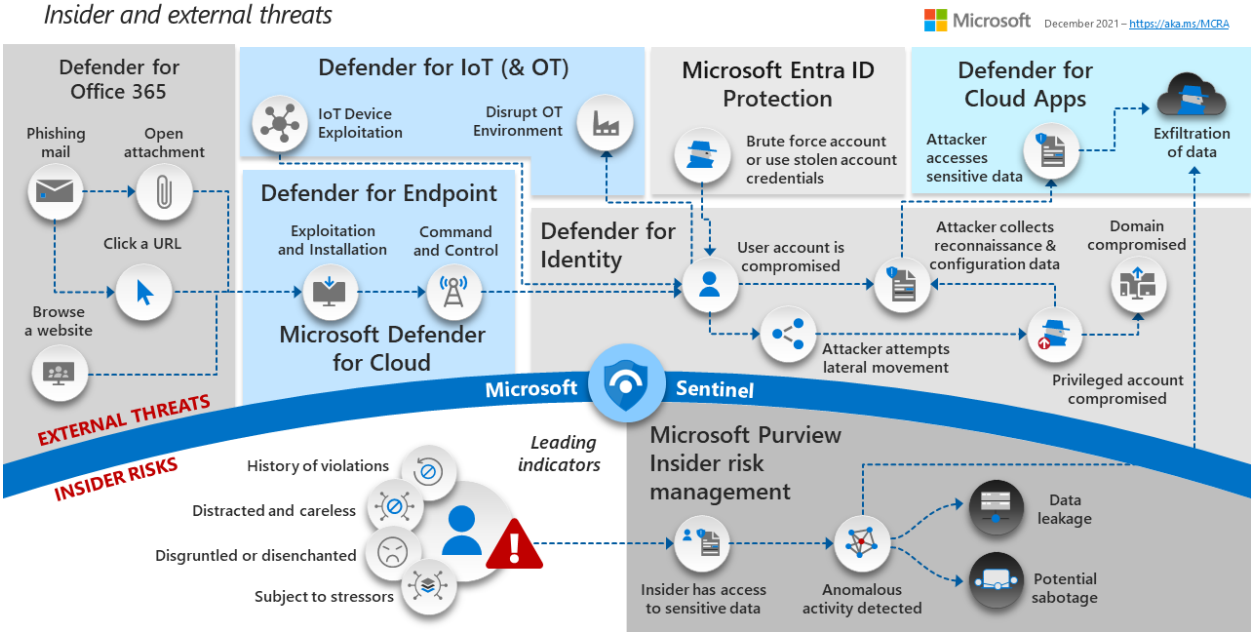
Defend across attack chains

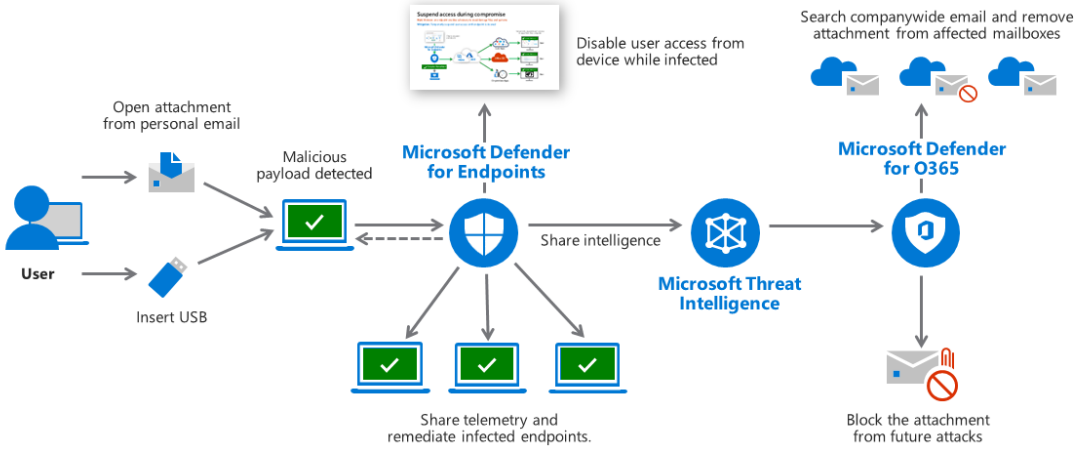
Insider and external threats



Compromised endpoint

Risk: Devices can be infected by **personal email, USB, and other vectors**

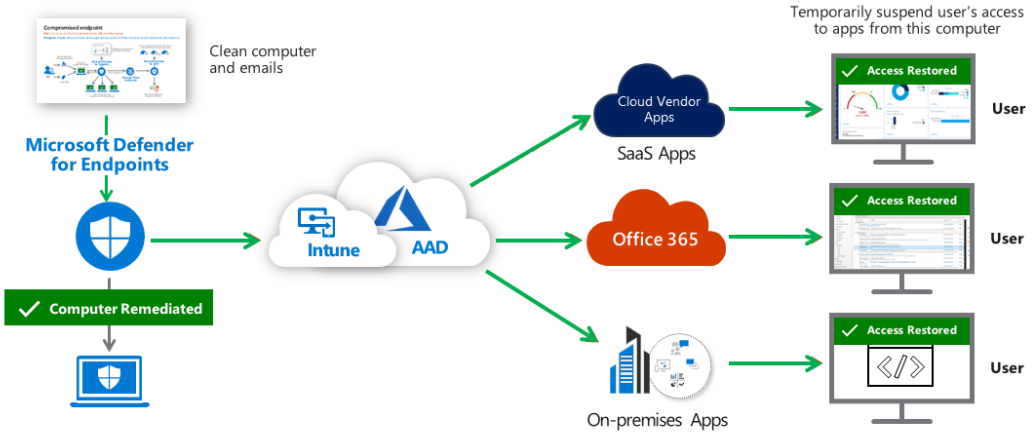
Mitigation: Rapidly detect and clean all managed devices, email, and other resources across environment and customers



Suspend access during compromise

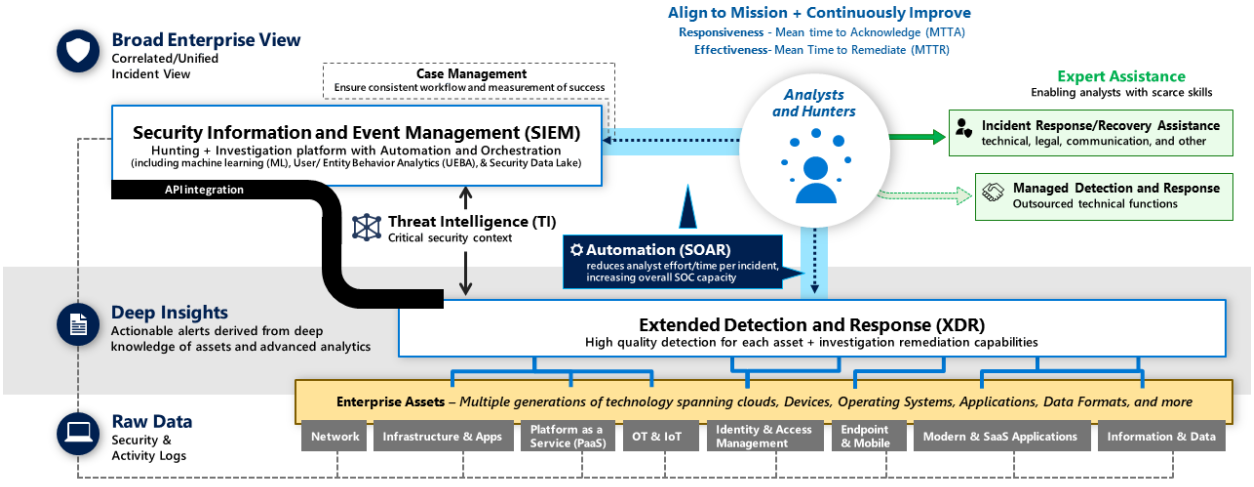
Risk: Malware on endpoint enables adversary to steal/damage files and systems

Mitigation: Temporarily suspend user access until endpoint is cleaned

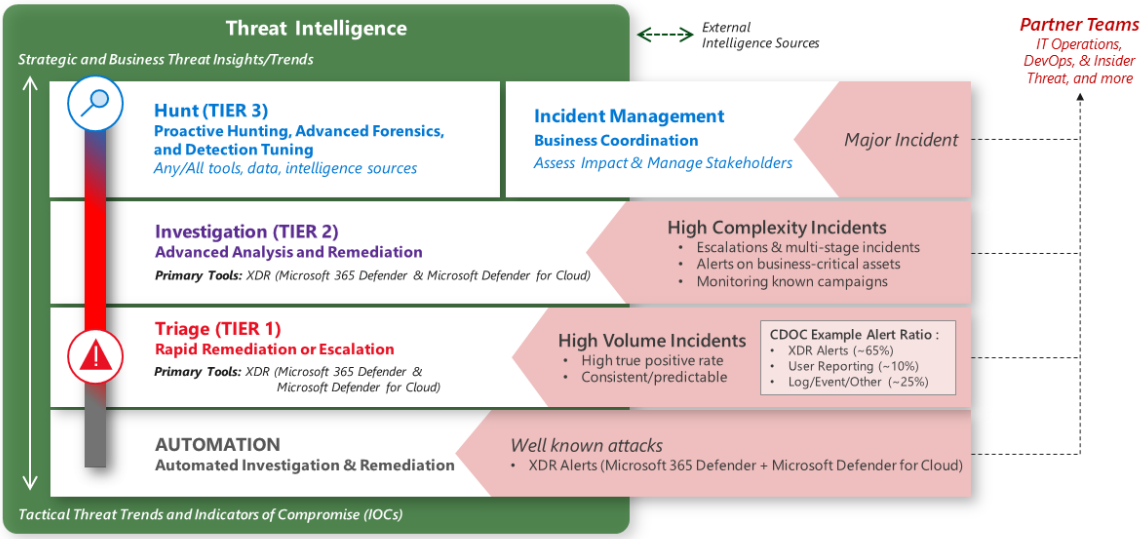


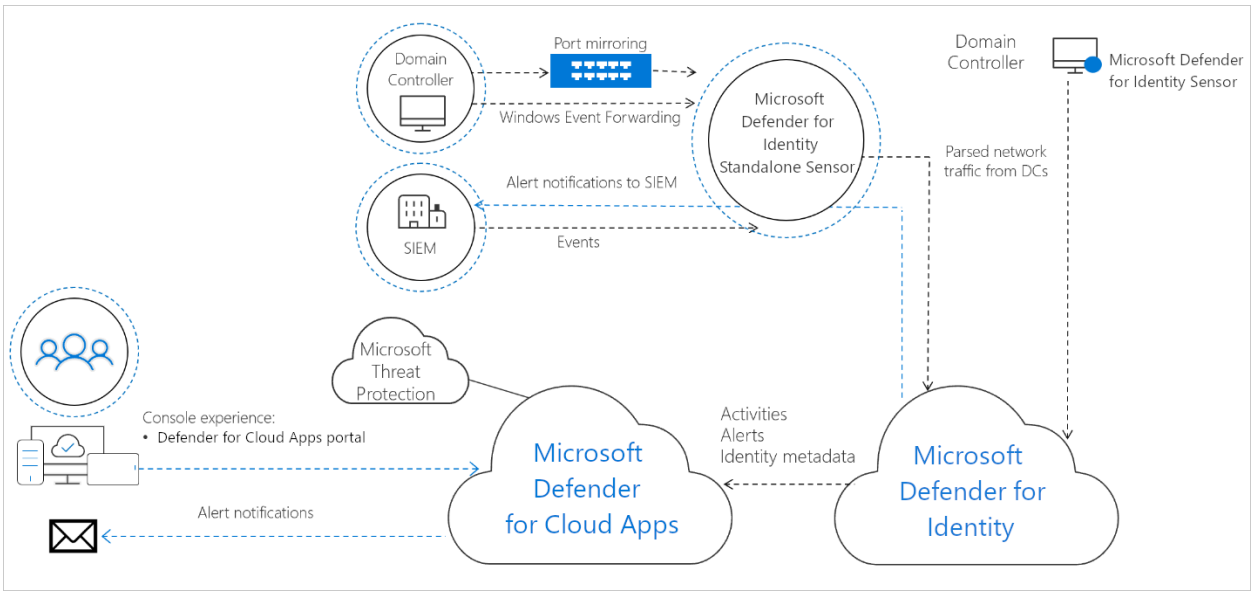
Modern Security Operations

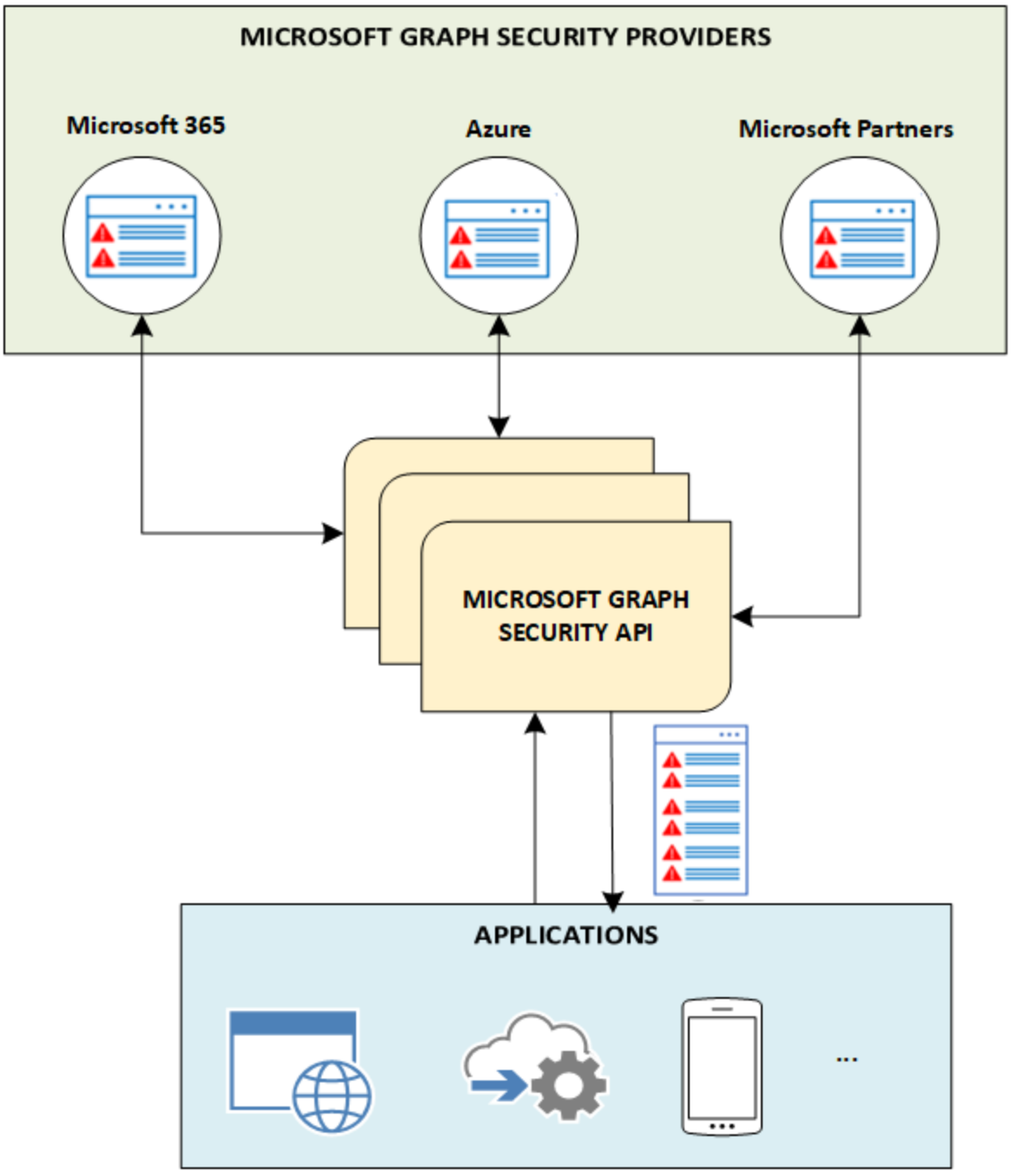
People-Centric function focused on quality, responsiveness, and rapid remediation

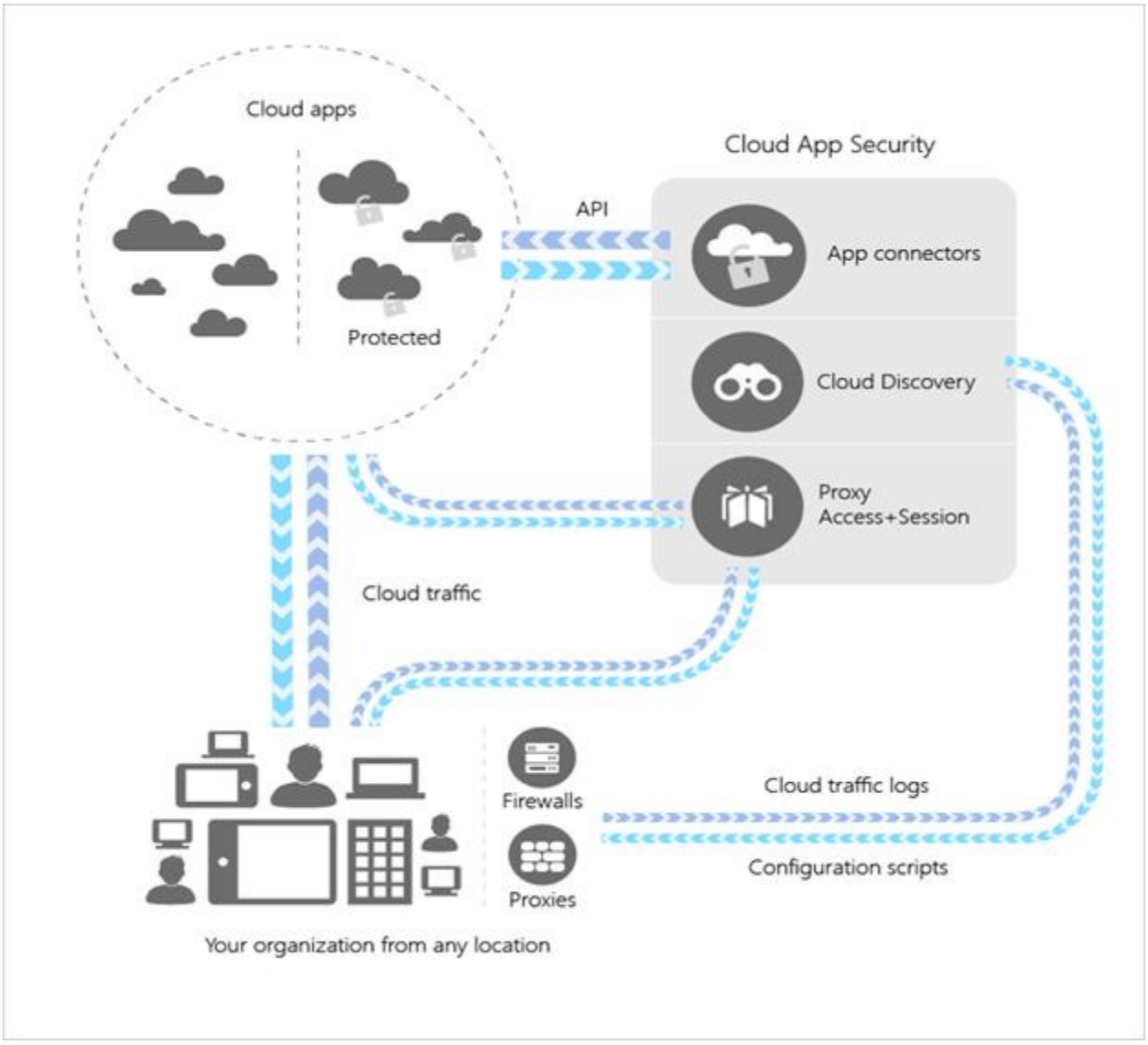


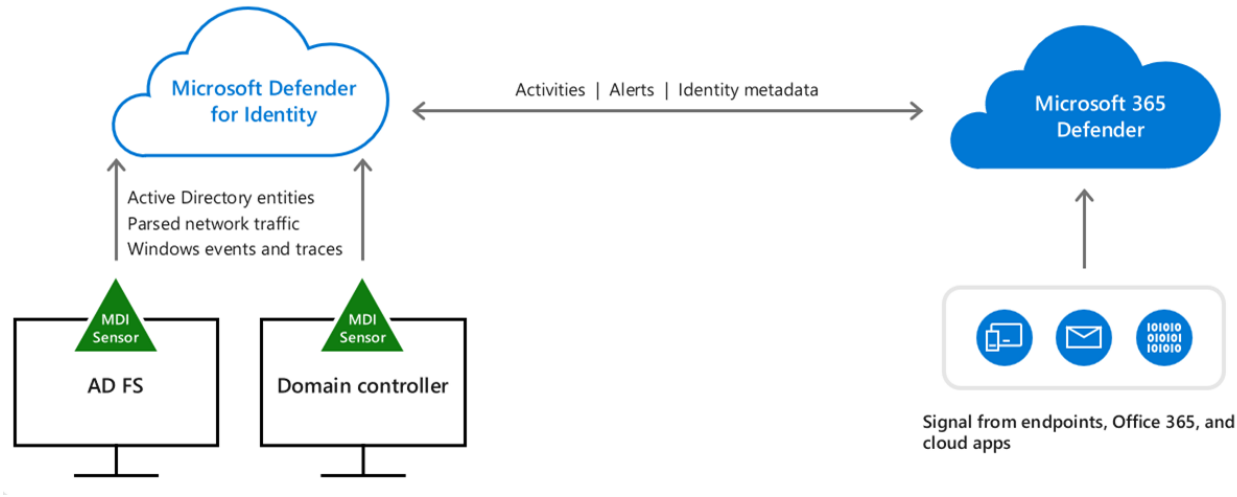
Security Operations Model – Functions and Tools

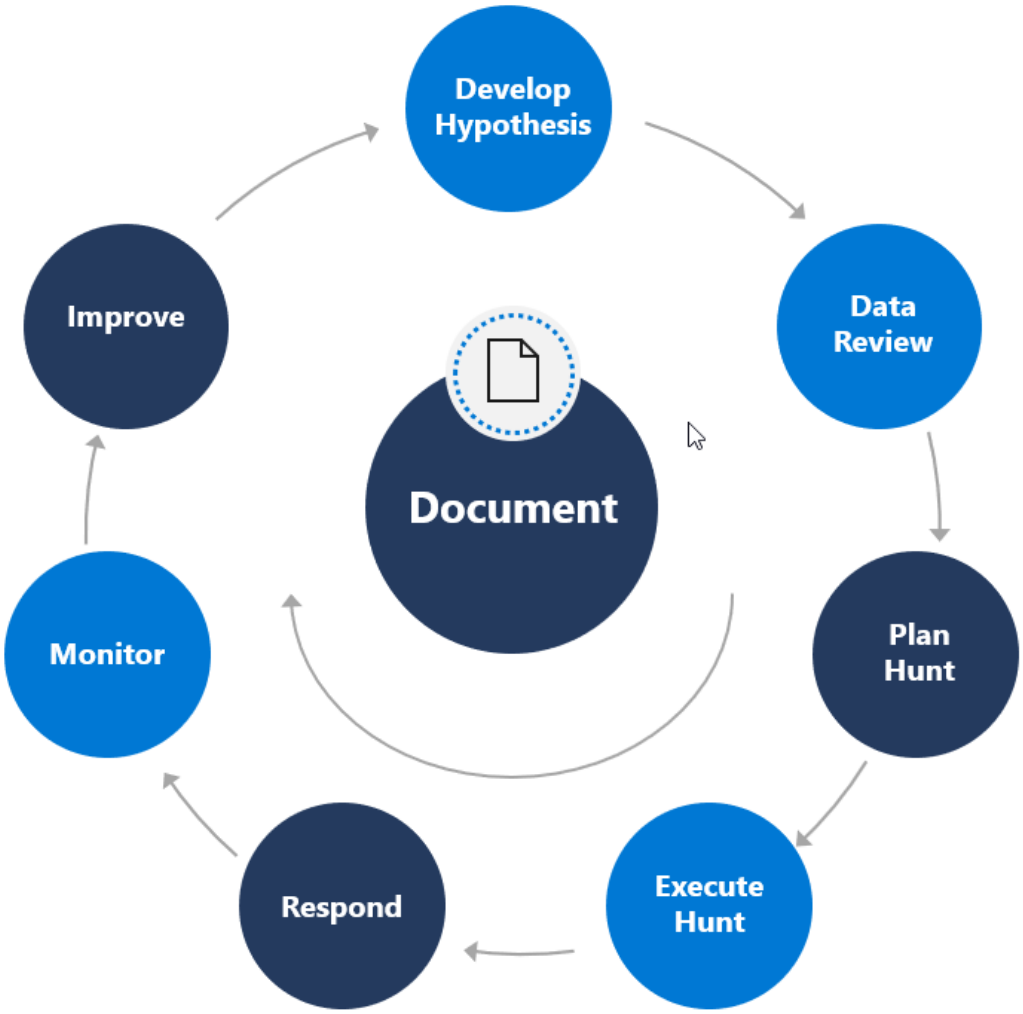





MICROSOFT GRAPH SECURITY PROVIDERS
Microsoft 365
Azure
Microsoft Partners
MICROSOFT GRAPH SECURITY API
APPLICATIONS
...


Cloud apps
Protected
Cloud App Security
API
App connectors
Cloud Discovery
Proxy
Access+Session
Cloud traffic
Firewalls
Proxies
Cloud traffic logs
Configuration scripts
Your organization from any location


Microsoft Defender for Identity
Activities | Alerts | Identity metadata
Microsoft 365 Defender
Active Directory entities
Parsed network traffic
Windows events and traces
MDI Sensor
AD FS
MDI Sensor
Domain controller
Signal from endpoints, Office 365, and cloud apps


Develop Hypothesis
Data Review
Plan Hunt
Execute Hunt
Respond
Monitor
Improve
Document