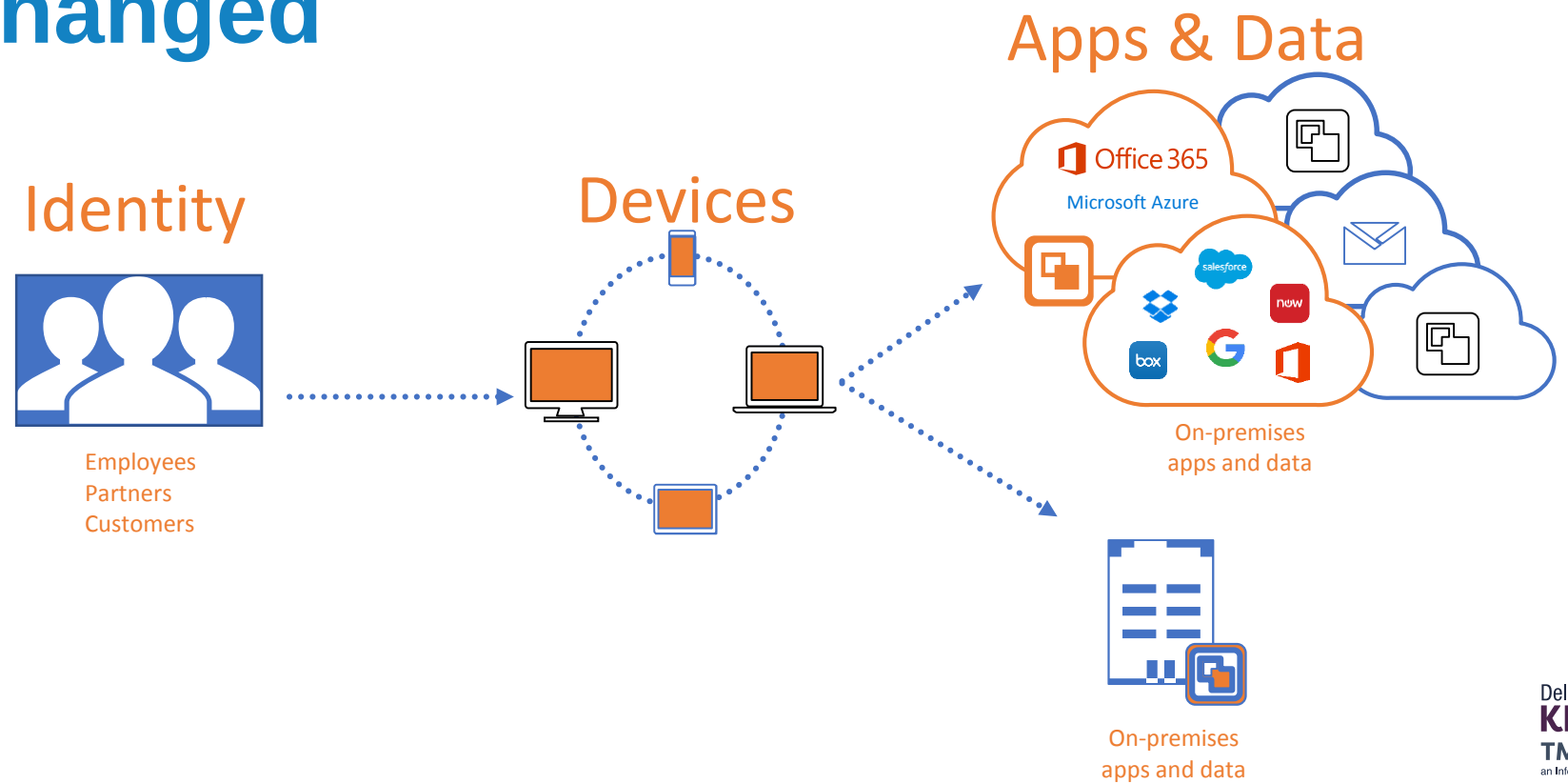
IT/Dev CONNECTIONS

Stopping Malicious Users with Office 365 Cloud App Security

Riaz Javed
Lead Architect
PCM Inc.

Delivered by KNect365 TMT an Informa business

The security landscape has changed



Microsoft Cloud App Security

Cloud-delivered service bringing visibility and control to cloud apps

Committed to support third-party cloud apps

Available as: standalone and in E5

What to Consider

Access control

Employee downloads customer details from an airport kiosk.

How can I detect and limit access?

Shadow IT

Office 365 is rolled out.
How do I know which groups are using other apps?

Threat prevention

How do I know if my users have been breached?

Access control

An employee publicly shares a sensitive file in the cloud.
How can I detect that?

Framework to Secure your Cloud Apps

Cloud discovery

Information protection

Threat prevention

In-session control

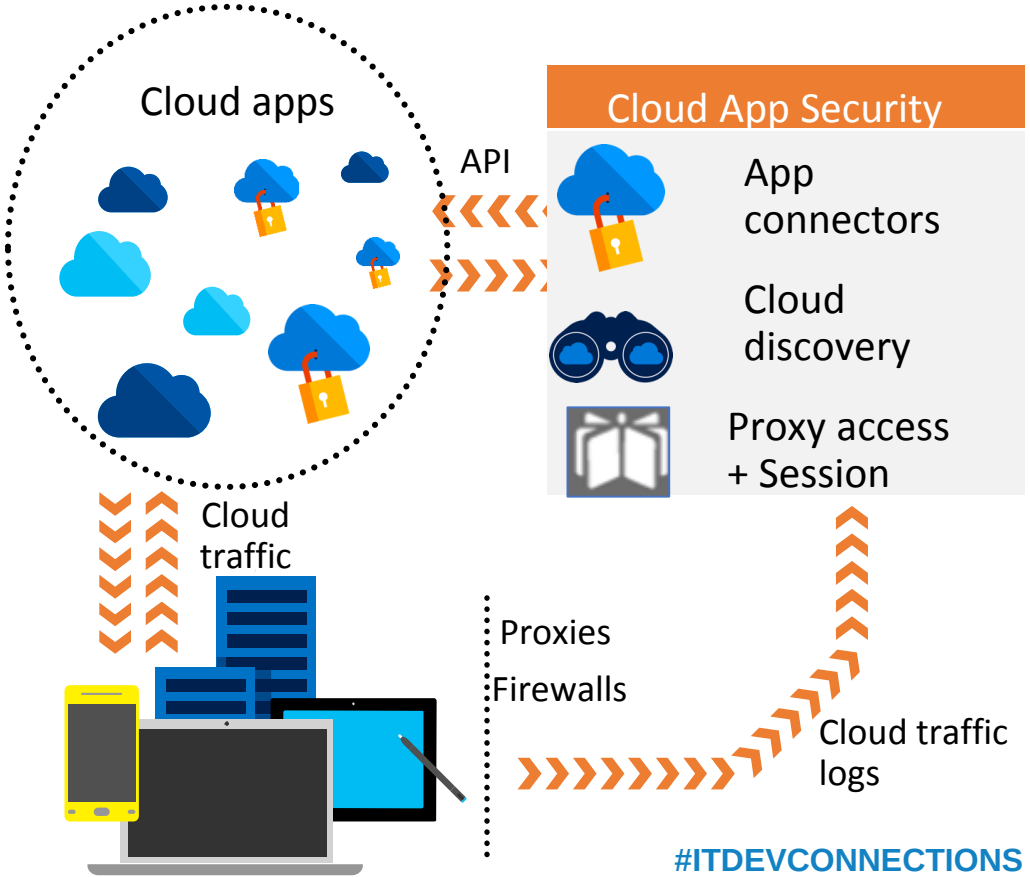
DISCOVER > INVESTIGATE > CONTROL > PROTECT

IT/Dev CONNECTIONS

Cloud App Security Architecture

Delivered by KNect365 TMT an Informa business

Architecture and how it works



Discovery

- Use traffic logs to discover and analyze which cloud apps are in use

Sanctioning and un-sanctioning

- Sanction or block apps in your organization using the cloud app catalog

App connectors

- Leverage APIs provided by various cloud app providers

Conditional Access

- Real-time visibility and control over access to and activities performed within your cloud environment

Deploy Cloud App Security in 4 simple steps

- Create a trial tenant
- Upload discovery logs
- Connect a sanctioned SaaS app
- Configure initial policies

Discovery

Shadow IT discovery

Discover cloud apps in use across your networks

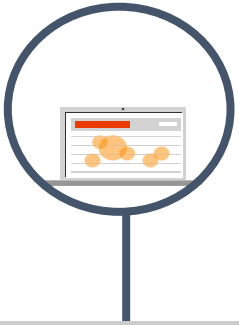
Investigate users and source IP cloud usage

Un-sanction, sanction and protect apps

Cloud app risk assessment

Risk scoring for 13,000+ cloud apps

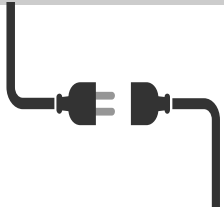
60+ security and compliance risk factors



Alert on risky cloud usage

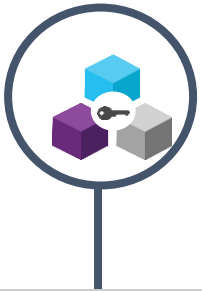
Anomalous usage alerts

New apps and trending apps alerts



Your network appliances

Information Protection for Cloud Apps



Gain cloud data visibility

Visibility to sharing level and classification labels

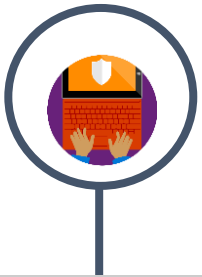
Quantify exposure and risk

Detect and manage 3rd apps access

Enforce DLP policies & control sharing

Govern data in the cloud with granular DLP policies

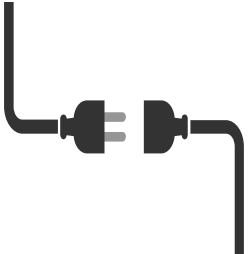
Leverage Microsoft and 3rd party DLP engines for classification



Identify policy violations

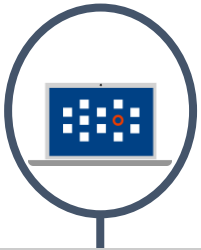
Investigate incidents and related activities

Quarantine and permissions removal



AIP, 3rd party DLP

Threat detection

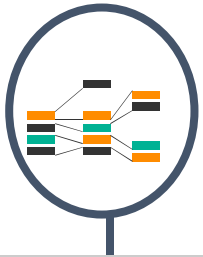


Behavioral analytics

Support sharing level and classification labels

Quantify exposure and risk

Detect and manage 3rd apps access



Advanced investigation

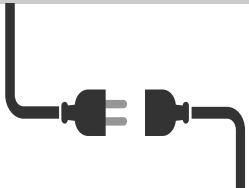
Advanced incident Investigation tools

Pivot on users, file, activities and locations

Customize detections based on your findings

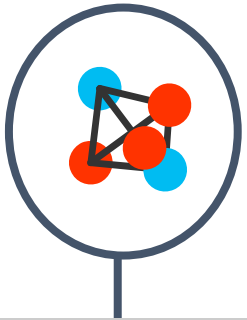
Leverage Microsoft Intelligent Security Graph

Unique insights, informed by trillions of signals across Microsoft's customer base



Microsoft Intelligent Security Graph, 3rd party SIEM

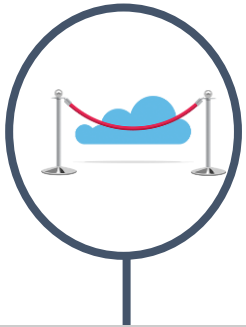
In-Session Control



Context-aware session policies

Control access to cloud apps based on user, location, device and app

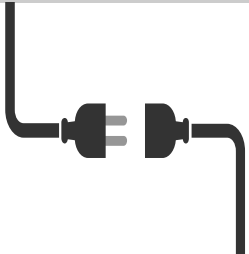
Supports any SSO, any SAML-based app, any OS



Limit sessions of unmanaged devices

Enforce browser-based “view only” mode for risky sessions

Limit access to sensitive data



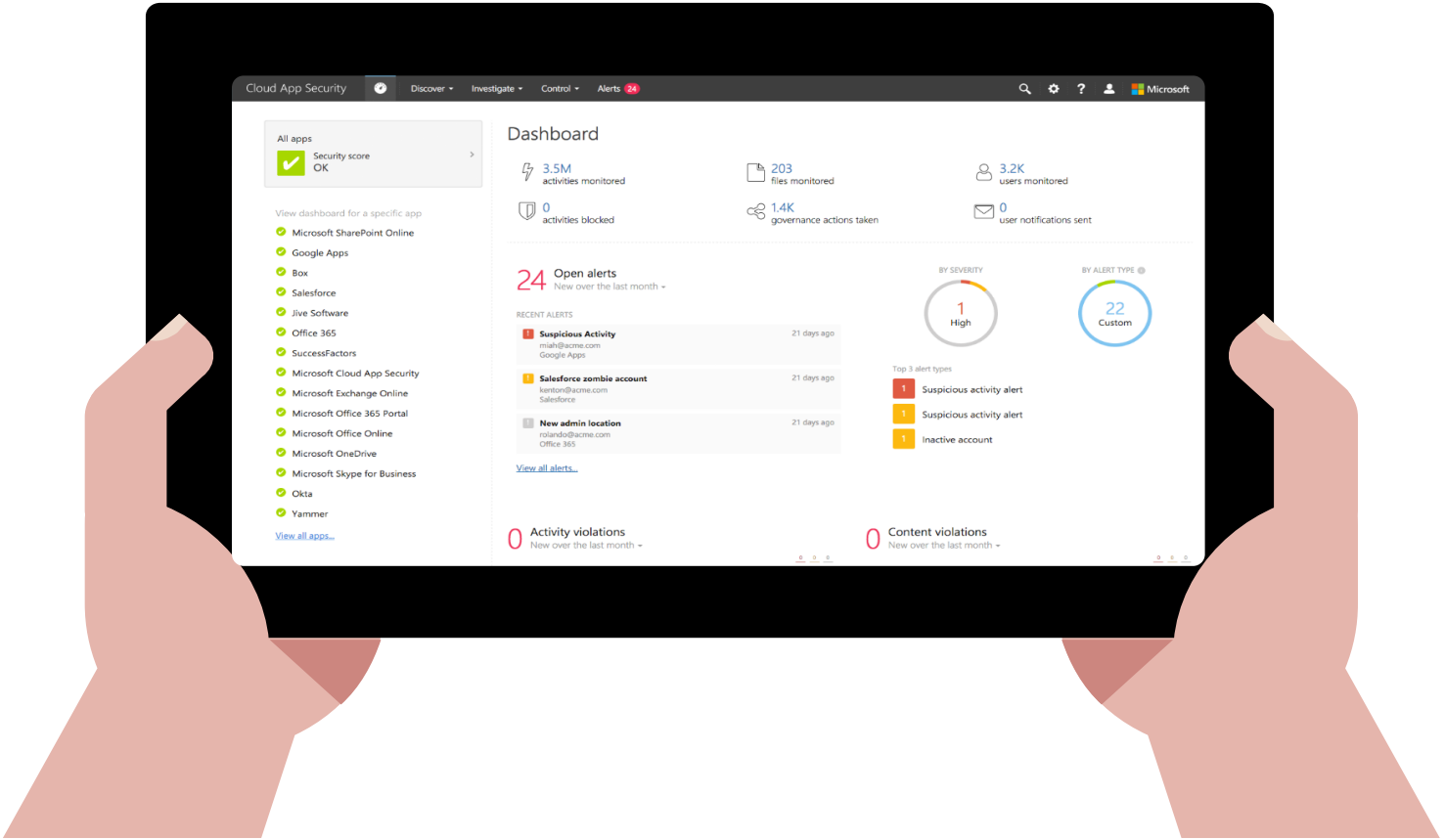
Azure Active Directory, Device Registration Service

Try Cloud App Security

www.cloudappsecurity.com

Try free for 30 days or Request a demo

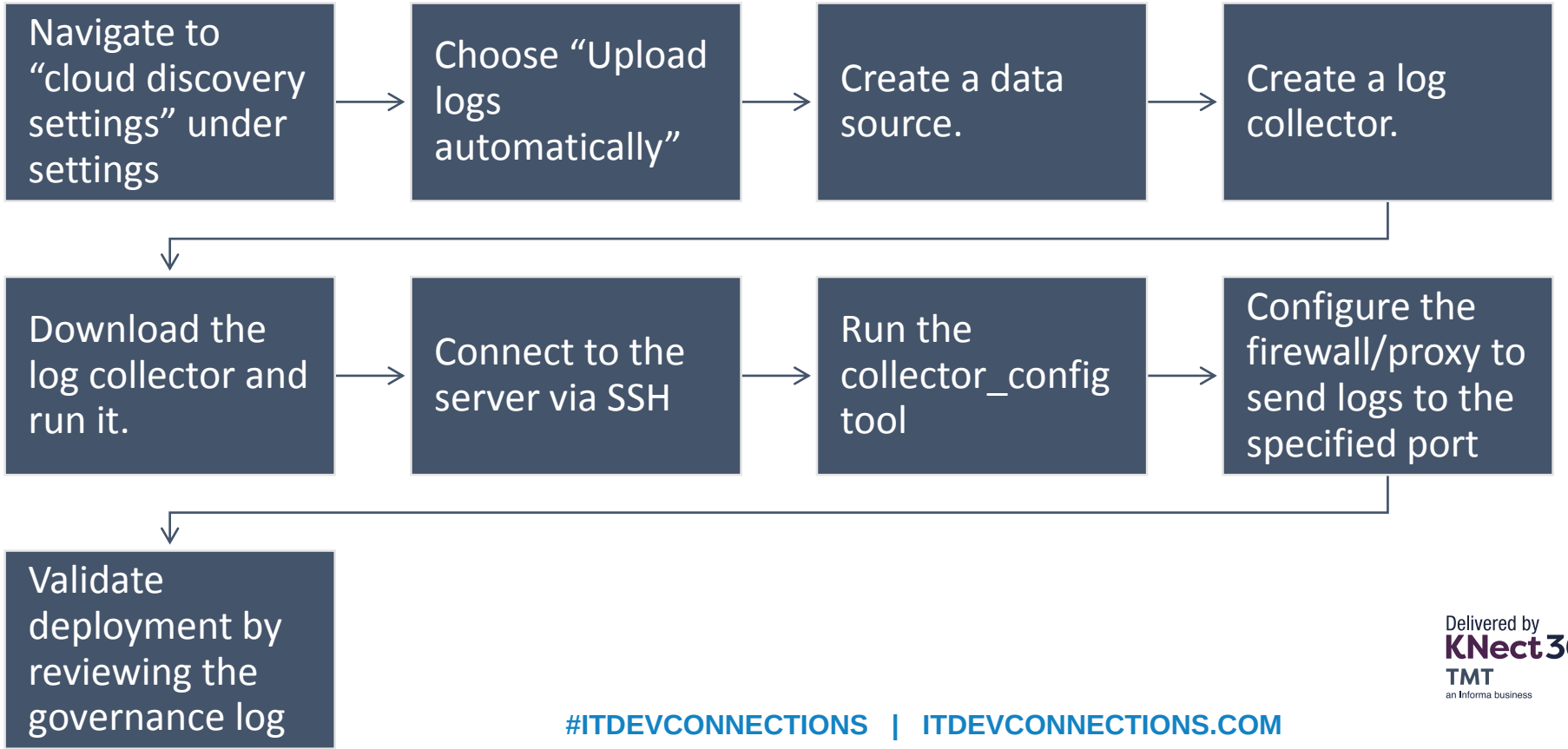
Cloud App Security portal overview



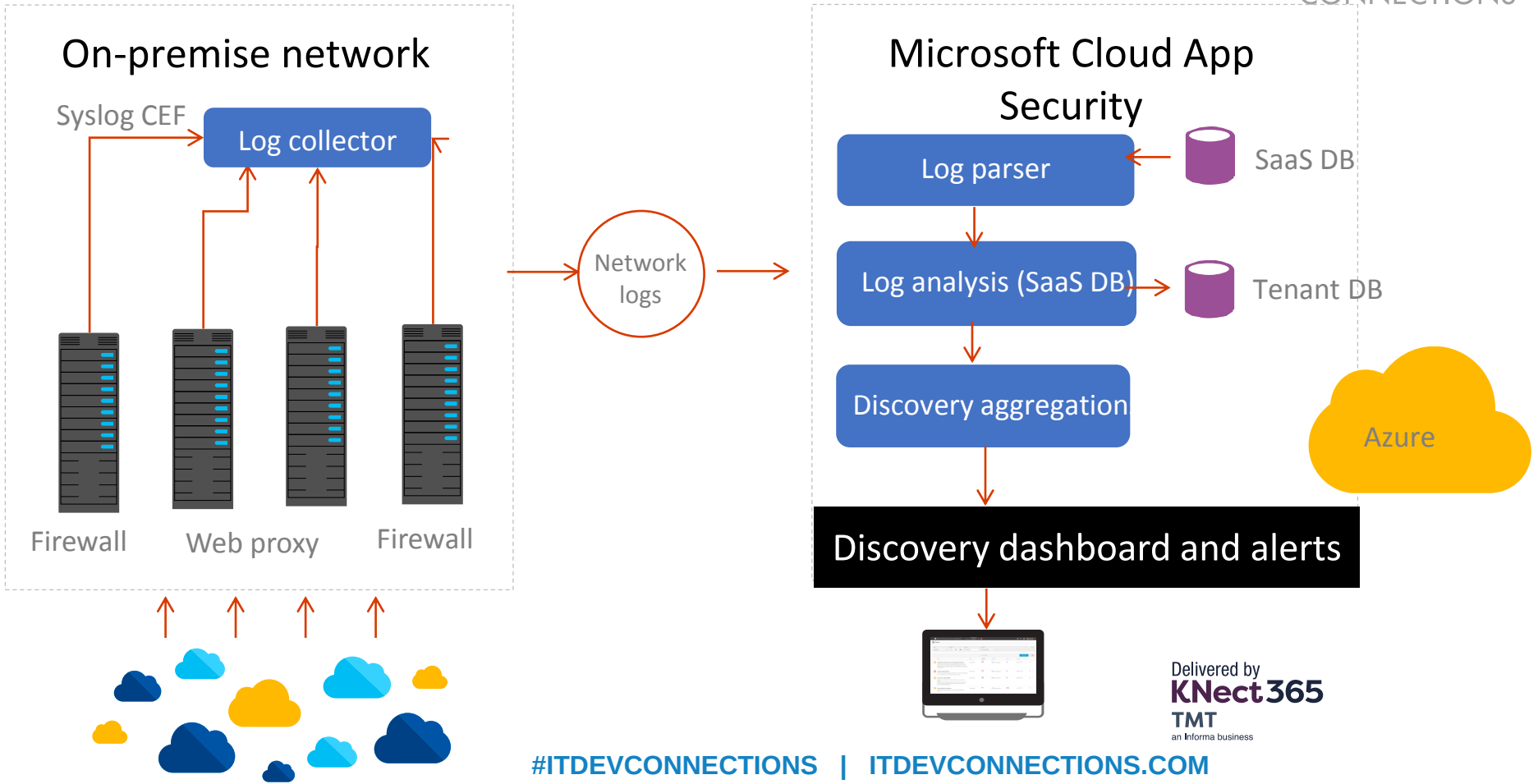
Create a Cloud Discovery snapshot report

- Export logs manually from a firewall/proxy node
- Navigate to the discovery tab and click on “upload logs”
- Fill in the report name and description
- Choose the data source according to your network appliance
- Upload the file and wait until the report is created

Upload discovery logs – Continuous upload



Discovery Architecture



Connecting a Sanctioned App

Navigate to Settings > “Sanctioned apps”

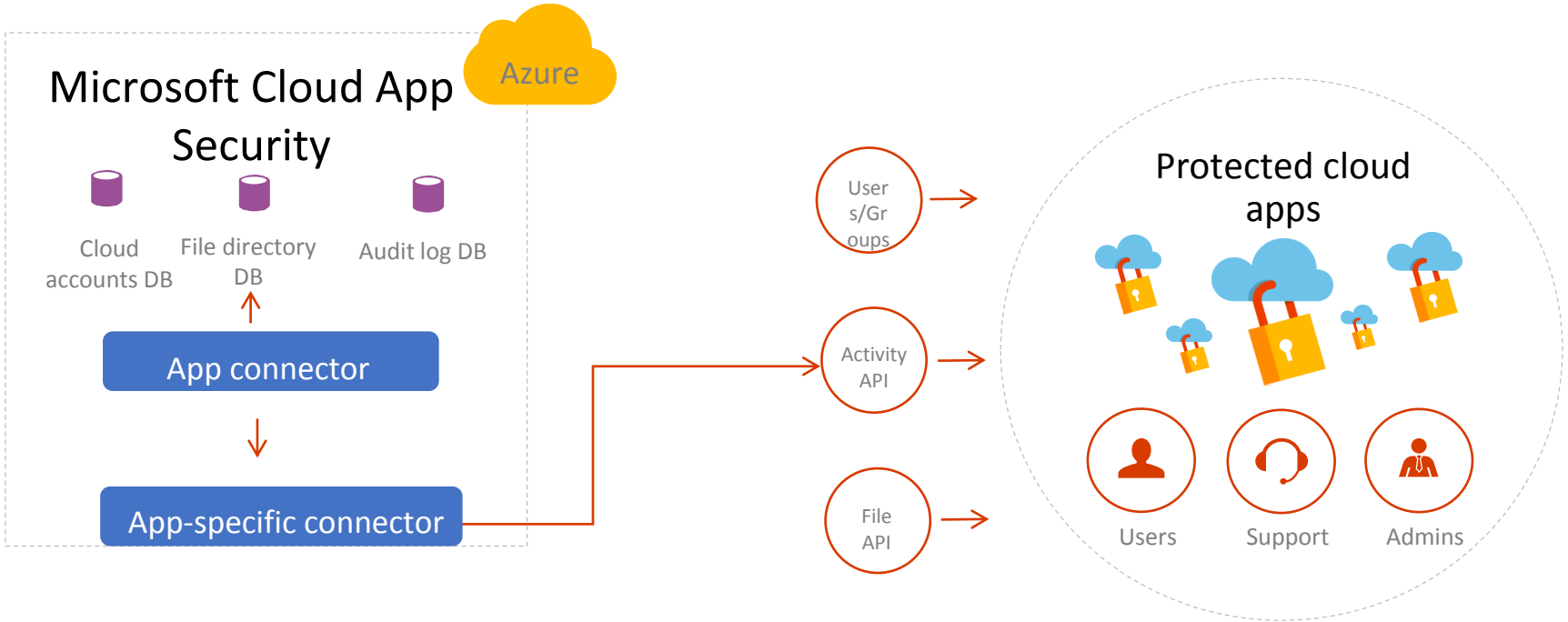
Go to “Connect an app” and choose the relevant app from the list.

Login with an admin user and approve the OAuth request

Validate deployment with “Test API”

Expect initial audit logs from the app within minutes to an hour

App Connector Architecture



Set your First Activity Policy

Navigate to the Policies page

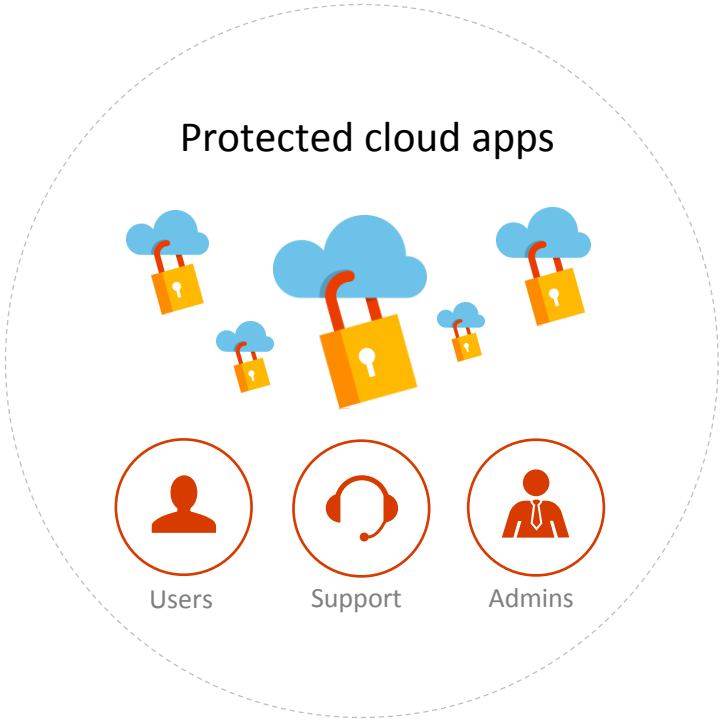
Create a policy and choose “activity policy”

Choose a template, for example, “Mass download by a single user”

Customize parameters, for example, change threshold to 10 downloads

Customize actions in response

Activity and Anomaly Detection Architecture



Event enrichment

Geo-location database

Alerts engine

Microsoft Threat Intelligence Center

e.g. risky IP addresses

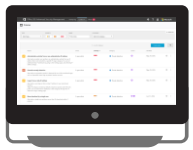
Users/ Groups

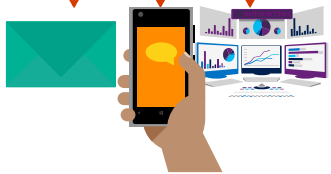
Activity API

Based on big data and machine learning
- Anomaly detection
- Activity policy evaluation

Alert investigation & notification

Azure





Delivered by KNect365 TMT an Informa business

Set up your first Policy

Navigate to the policies page

Create a policy and choose “file policy”

Choose a template, for example, “File containing PCI detected in the cloud”

Customize policy, for example, narrow scope for “Access level” equals Public

Customize actions in response

Files and Data Control Architecture