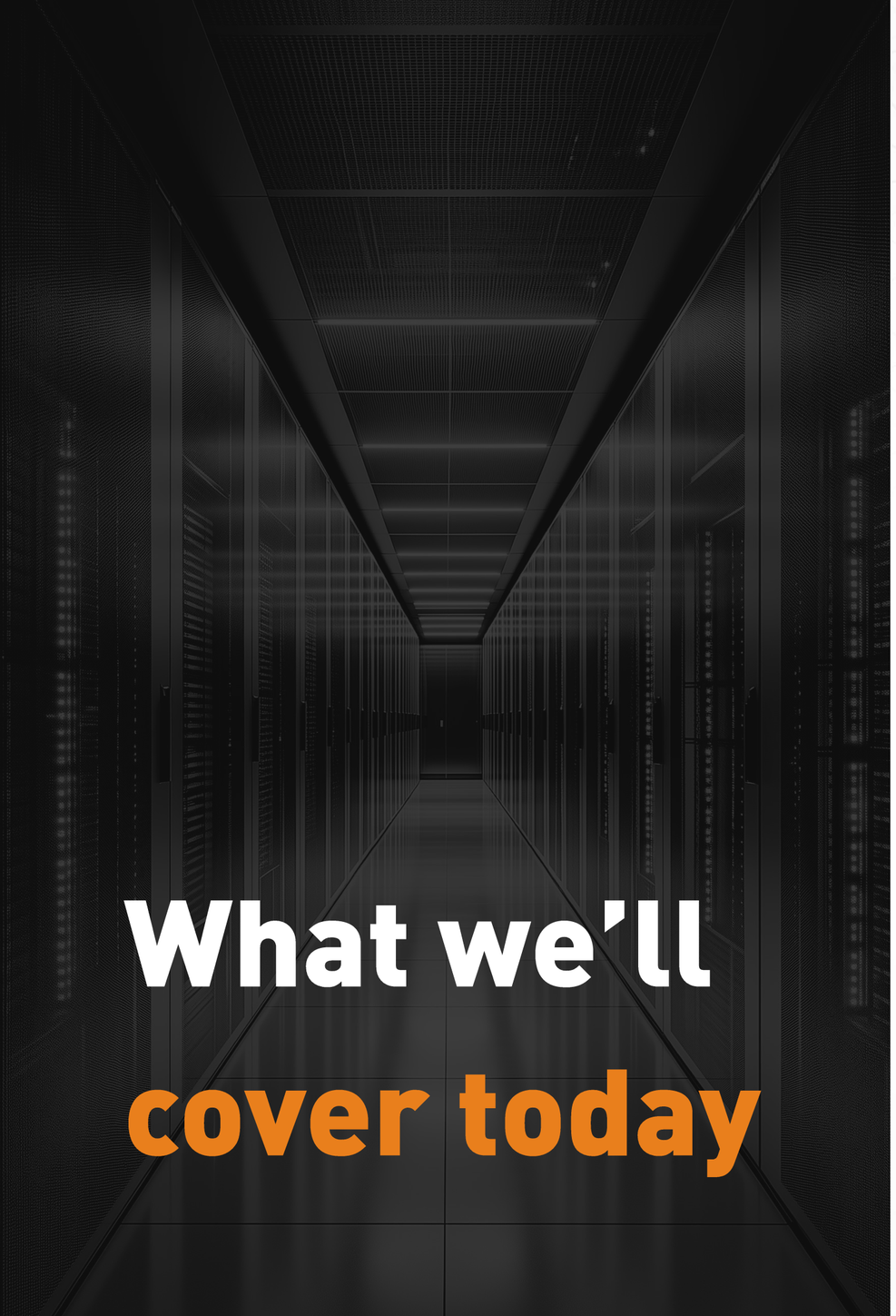
SPARTANS SECURITY

MACSeye

Data Governance and Protection

Louay Ghashash
Jane Harford

spartanssec.com



What we'll cover today

- Introduction
- Using Purview for Data Security and Governance
- MGGS Data Governance Journey
- Next Steps

SPARTANS SECURITY

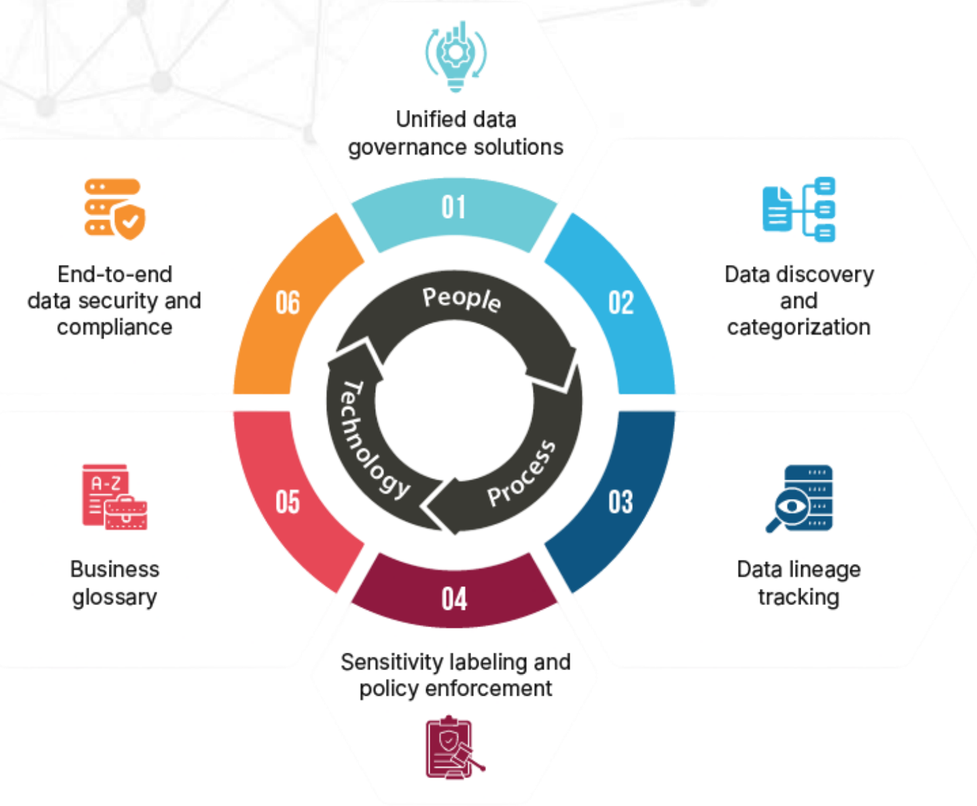
Using Purview

For Data and Security Governance

Using Purview

For Data Security and Governance

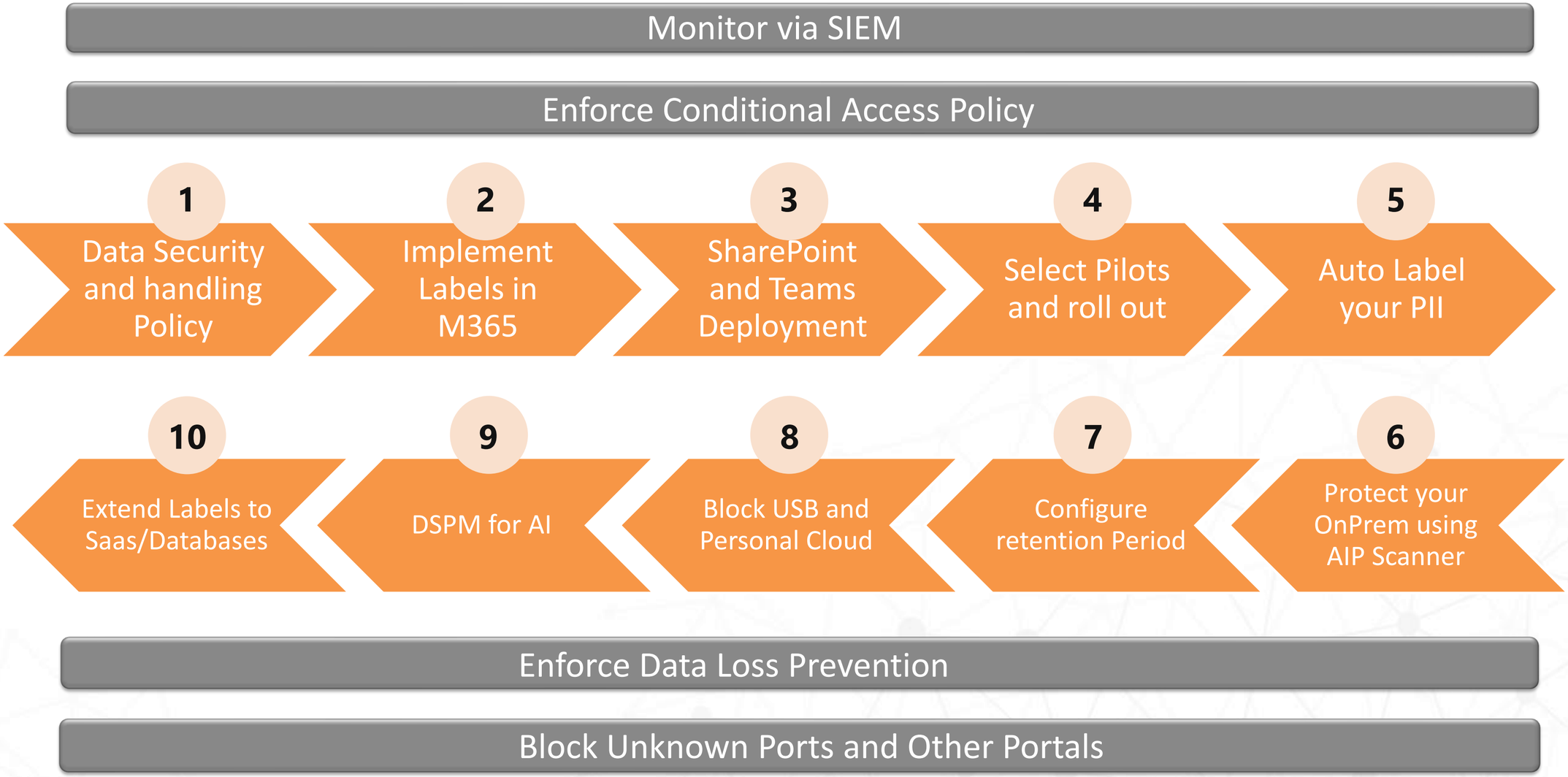
- Data Protection for School & Community
- Compliance with legal and regulatory requirements
- Managing risk of BYOD
- Managing the risk of using AI
- Managing risk of accidental data loss
- Detect and contain data breaches



Getting Started

- Establish Data Governance Sponsorship
- Define Asset owners across applications and data
- Develop Data Classification
- Commence Implementing Purview Across your unstructured data

Data Governance Journey



Rollout Tips

- Start Simple
- Commence in Discovery Now
- Use 4 or 5 Classifications ONLY
- Define common use cases first
- Help staff by giving clear example
- Trial with champions and departments
- Seek feedback on use
- Don’t ignore aesthetic of the labels

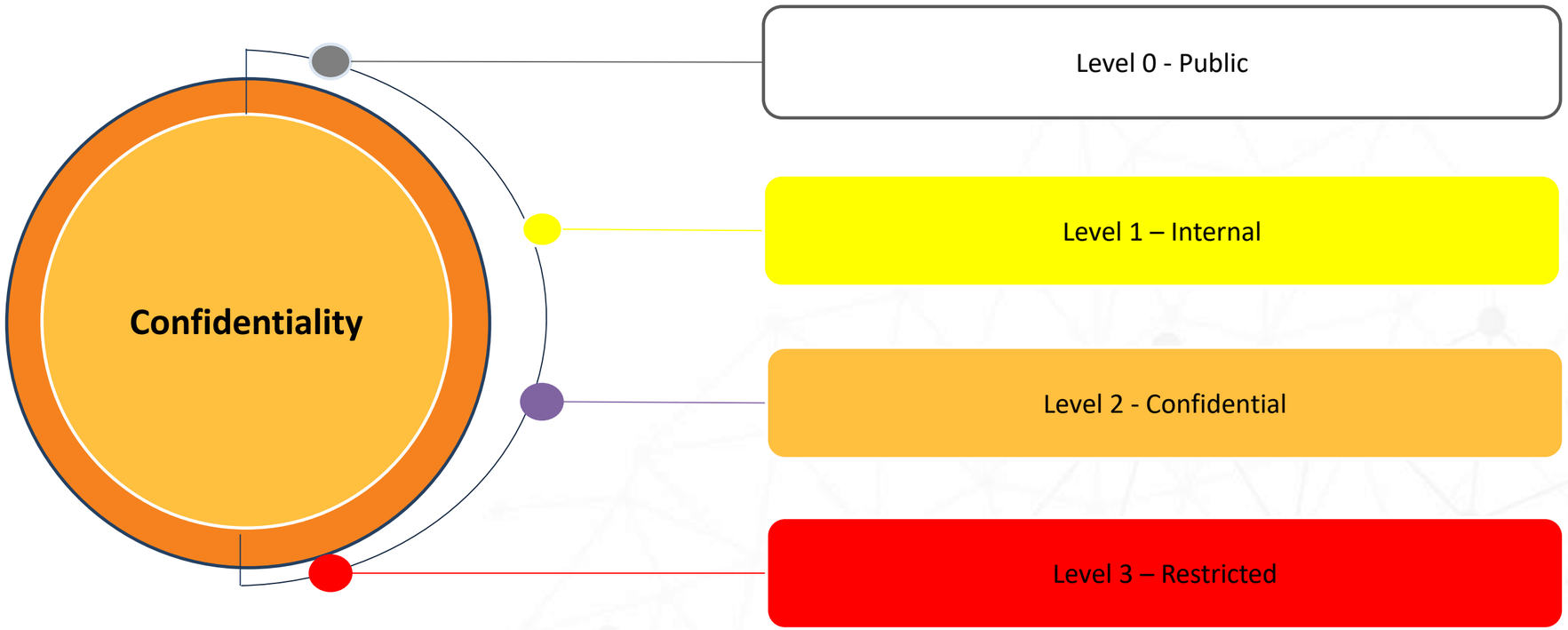
SPARTANS SECURITY

MACSEYE

Data Security and Governance Journey

Rollout Tips

The **Confidentiality** criterion ensures that information is protected from unauthorised access, disclosure, or dissemination. Information must only be accessible to individuals who have the appropriate permissions or a legitimate need-to-know. Breaches of confidentiality can result in significant harm to individuals or the School, including reputational damage, legal repercussions, and loss of trust.



How to Classify

- Data should be classified according to:
  - Confidentiality
  - Sensitivity
  - Retention period
  - Value and risk to the school
- When in doubt, opt for higher classification
- Always provide staff with use cases for the most common data classifications

Classification Decisions

User Discretion

- Up to the user
- Users should have the ability to
- overwrite previous classification

Content Based

- PII Data Detection
- Specific Keyword (e.g. Board Presentation)
- School specific data (e.g. INV-123 for invoices)

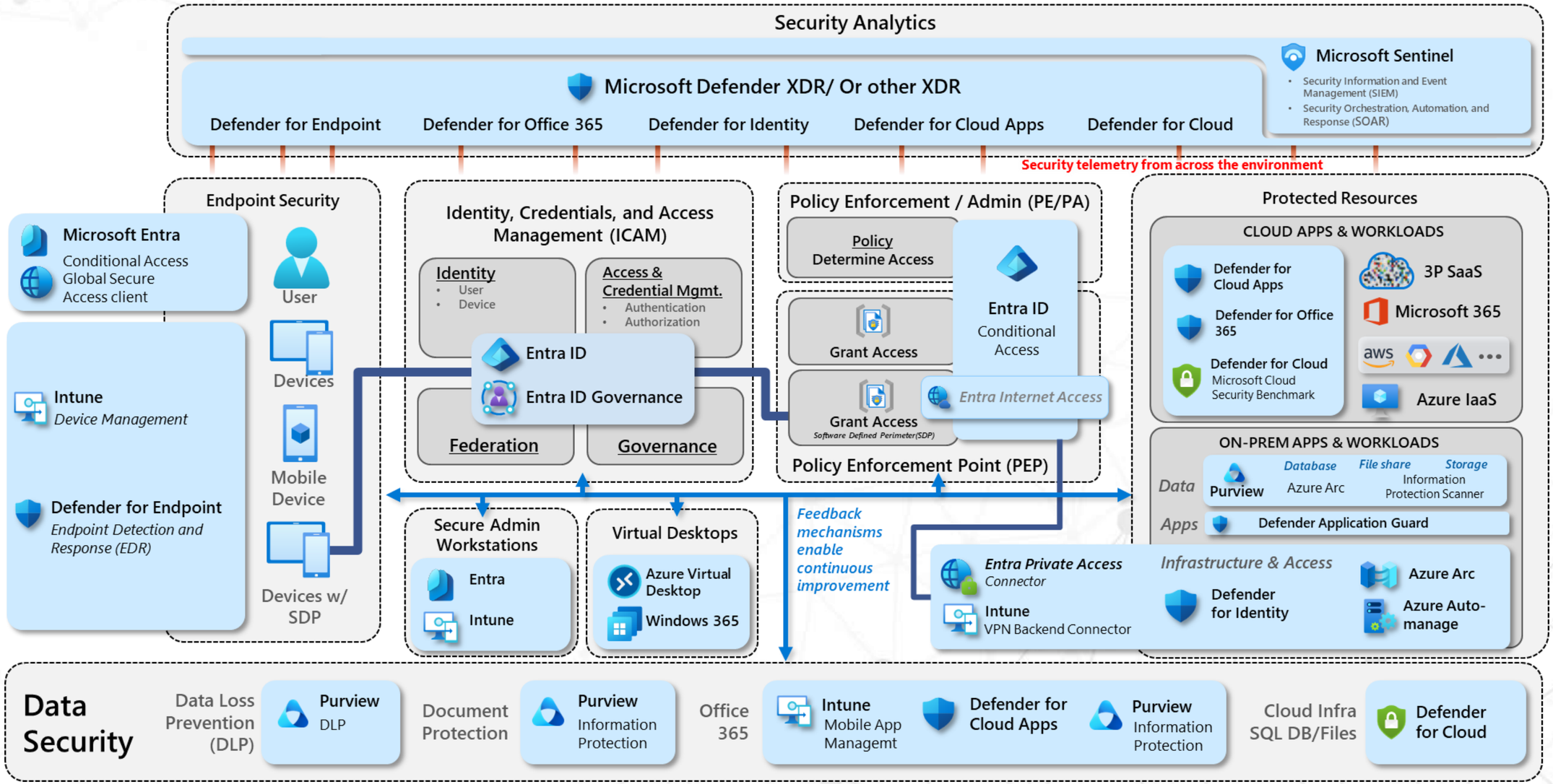
Location Based

- SharePoint
- Local On-Prem Storage
- Cloud

Don't Ignore Leaky Taps

- Block USB (or block uploading Classified document to USB
- Block access to personal cloud storage
- Block sensitive information upload to AI
- Block unapproved AI
- Insider Risk Management policy is a must
- Strong Conditional Access Policy is a foundation to secure data
- Don’t forget Data Retention
- Target your Database and SaaS after finishing implementation to M365/Azure

Zero Trust Reference Architecture



Link to Download

SPARTANS SECURITY

1300 20 90 23

info@spartanssec.com

46 Dover St, Cremorne, VIC, 3121