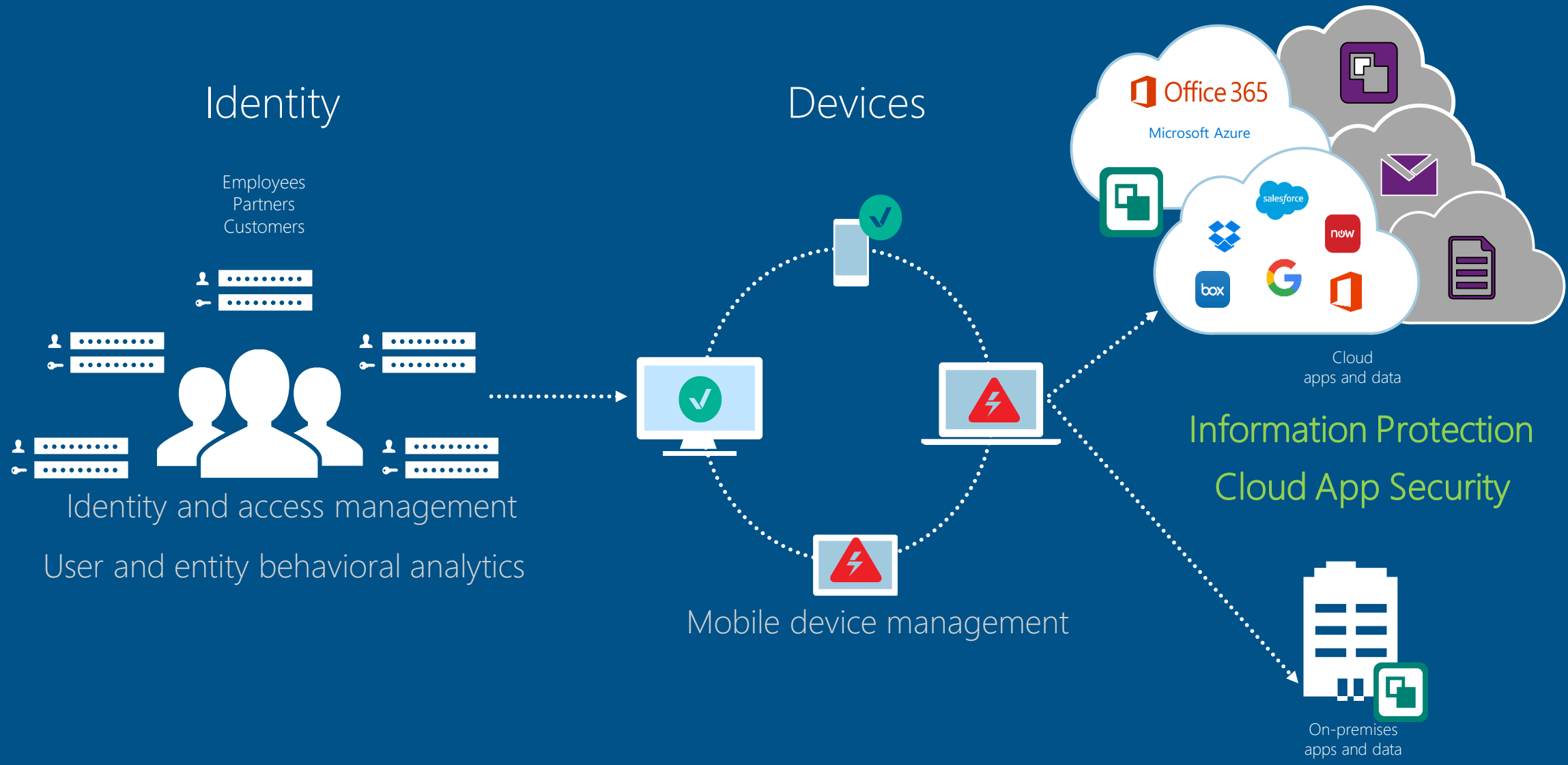
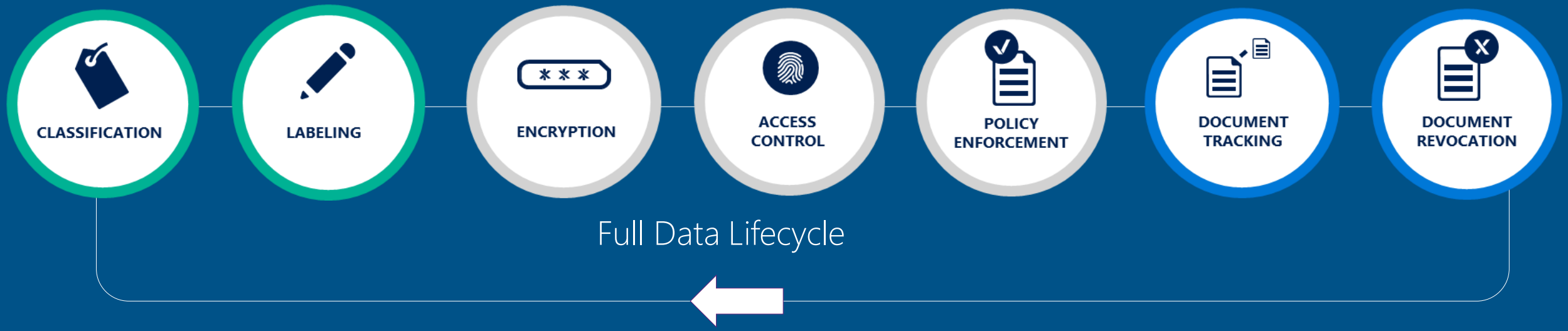
Control your data with Azure Information Protection, Office 365 DLP and Cloud App Security!

Jochen Nickel | inovit GmbH
Solution Architect
@jochennickel
https://www.inovit.ch

New Security Perimiter



Azure Information Protection

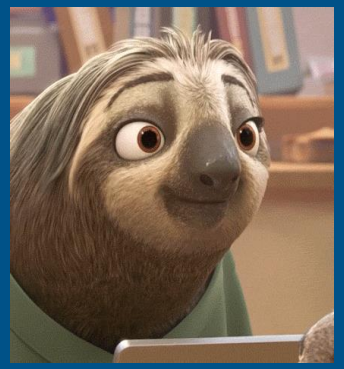


Classification and labeling process

4

ACT

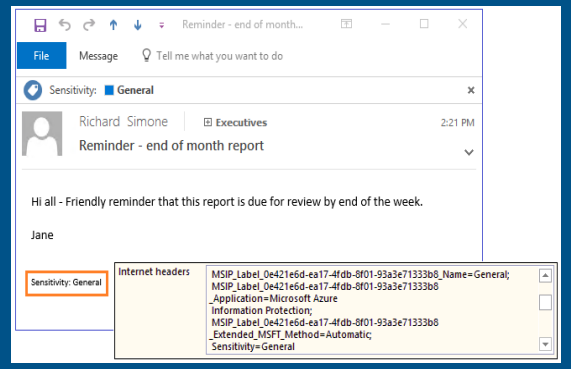
Reclassify data



1

PLAN

Identify data assets
Identify data custodian
Develop protection profiles



2

DO

Deploy classification program
Implement enforcement technologies

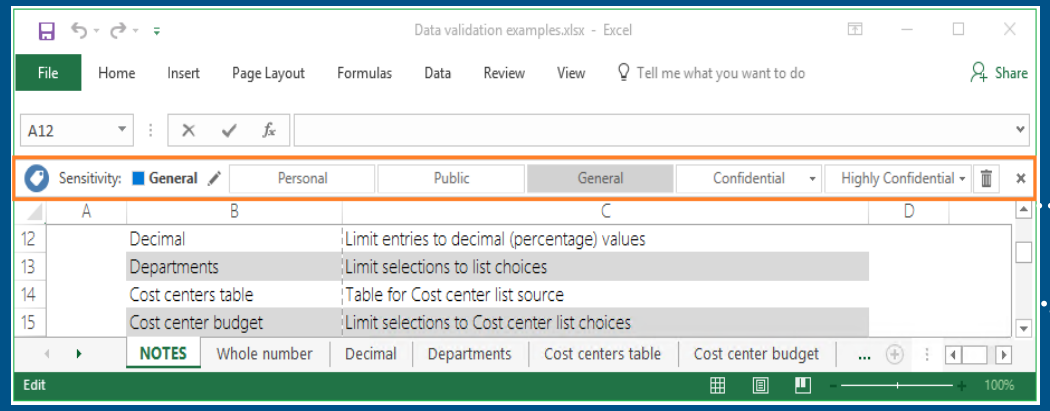
3

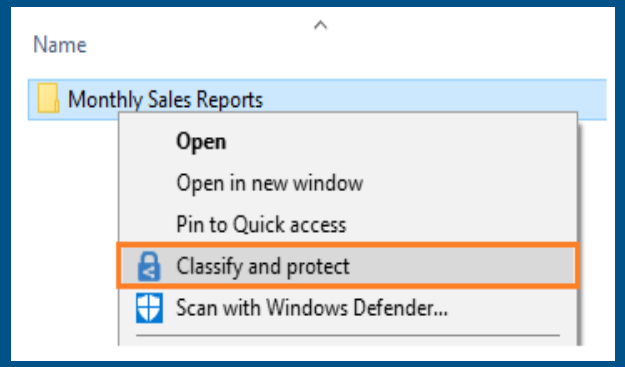
CHECK

Review classification
Report/log

Encryption | Access | Policy

Control | Enforcement



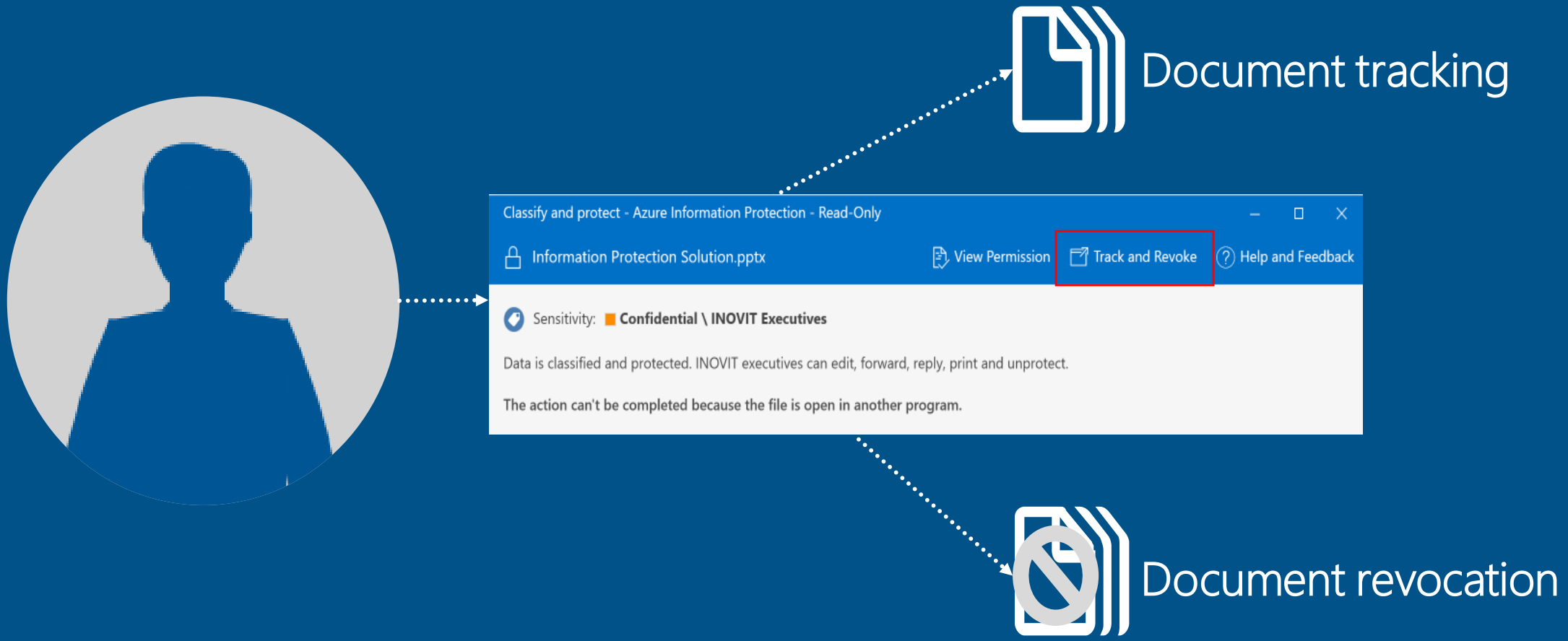


Azure Active Directory
Azure Information Protection
Azure Rights Management Services
Azure Key Management

HYOK

AD Rights Management Services
RMS Connector
Hardware Security Module

Document Tracking and Revoke Permissions



Cloud App Security

Access control

Data protection

Policy Enforcement Point
(PEP)

Cloud access security broker
(CASB)

Threat prevention

Shadow IT

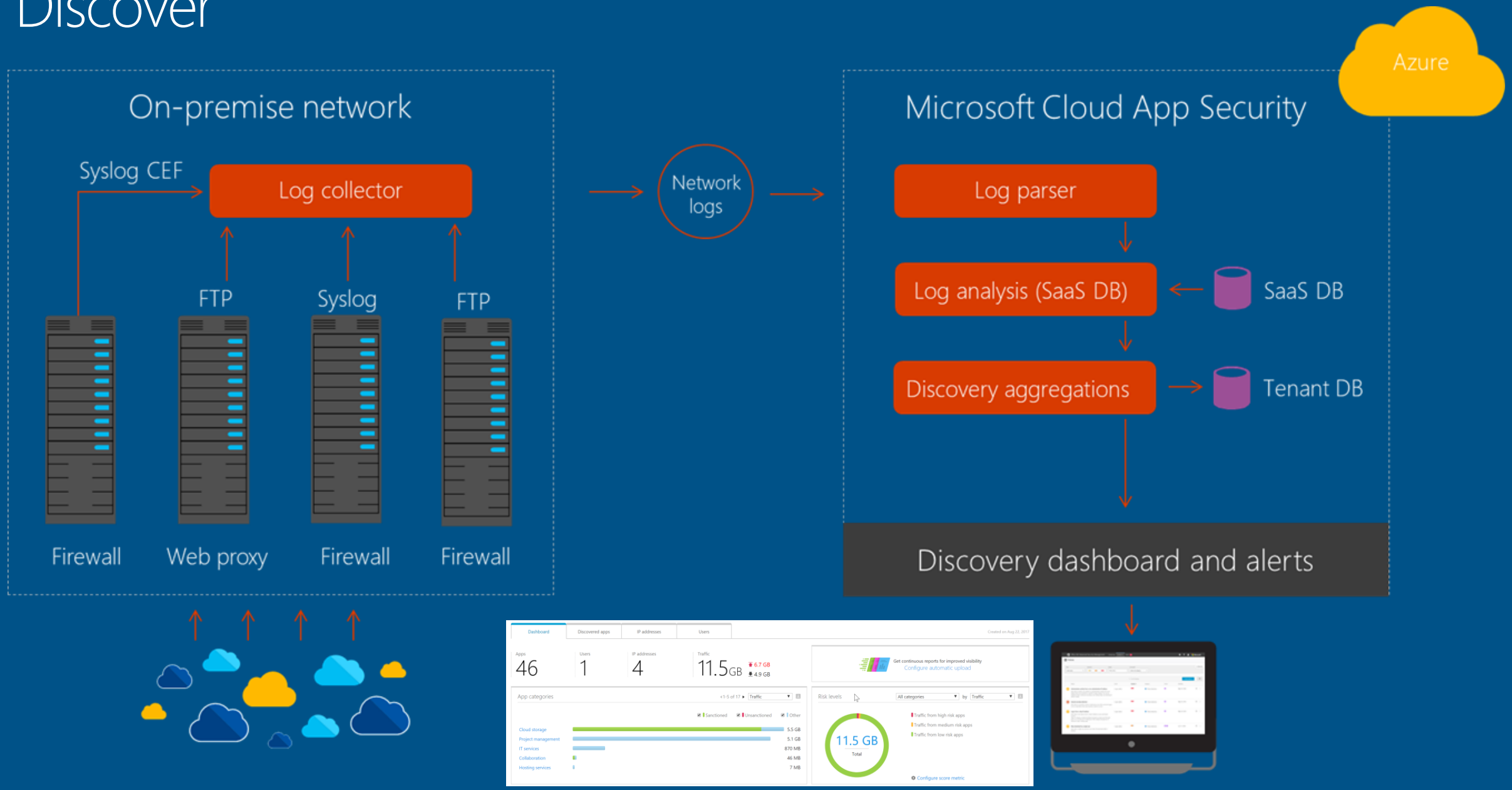
App connectors

Cloud traffic logs

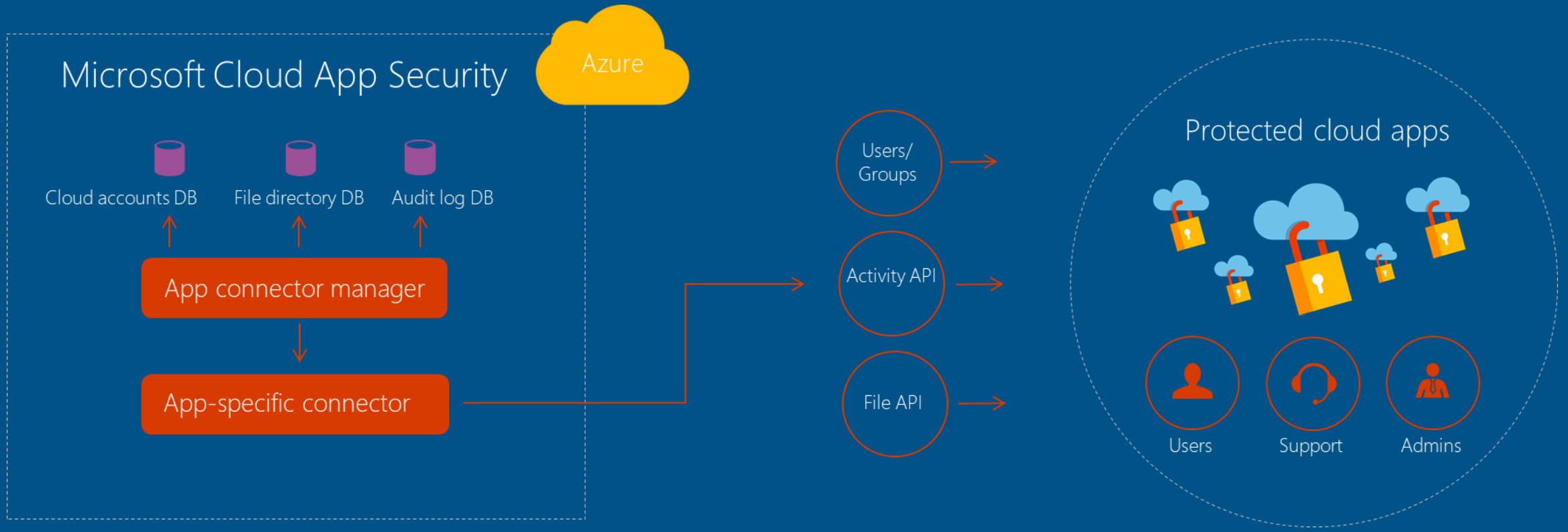
Cloud App Security vs Office 365

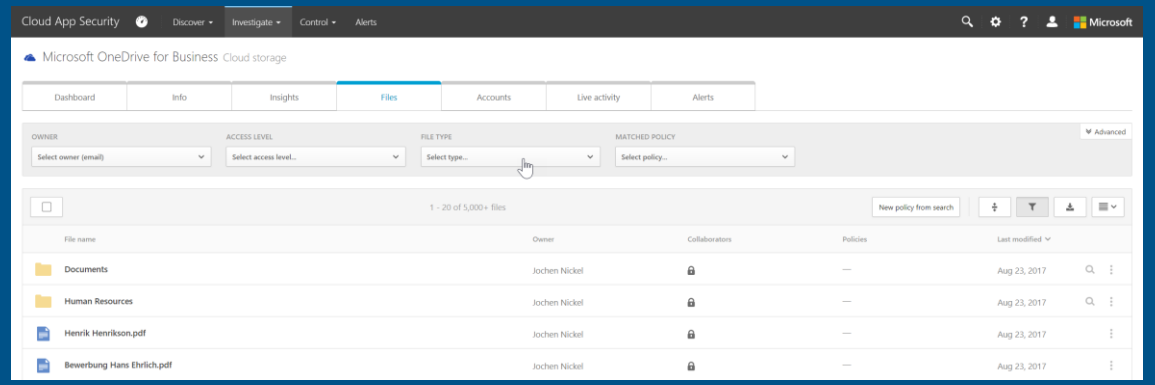
	Cloud App Security	Office 365 Advanced Security
App Discovery	▪ Discovers more than 13'000 apps and provides an automated risk score ▪ Provides ongoing risk assessment for discovered services ▪ (usage patterns, upload/download traffic anonmalies) ▪ Anomaly detection for discovered apps	▪ Discovers apps that have similar functionality to Office 365 ▪ Manual log upload
Data control	▪ Policy setting and enforcement ▪ DLP and data sharing controls all sanctioned apps ▪ Identify and control apps connected to supported cloud services with the availability to revoke access ▪ Azure AD Premium for user and session access control, SAML proxy for non-Azure AD customers for any app	▪ Existing Office DLP (E3 and above) ▪ Azure AD Premium for user and session access control ▪ Identify and control apps connected to Office 365 with the availability to revoke access
Threat prevention	▪ Alerts dashboard includes all policy violations, threat detection and anomaly detection across SaaS apps ▪ Manual or automatic alert remediation	▪ Anomaly detection and security alerts for Office 365 ▪ Manual or automatic alert remediation

Discover

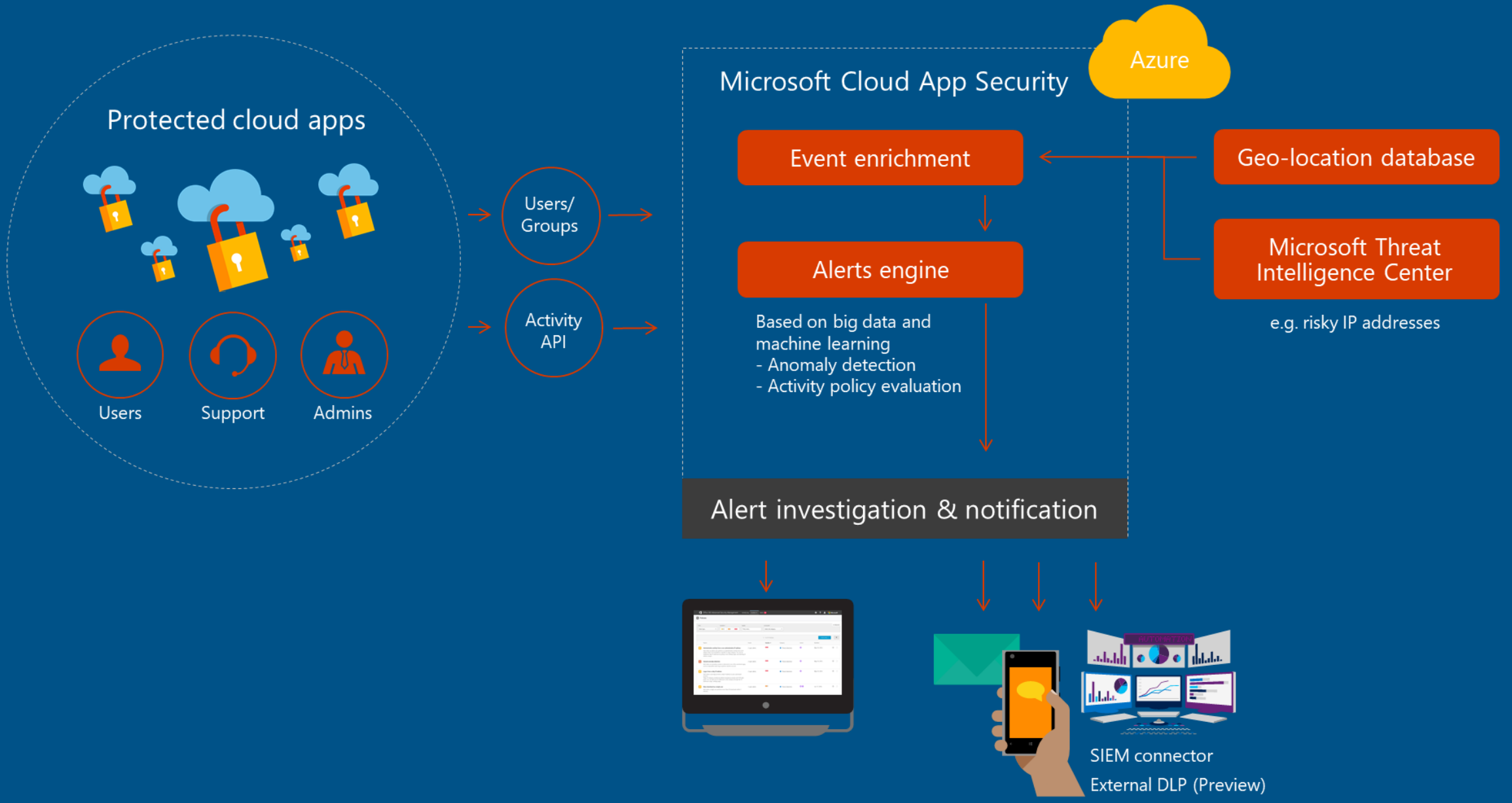

On-premise network
Syslog CEF
Log collector
FTP
Syslog
FTP
Firewall
Web proxy
Firewall
Firewall
Network logs
Azure
Microsoft Cloud App Security
Log parser
Log analysis (SaaS DB)
SaaS DB
Discovery aggregations
Tenant DB
Discovery dashboard and alerts
Dashboard
Discovered apps
IP addresses
Users
Apps
46
Users
1
IP addresses
4
Traffic
11.5GB
6.7 GB
4.9 GB
Get continuous reports for improved visibility
Configure automatic upload
App categories
Sanctioned
Unsanctioned
Other
Cloud storage
5.5 GB
Project management
5.1 GB
IT services
870 MB
Collaboration
46 MB
Hosting services
7 MB
Risk levels
All categories
by
Traffic
11.5 GB
Total
Traffic from high risk apps
Traffic from medium risk apps
Traffic from low risk apps
Configure score metric

Investigate

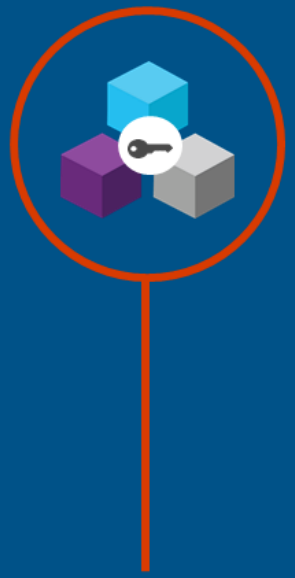




Control


Protected cloud apps
Users
Support
Admins
Users/ Groups
Activity API
Microsoft Cloud App Security
Azure
Event enrichment
Alerts engine
Based on big data and machine learning
- Anomaly detection
- Activity policy evaluation
Geo-location database
Microsoft Threat Intelligence Center
e.g. risky IP addresses
Alert investigation & notification
SIEM connector
External DLP (Preview)

Protection



Gain cloud data visibility

Visibility to sharing level and classification labels

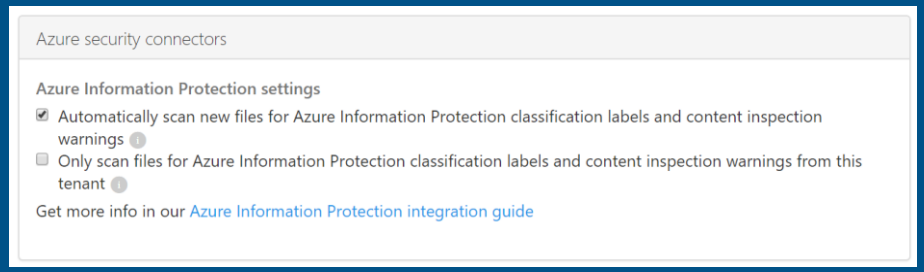
Quantify exposure and risk

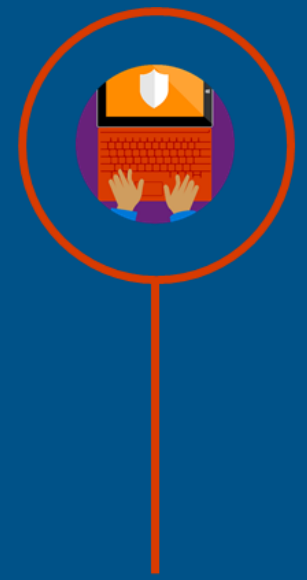
Detect and manage 3rd apps access

Enforce DLP policies & control sharing

Govern data in the cloud with granular DLP policies

Leverage Microsoft and 3rd party DLP engines for classification





Identify policy violations

Investigate incidents and related activities

Quarantine and permissions removal

Many thanks!