Risks around unstructured Data within Microsoft 365

Introductions

Lee Morgan
Senior Investigator – Digital Forensics & Incident Response (DFIR) - CyberCX

Lee is a cyber security enthusiast with over 5 years' experience working in IT security and Digital Forensics.

Holding multiple IT Forensics certifications from the Global Information Assurance Certification, Lee has been able to develop and apply deep level specialist expertise used in the real world to help customers respond to incidents.

Jacob Estrin
Director – Microsoft Cloud – CyberCX

Jacob has over 15 years of experience working in ICT across a broad range of roles. With a focus and passion around Microsoft cloud security and enabling the use of technology in organisations, he works closely with customers to drive security maturity within their cloud platforms.

Jacob holds a CISSP certification an Executive Masters of Business and multiple Microsoft Certifications. At CyberCX, Jacob is a leader in the Cloud Security and Solutions practice accountable for the delivery of Microsoft Cloud solutions.

What is Unstructured Data?

Why do attackers target unstructured data?

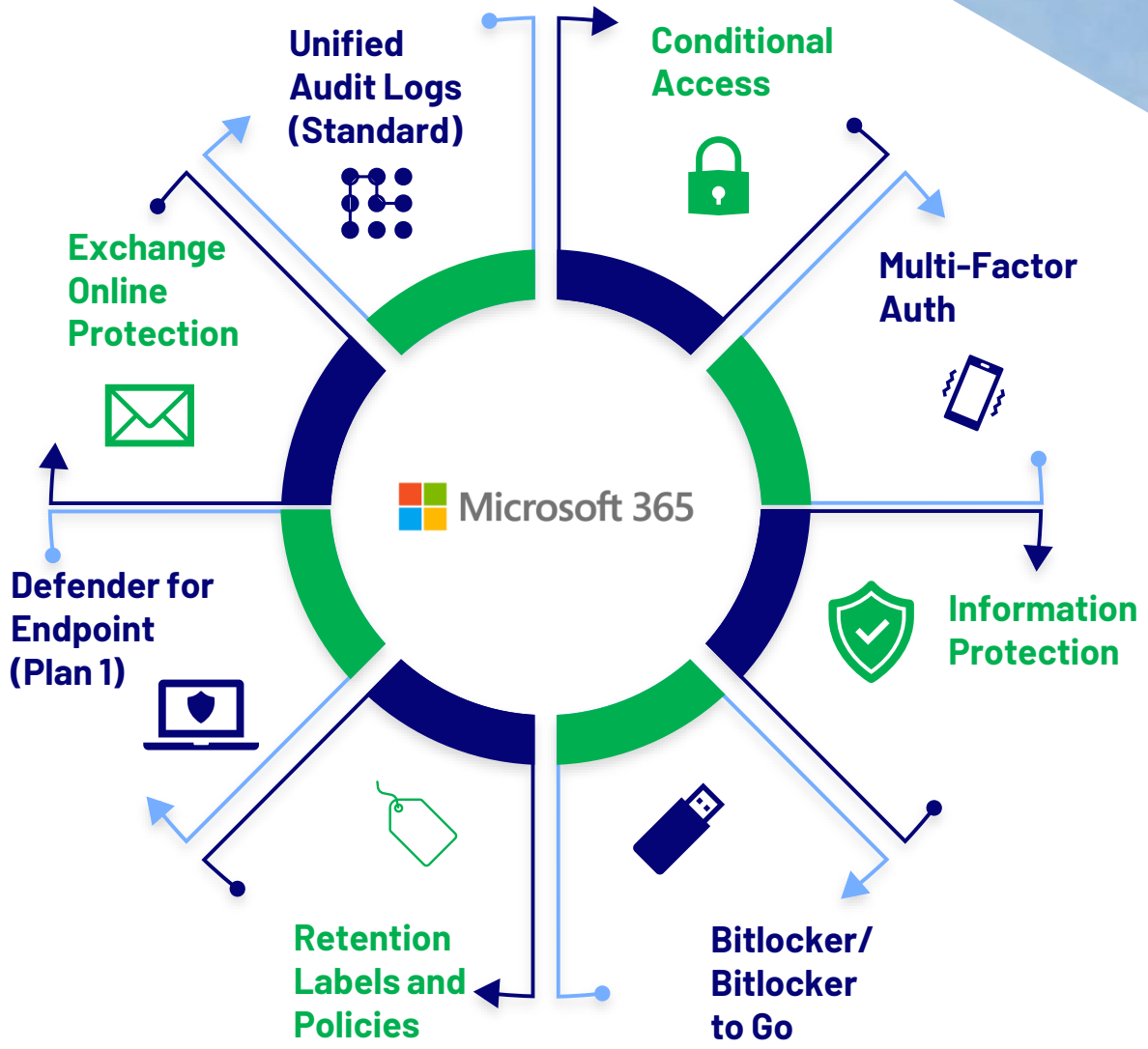
Cyber Criminals

- Perform financial fraud
- Data Theft Extortion
- Business Email Compromise
- Gain access to systems

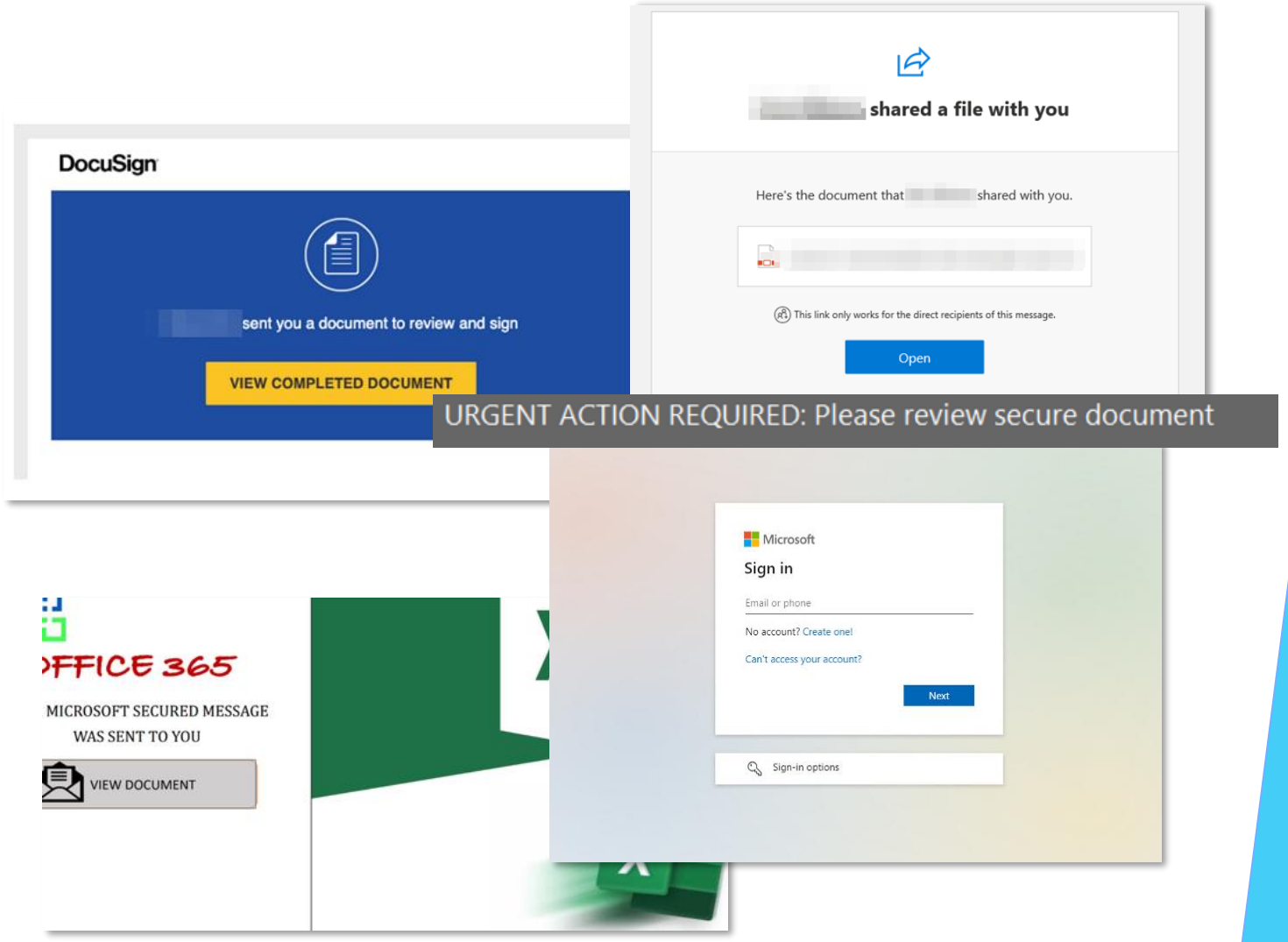
Nation-States

- Espionage
- Long-term persistence
- Disruption
- Disinformation

What can you do about it?



Scenario 1: Business Email Compromise (BEC)



Mitigations

- Unified Access Logs
- Mail Forwarding

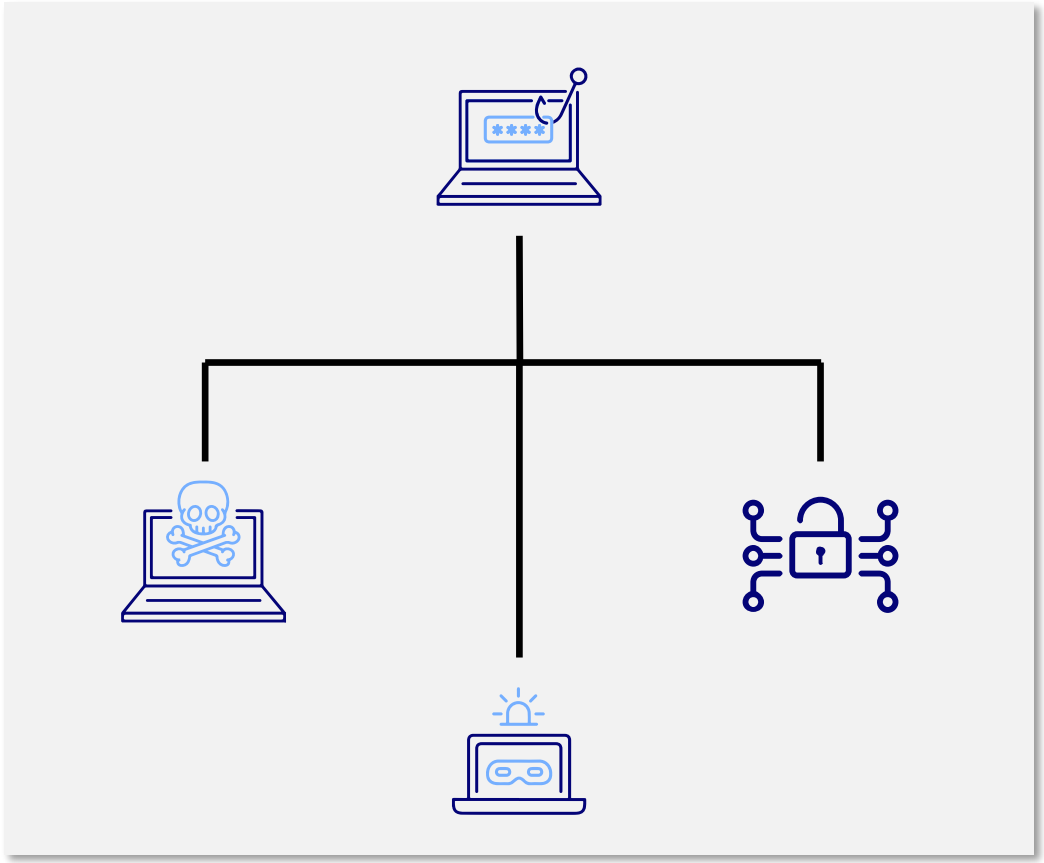
Scenario 1: Investigation

Scenario 2: Impersonation and Invoice Fraud

Mitigations

- DMARC
- DKIM
- SPF

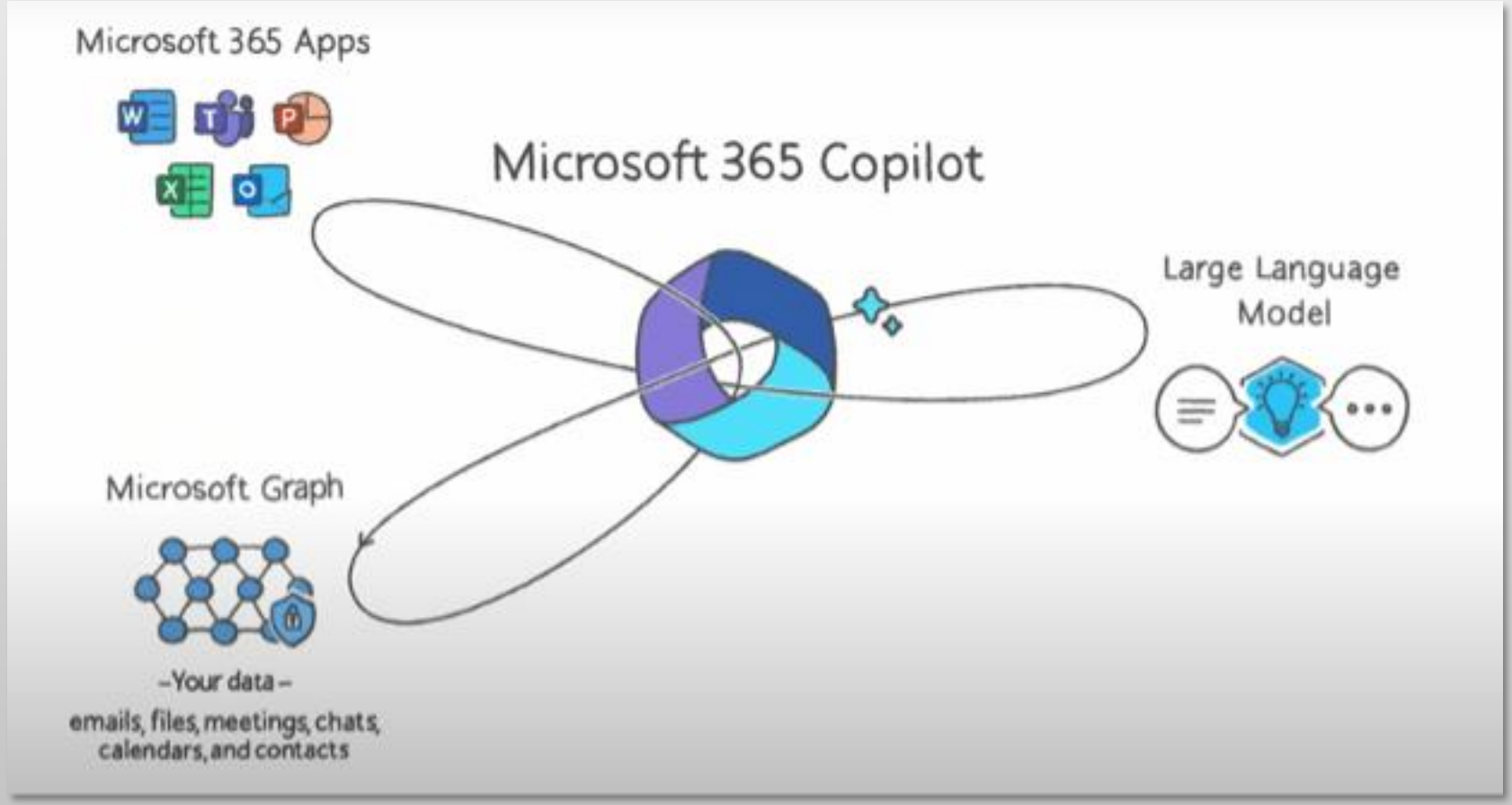
Scenario 3: Follow on Attacks (LM)



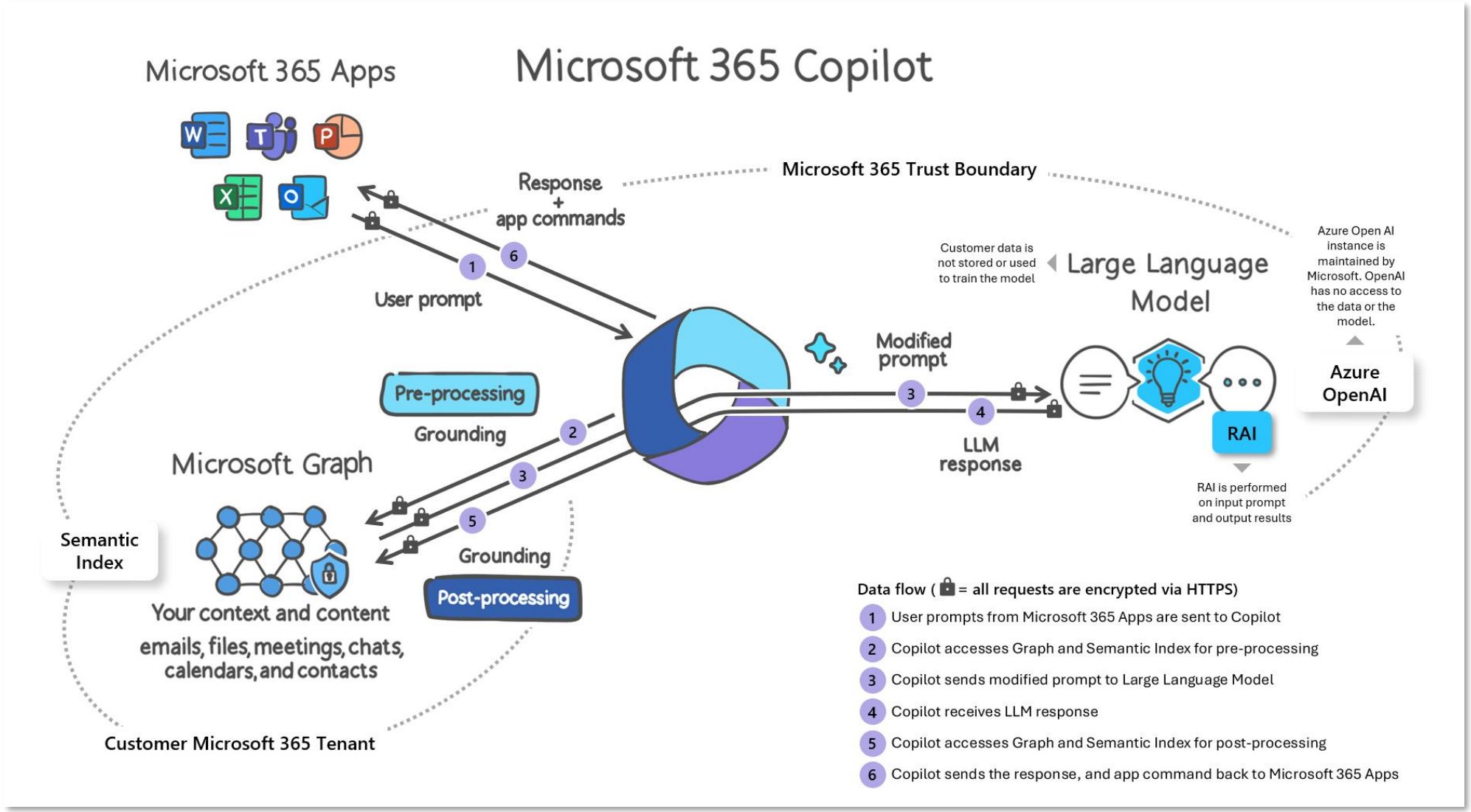
Mitigations

- Access Reviews
- Conditional Access – MFA
- Conditional Access – Authentication Context

M365 Copilot Architecture



Copilot Architecture



M365 Copilot Risks

- Sensitive data inadvertently exposed internally
- Unethical Use
- Being leveraged as a tool for intelligence gathering

How to Prepare

- Identify and protect sensitive content
  - SharePoint site settings (Privacy)
  - Purview (Sensitivity Labels)
- Modify Sharing Permissions


Contact
REPORT A CYBER INCIDENT
Ransomware and Extortion
Latest Intelligence

Demo