



Adding custom intelligence to Microsoft Graph

Mark Stafford

Microsoft Graph: the API for M365

The screenshot displays the Microsoft Graph Explorer web application. The browser's address bar shows the URL `https://developer.microsoft.com/en-us/graph/graph-explorer#`. The page header includes the Microsoft logo and navigation links for Solutions, Graph Explorer, More, and My Apps. A search icon is also present.

The main interface is divided into a left sidebar and a main content area. The sidebar, titled "Graph Explorer", contains an "Authentication" section with a "Sign in with Microsoft" button, and a "Sample Queries" section with a list of queries under "Getting Started":

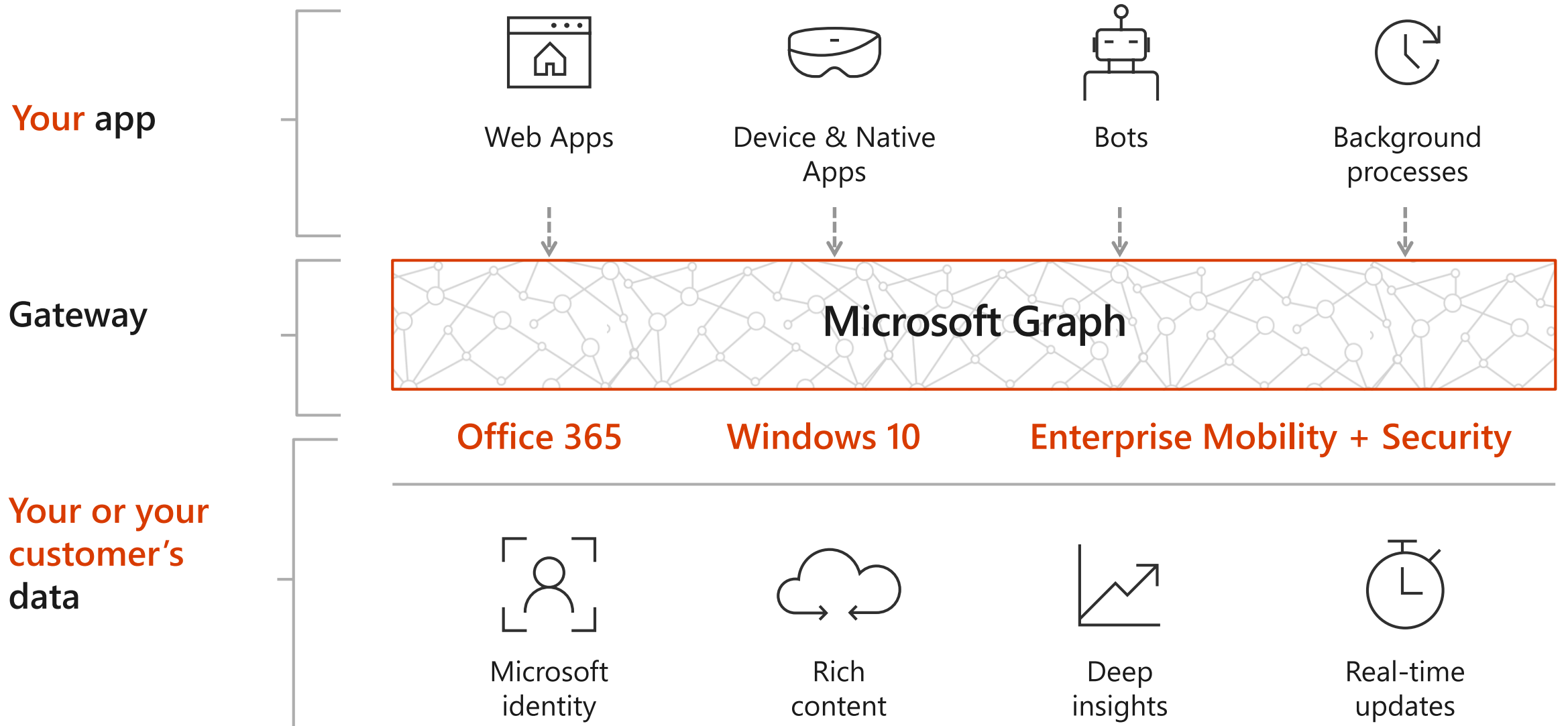
- GET my profile
- GET my photo
- GET my mail
- GET all the items in my drive
- GET items trending around me
- GET my manager

Under "Outlook Mail", there is a query: GET my high important mail.

The main content area shows a query execution interface. The "Request" section is active, displaying a GET request to `https://graph.microsoft.com/v1.0/me/`. Below this, there are tabs for "Request Body" and "Request Headers". The "Response Preview" section is also active, showing the following JSON response:

```
{
  "@odata.context": "https://graph.microsoft.com/v1.0/$metadata#users/$entity",
  "id": "48d31887-5fad-4d73-a9f5-3c356e68a038",
  "businessPhones": [
    "+1 412 555 0109"
  ],
  "displayName": "Megan Bowen",
  "givenName": "Megan",
  "jobTitle": "Auditor",
  "mail": "Megan.Bowen@contoso.com"
}
```

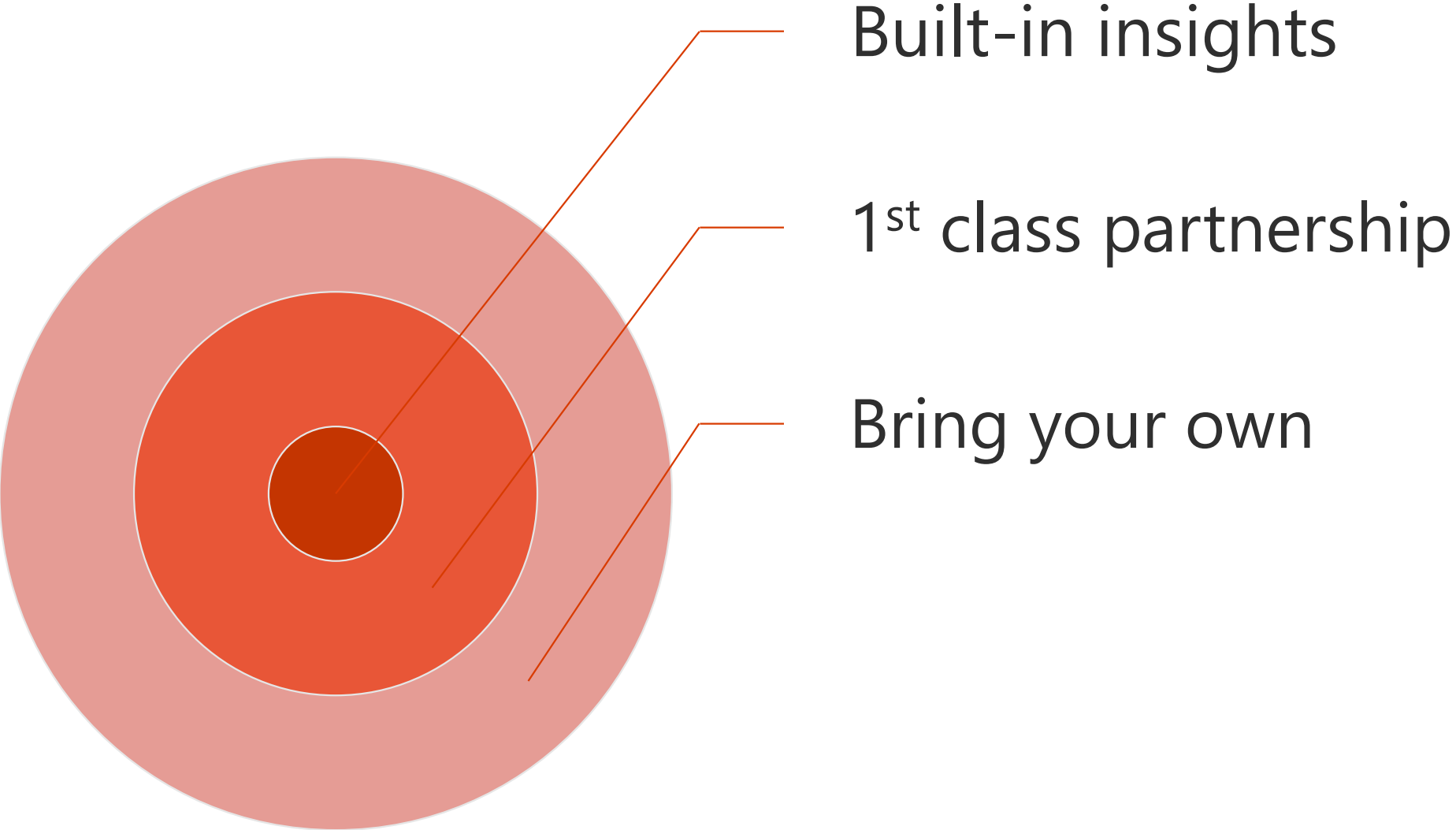
Gateway to **your** data in the Microsoft cloud



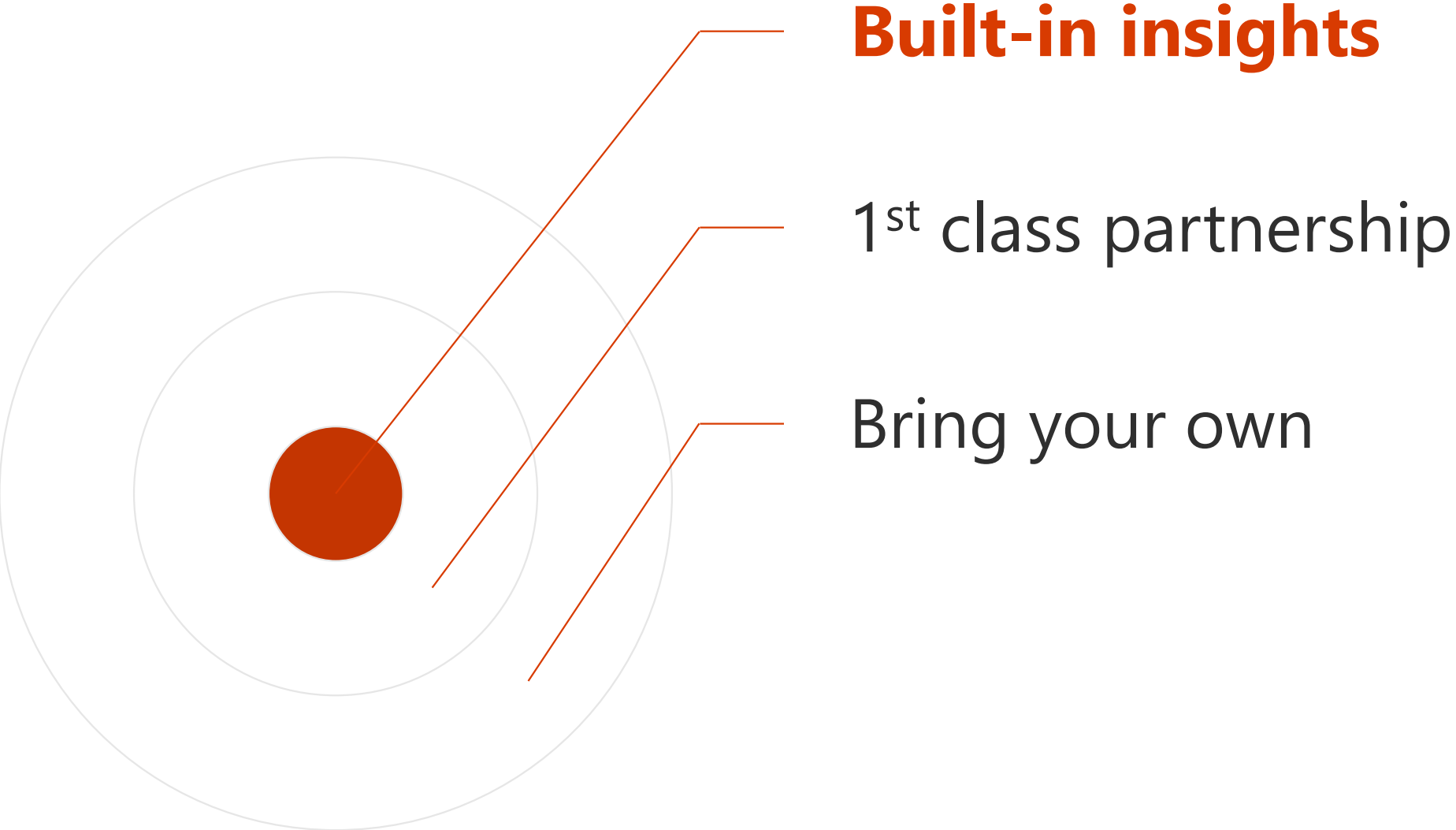
Problem

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

Intelligence strategies



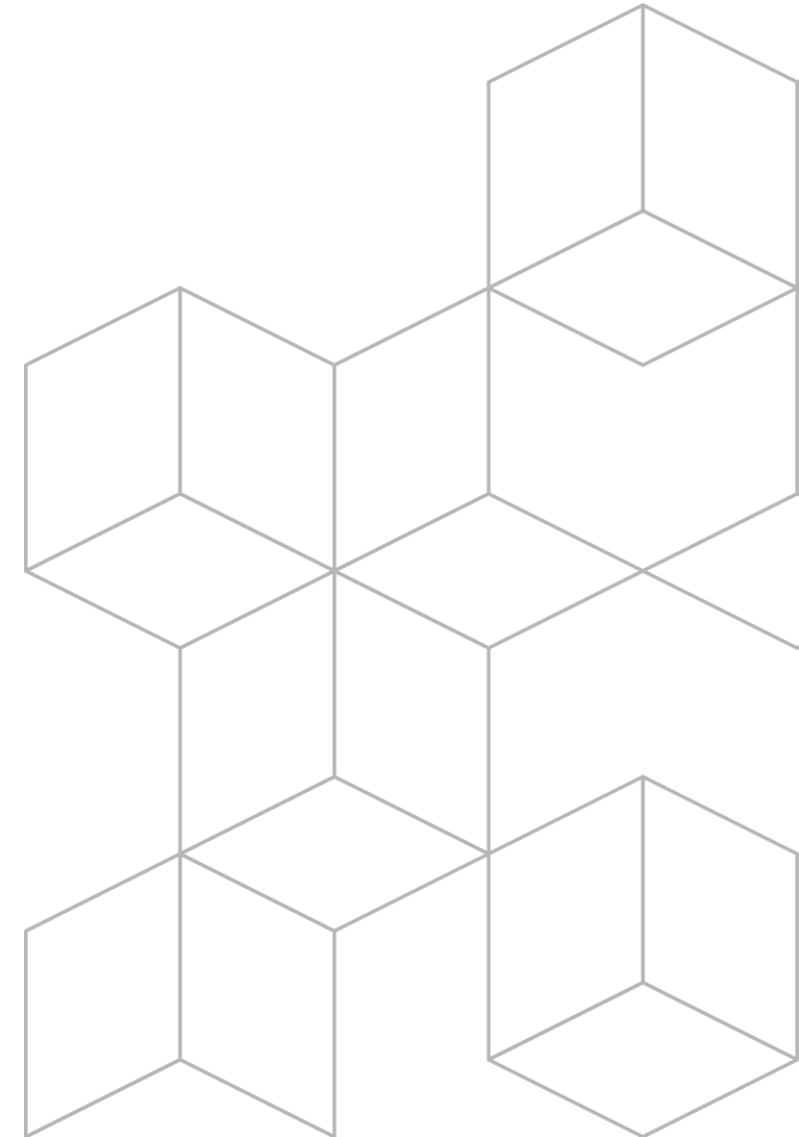
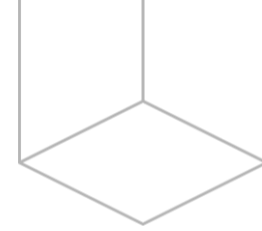
Intelligence strategies



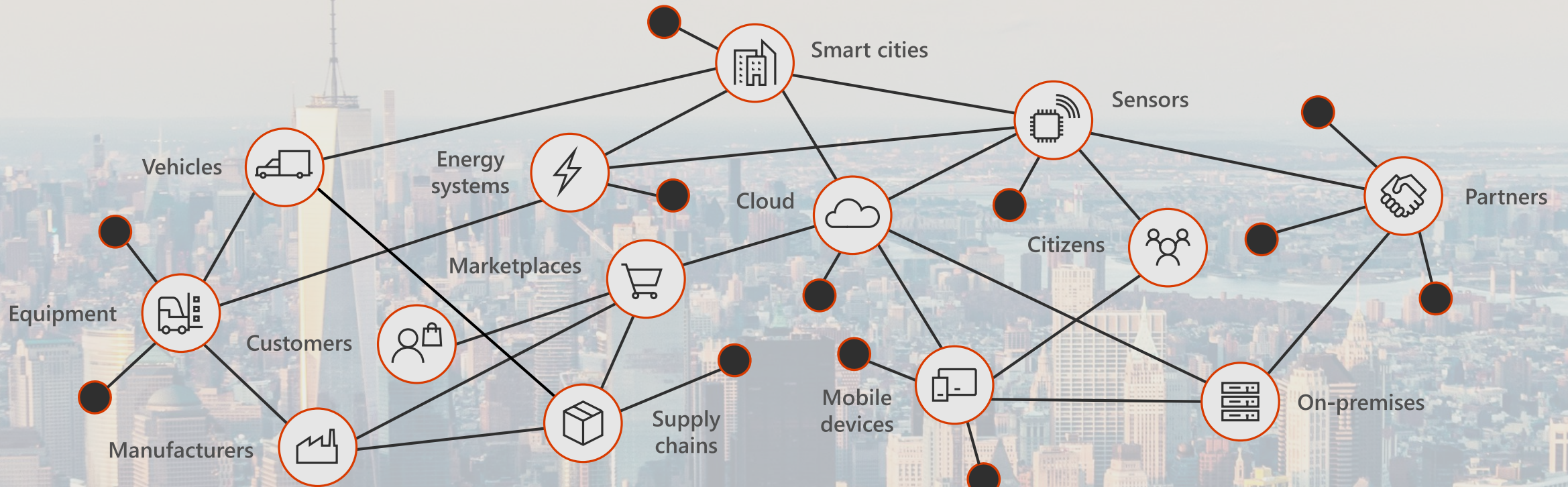
Built-in insights

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

Harnessing the power of the Intelligent Security Graph



The digital estate



Anomaly
detection

Endpoint
protection

Hybrid cloud
security

Data & application
security

Fraud
prevention

Data loss
prevention

Infrastructure
security

Threat
management

Security
management

150+ security controls
500+ vendors

Data center
security

Cloud Access
Security Broker

Information rights
management

Identity & access
management

Compliance
tools

Threat
detection

IoT
security

Email
security



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

Office 365 Advanced
Threat Protection



400B
emails
analyzed

Azure Security Center



1.2B
devices scanned
each month

930M
threats
detected on
devices every
month



Azure Information
Protection

450B
monthly
authentications

security alerts
from an
ecosystem of
connected
solutions

Enterprise security
for **90%** of
Fortune 500



Windows Defender Advanced
Threat Protection



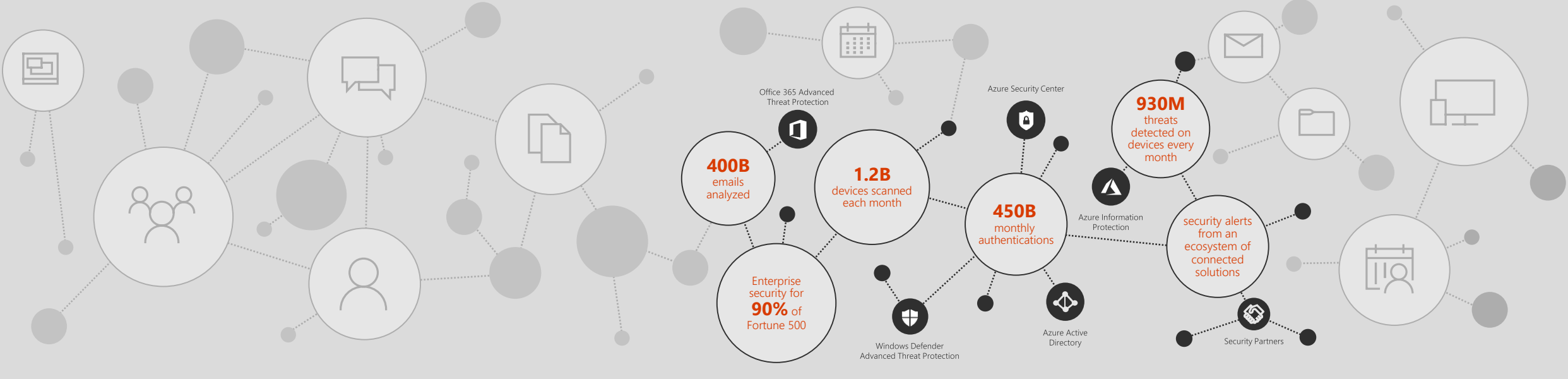
Azure Active
Directory



Security
Partners

Now accessible through Microsoft Graph

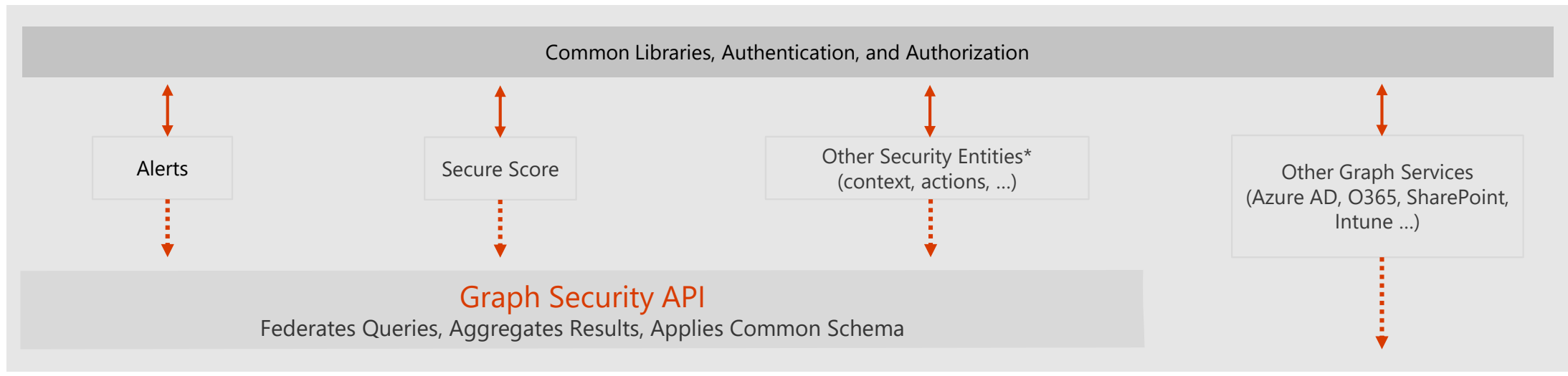
Gateway to your data in the Microsoft cloud



Apps

Security applications ANOMALI DEMISTO	SIEM + log analytics splunk IBM sumologic Radars	Your custom app
--	---	---------------------

Microsoft Graph



Security Providers

Windows Defender ATP	Office 365 ATP	Azure ATP	Azure AD Identity Protection	Cloud Application Security	Azure Security Center	Azure Info Protection	Intune

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



Check Point
SOFTWARE TECHNOLOGIES LTD

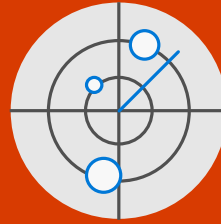


Microsoft Graph Security API

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



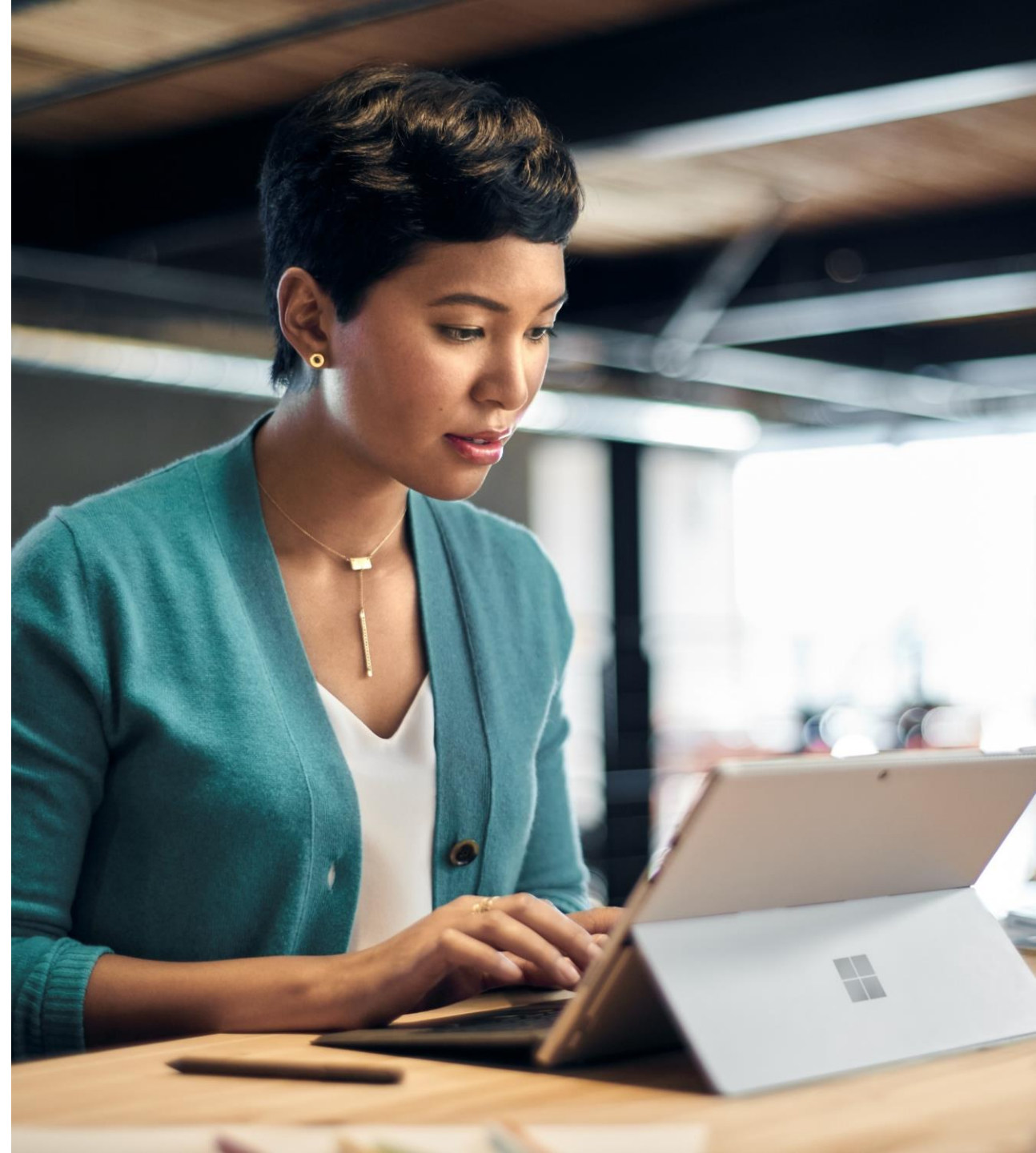
Secure Score

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

The screenshot displays the Microsoft Graph Security API dashboard. At the top, it shows the 'Secure Score' as 431 / 657. Below this, there are four summary cards: 'Active alerts' (High: 21, Medium: 39, Low: 8, Informational: 2), 'Users at risk' (listing Patti Fernandez, Aldo Muller, Christie Cline, and Delia Dennis), and 'Hosts at risk' (listing Ad-Domain-Controller, Lap-Pattif, App-Server-Exchange, and Ip-10-0-10-66). The main section is titled 'Select alerts to view' and includes filters for Top X (1), Severity (All), Category (All), Start Date Time, Status (All), Provider (All), End Date Time, User Account, and Host Name. Below the filters, there are SDK and REST query examples. The 'Matching alerts' table lists various alerts, with 'Suspicious Powershell Activity Detected' highlighted. The right sidebar shows 'Alert details' for the selected alert, including its title, description, and recommended actions.

Microsoft Graph Security API Home About

Secure Score
431 / 657
Secure Scores

Active alerts

High	21
Medium	39
Low	8
Informational	2

Users at risk

Patti Fernandez	2	2	0	1
Aldo Muller	1	2	2	0
Christie Cline	1	2	1	0
Delia Dennis	1	2	0	0

Hosts at risk

Ad-Domain-Controller	3	0	0	0
Lap-Pattif	2	0	0	1
App-Server-Exchange	2	0	0	0
Ip-10-0-10-66	1	1	1	0

Select alerts to view

Top X: 1 | Severity: All | Category: All | Start Date Time: | End Date Time: | Status: All | Provider: All

User Account: | Host Name: | Get alerts

C# SDK Query: `await graphClient.SecurityAlerts["D16B2923-2134-4F94-9FF1-B40761EA3E1D"].Request().GetAsync()`

REST Query: `https://graph.microsoft.com/v1.0/security/alerts/D16B2923-2134-4F94-9FF1-B40761EA3E1D` | Subscribe

Matching alerts

Title	Severity	Status	Created DateTime	Provider
Sign-in from an unfamiliar location	Low	InProgress	09/20/2018 10:03 AM	Azure AD Identity Protection
Azure Information Protection anomalous data access	Low	NewAlert	09/20/2018 11:10 AM	Azure Information Protection
Suspicious Powershell Activity Detected	Medium	InProgress	09/20/2018 09:06 AM	Azure Security Center
Mass share	Medium	NewAlert	09/21/2018 02:33 PM	Cloud Application Security
Active attack EXPLOITED in QA	High	NewAlert	09/13/2018 08:13 AM	Contrast Security
User Authentication Failed	Medium	NewAlert	09/11/2018 02:06 AM	Illumio PCE
Blocked Traffic	High	NewAlert	09/20/2018 10:07 PM	Illumio VEN
Managed Device Christie's iPhone is not Compliant	Medium	NewAlert	09/19/2018 08:34 PM	Intune
Phish alert	Medium	NewAlert	09/20/2018 08:42 AM	Office 365

Alert details | User & Hosts | Manage alert | Subscriptions

Title | Created
Suspicious Powershell Activity Detected | 9/20/2018 9:06:55 AM +00:00

Description
Analysis of host data detected a powershell script running on LAP-DOUG that has features in common with known suspicious scripts. This script could either be legitimate activity, or an indication of a compromised host.

Recommended actions
There are no items

Comments
There are no comments

- Source Materials
- User accounts
- Hosts
- Network connections
- Processes

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

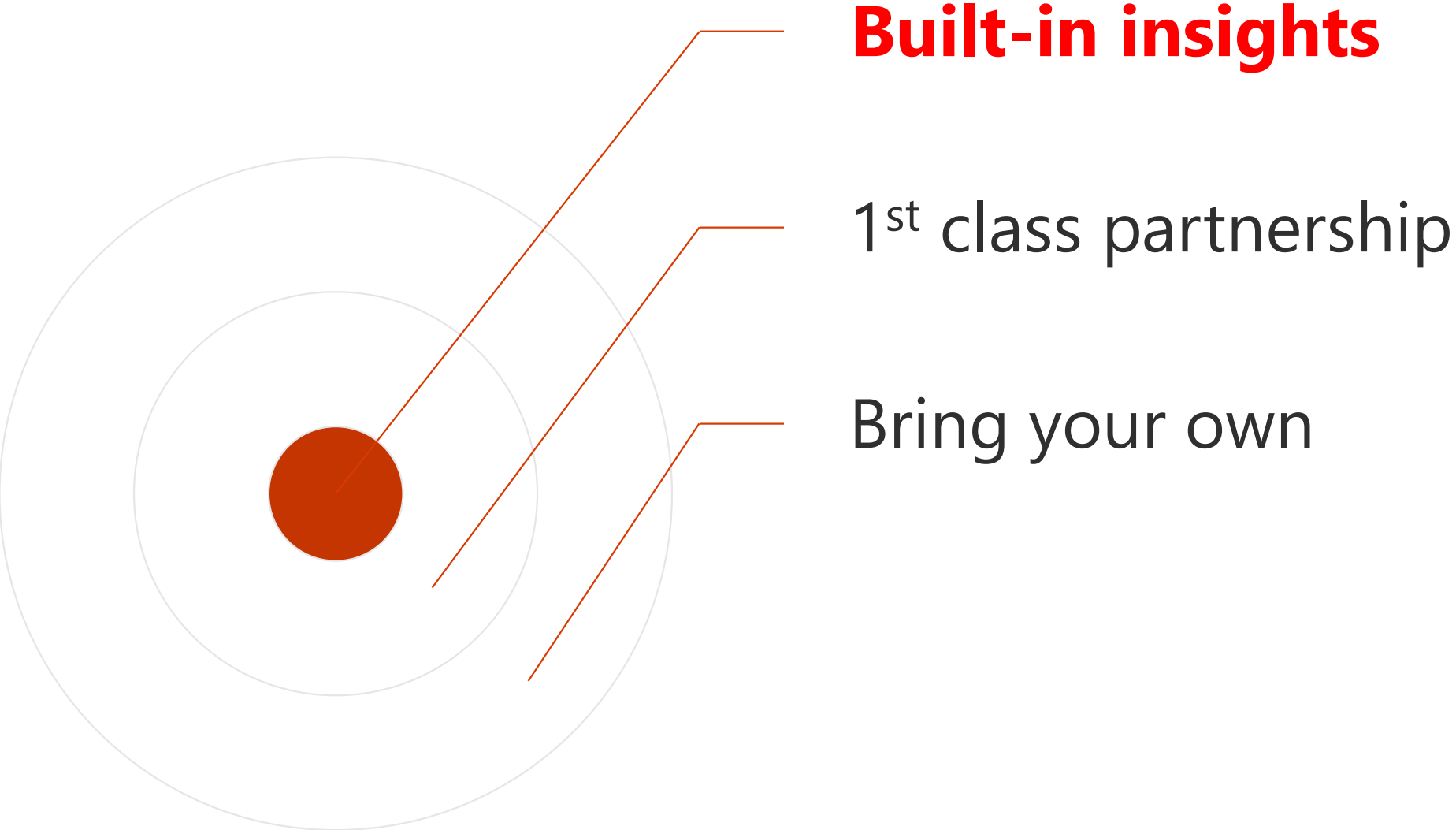
Join the Tech Community

<https://aka.ms/graphsecuritycommunity>

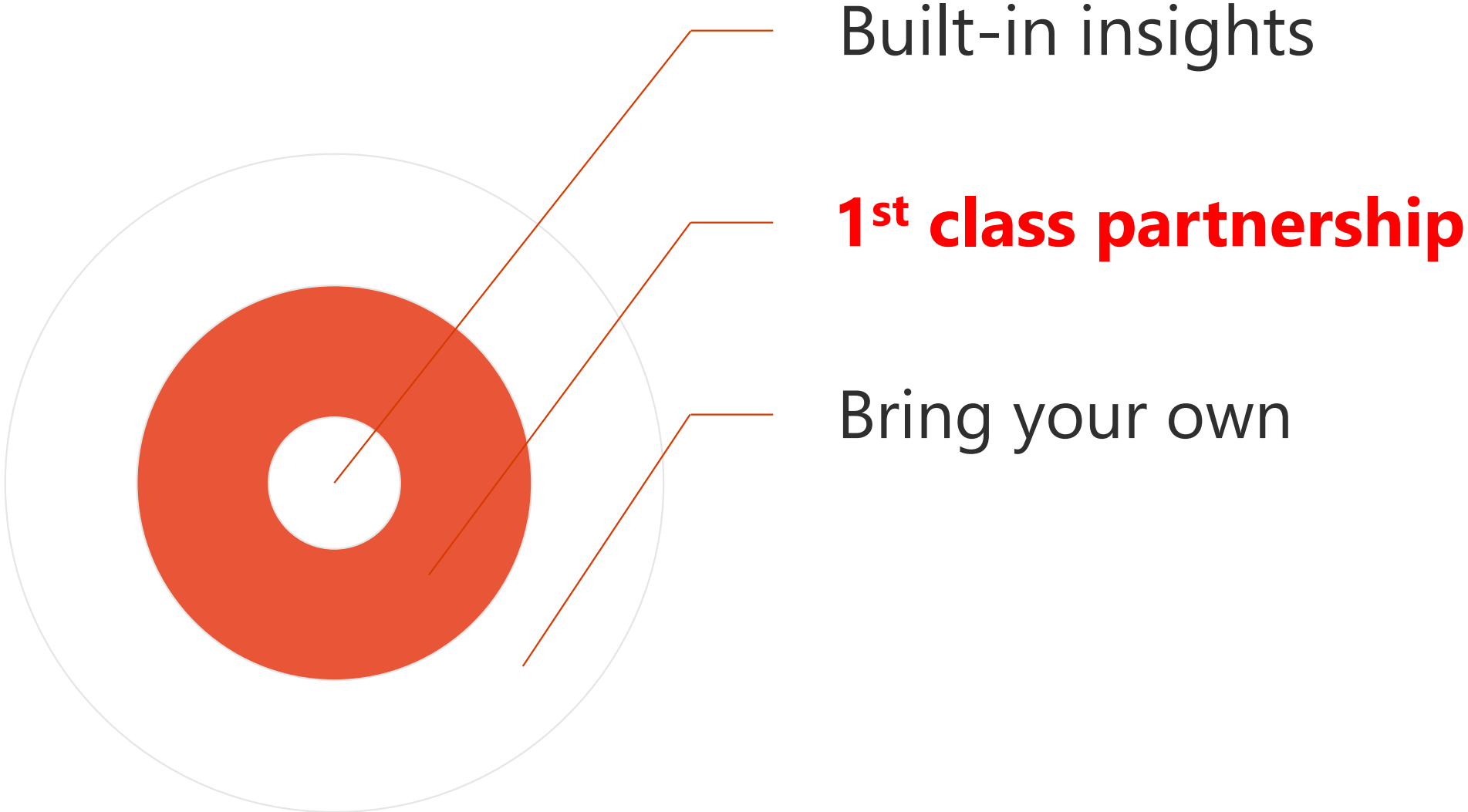
Follow the discussion on Stack Overflow

<https://stackoverflow.com/questions/tagged/microsoft-graph-security>

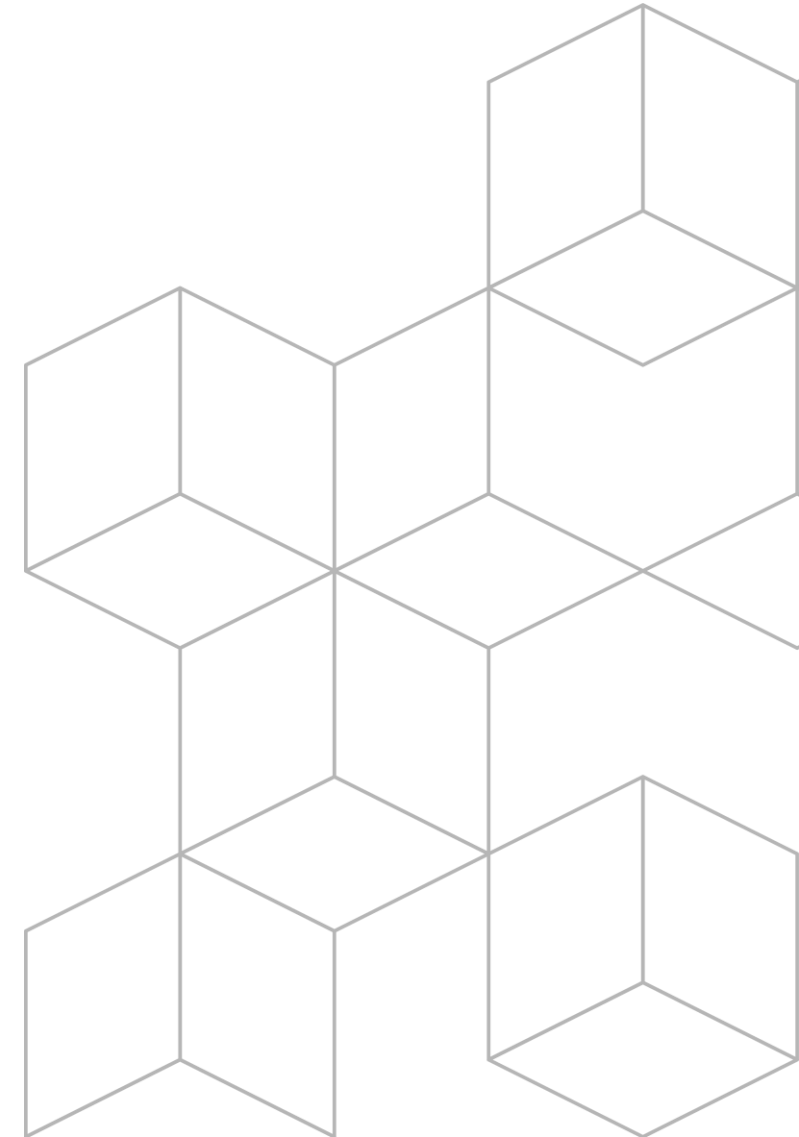
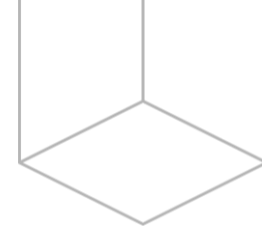
Intelligence strategies



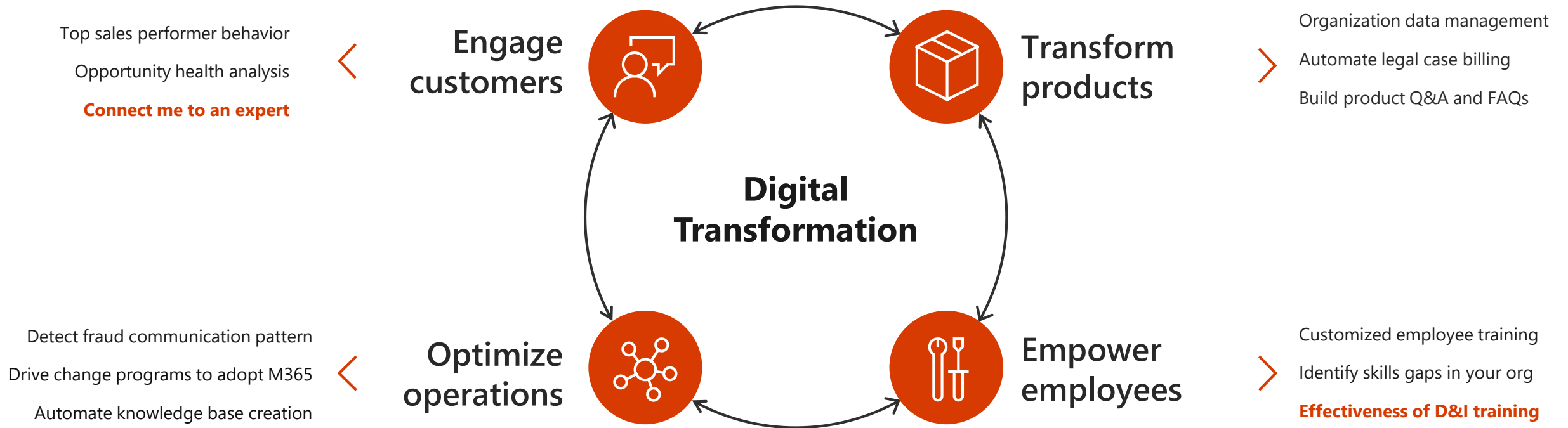
Intelligence strategies



Getting started with Microsoft Intelligence Platform



What are customers trying to do?



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

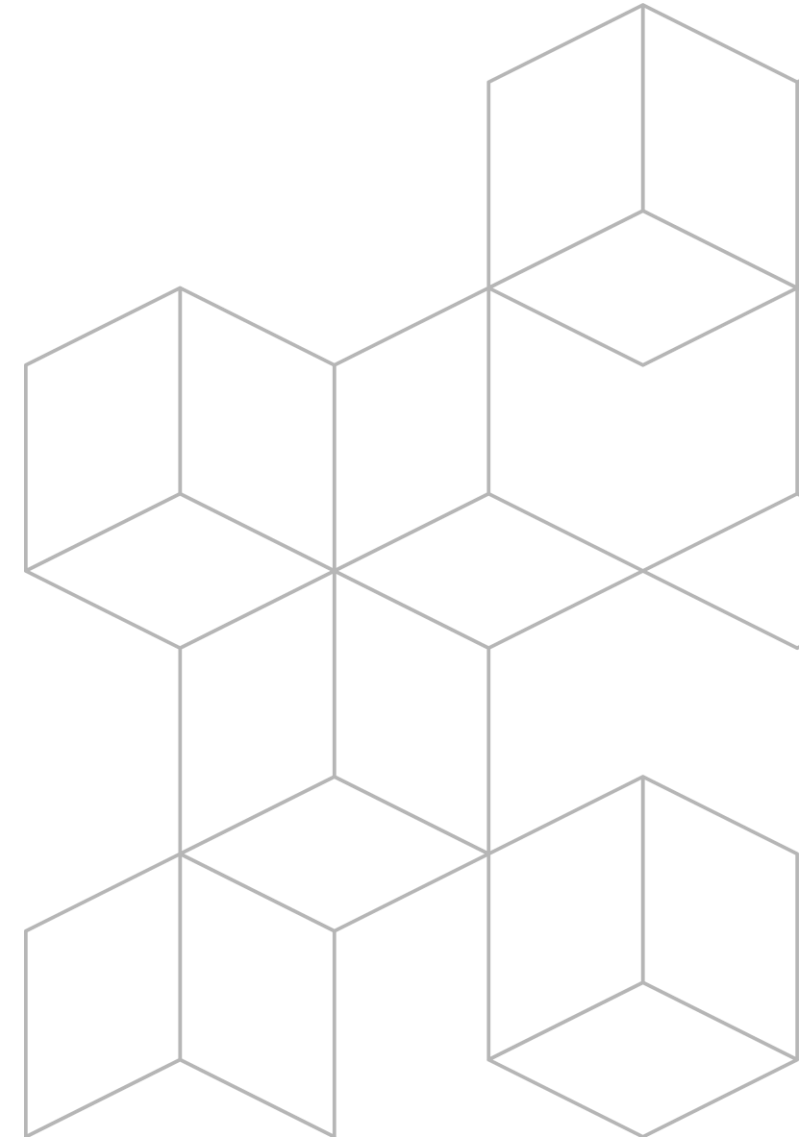
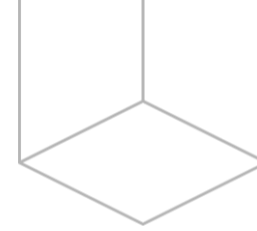


Data Governance & Security

Data controller has visibility over data
throughout its entire lifecycle

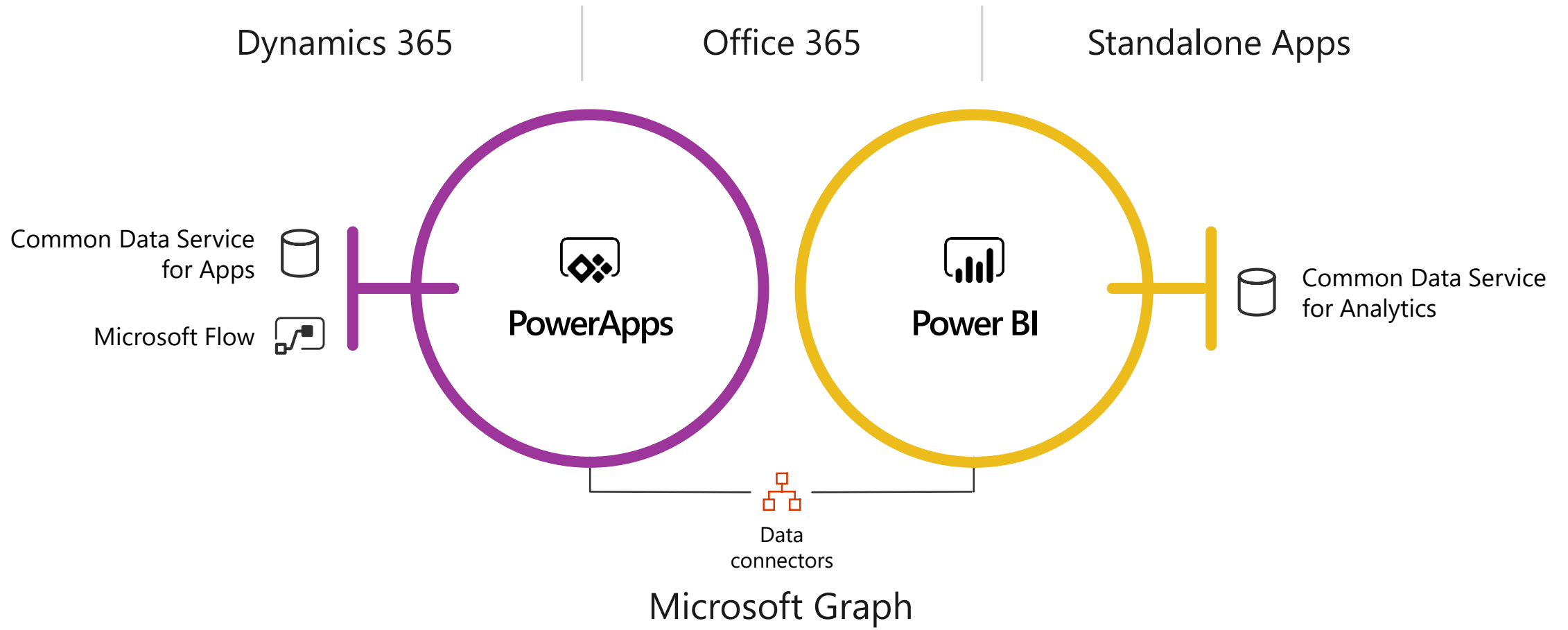


PowerApps for citizen developers



Empowering Citizen Developers

Microsoft Graph ❤️ Business Application Platform



Demo

PowerApps

The screenshot displays the Microsoft PowerApps application interface. On the left is a navigation pane with the following options: Home, Learn, Apps, Create (highlighted), Data, Business logic, and Solutions. The main area features several app tiles:

- Meeting Capture**: An all-in-one meeting capture tool. View meeting details, capture notes and pictures of whiteboards, assign tasks and send to all meeting attendees in one click. Includes a "Make this app" button.
- Onboarding Tasks**: A dashboard for user onboarding with sections for "My profile" (Lucy Miller, Sr. Marketing Manager), "To-do list", and "Quick resources".
- Service Desk**: A dashboard for managing tickets with a "REQUEST - LEAVE" header and a "My Learn Requests" sidebar. It shows metrics for 11 tickets, 1 new ticket, 5 in progress, 2 closed, and 3 on hold. Key items include "Need monitor for new hire", "Need a projector & speakers", and "Need a printer for new hire".
- Site Inspection**: A tile for site inspection.
- Help Desk**: A tile for help desk requests.
- Leave Request**: A tile for leave requests.

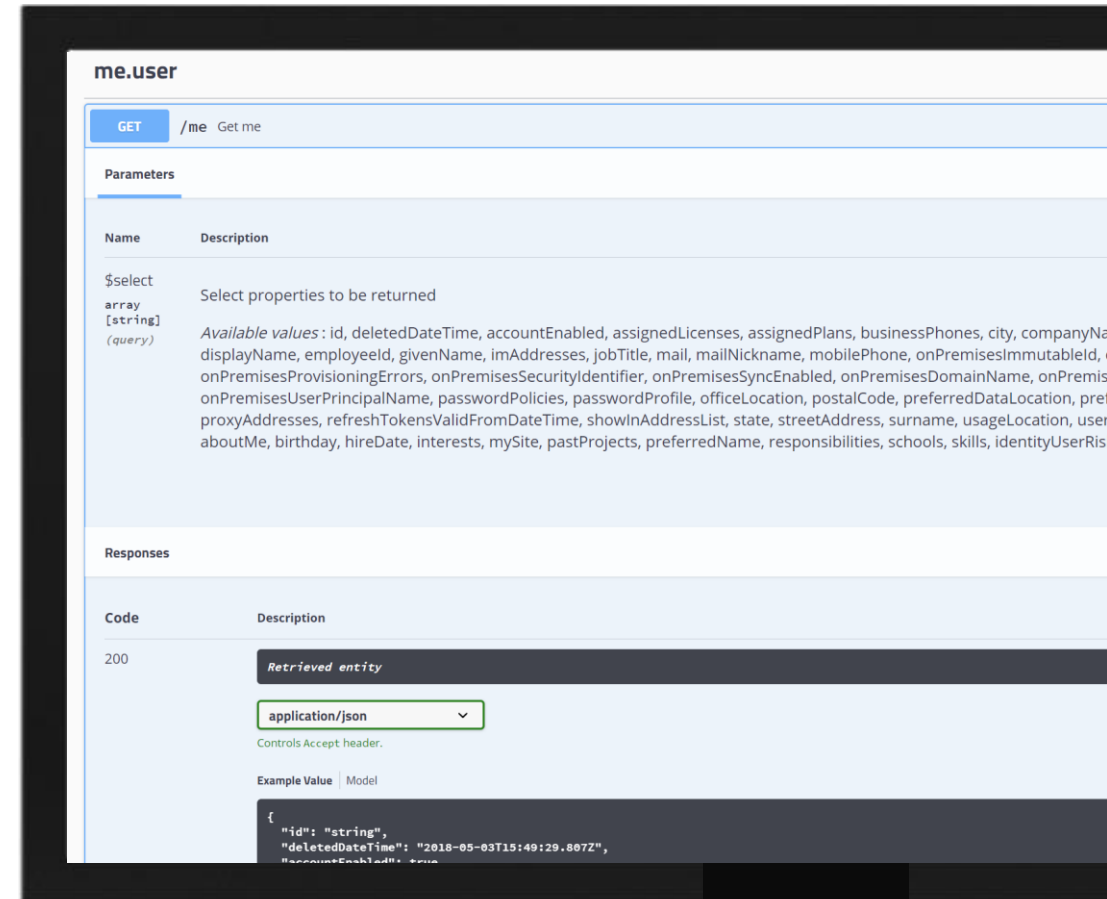
First look: OpenAPI 3.0 (fka Swagger)

Most common API description format

Describes “first level” of Graph

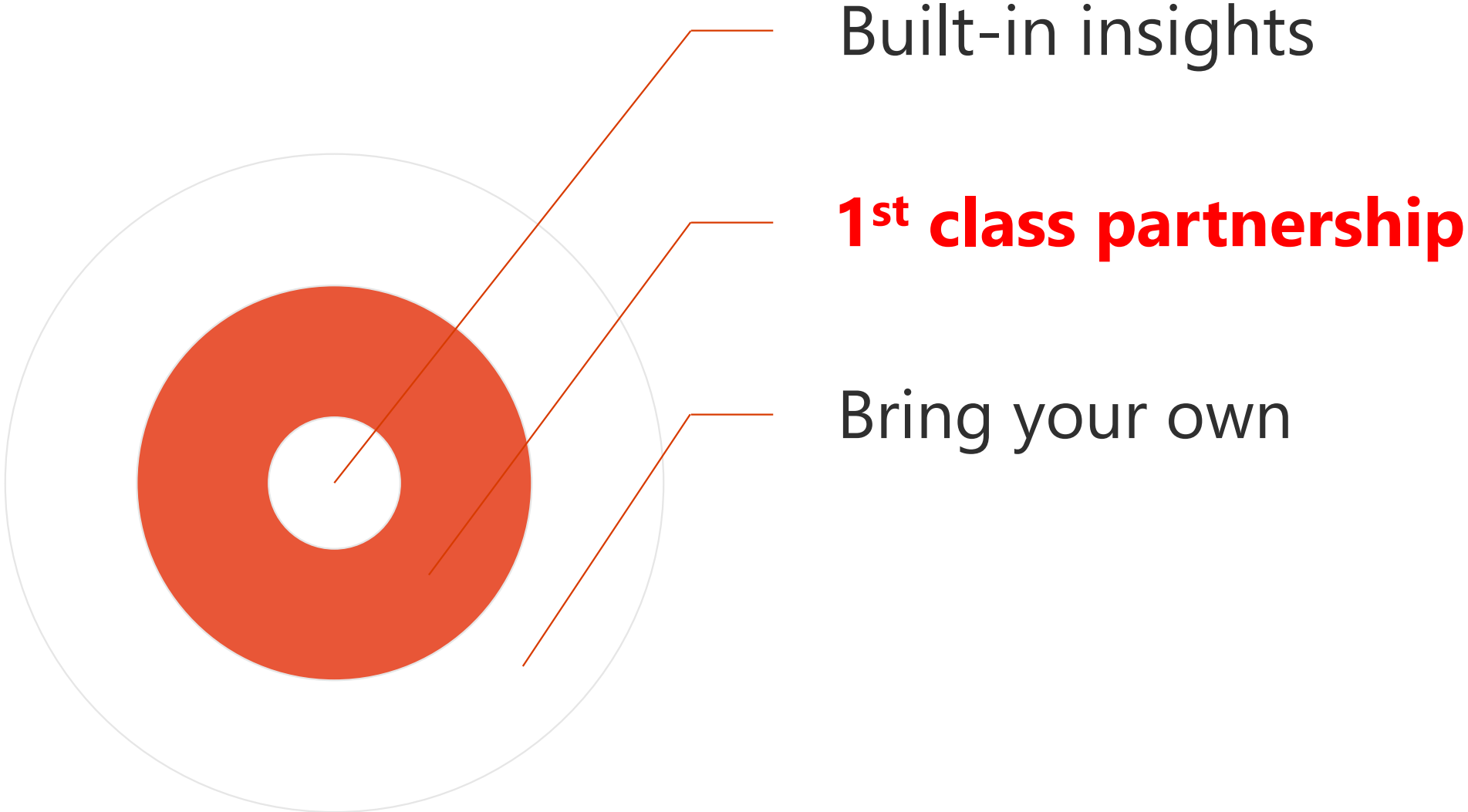
Use in any tool that supports OAS 3.0

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

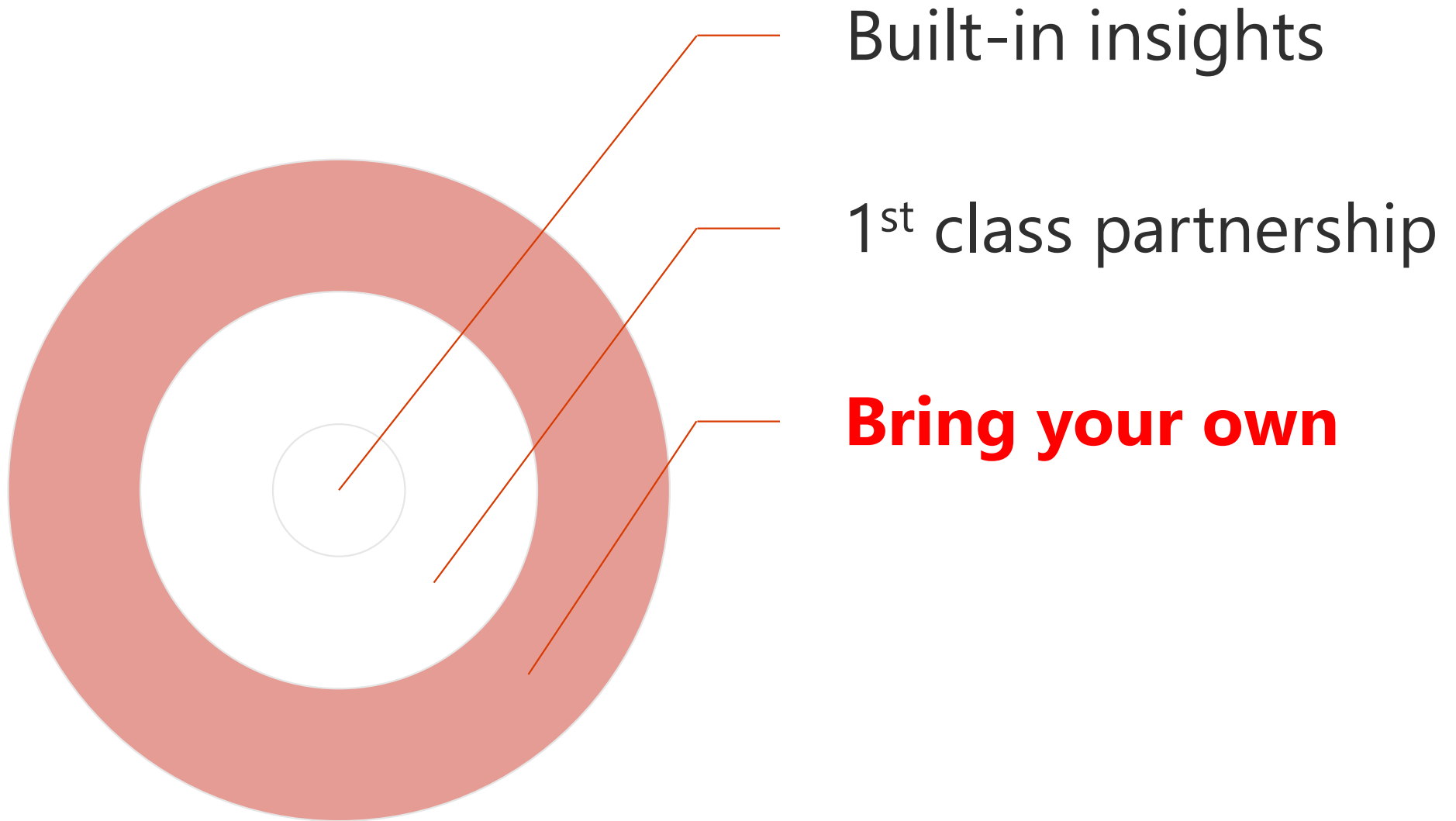


<https://github.com/microsoftgraph/microsoft-graph-openapi>

Intelligence strategies



Intelligence strategies



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

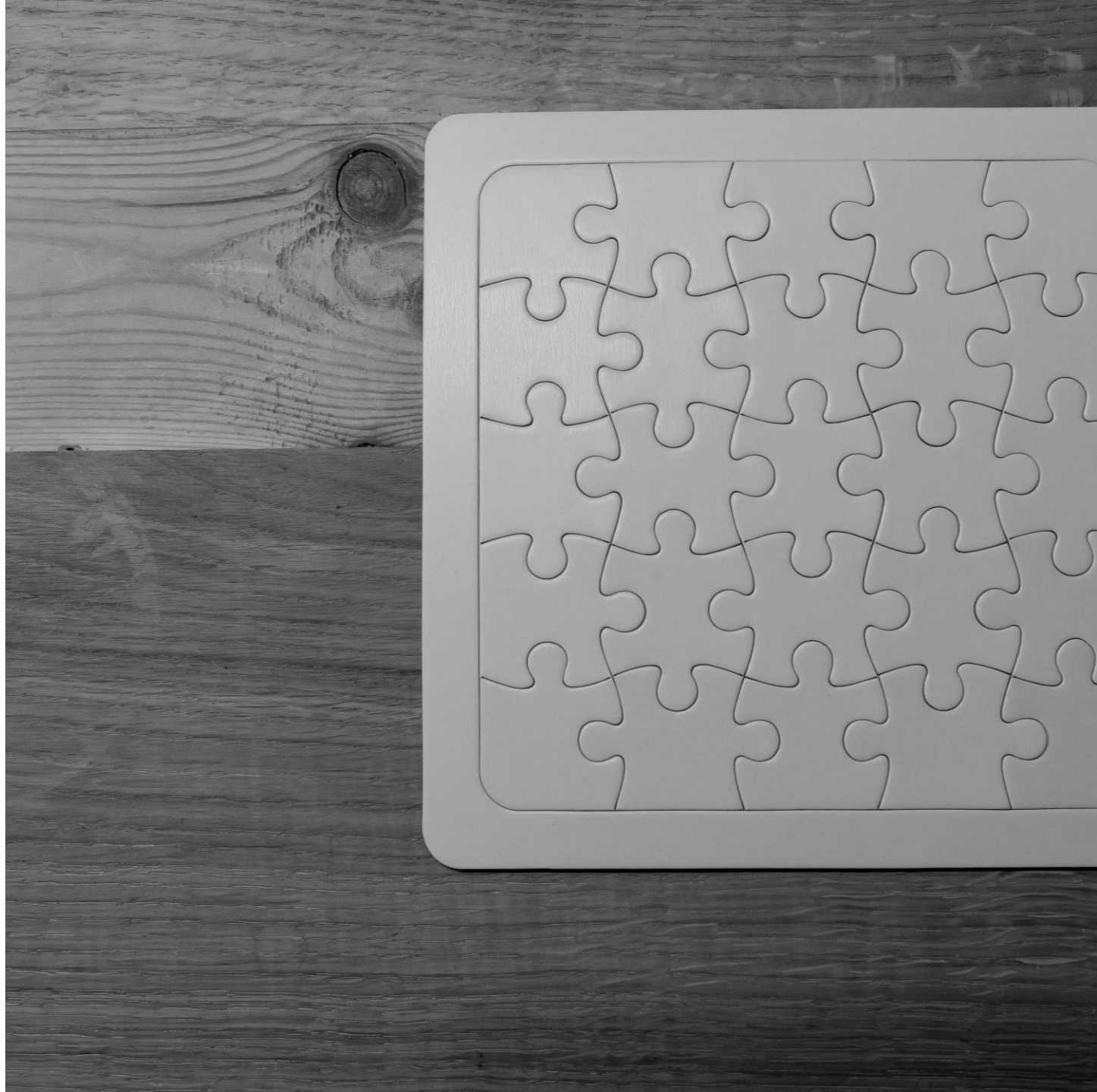
Way to access it

One endpoint
One auth key
One set of docs
One SDK

**Graph will
rarely be 100%**



**Supplement
with other data
and intelligence**



Microsoft
Graph

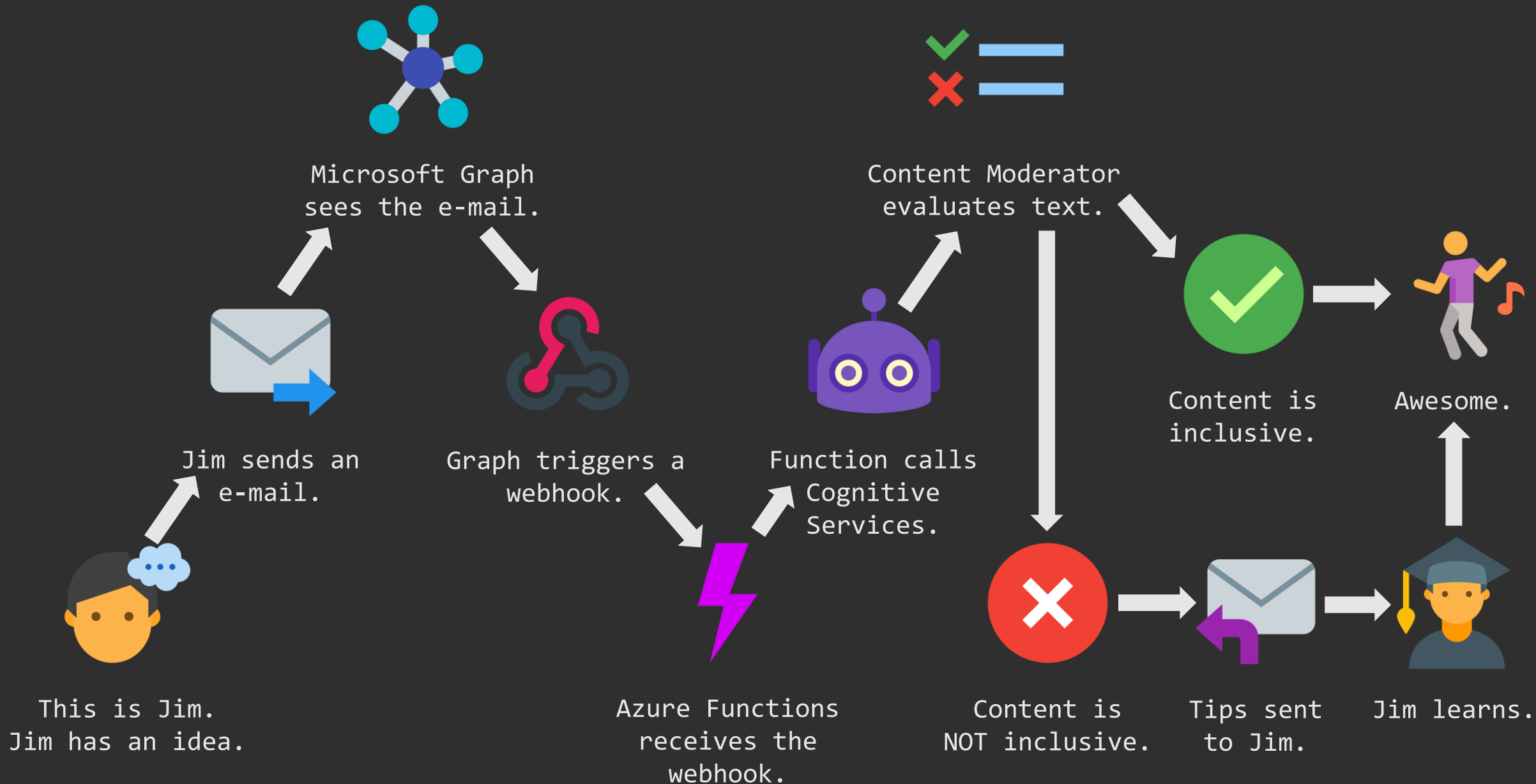


Cognitive
Services

“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

The screenshot displays the Microsoft Azure portal interface. At the top, the search bar contains the text "Search resources, services, and docs". The breadcrumb navigation shows "Home > incl - ScreenEmailFunc". The main heading is "incl - ScreenEmailFunc" with the subtitle "Function Apps".

The left-hand navigation pane includes a search bar with "incl" entered, a dropdown menu for "All subscriptions", and a tree view showing the hierarchy: "incl" > "Functions (Read Only)" > "ScreenEmailFunc". Below this, there are action buttons for "Integrate", "Manage", and "Monitor", along with "Proxies (Read Only)" and "Slots (preview)".

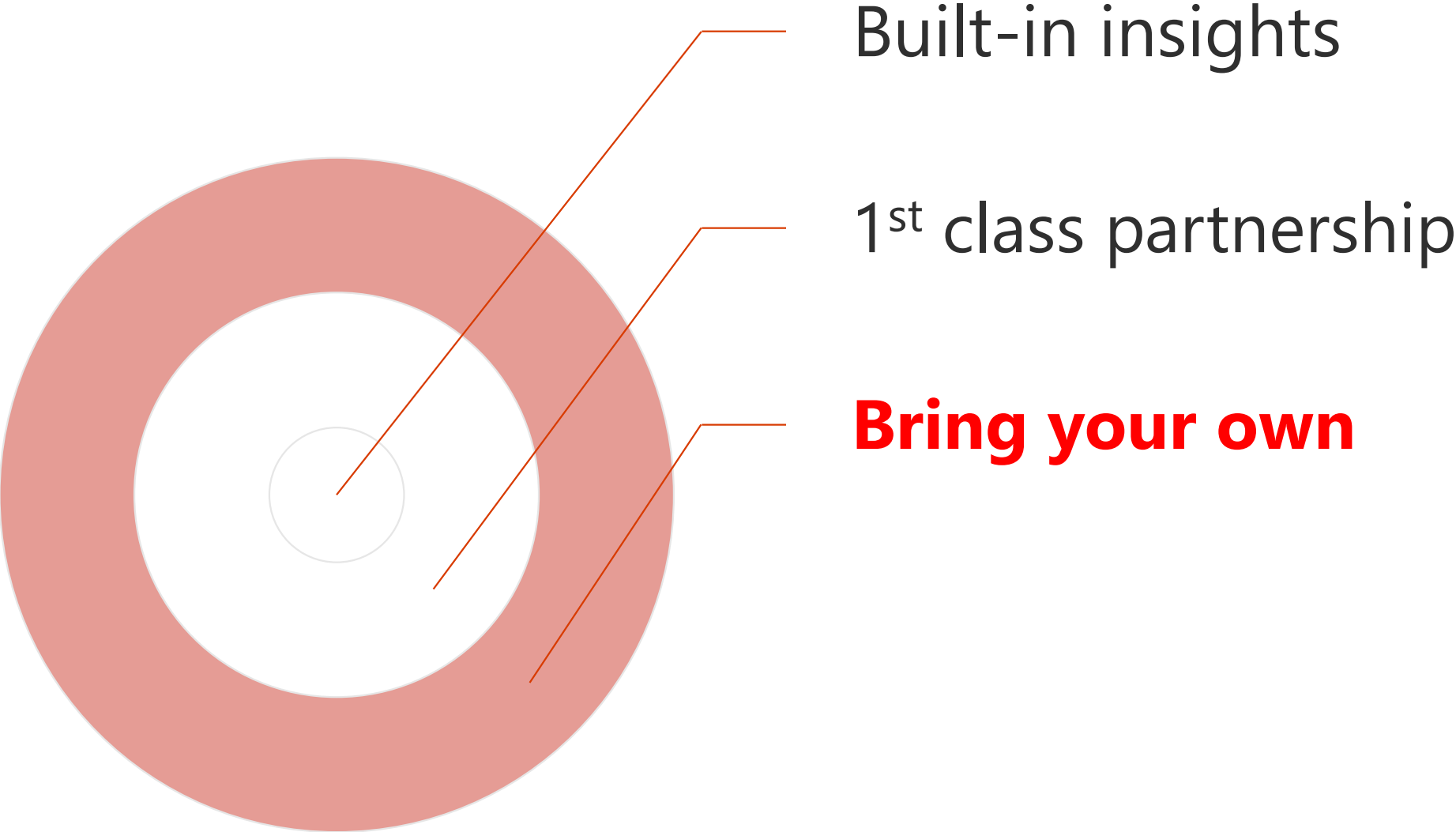
The main content area shows the configuration for the function app. A code snippet is visible with the following content:

```
15     "scriptFile": "../bin/IFL.dll",  
16     "entryPoint": "IFL.ScreenEmailFunc.Run"  
17 }
```

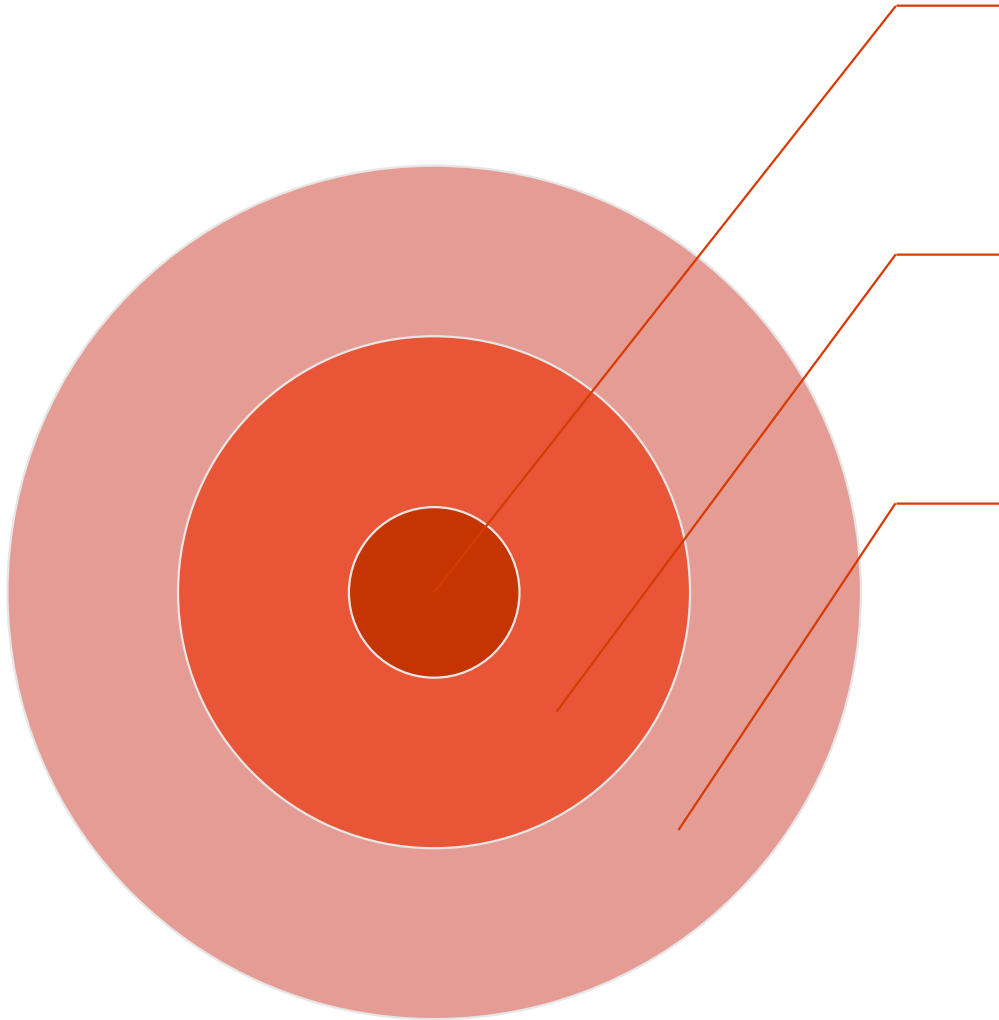
Below the code, there are tabs for "Logs", "Errors and warnings", and "Console". The "Logs" tab is active, displaying a log stream with the following entries:

```
2018-11-16T23:29:37 Welcome, you are now connected to log-streaming se  
2018-11-16T23:30:35.252 [Info] Function started (Id=223afddf-e4c3-4fa3-  
2018-11-16T23:30:35.281 [Info] webhook was triggered!  
2018-11-16T23:30:35.281 [Info] validated webhook.  
2018-11-16T23:30:35.297 [Info] Function completed (Success, Id=223afddf-  
Duration=46ms)  
2018-11-16T23:31:37 No new trace in the past 1 min(s).  
2018-11-16T23:31:41.772 [Info] Function started (Id=98ef1266-036f-44ba-  
2018-11-16T23:31:41.787 [Info] webhook was triggered!  
2018-11-16T23:31:41.806 [Info] Hook received for subscription: '0d3520e  
'users/798784e1-b452-4075-b356-  
7cb01632276f/messages/AAMkAGY1Zjk2Yjd1LTkxNDUeTNDFlmYS04NWE0LTVjNDkzODFkY  
J3To0lIRSDiSnMAAAAAAJAAA9Ssiv2-J3To0lIRSDiSnMAAASK1nrAAA=', changeType
```

Intelligence strategies



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!



Thank you