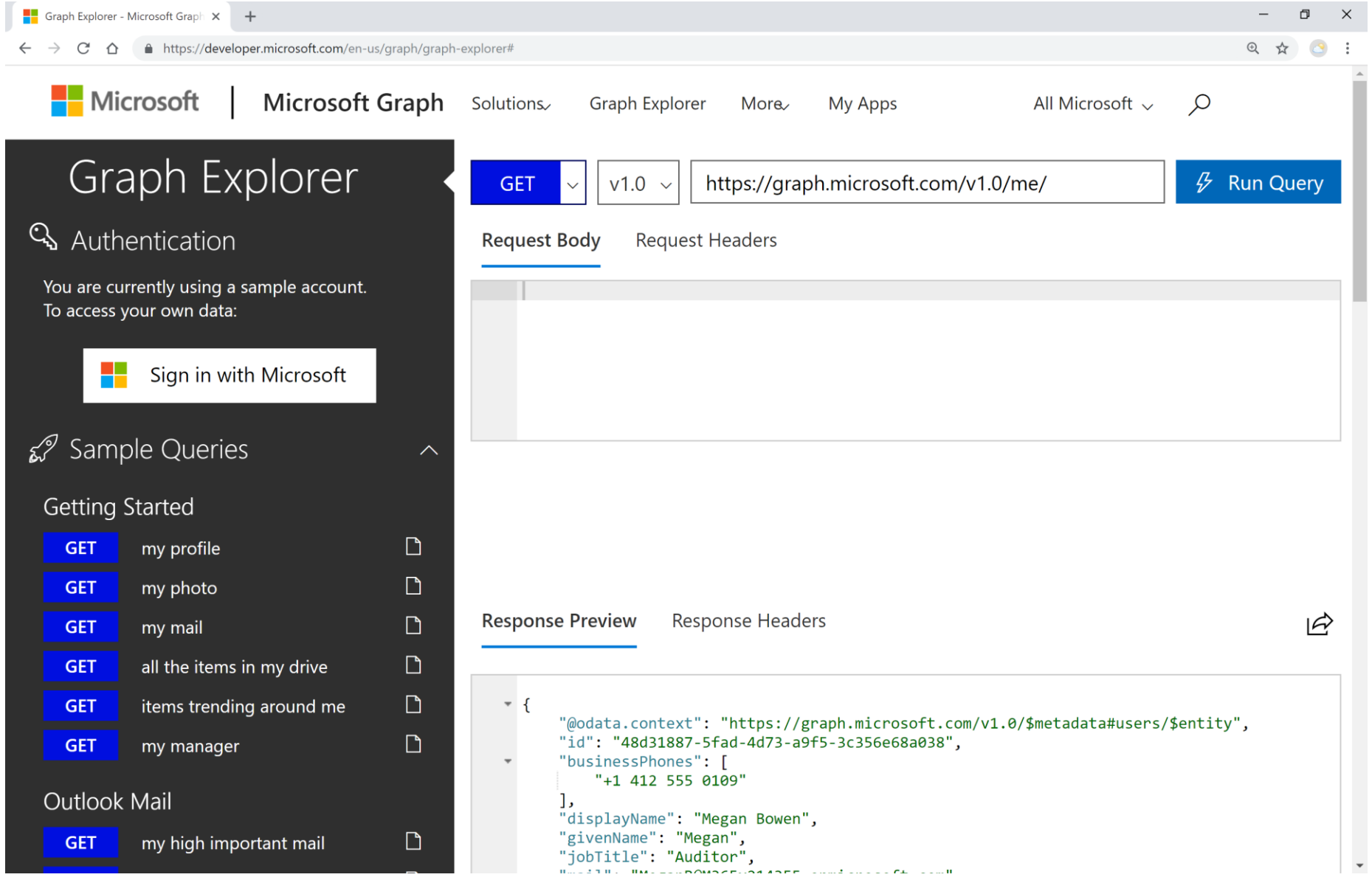
Microsoft 365

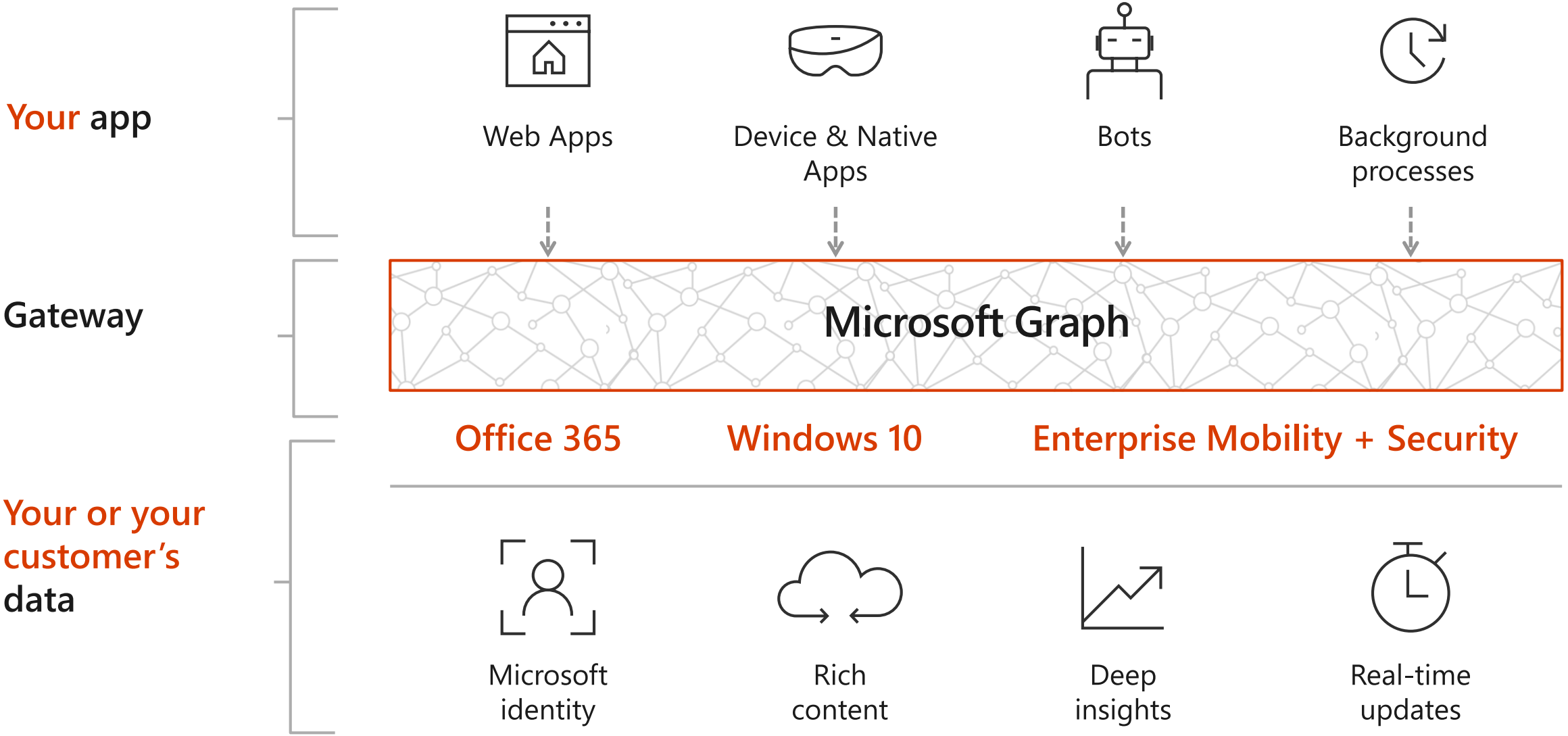
Adding custom intelligence to Microsoft Graph

Mark Stafford

Microsoft Graph: the API for M365



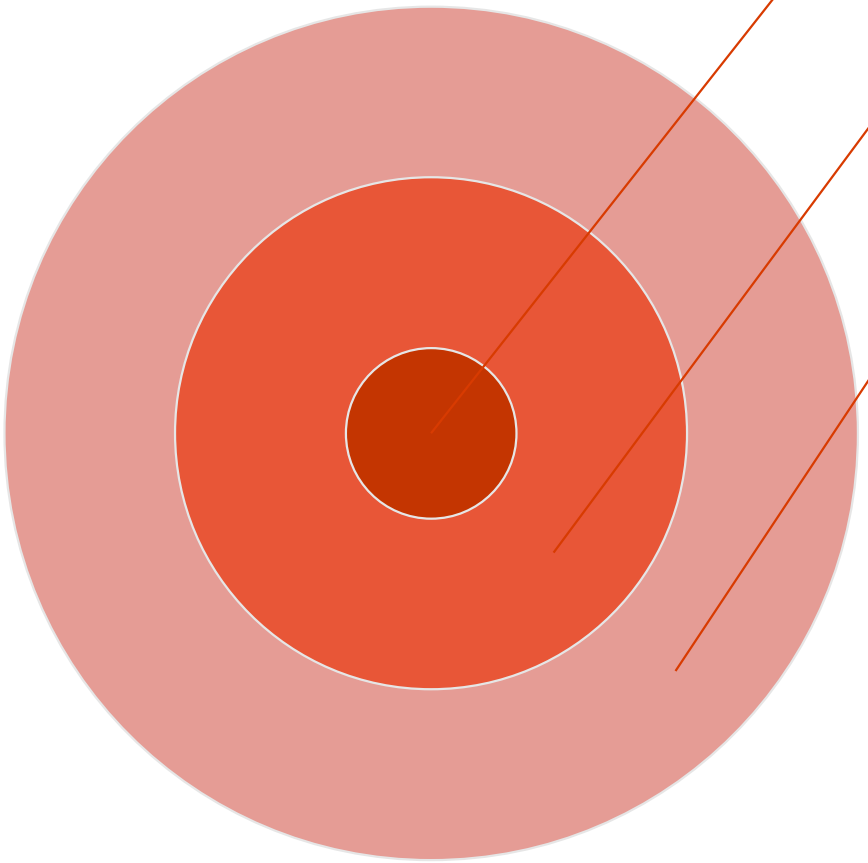
Gateway to your data in the Microsoft cloud



Problem

Microsoft Graph has tons of data…
but how do we add intelligence?

Intelligence strategies

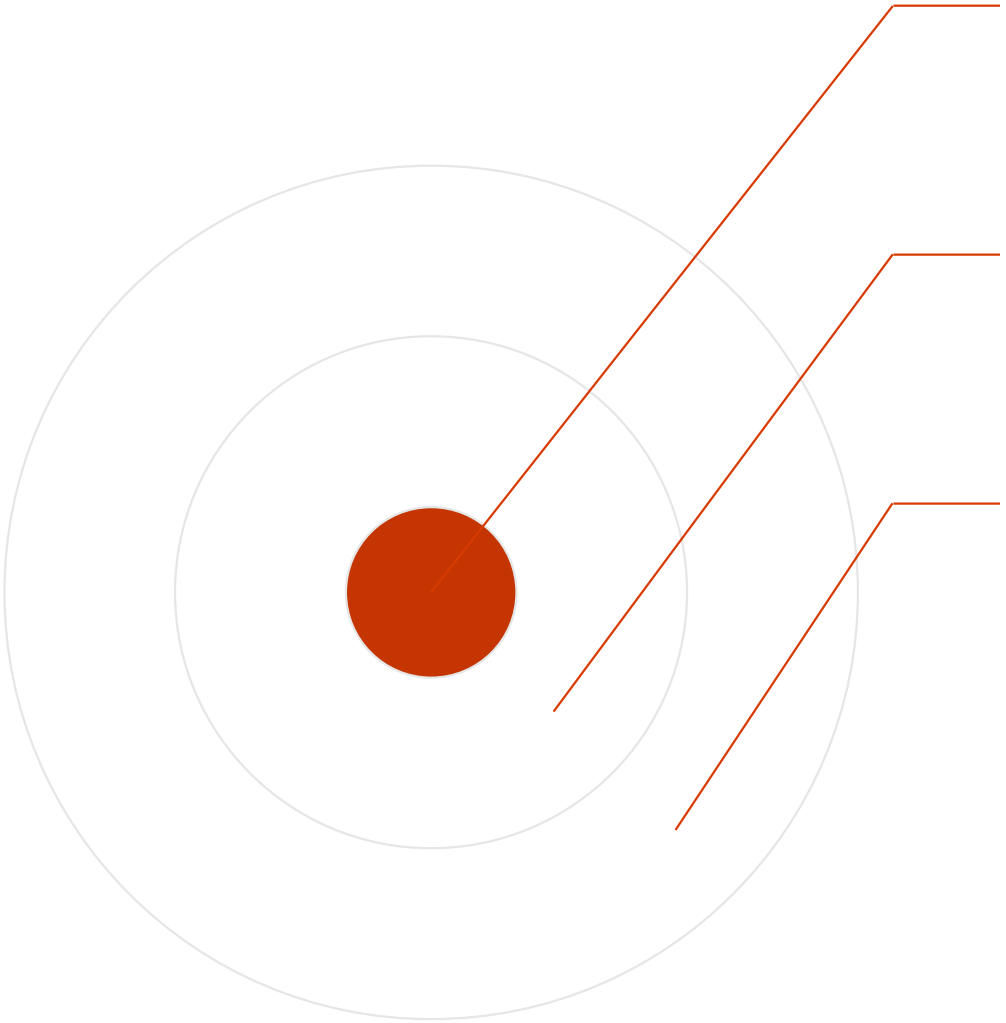


Built-in insights

1st class partnership

Bring your own

Intelligence strategies



Built-in insights

1st class partnership

Bring your own

Built-in insights

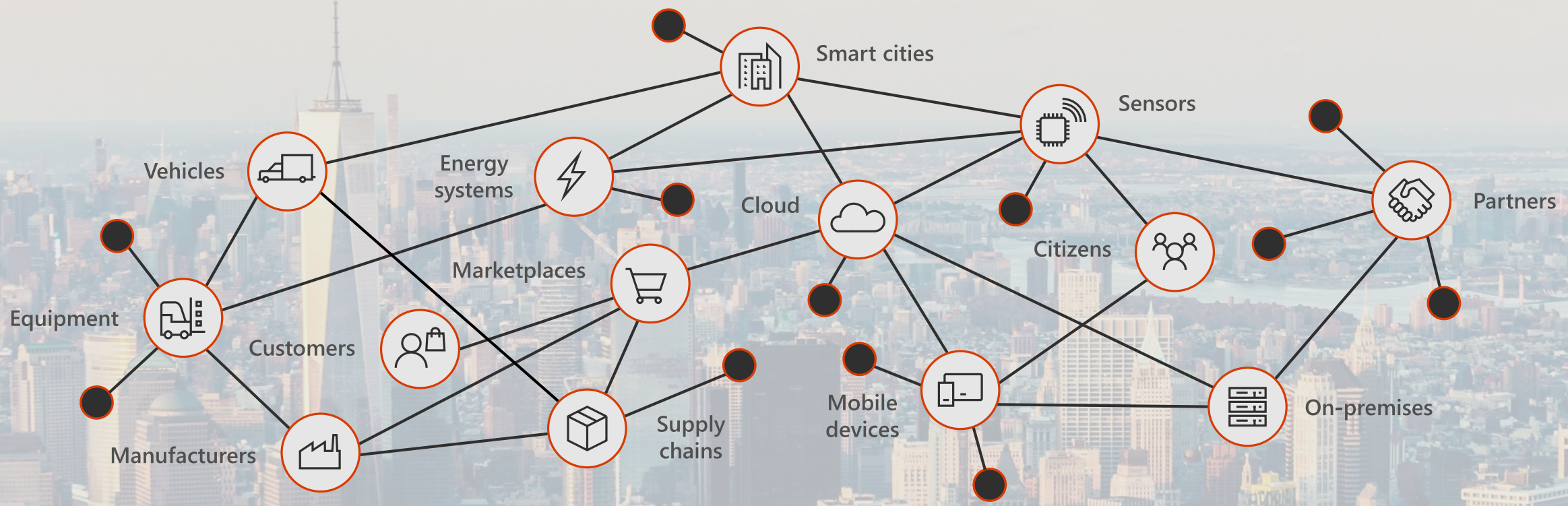
- O365
  - People
  - Insights
- Enterprise Mobility + Security
  - Security API
- Windows
  - Spatial Analytics

Microsoft

BRK2012

Harnessing the power of the Intelligent Security Graph

The digital estate



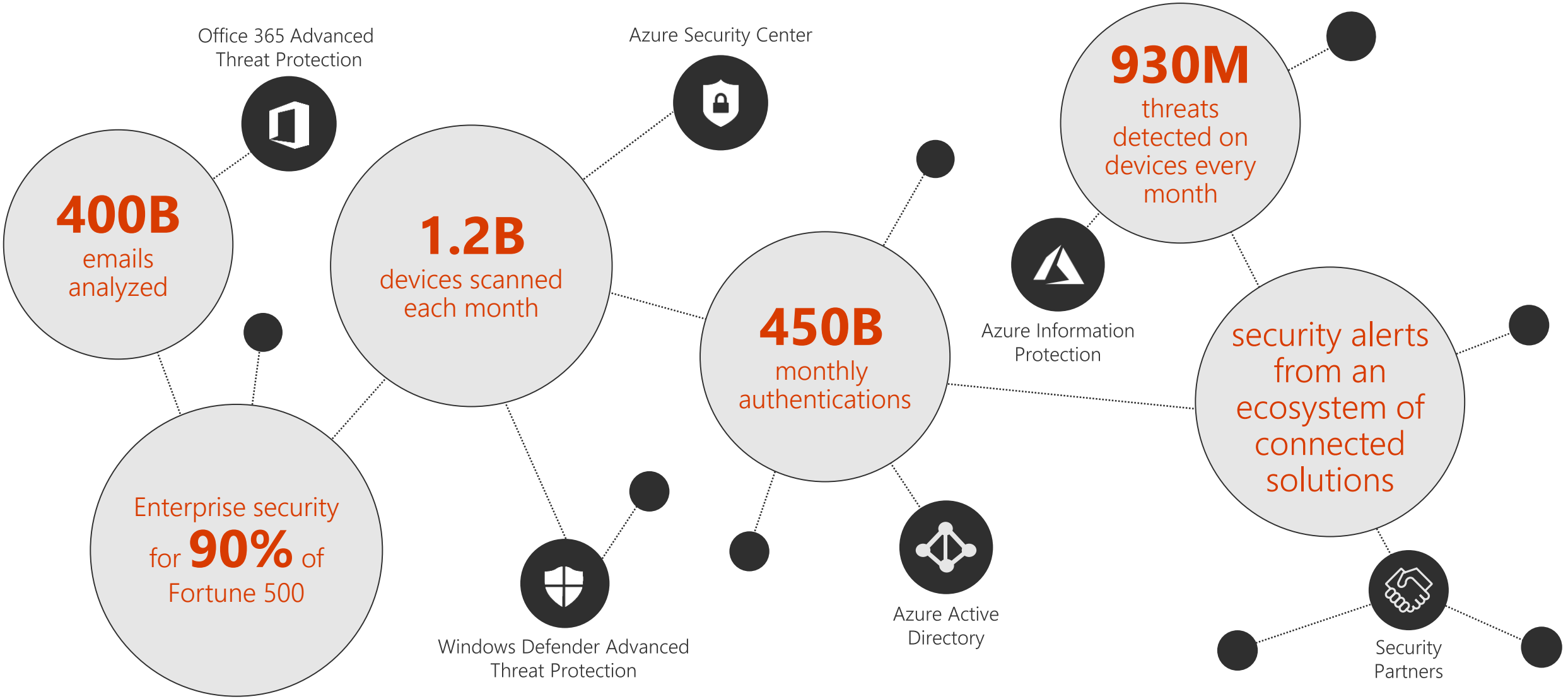
150+ **security controls**
500+ **vendors**

challenges + opportunities

integrating with customers' existing security tools and workflows

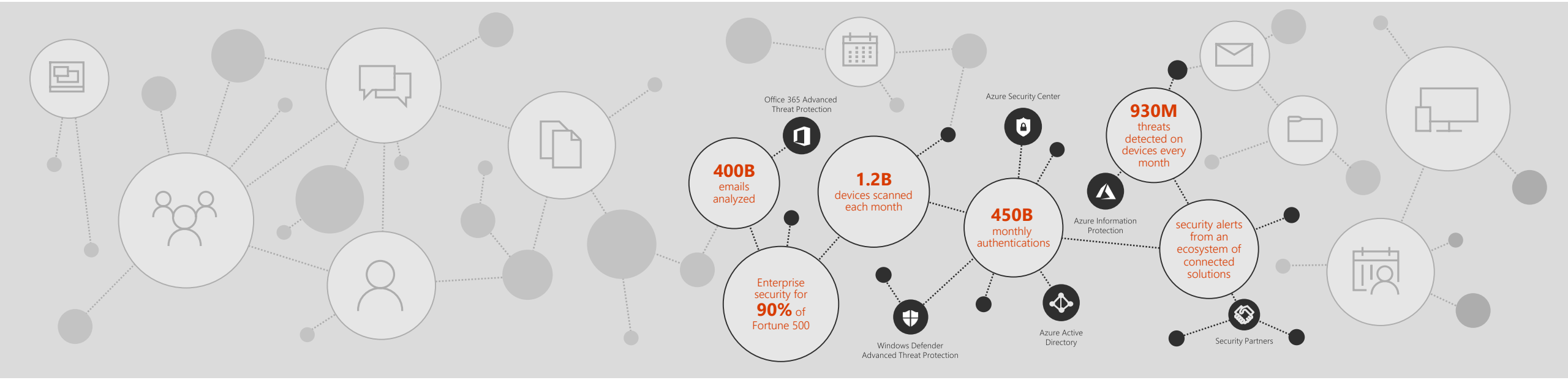
connecting customers' security technologies to streamline operations and improve threat defense

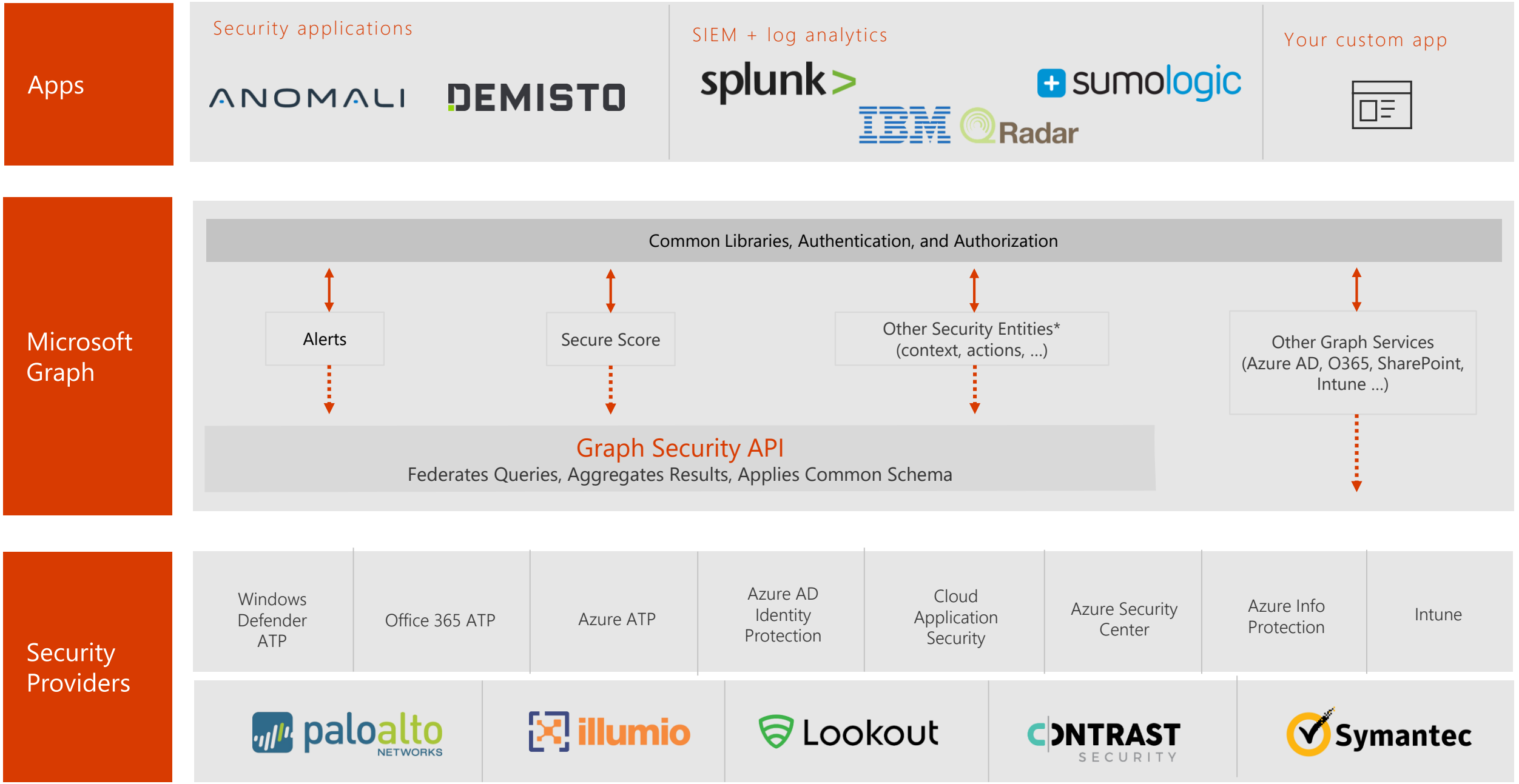
Security intelligence powered by trillions of signals



Now accessible through Microsoft Graph

Gateway to your data in the Microsoft cloud




Apps
Security applications
ANOMALI
DEMISTO
SIEM + log analytics
splunk>
sumologic
IBM
Radar
Your custom app
Microsoft Graph
Common Libraries, Authentication, and Authorization
Alerts
Secure Score
Other Security Entities*
(context, actions, ...)
Other Graph Services
(Azure AD, O365, SharePoint, Intune ...)
Graph Security API
Federates Queries, Aggregates Results, Applies Common Schema
Security Providers
Windows Defender ATP
Office 365 ATP
Azure ATP
Azure AD Identity Protection
Cloud Application Security
Azure Security Center
Azure Info Protection
Intune
paloalto NETWORKS
illumio
Lookout
CONTRAST SECURITY
Symantec

Microsoft Intelligent Security Association

Collaboration strengthens protection

Teaming up with our security partners to build an ecosystem of intelligent security solutions that better defend against a world of increased threats

paloalto NETWORKS
zscaler
ANOMALI
DIGITALGUARDIAN
FORCEPOINT
ziften
SAVIYNT
Check Point SOFTWARE TECHNOLOGIES LTD
THREATCONNECT
IONIC
f5
Ping Identity
SailPoint
IMPERVA
Omada
SentinelOne
Lookout
Barracuda
Bitdefender

Microsoft Graph Security API

Unified access to security insights and actions across Microsoft products, services, and partners

Streamline alert correlation and management

Unlock context to inform security operations

Simplify orchestration and automation

Secure Score

Understand your Microsoft security position and get guidance on how to improve it

- Visibility into Office 365, EMS, and Windows 10 security posture
- Learn what security features are available to reduce risk while helping you balance productivity and security
- View 90 days of historical data on controls used and score

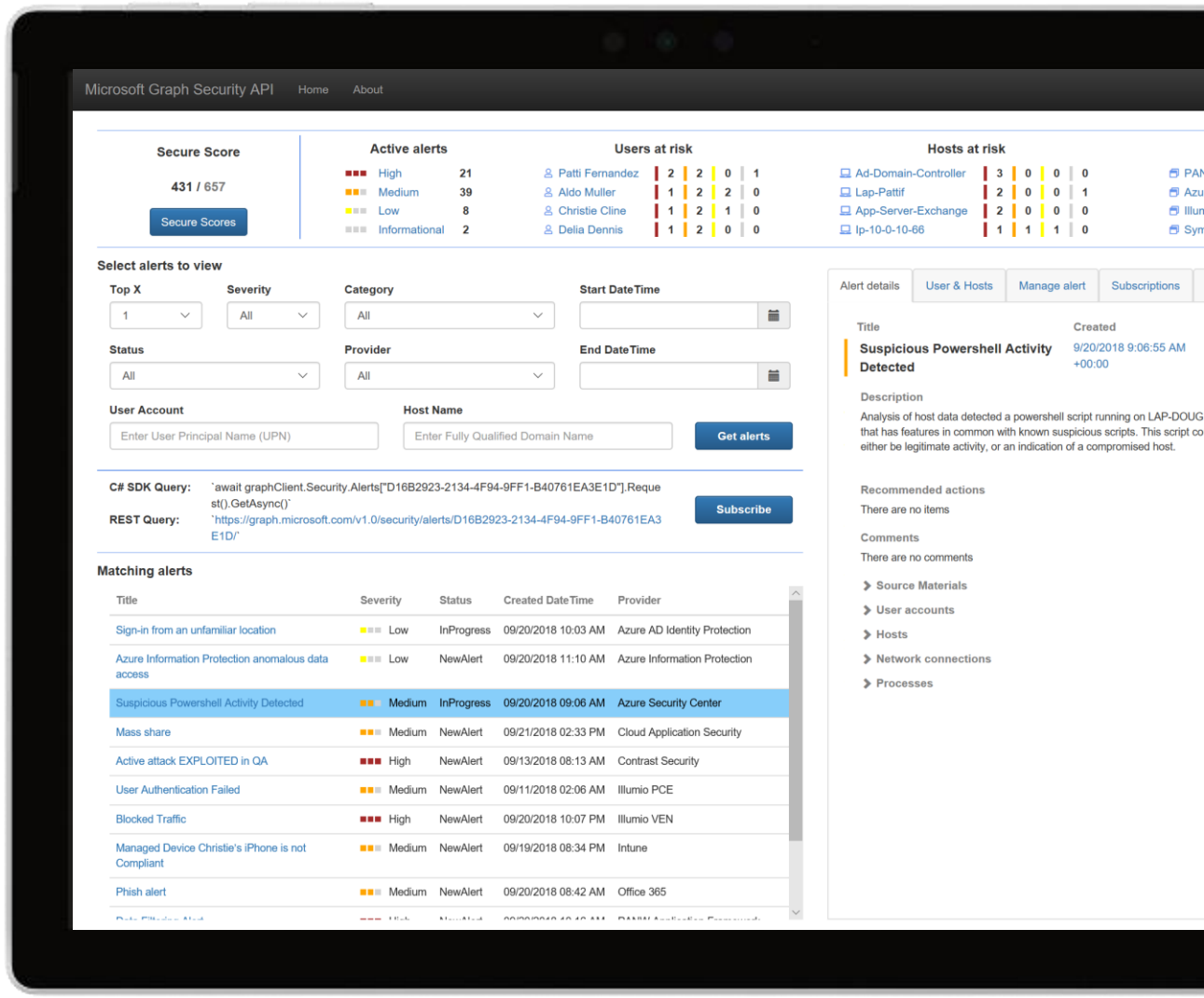
Risky users

Leverage all the sophistication of Microsoft's security platform to identify risky users

- Use filtered queries to get all risky users or just users with a high level of risk; augment filters with other context
- Subscribe to notifications for all new or updated risky users matching your criteria
- Take action on risky users by using the full context of Microsoft Graph – enforce policies, disable devices, etc

Demo

Graph Security API



Technical resources

Documentation

Review the documentation
https://aka.ms/graphsecuritydocs

Learn how to stream alerts to your SIEM
https://aka.ms/graphsecuritySIEM

Read the white paper:
https://aka.ms/graphsecuritywhitepaper

Code

Code samples:
https://aka.ms/graphsecurityapicode

Download SDKs
https://aka.ms/graphsecuritysdk

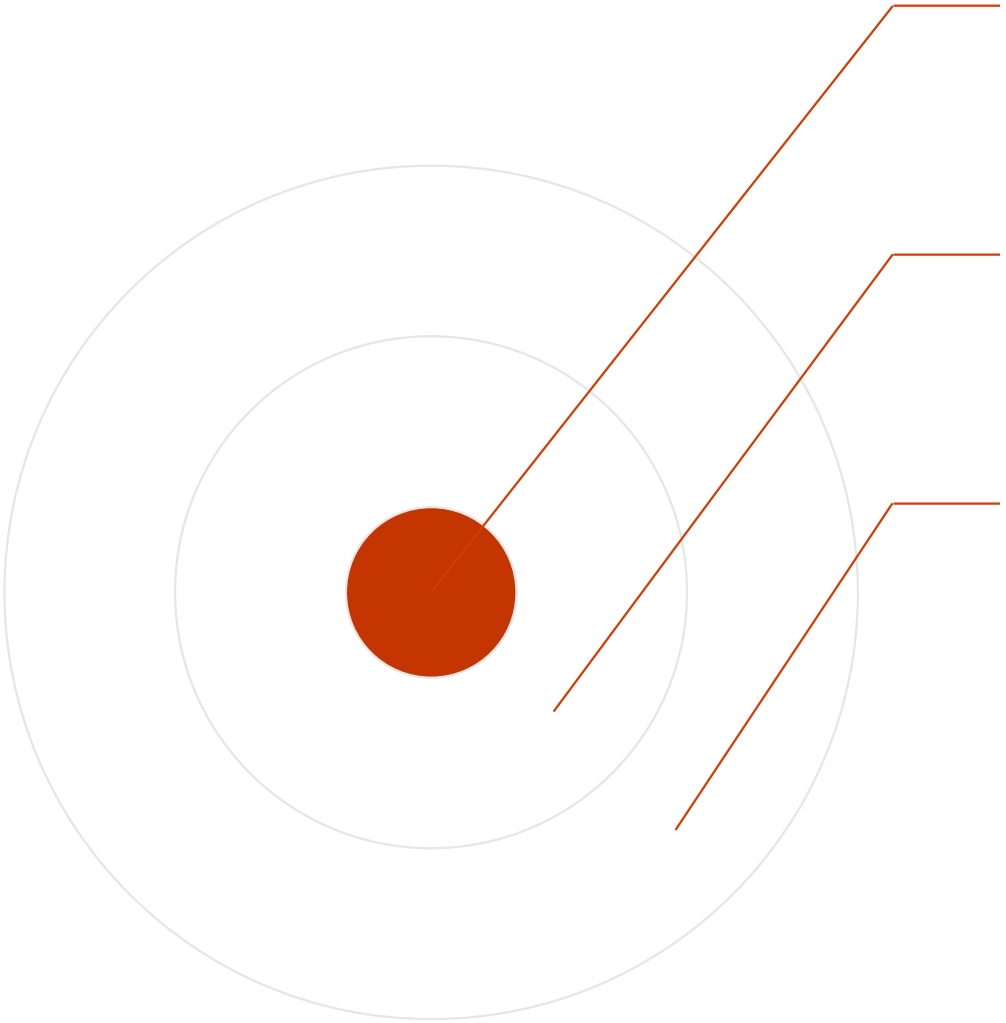
Explore in Microsoft Graph
https://developer.microsoft.com/en-us/graph/graph-explorer

Communities

Join the Tech Community
https://aka.ms/graphsecuritycommunity

Follow the discussion on Stack Overflow
https://stackoverflow.com/questions/tagged/microsoft-graph-security

Intelligence strategies

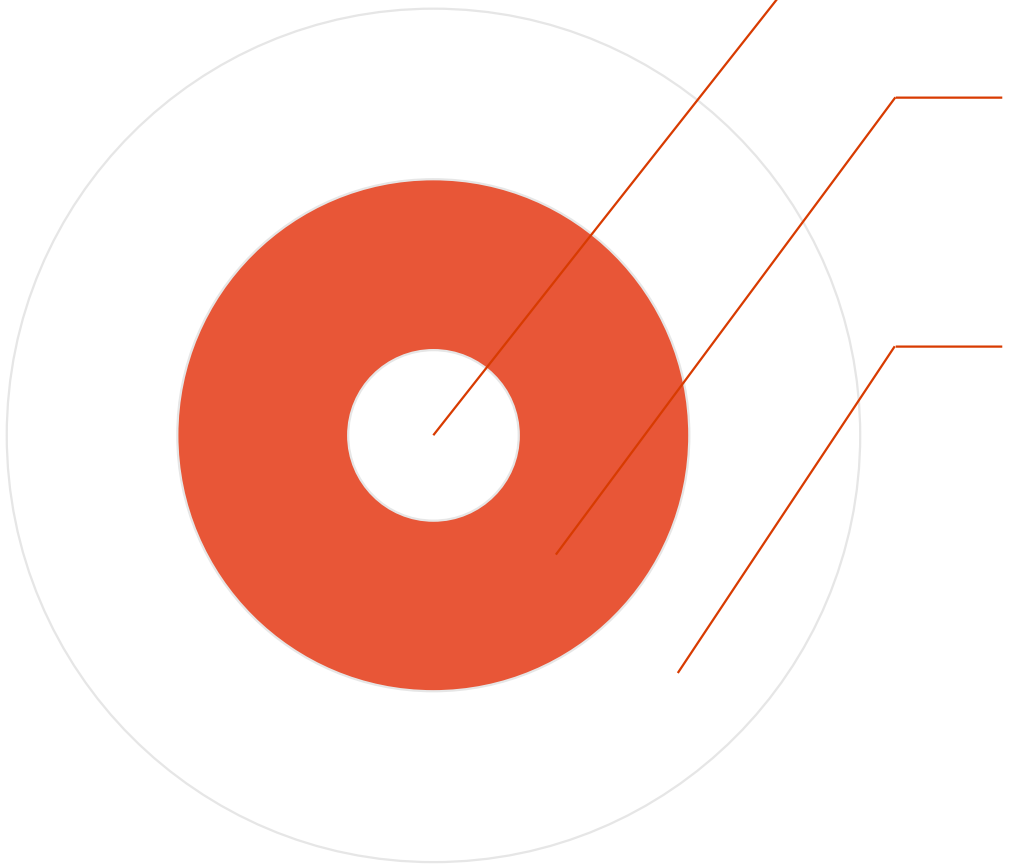


Built-in insights

1st class partnership

Bring your own

Intelligence strategies



Built-in insights

1st class partnership

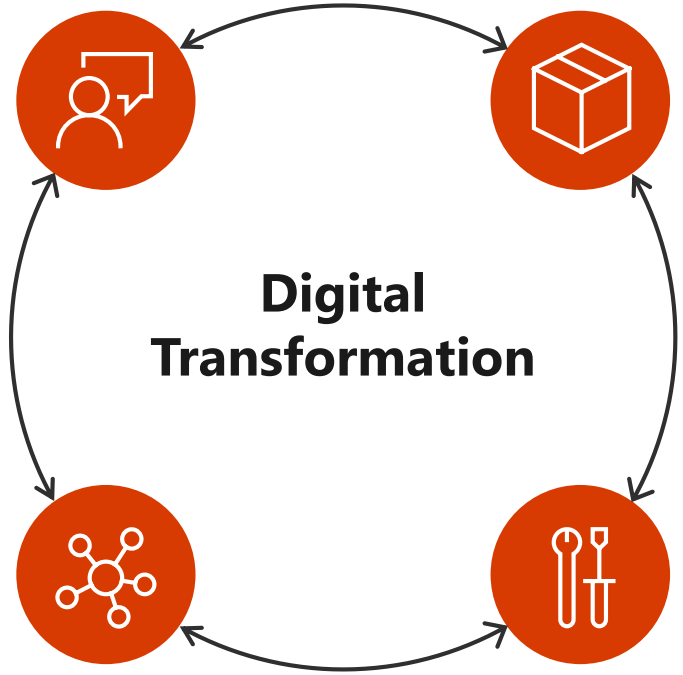
Bring your own

Microsoft

BRK3289

Getting started with Microsoft Intelligence Platform

What are customers trying to do?



Engage customers

Top sales performer behavior

Opportunity health analysis

Connect me to an expert

Transform products

Organization data management

Automate legal case billing

Build product Q&A and FAQs

Optimize operations

Detect fraud communication pattern

Drive change programs to adopt M365

Automate knowledge base creation

Empower employees

Customized employee training

Identify skills gaps in your org

Effectiveness of D&I training

Analytics & Insights on Organizational Data

Data access @ scale

is expensive, requiring complicated ETL engineering pipelines

Data Privacy

is difficult given limited administrative controls and inflexible consent model

Data Governance & Security

is reinvented by each application, with no common patterns for developers

Microsoft Graph data connect

Secure data platform enabling Analytics and Insights for Microsoft 365

Data access @ scale

Dataset based access rather than real time API based access

Data Privacy

Row and column level scoping with advanced filtering capability

Data Governance & Security

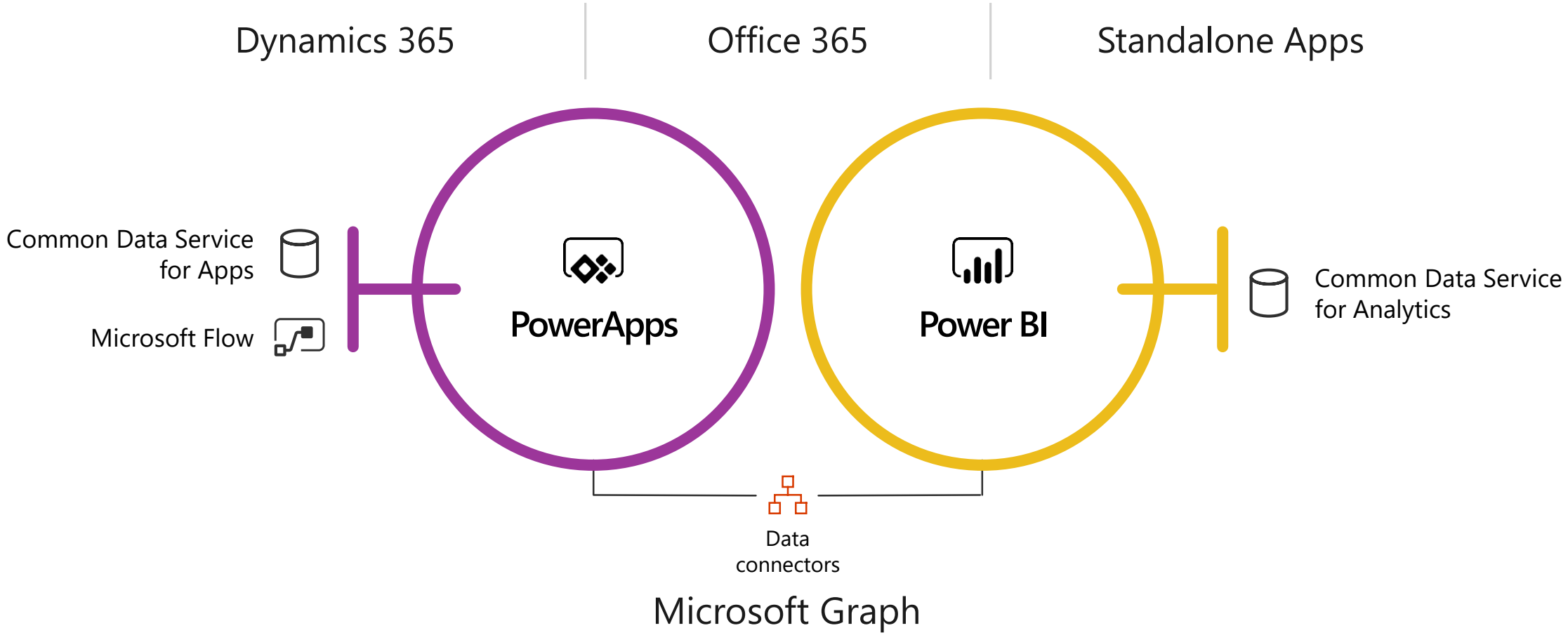
Data controller has visibility over data throughout its entire lifecycle

Microsoft

PowerApps for citizen developers

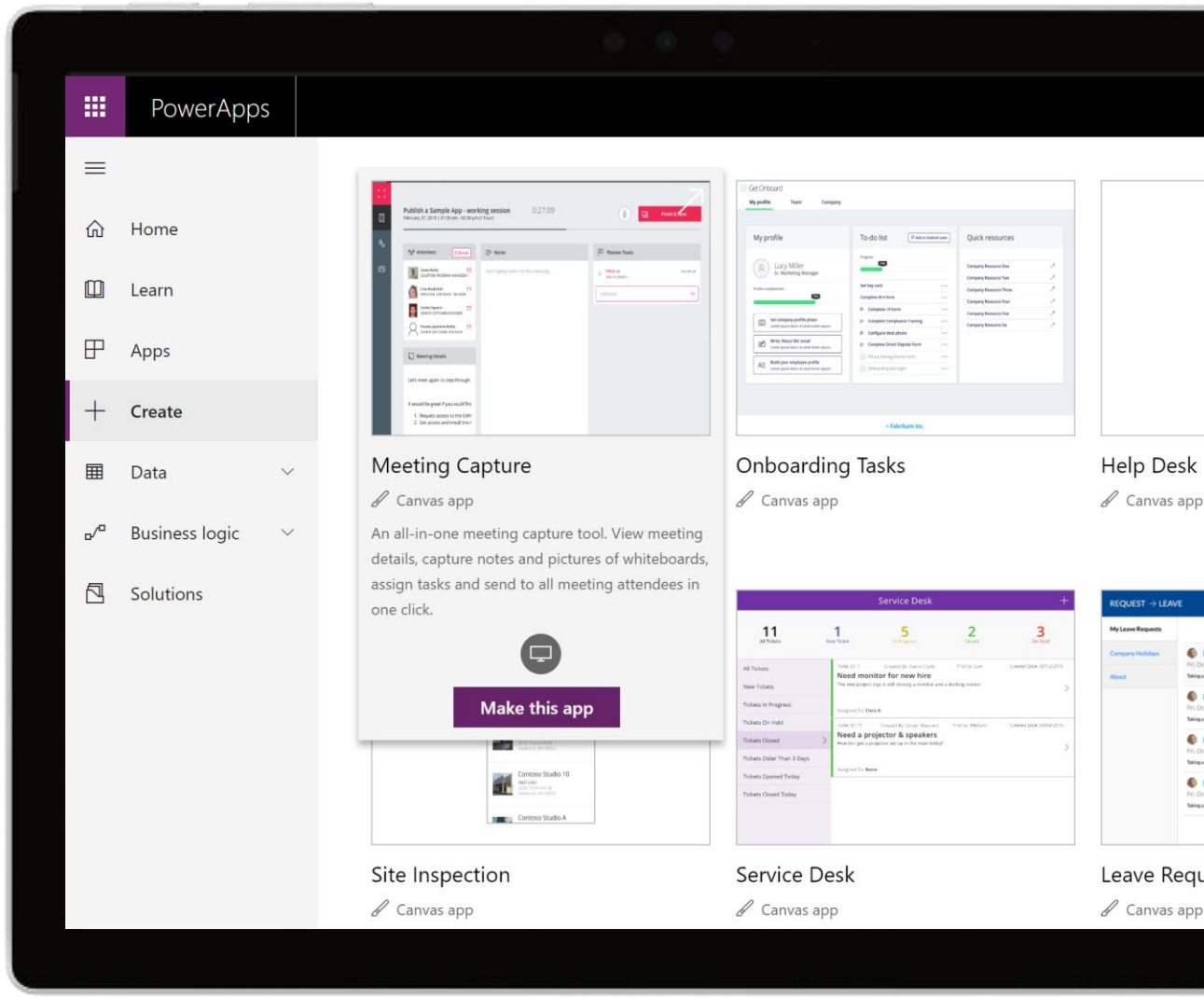
Empowering Citizen Developers

Microsoft Graph ♥ Business Application Platform



Demo

PowerApps



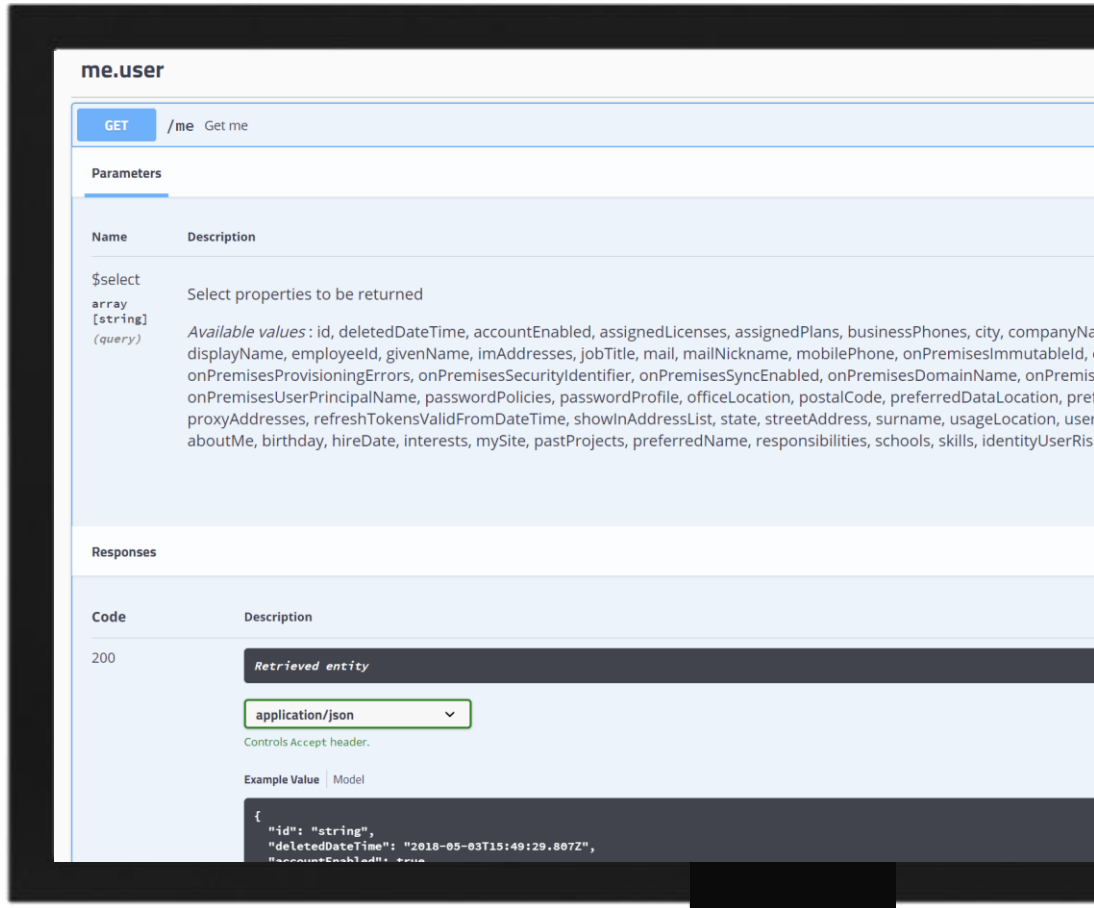
First look: OpenAPI 3.0 (fka Swagger)

Most common API description format

Describes “first level” of Graph

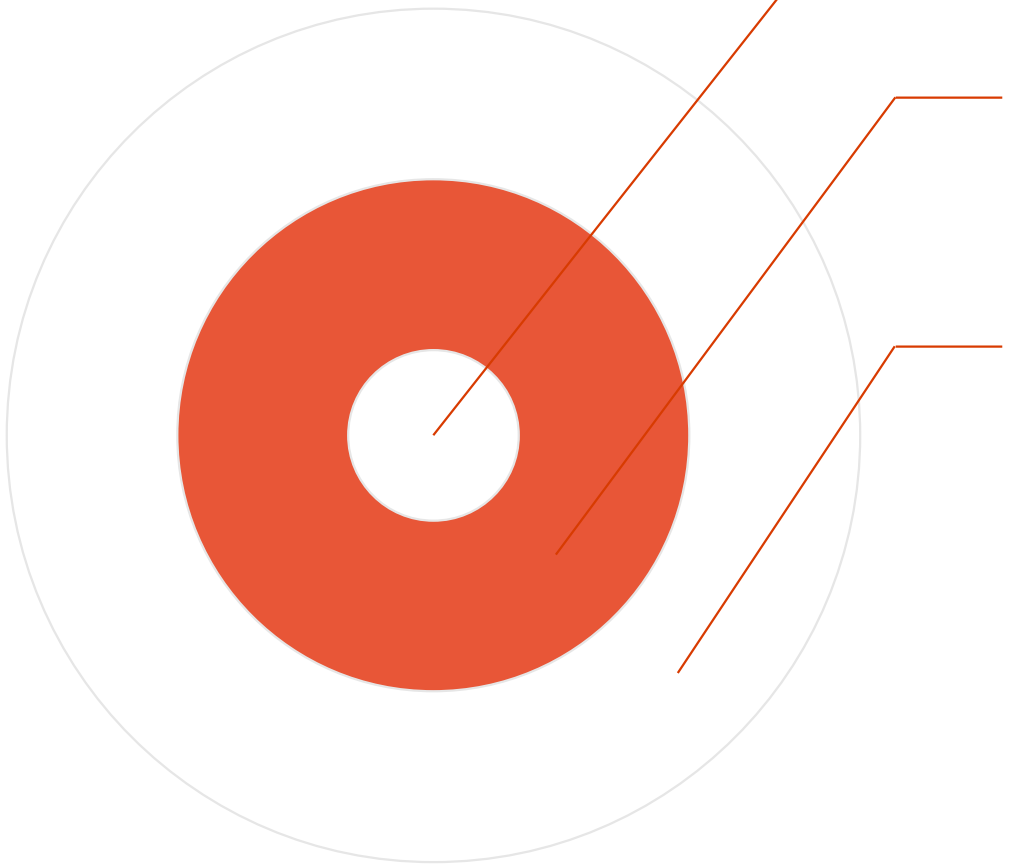
Use in any tool that supports OAS 3.0

Available by July for all Graph versions (~/api-docs)



https://github.com/microsoftgraph/microsoft-graph-openapi

Intelligence strategies

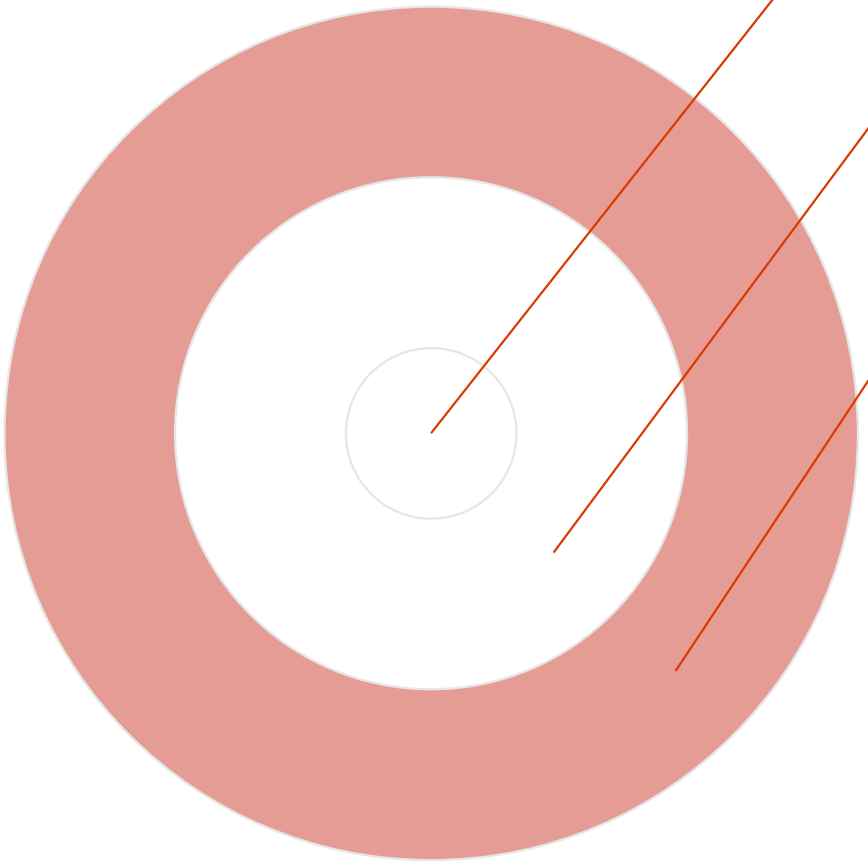


Built-in insights

1st class partnership

Bring your own

Intelligence strategies



Built-in insights

1st class partnership

Bring your own

Microsoft Graph promise

https://graph.microsoft.com

ALL

Your data across Microsoft 365

Office 365
Windows 10
EMS

ALL

Types of users

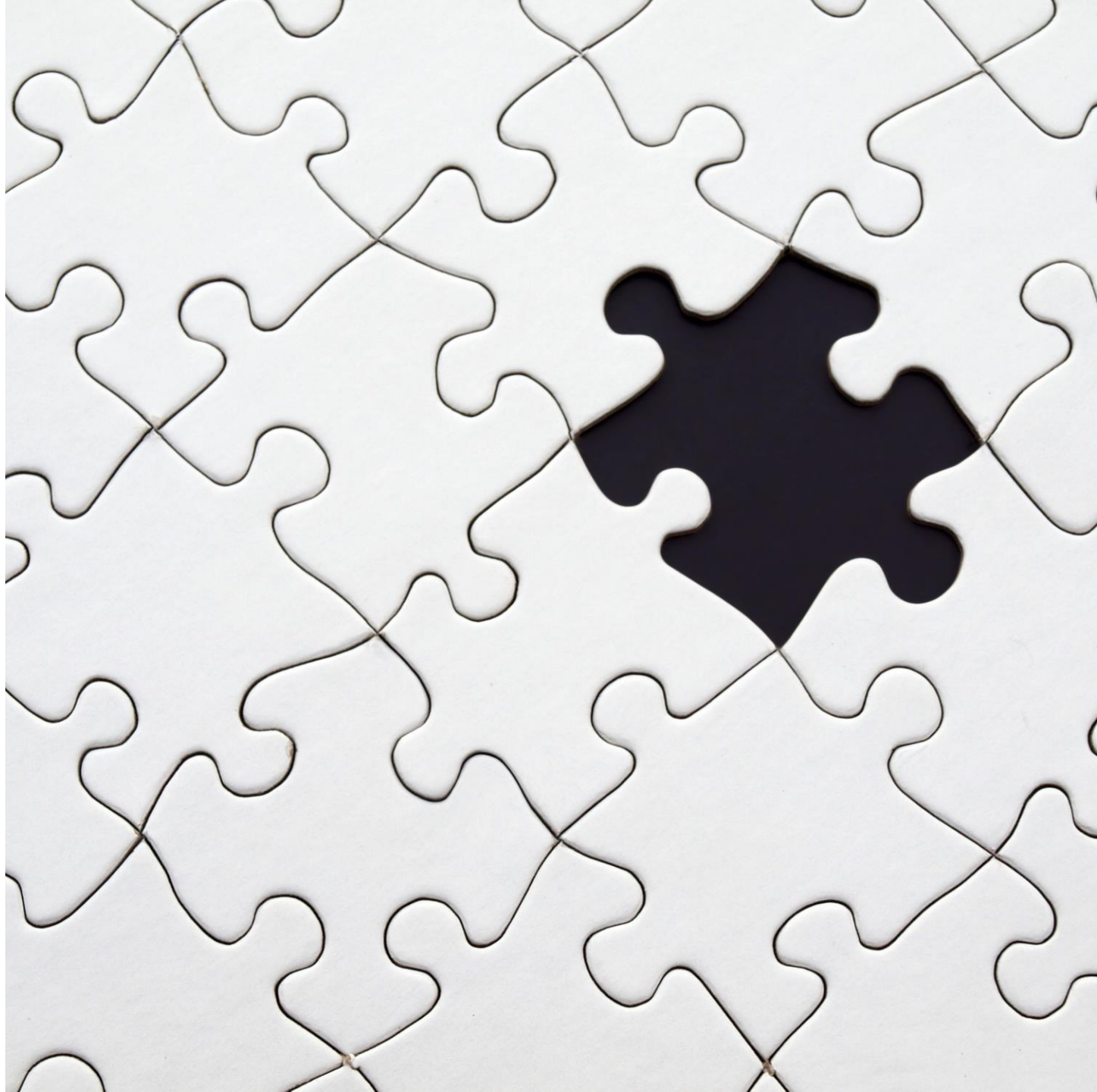
Corporate (@fabrikam.com)
Consumer (@outlook.com)

ONE

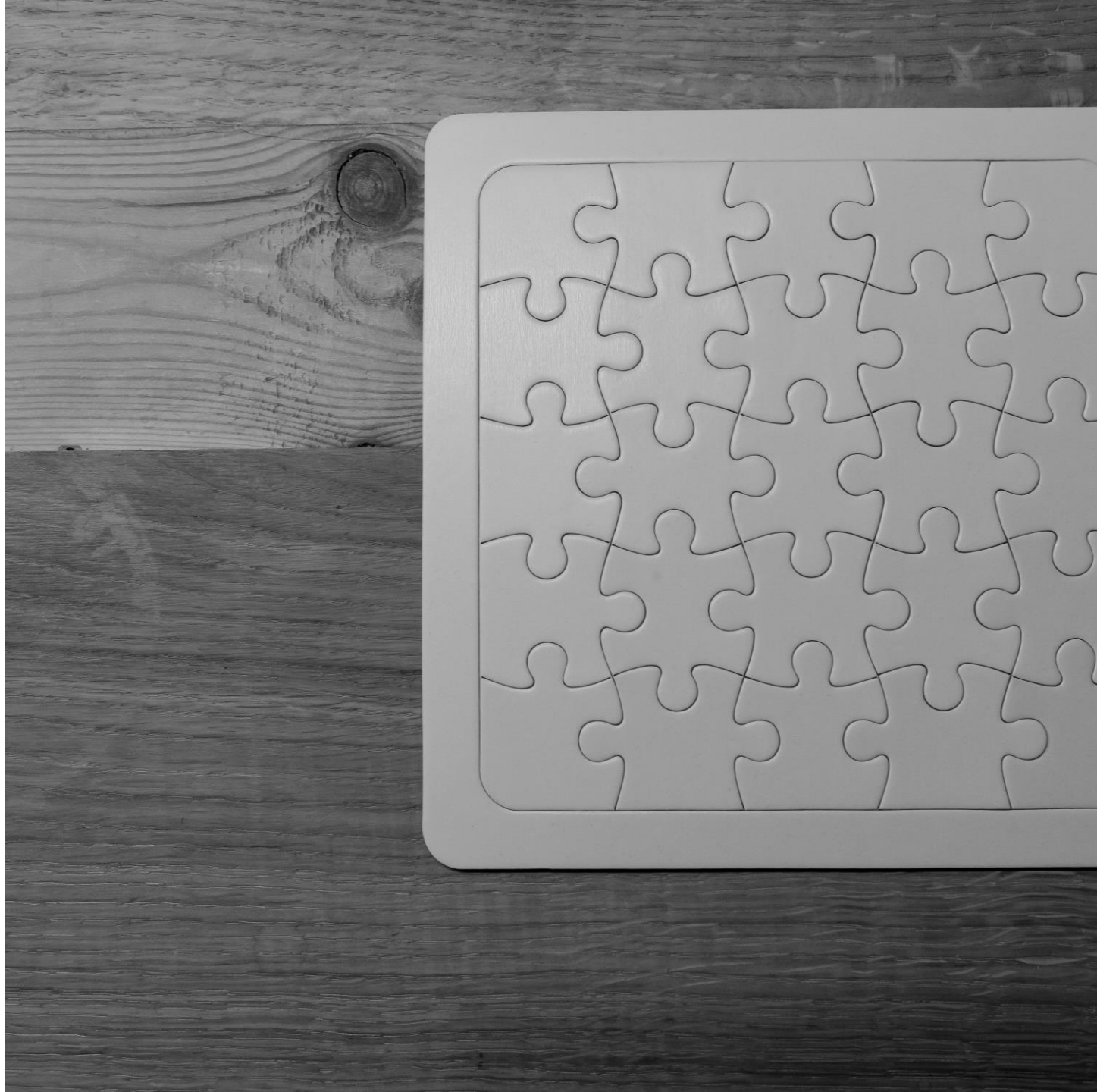
Way to access it

One endpoint
One auth key
One set of docs
One SDK

Graph will rarely be 100%



Supplement with other data and intelligence

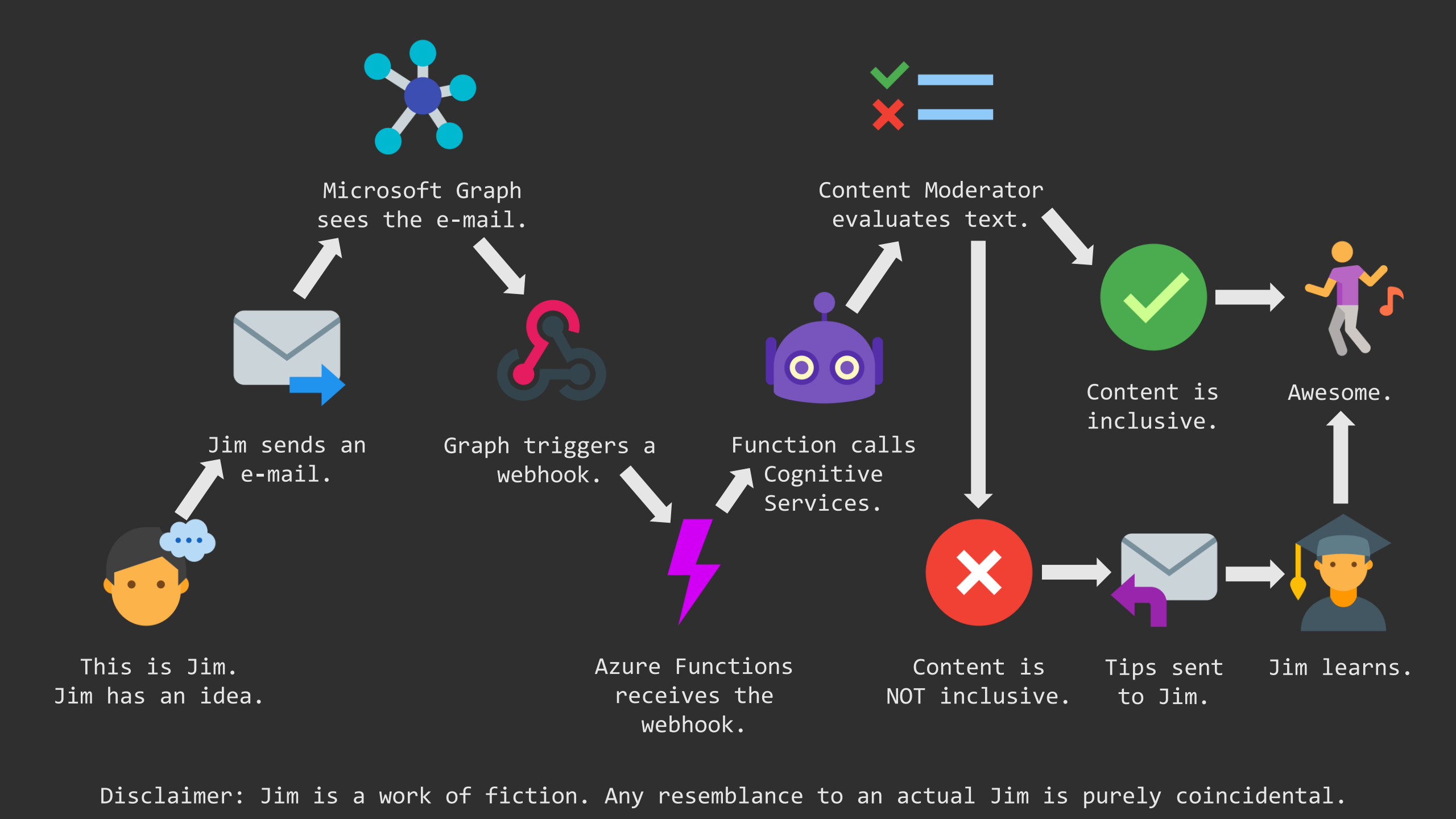


Microsoft Graph

Cognitive Services

“There exists, for everyone, a sentence - a series of words - that has the power to destroy you. Another sentence exists, another series of words, that could heal you.”

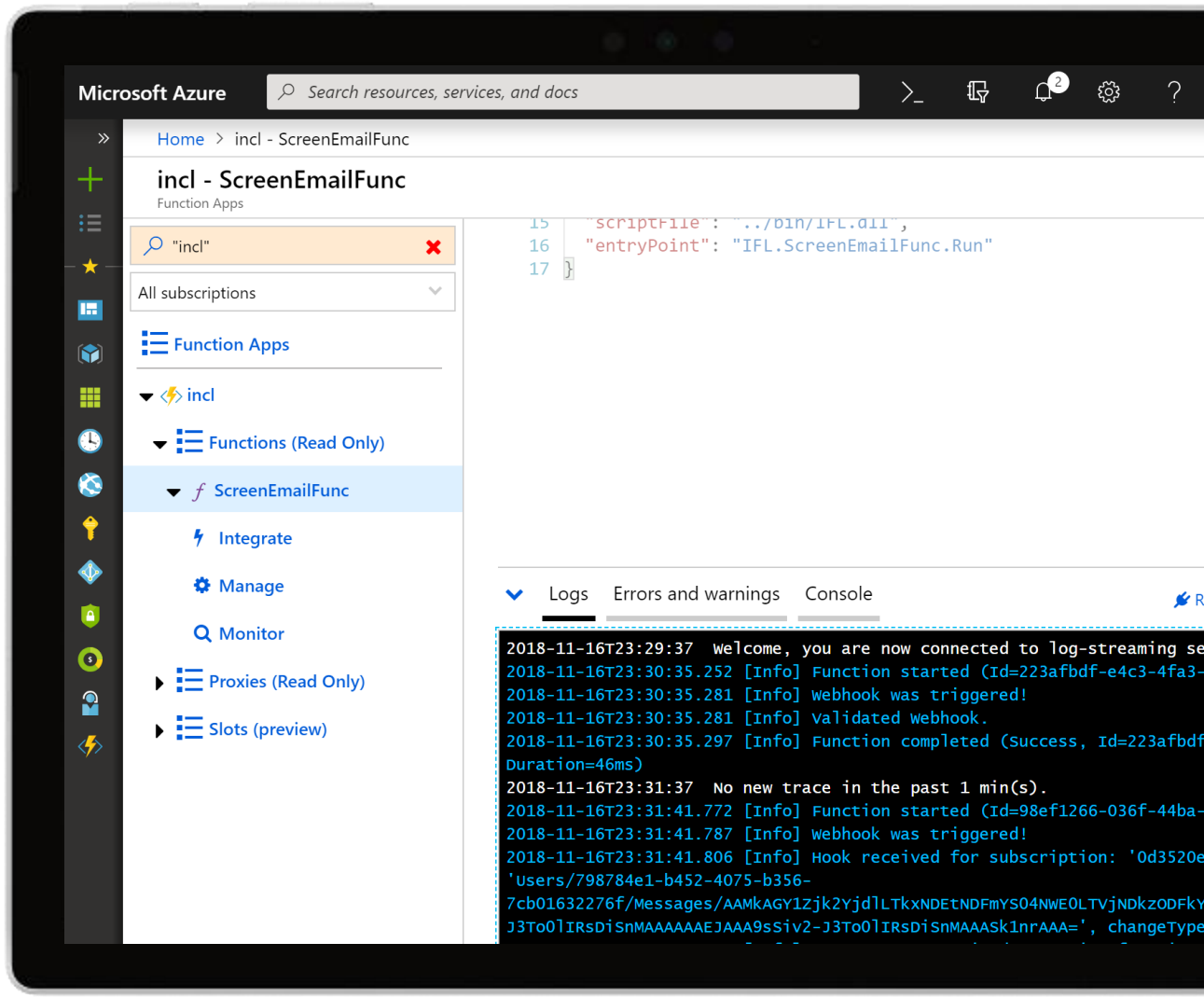
— Philip K. Dick, VALIS



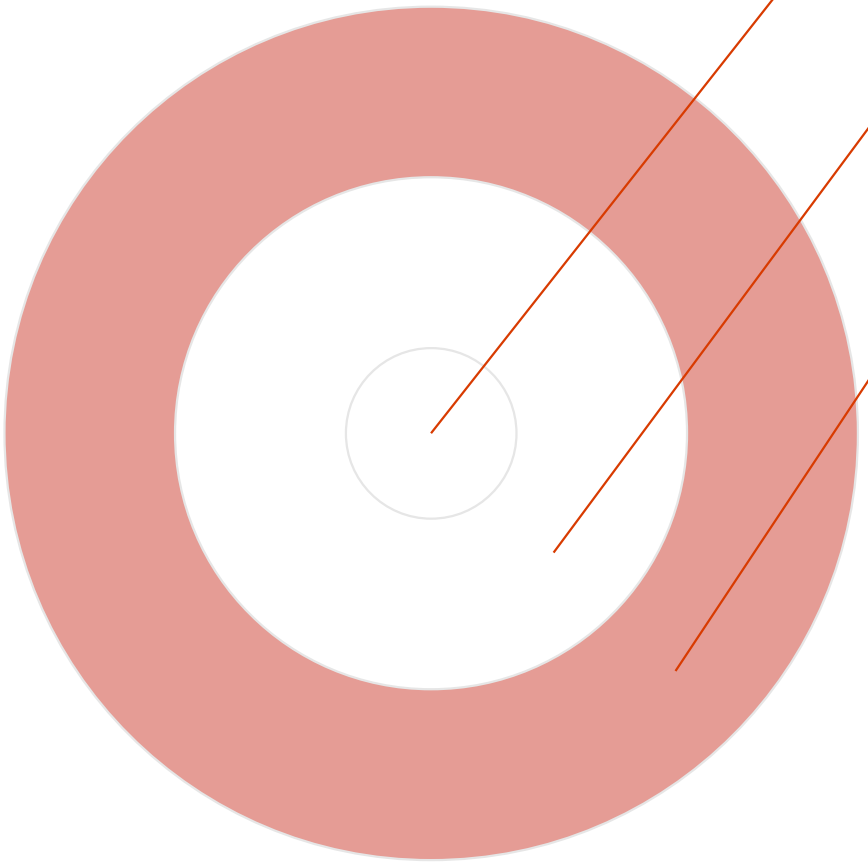
Disclaimer: Jim is a work of fiction. Any resemblance to an actual Jim is purely coincidental.

Demo

Custom intelligence



Intelligence strategies

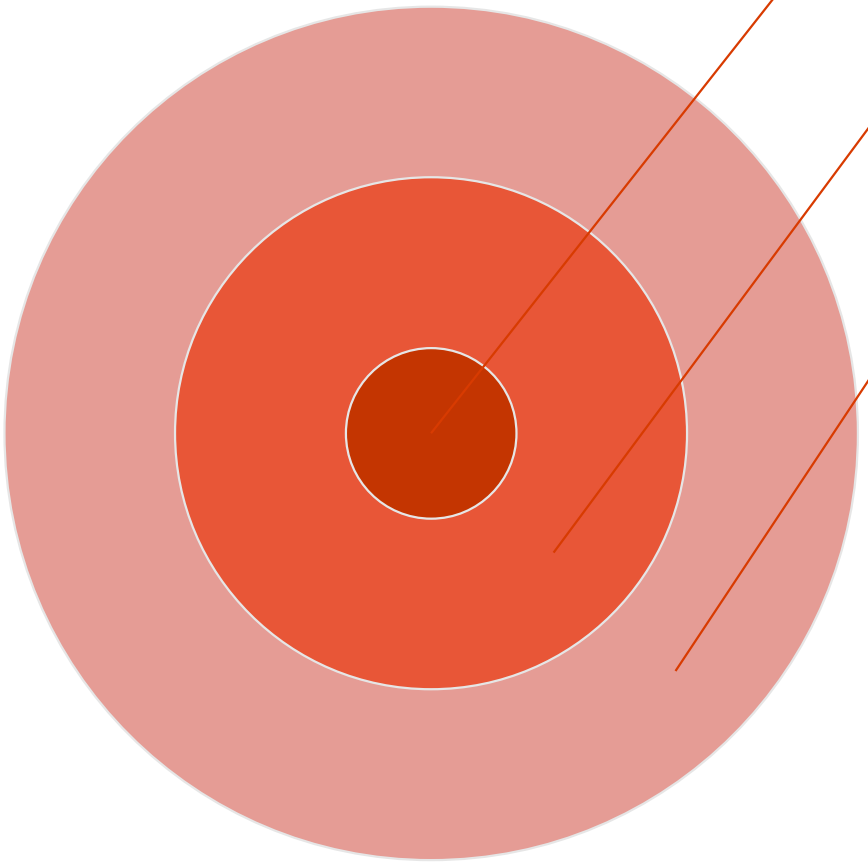


Built-in insights

1st class partnership

Bring your own

Intelligence strategies



Built-in insights

Security, Spatial Analytics

1st class partnership

Managed Access, PowerStack

Bring your own

Webhooks + ?

Next steps

1. Try Graph Explorer right now: aka.ms/ge

2. Join other Graph talks and labs

3. Brainstorm creative ideas or try this one: aka.ms/incl

4. Build awesome, intelligent apps 

5. Profit!

Microsoft 365

Thank you