It’s 4pm

Do you know where your data is travelling to?

Michael Rueefli
Partner | Solutions Architect @ scopewyse gmbh
Microsoft Azure MVP

michael.rueefli@scopewyse.com
http://www.miru.ch
@drmiru

About me

- Partner @ scopewyse GmbH
- Microsoft Azure MVP
- Cloud enthusiast
- Tech geek
- Community guy

in https://ch.linkedin.com/in/drmiru

www.miru.ch

www.facebook.com/drmiru

@drmiru

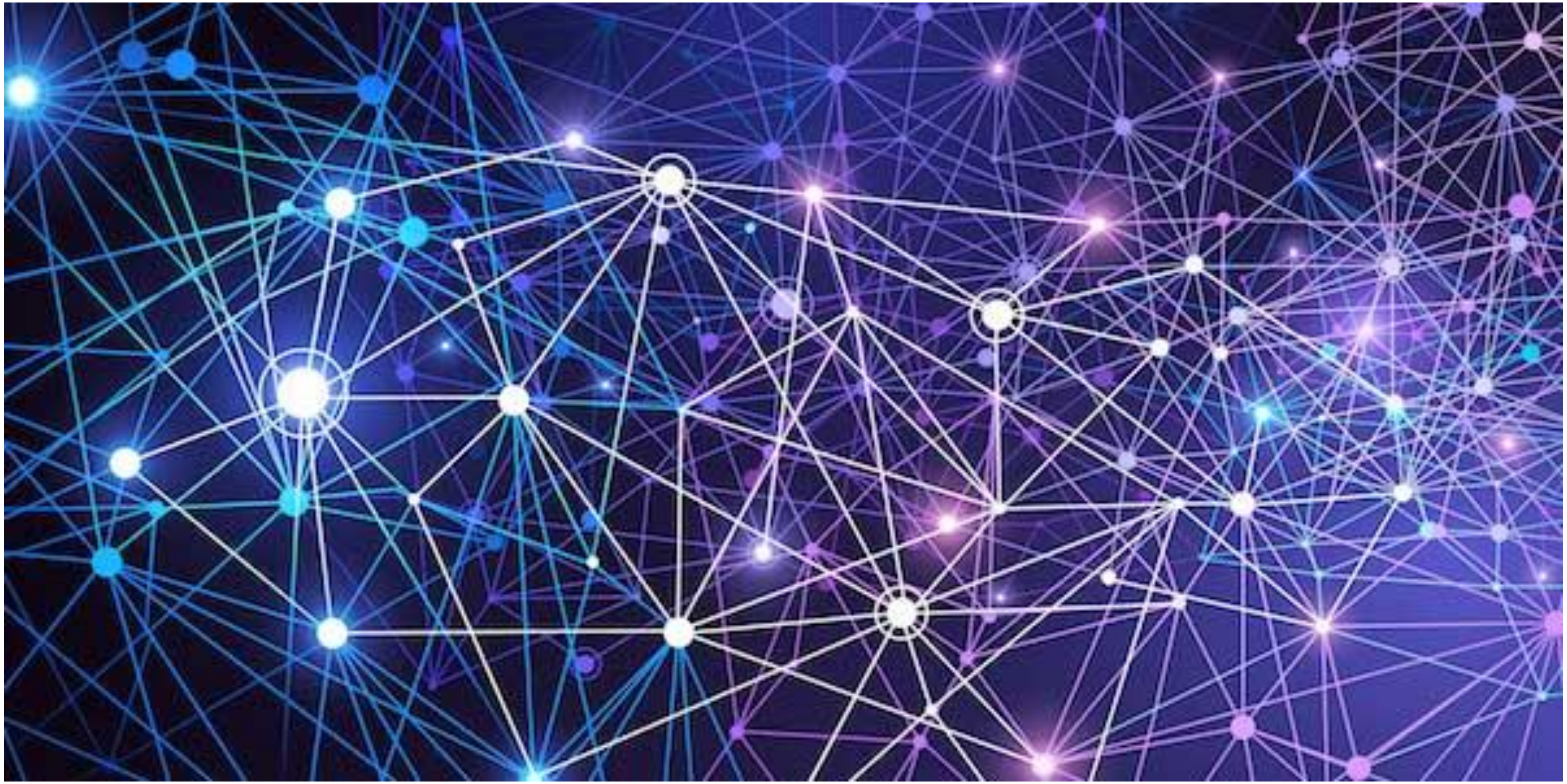
What to expect from this session

- The brave new world - why companies need a CASB
- Key capabilities of Microsoft Cloud App Security
- Architecture & integration
- How to start
- Licensing
- Q&A

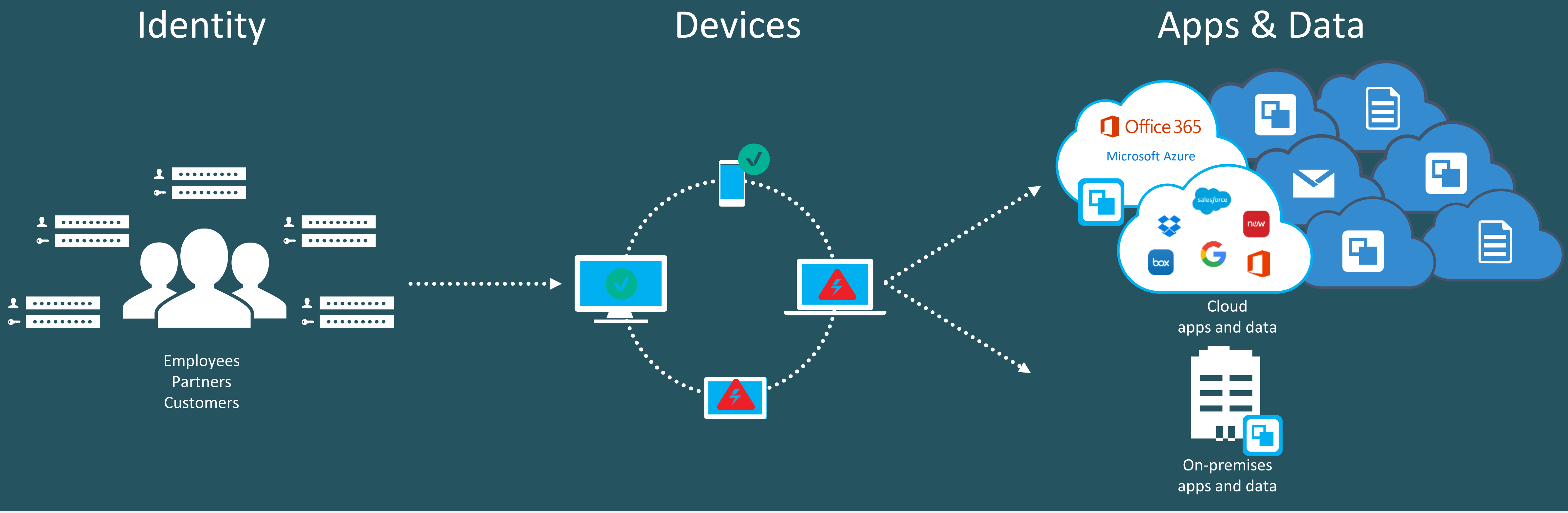
Fiction….

1	*“Our company is not using cloud services yet”*
2	*“Our application is hosted somewhere externally, we don't have any control”*
3	*“Our employees are instructed not to share confidential data on dropbox”*

Reality...



The Security Landscape has changed



Transition to cloud & mobility + New attack landscape = Current defenses not sufficient

What is a CASB (cloud app security broker)?

- On-premises or cloud-based service
- Monitors activities between users and cloud applications
- Enforces security policies

Why companies might need a CASB

Visibility

detect all cloud services; assign each a risk ranking; identify all users and third-party apps able to log in

Data security

identify and control sensitive information (DLP); respond to classification labels on content

Threat protection

offer adaptive access control (AAC); provide user and entity behavior analysis (UEBA); mitigate malware

Compliance

supply reports and dashboards to demonstrate cloud governance; assist efforts to conform to data residency and regulatory compliance requirements

Microsoft Cloud App Security

Key Capabilities

Cloud discovery

Discover all cloud usage in your organization

Information protection

Monitor and control your data in the cloud

Threat prevention

Detect usage anomalies and security incidents

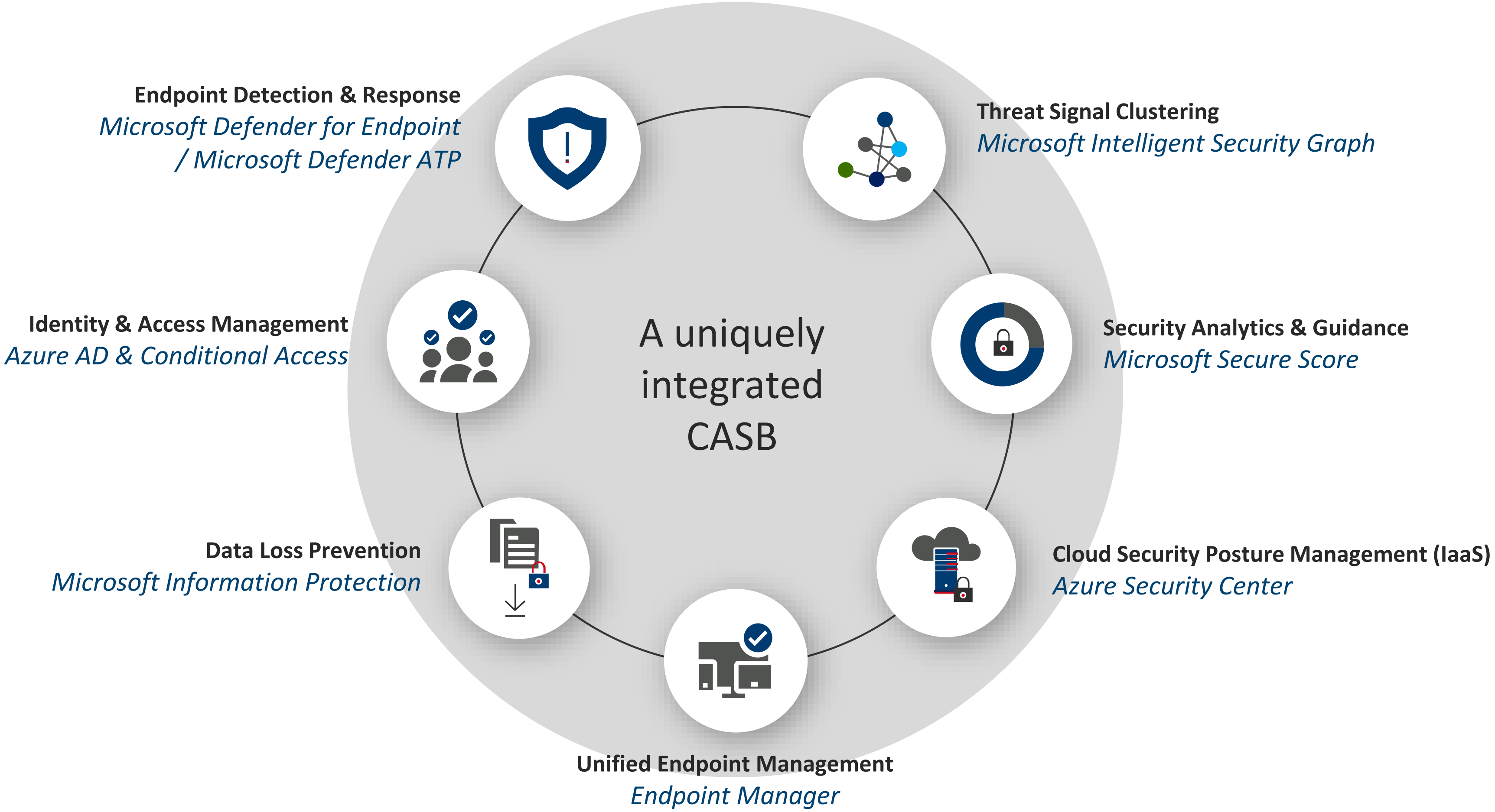
In-session control

Control and limit user access based on session context

DISCOVER > INVESTIGATE > CONTROL > PROTECT

MICROSOFT CLOUD APP SECURITY (MCAS)

Uniquely integrated security



A uniquely integrated CASB

Endpoint Detection & Response
Microsoft Defender for Endpoint / Microsoft Defender ATP

Threat Signal Clustering
Microsoft Intelligent Security Graph

Identity & Access Management
Azure AD & Conditional Access

Security Analytics & Guidance
Microsoft Secure Score

Data Loss Prevention
Microsoft Information Protection

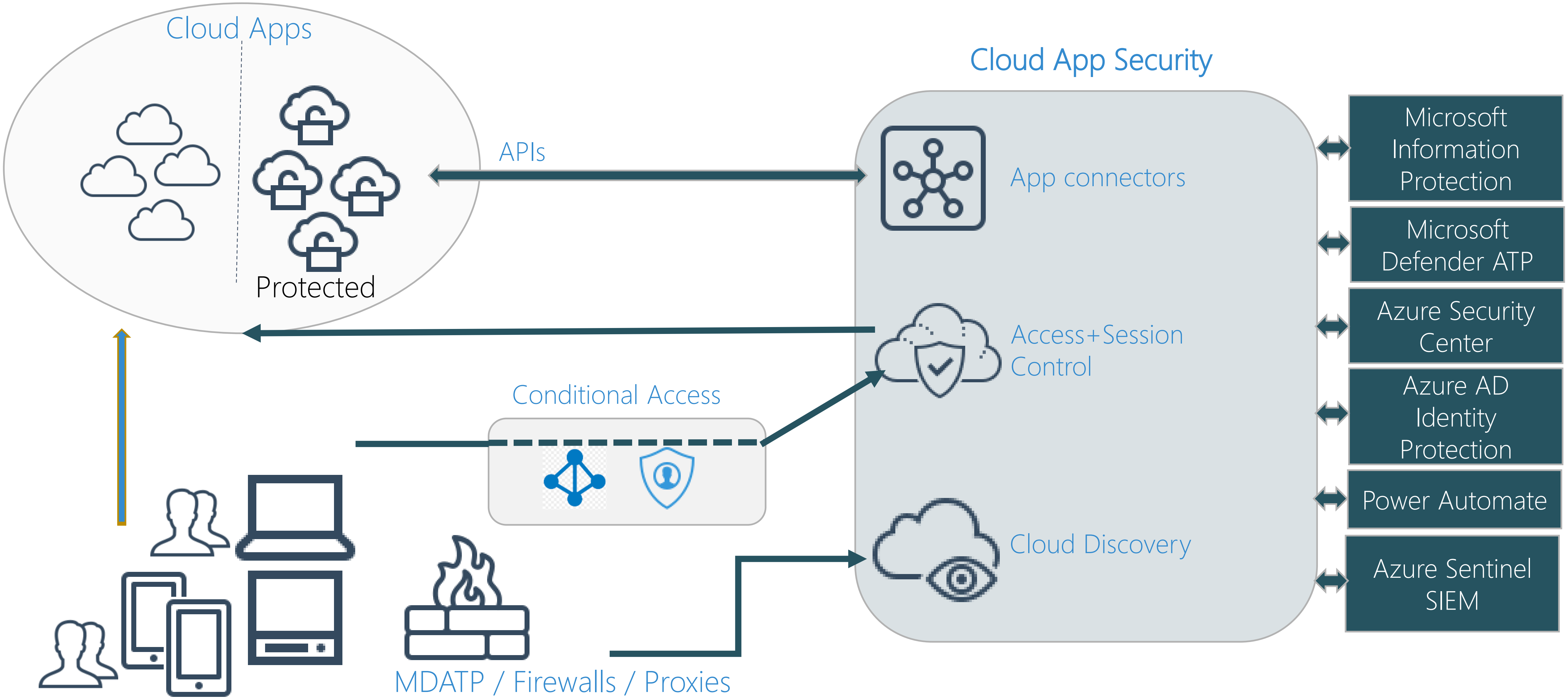
Cloud Security Posture Management (IaaS)
Azure Security Center

Unified Endpoint Management
Endpoint Manager

Live DEMO: Portal Overview

Discovered Apps
Activity Log
Files
Security Configuration
oAuth apps
Alerts

MCAS Architecture



CAS Policies

Activity Policy	Monitor unexpectedly high rates of certain activity types	Detect and Report
Anomaly detection Policy	Monitor unusual activities that differ from users or organization baseline	
App discovery Policy	Alert and notify when new apps are discovered	
Cloud discovery anomaly detection Policy	Uses cloud app discovery logs and search for unusual occurrences	
Access Policy	Realtime monitoring and control over user logins to your cloud apps	Block
Session Policy	Realtime monitoring and control over browser-based app activities	

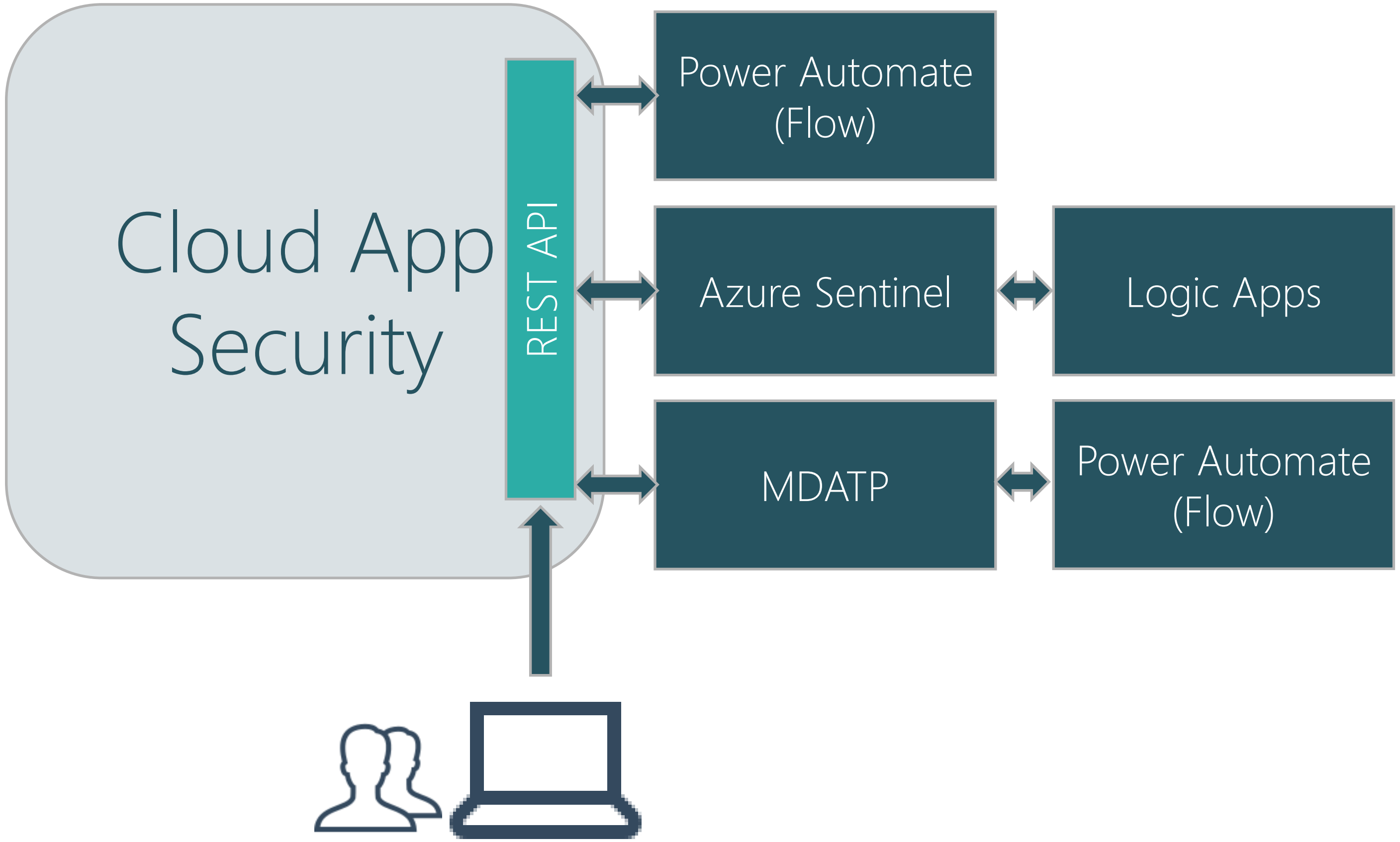
Live DEMO:

Policies
End user experience

My boss said: “Sharing data with the cloud is easy”

Automation Options

- Automated Response
- Incident Creation
- Reporting



Live DEMO:

Automated blocking of a rogue user

HAHA!: “Look, they don’t even block Facebook in here”

How to get started – 5 easy steps

1. Get Licenses (Trial available)
2. Upload discovery logs or integrate with MDATP
3. Connect sanctioned SaaS apps
4. Activate integrations (MDATP, MIP, ASC)
5. Configure initial policies (start small)

Licensing

- Discovery & Reporting
  - M365 E3
  - M365 E3 Security AddOn
- Control & Policy Enforcement
  - M365 E5
  - M365 E5 Security
  - M365 E5 Compliance

Key Takeaway – MCAS Top 5 use cases

- Detect shadow cloud apps
- Discover privileged oAuth Apps
- Block unsanctioned cloud apps
- Prevent data exfiltration
- Detect anomalies in user / endpoint behavior

Thanks to our Sponsors!

ACP IT for innovators.

THOMAS KRENN®

FORTINET®

PowerShell UsergroupAustria

smartpoint bewegt digitales

TECHATIVE enhance success in an agile world

NiCE IT Management Solutions www.nice.de

CloudGuard

secureguard

Q&A

Thank you!

Michael Rueefli
Partner | Cloud Solutions Architect | Azure MVP
michael.rueefli@scopewyse.com

REST API Example (show files matching MIP label)

```
$token = ‘<place your API token here>’
$tenantName = «<your tenant name>«
$labelName = «<label name>"

#Create auth header
$authHeader = @{

    'Content-Type'='application/x-www-form-urlencoded'

    'Authorization'='Token ' + $token

}

#construct REST URL
$url = "https://$tenantName.eu2.portal.cloudappsecurity.com/api/v1/files/"

#Set Filter
$filter = @"

{

    "filters": {

        "fileLabels": {

            "eq": ["$labelName"]

        }

    }

}

"@

#Execute REST call
$result = Invoke-RestMethod -Method Post -Uri $url -Headers $authHeader -Body $filter



#Display Result
$result.data | Select name_l,filePath,ownerAddress | Out-GridView
```