Microsoft

Microsoft Ignite

The Tour

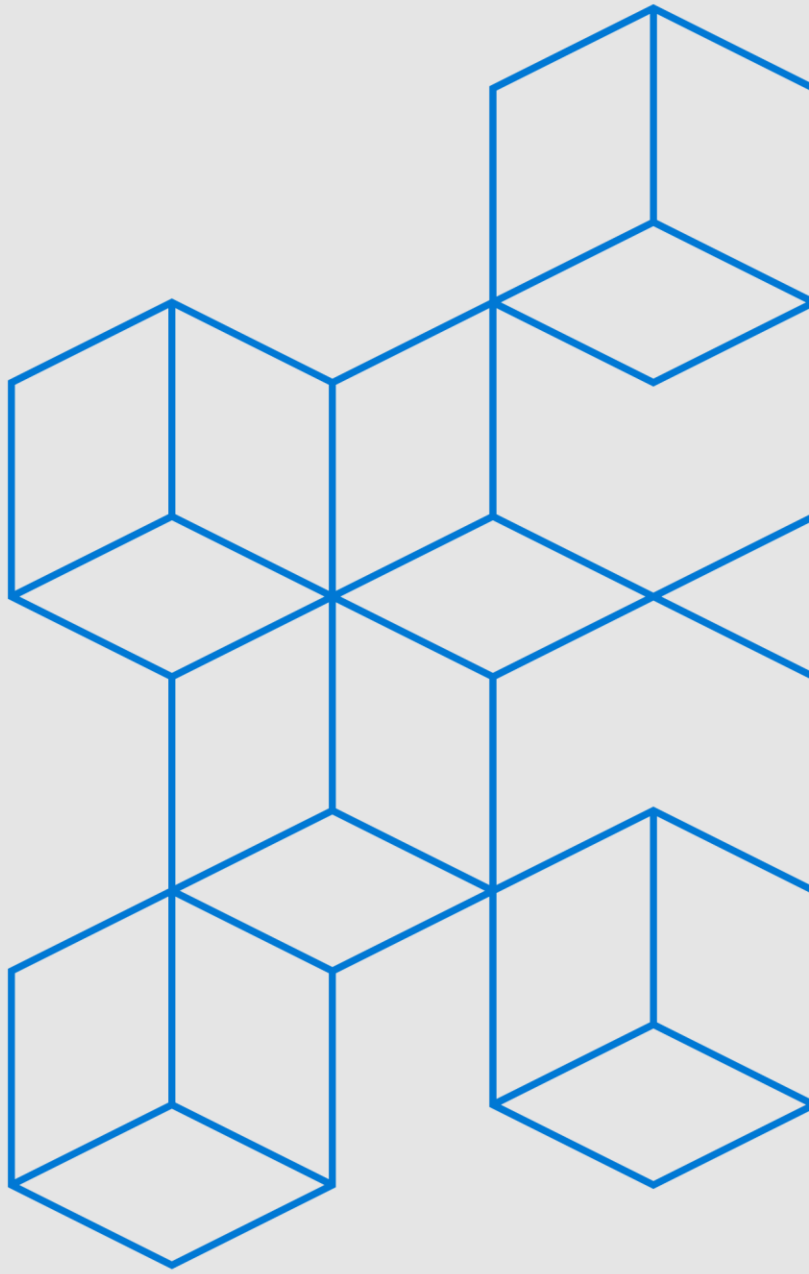
Learn. Explore. Connect.

London, England

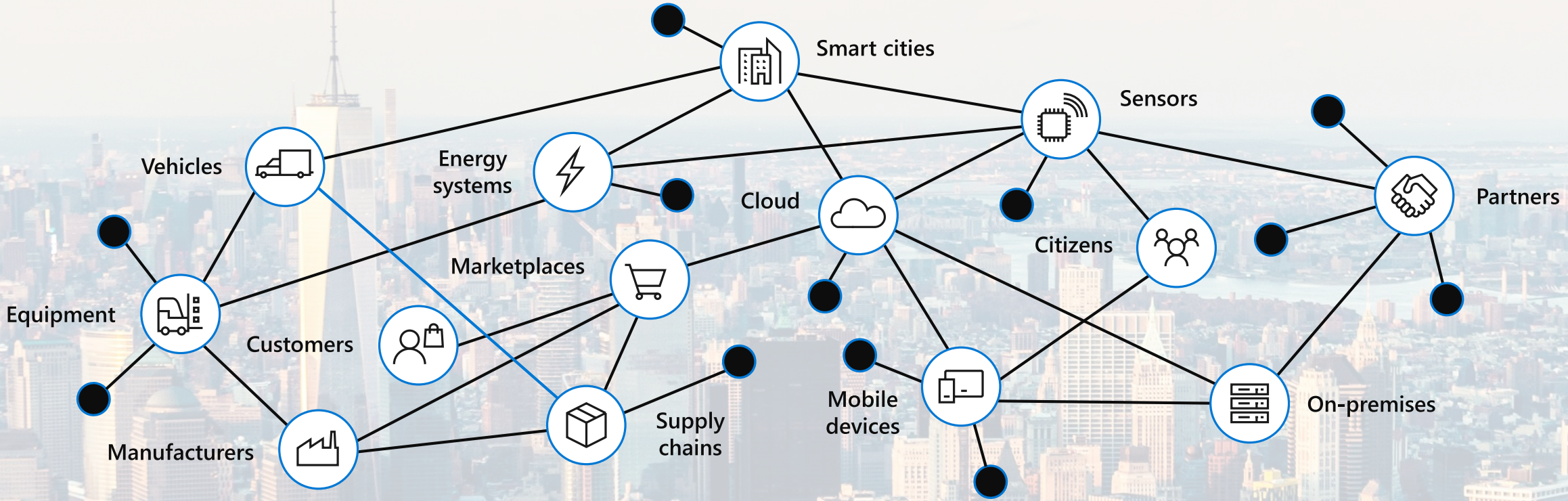
Microsoft

Unlocking security insights with Microsoft Graph Security API

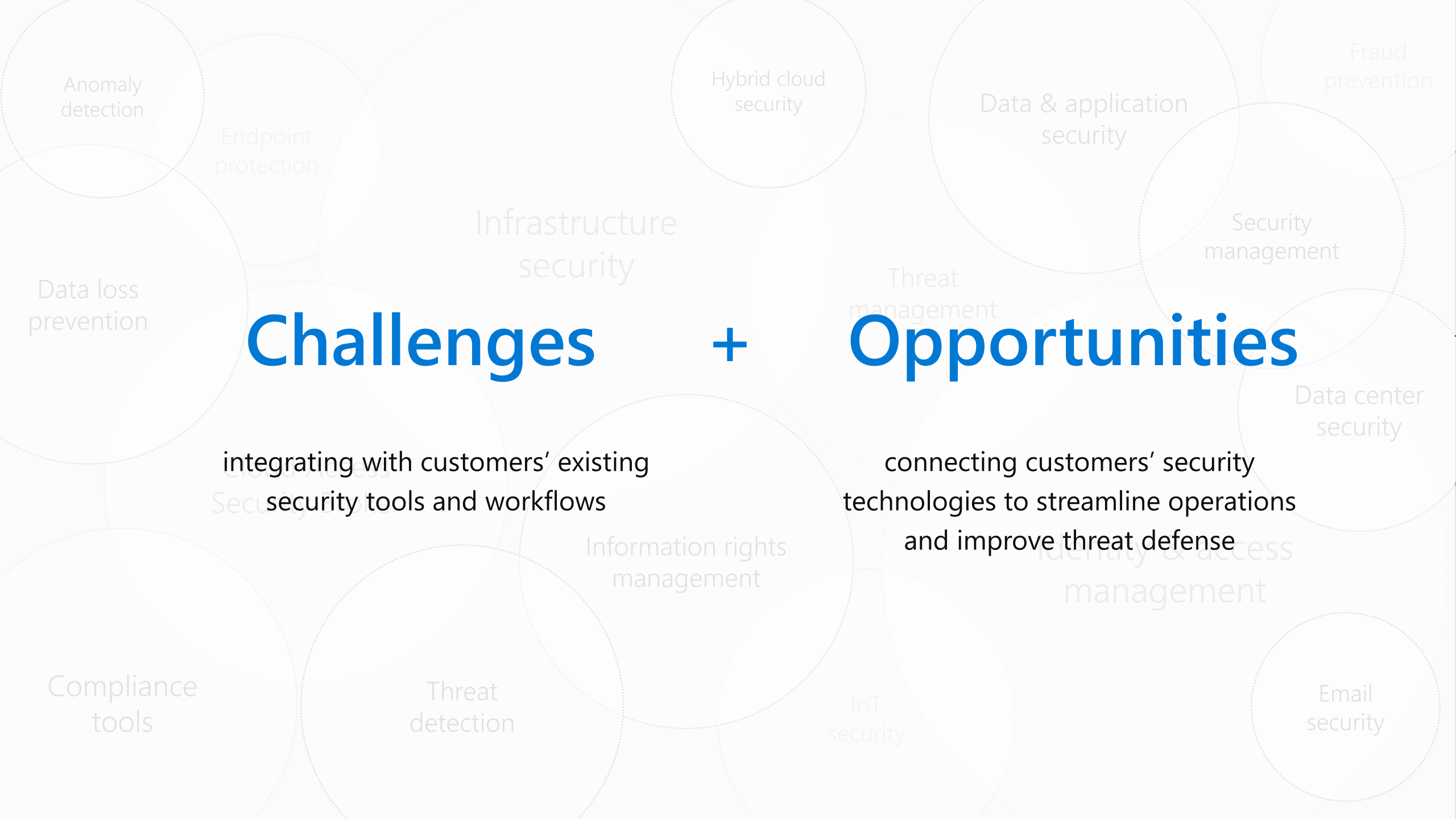
Jaap Brasser – CDM MVP
Technical Marketing Engineer @ Rubrik
@jaap_brasser



The digital estate



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

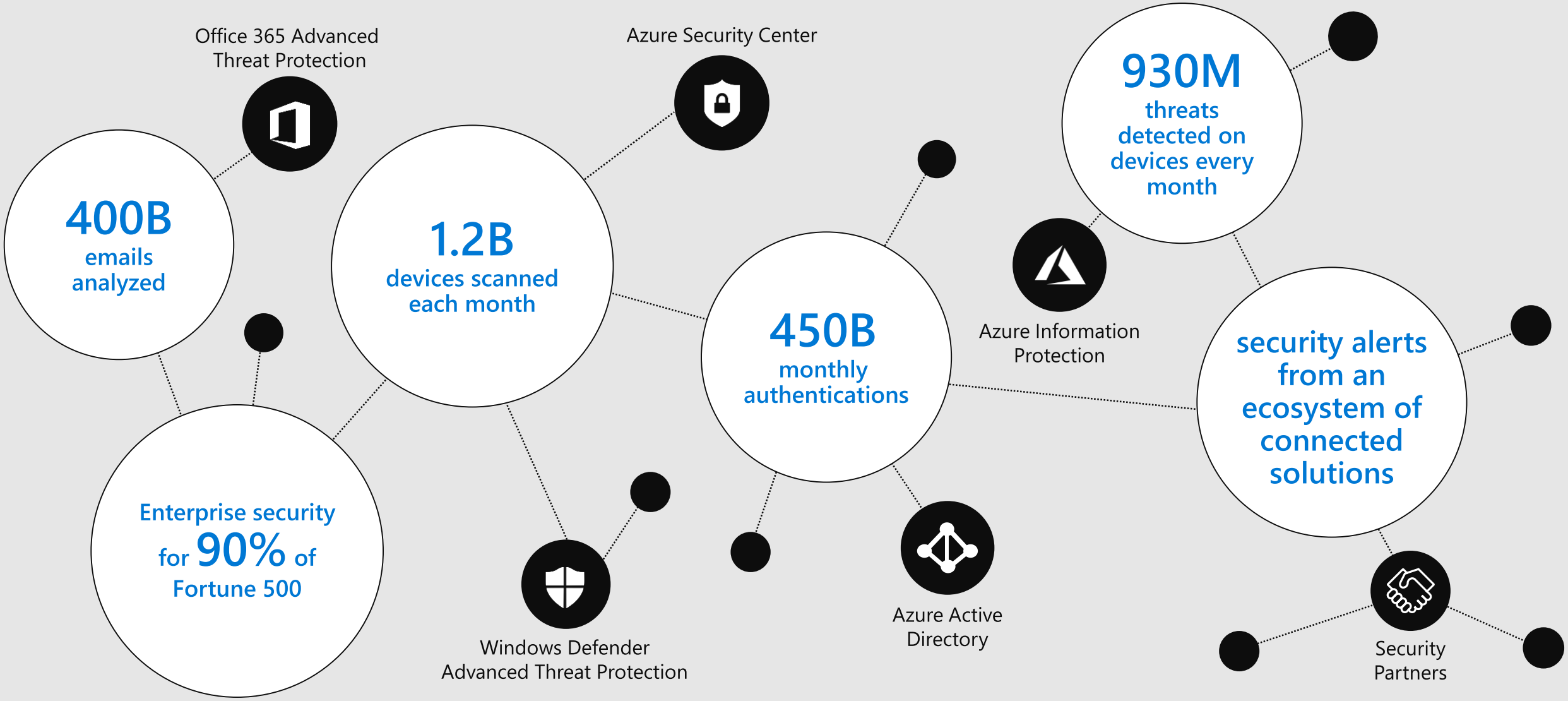


Challenges + Opportunities

integrating with customers' existing security tools and workflows

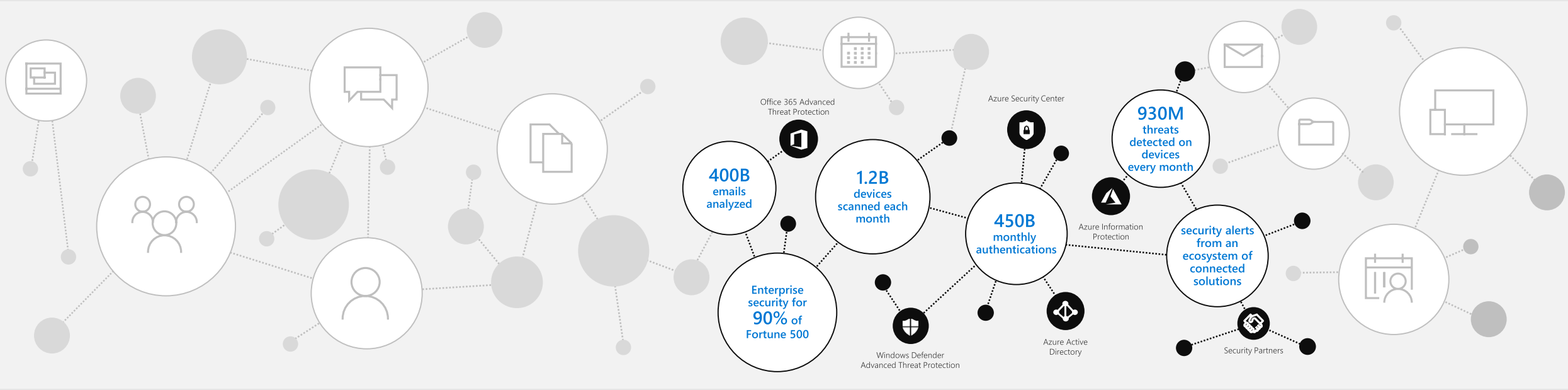
connecting customers' security technologies to streamline operations and improve threat defense

Security intelligence powered by trillions of signals



Now accessible through Microsoft Graph

Gateway to your data in the Microsoft cloud



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

What is the Security API?

It is:

- Unified REST API for integrating security products
- Uniform schema for security entities
- Part of the Microsoft Graph
- Gateway to Microsoft and partner security services
- Included with Microsoft services—no extra cost

It is not:

- Log collector
- Threat intel feed or sharing platform
- Dashboard or web portal
- SIEM

Apps

Security applications

ANOMALI

DEMISTO

SIEM + log analytics

splunk>

sumologic

IBM QRadar

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

Alerts

Connect and enrich alerts from multiple sources to more easily understand the scope and impact of an attack

- Use filtered queries to get all alerts for a specific user, device, or file when investigating a specific threat
- Subscribe to notifications for all new or updated alerts matching your criteria
- Keep alert status and assignments in sync, tag alerts with context, and capture comments for visibility to all workflows

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

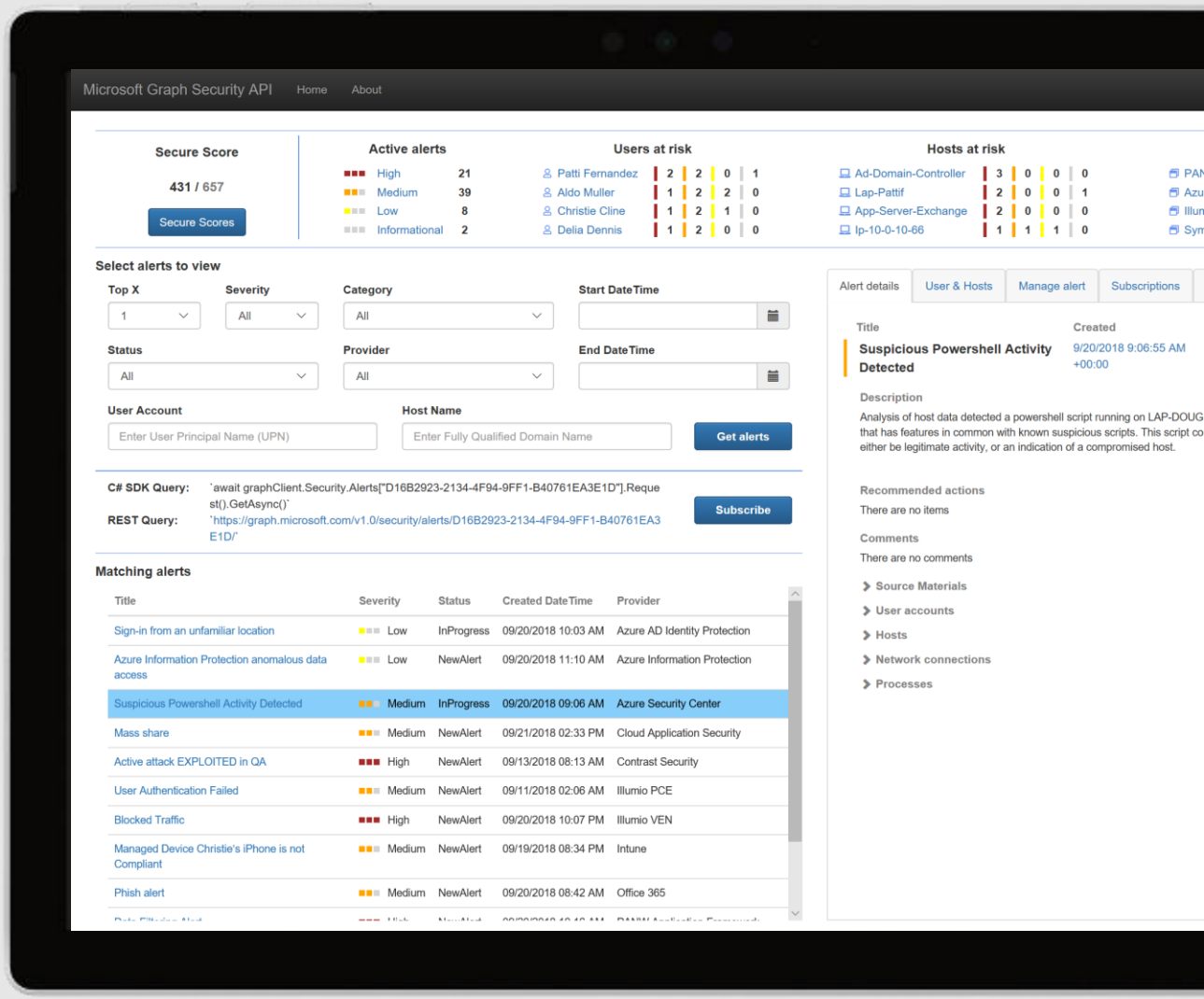
Context

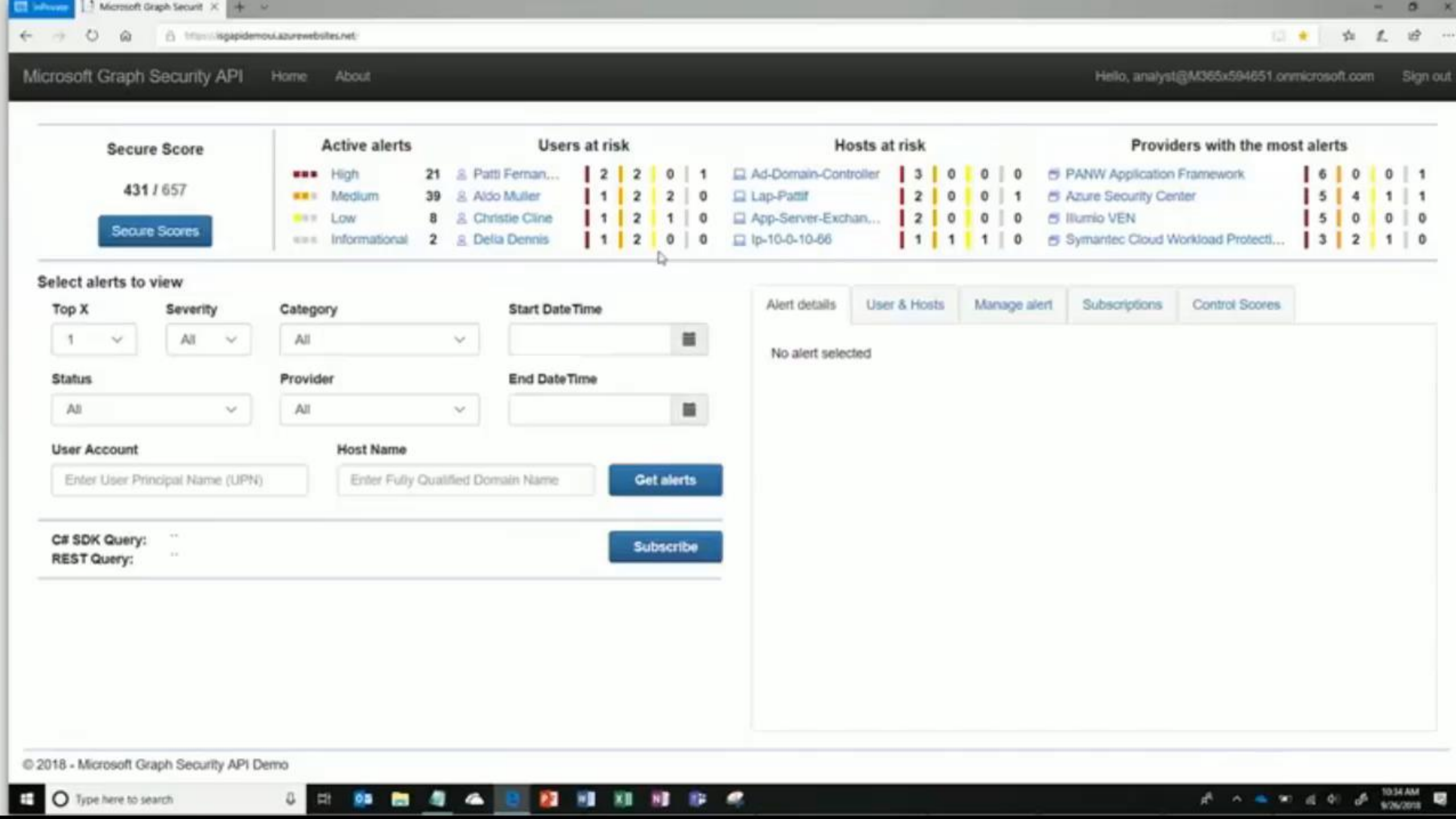
Tap into additional context from Microsoft Graph services to inform threat response

- Learn more about a potentially compromised user from Azure Active Directory
- Find out what devices are registered to a user from Microsoft Intune
- Access information about a user's meetings, mail, docs, and more

Demo

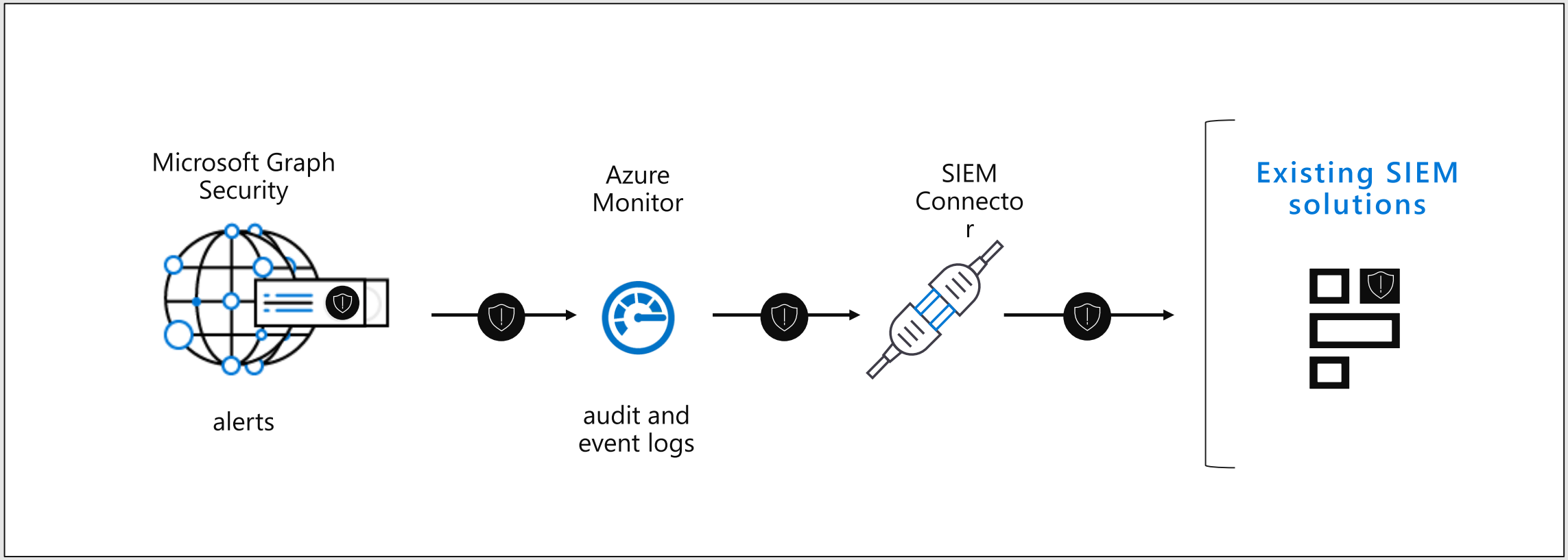
Graph Security API




Microsoft Graph Security API
Home
About
Hello, analyst@M365x594651.onmicrosoft.com
Sign out
Secure Score
431 / 657
Secure Scores
Active alerts
High 21
Medium 39
Low 8
Informational 2
Users at risk
Patti Fernan... 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-Exchan... 2 0 0 0
Ip-10-0-10-66 1 1 1 0
Providers with the most alerts
PANW Application Framework 6 0 0 1
Azure Security Center 5 4 1 1
Illumio VEN 5 0 0 0
Symantec Cloud Workload Protecti... 3 2 1 0
Select alerts to view
Top X
1
Severity
All
Category
All
Start DateTime
Status
All
Provider
All
End DateTime
User Account
Enter User Principal Name (UPN)
Host Name
Enter Fully Qualified Domain Name
Get alerts
C# SDK Query:
REST Query:
Subscribe
Alert details
User & Hosts
Manage alert
Subscriptions
Control Scores
No alert selected
© 2018 - Microsoft Graph Security API Demo
Type here to search

SIEM integration

Enables a unified pipeline (per tenant) to stream alerts in near real-time from Microsoft security services



What's next?

- Onboarding additional Microsoft and ecosystem products
- Unlock new security context through **Security Profiles**
- Add automation through **Actions** and **Configuration**
- Enable customers to bring their own **Threat Intelligence** to Microsoft
- Additional client SDKs and sample code through Microsoft Graph

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

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

Questions

- Twitter:
  - @jaap_brasser
  - #BRK3455 #MSIgniteOnTour
- Microsoft Tech Communities
- GitHub
  - github.com/jaapbrasser/events