





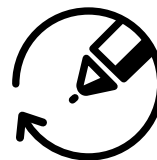
BlueVoyant®

# M365 E5 License: Where to start your licensing journey

# Security with Microsoft 365 E5

We're back! Dive into the M365 E5 license with us, wherever you are in your licensing story. We've collected your most pressing questions and help us review some of the best use cases we've found for the M365 bundles.

## Webinar Agenda:



Scenarios



Identity



Data



Endpoint



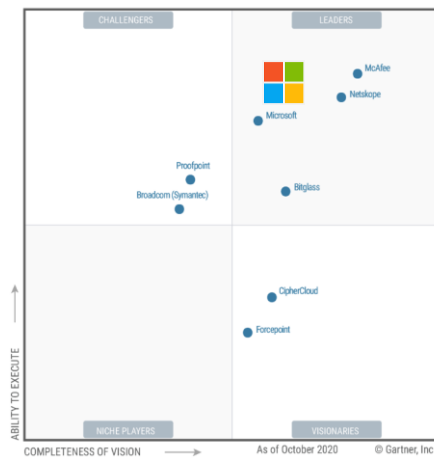
# M365 E5 License: Where to start your licensing journey

2021?

## Microsoft Security - a leader in 5 Gartner magic quadrants



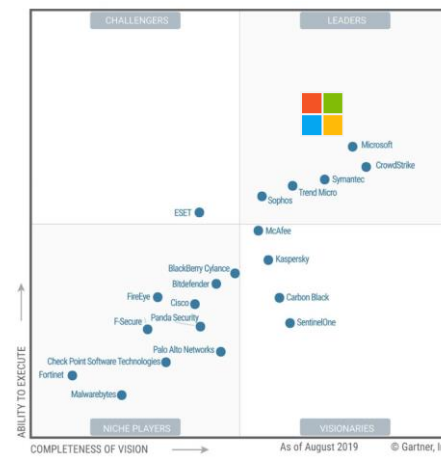
Access Management



Cloud Access Security Brokers



Enterprise Information Archiving



Endpoint Protection Platforms



Unified Endpoint Management Tools

\*Gartner "Magic Quadrant for Access Management," by Michael Kelley, Abhyuday Data, Henrique, Teixeira, August 2019

\*Gartner "Magic Quadrant for Cloud Access Security Brokers," by Steve Riley, Craig Lawson, October 2019

\*Gartner "Magic Quadrant for Enterprise Information Archiving," by Julian Tirsu, Michael Hoech, November 2019

\*Gartner "Magic Quadrant for Endpoint Protection Platforms," by Peter Firstbrook, Dionisio Zumerle, Prateek Bhajanka, Lawrence Pingree, Paul Webber, August 2019

\*Gartner "Magic Quadrant for Unified Endpoint Management Tools," by Chris Silva, Manjunath Bhat, Rich Doheny, Rob Smith, August 2019

These graphics were published by Gartner, Inc. as part of larger research documents and should be evaluated in the context of the entire documents. The Gartner documents are available upon request from Microsoft. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally, and is used herein with permission. All rights reserved.

# Complexity is the enemy of intelligent security

**70** from **35**

Security products      Security vendors

Is the average for companies  
with over 1,000 employees

[Nick McQuire, VP Enterprise Research CCS Insight.](#)

**\$1.37M**

On average that an  
organization spends annually  
in time wasted responding to  
erroneous malware alerts

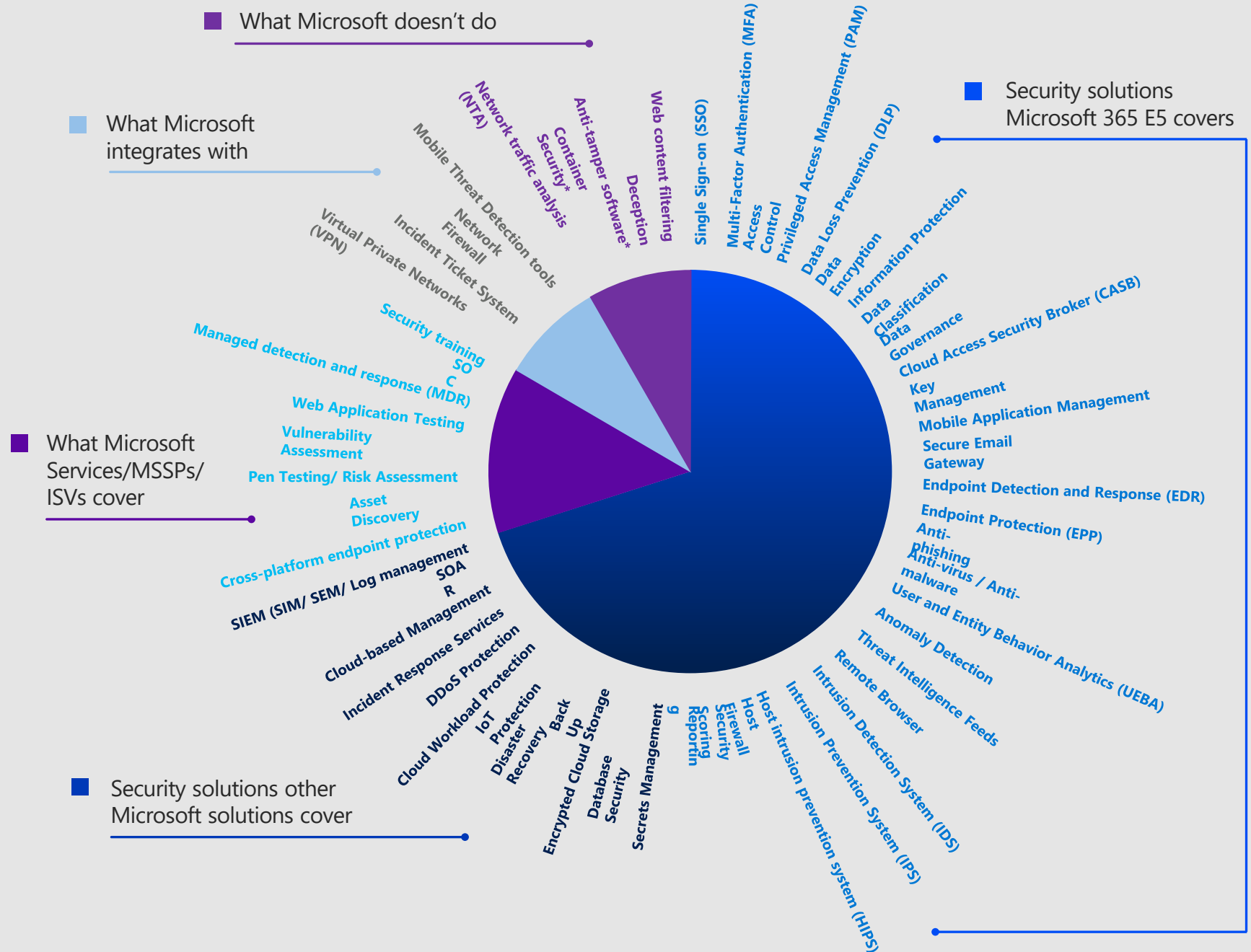
["The Cost of Insecure Endpoints" Ponemon Institute©  
Research Report, June 2017](#)

**1.87M**

Global cybersecurity  
workforce shortage by 2022

[Global Information Security Workforce Study 2017](#)

# Customers that have Microsoft 365 E5 Security can replace up to 26 other security vendors



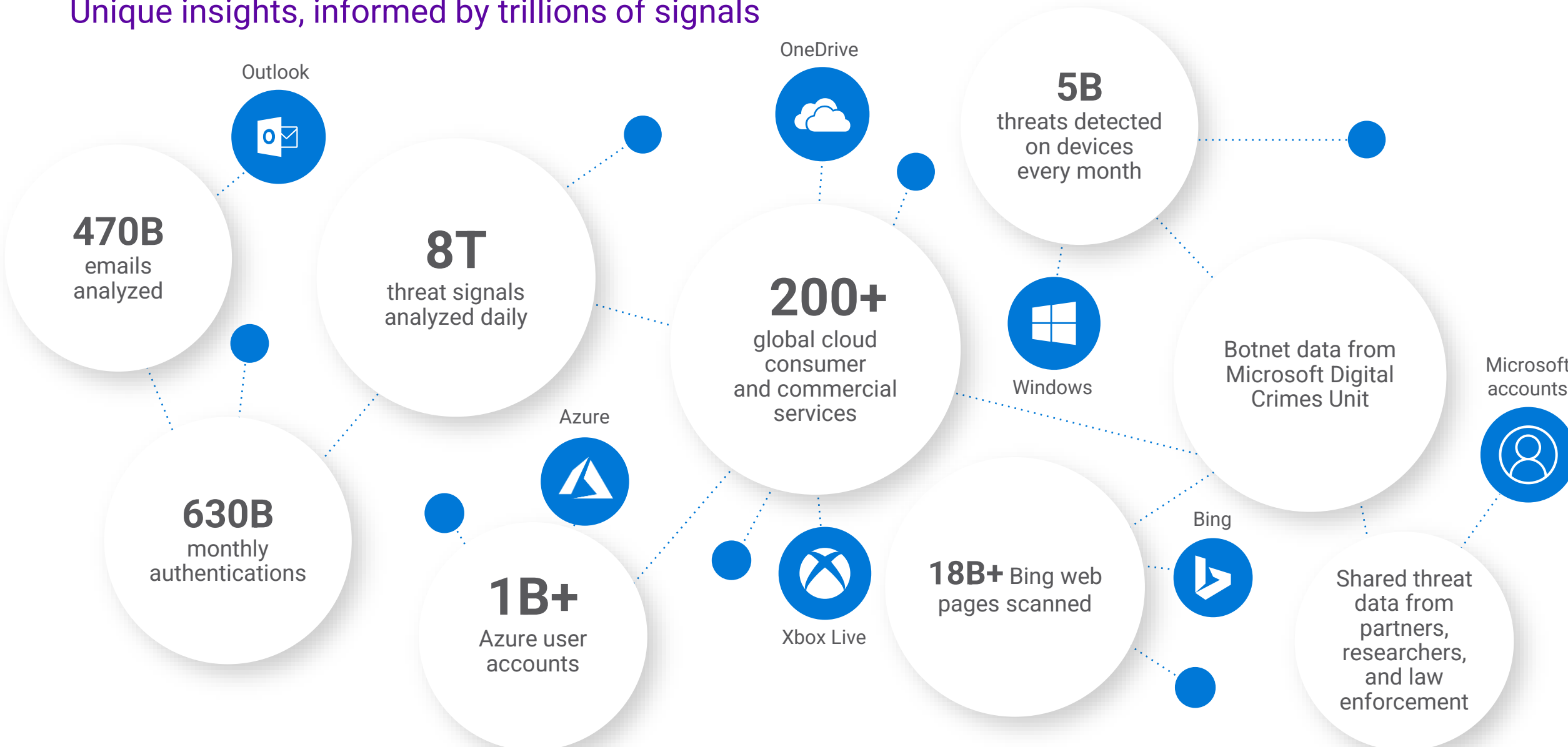
# Microsoft Intelligent Security Association





# Microsoft Intelligent Security Graph

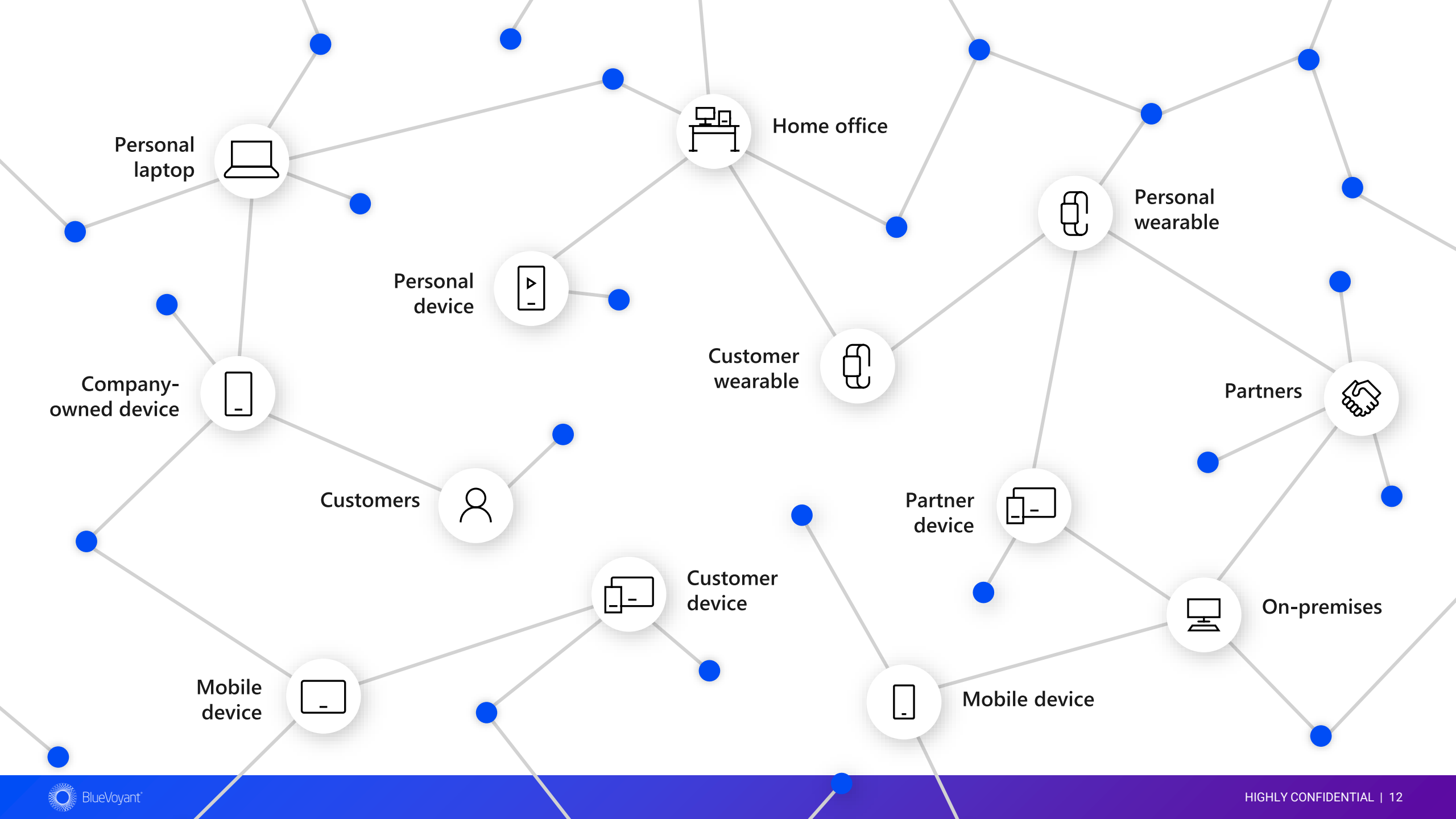
Unique insights, informed by trillions of signals

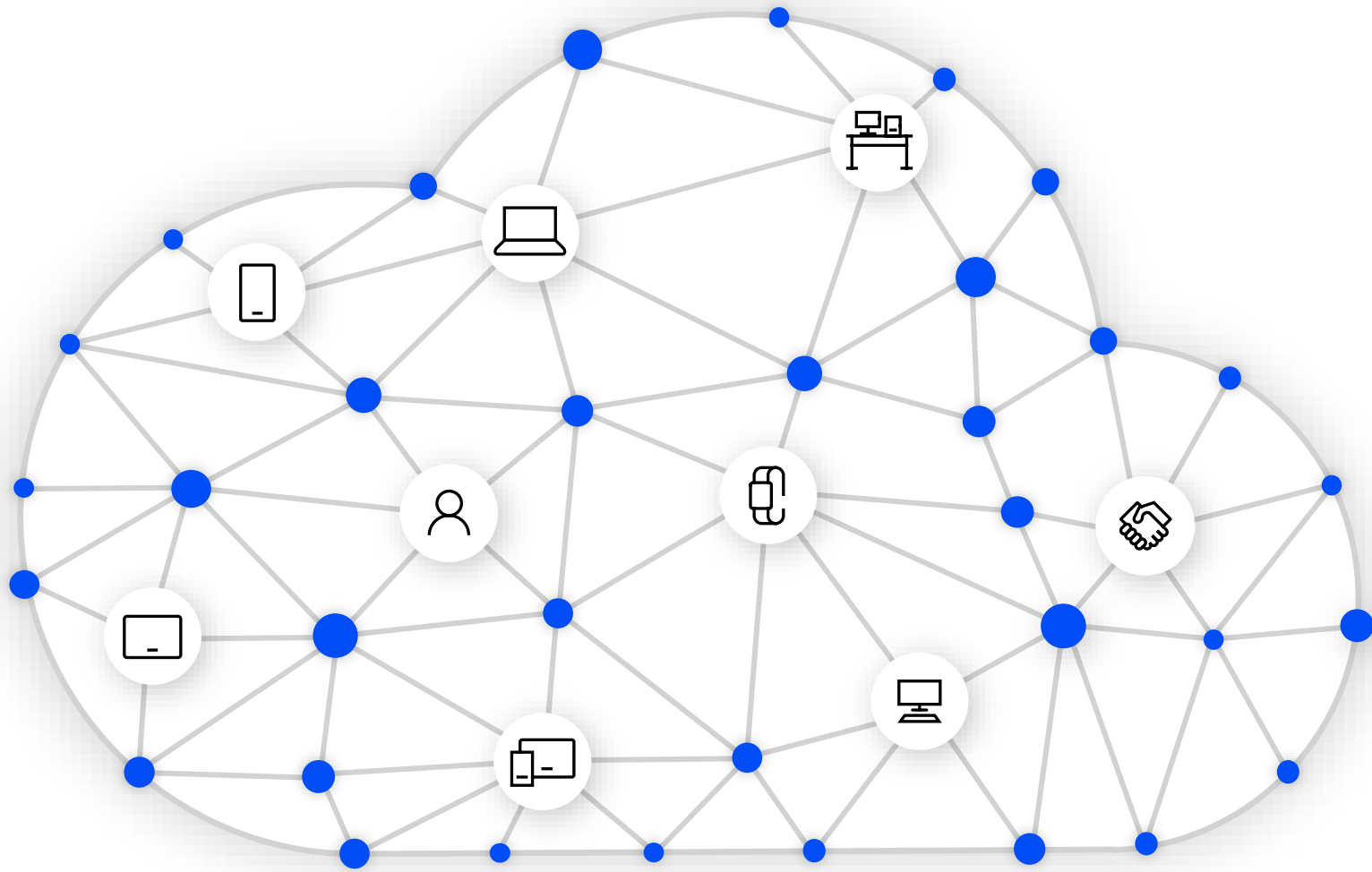


# M365 E5 License: Where to start your licensing journey

IDENTITY

# Why is Identity in the Cloud so important?



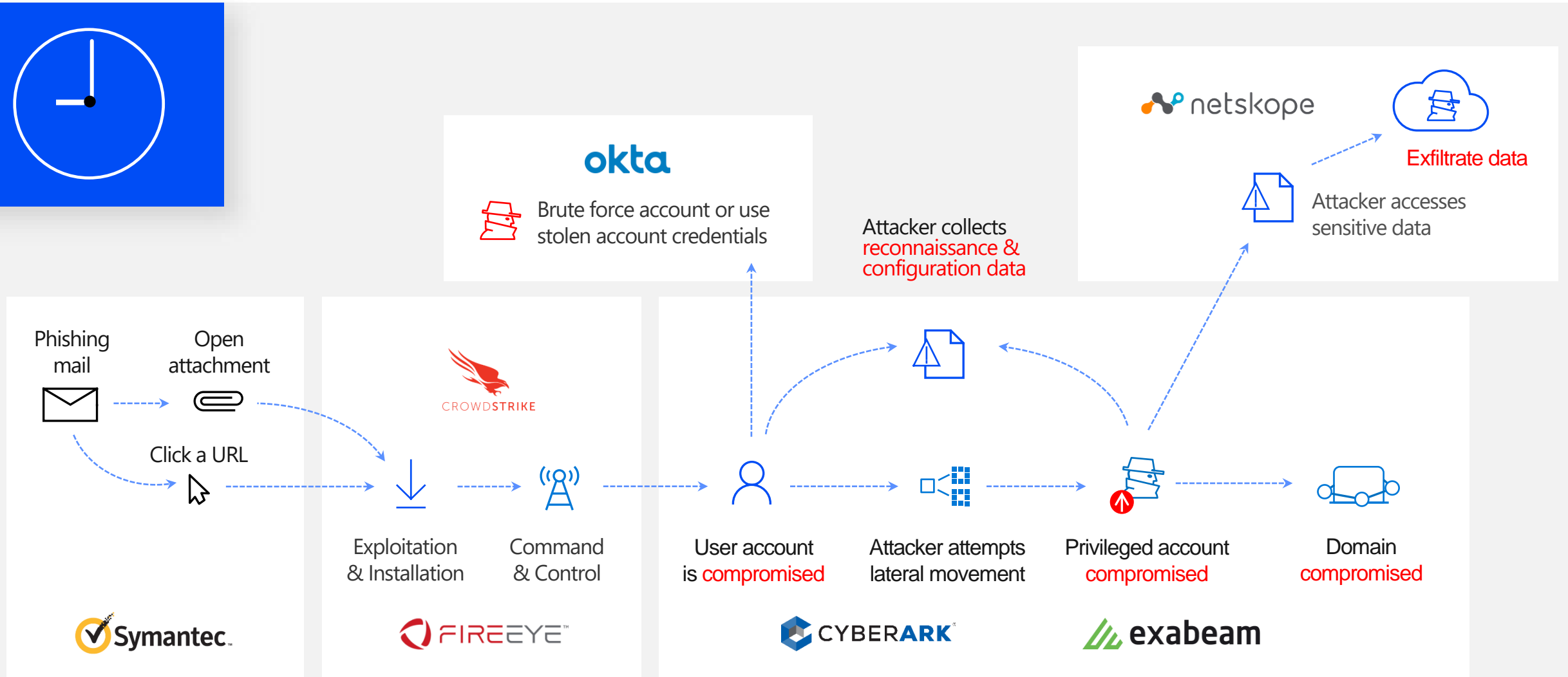


**“The future of cybersecurity...is in the cloud.”<sup>1</sup>**

<sup>1</sup> <https://go.forrester.com/blogs/tech-titans-google-and-microsoft-are-transforming-cybersecurity/>

How do I bridge my Identity solutions between  
on prem and cloud?

# Vendor complexity across the attack kill chain



# M365 Defender: Maximize Detection During Attack Stages

## Microsoft Defender for Office 365

Safeguards against malicious threats posed by email messages, links (URLs) and collaboration tools

Phishing mail



Opens attachment

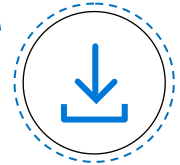


Clicks on a URL



User browses to a website

Exploitation & Installation



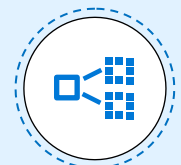
Command & Control



User account is compromised



Attacker attempts lateral movement



Privileged account compromised



Domain compromised



Attacker accesses sensitive data



Exfiltrate data



## Azure AD Identity Protection

Identity protection & conditional access



Brute force account or use stolen account credentials

## Microsoft Defender for Endpoint

Endpoint Detection, Protection and Response

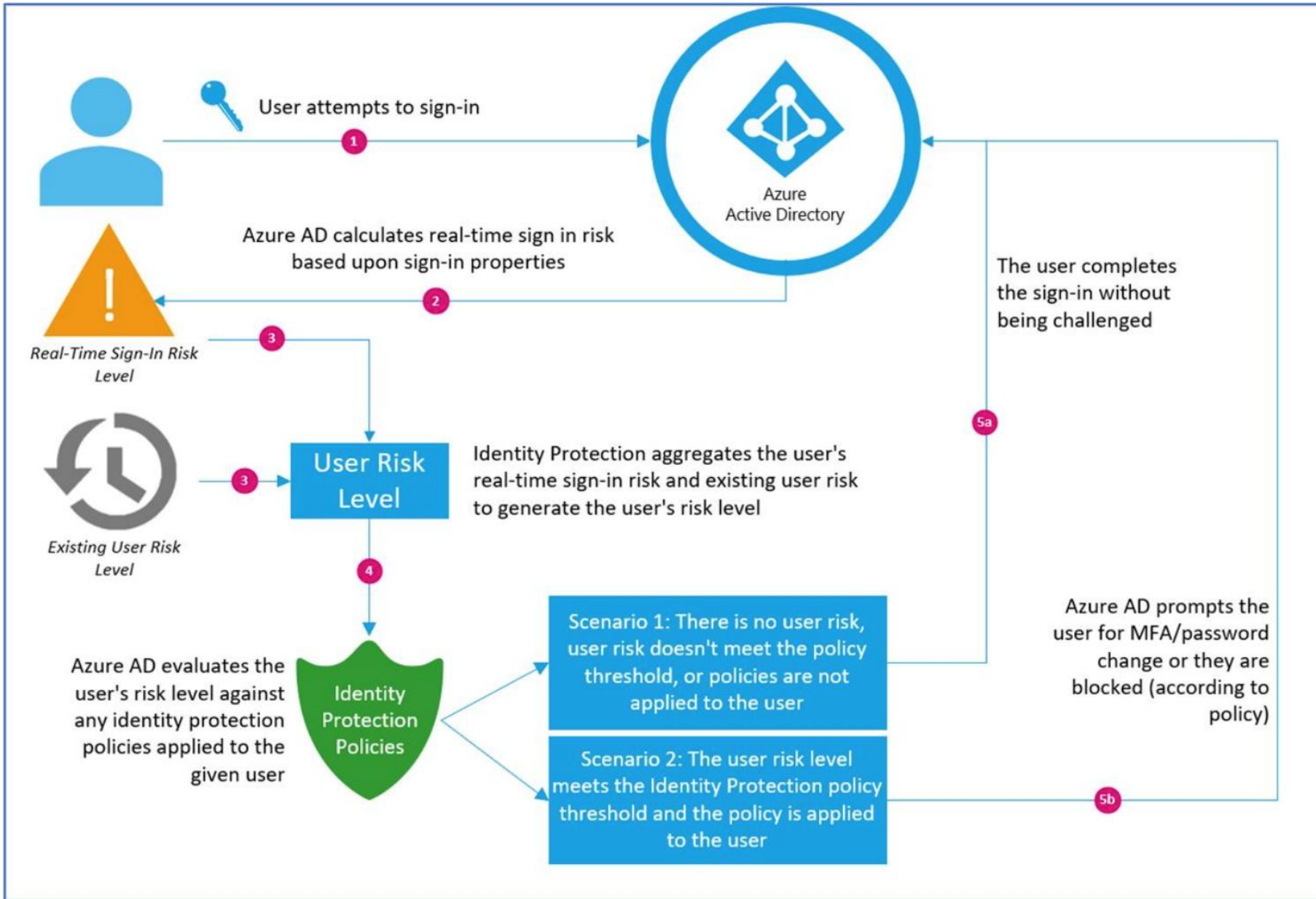
## Microsoft Defender for Identity

## Cloud App Security

Extends protection & conditional access to other cloud apps

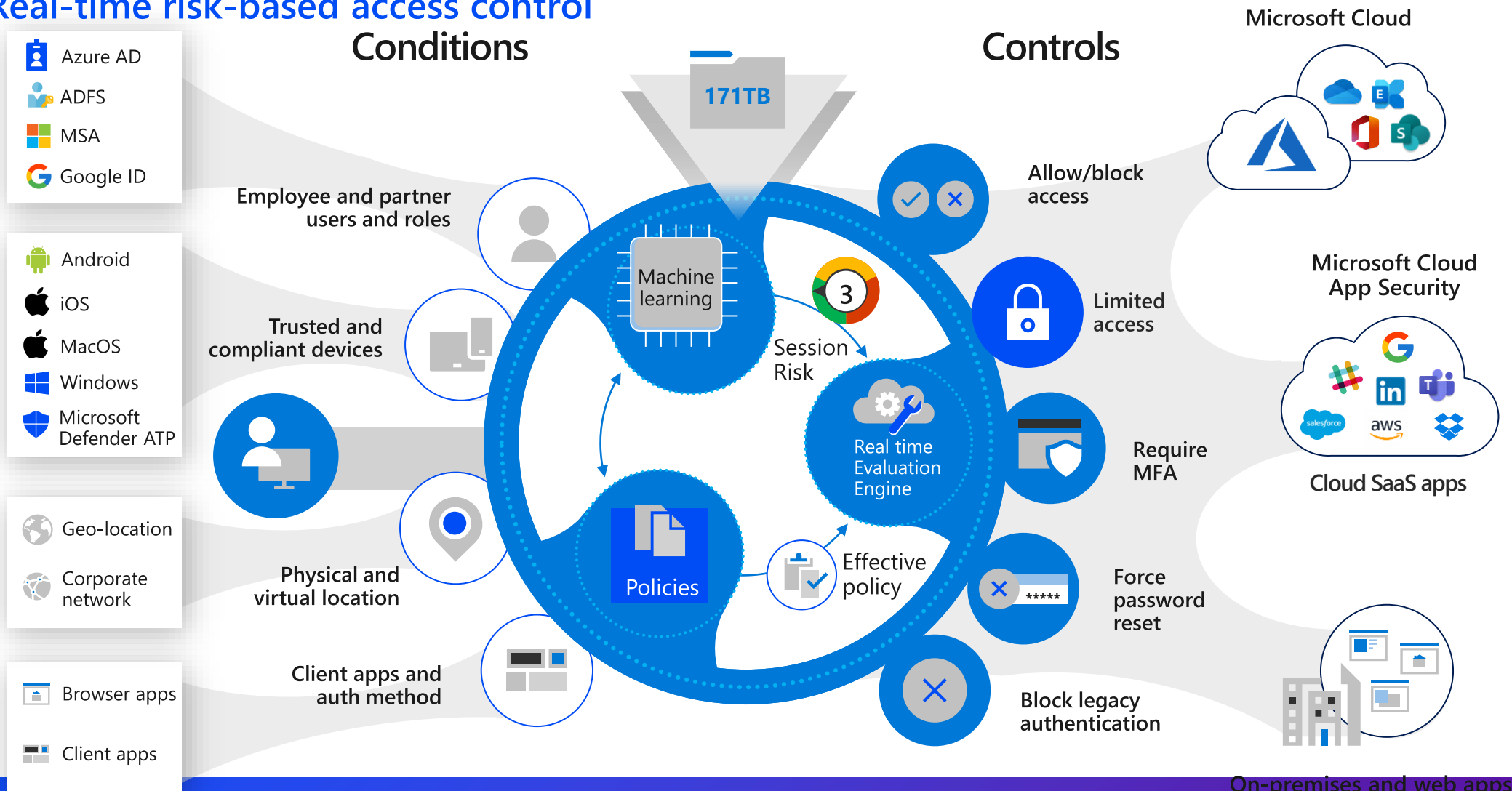


Where is the best place to start?



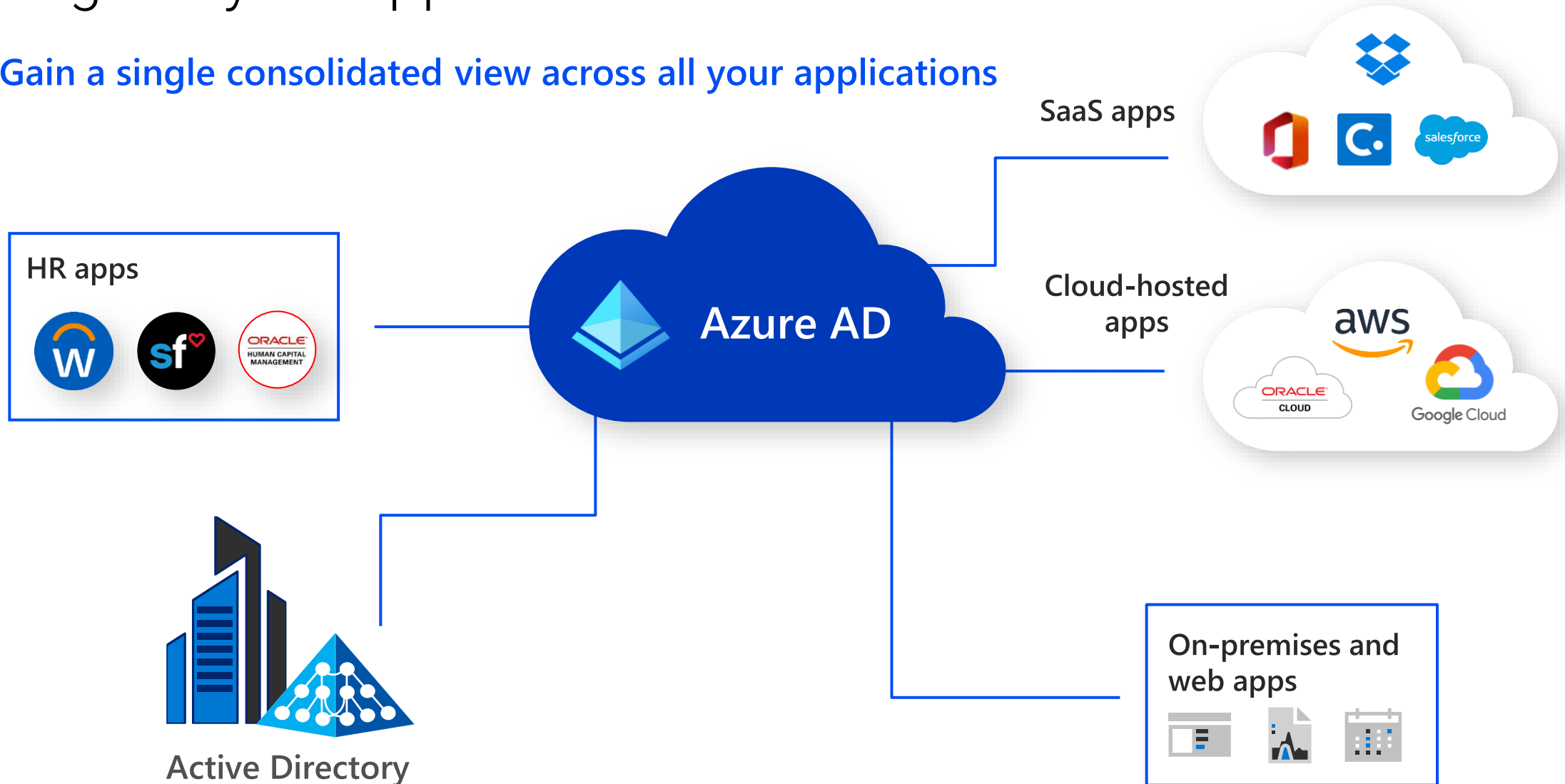
# Conditional Access + Identity Protection

- Real-time risk-based access control

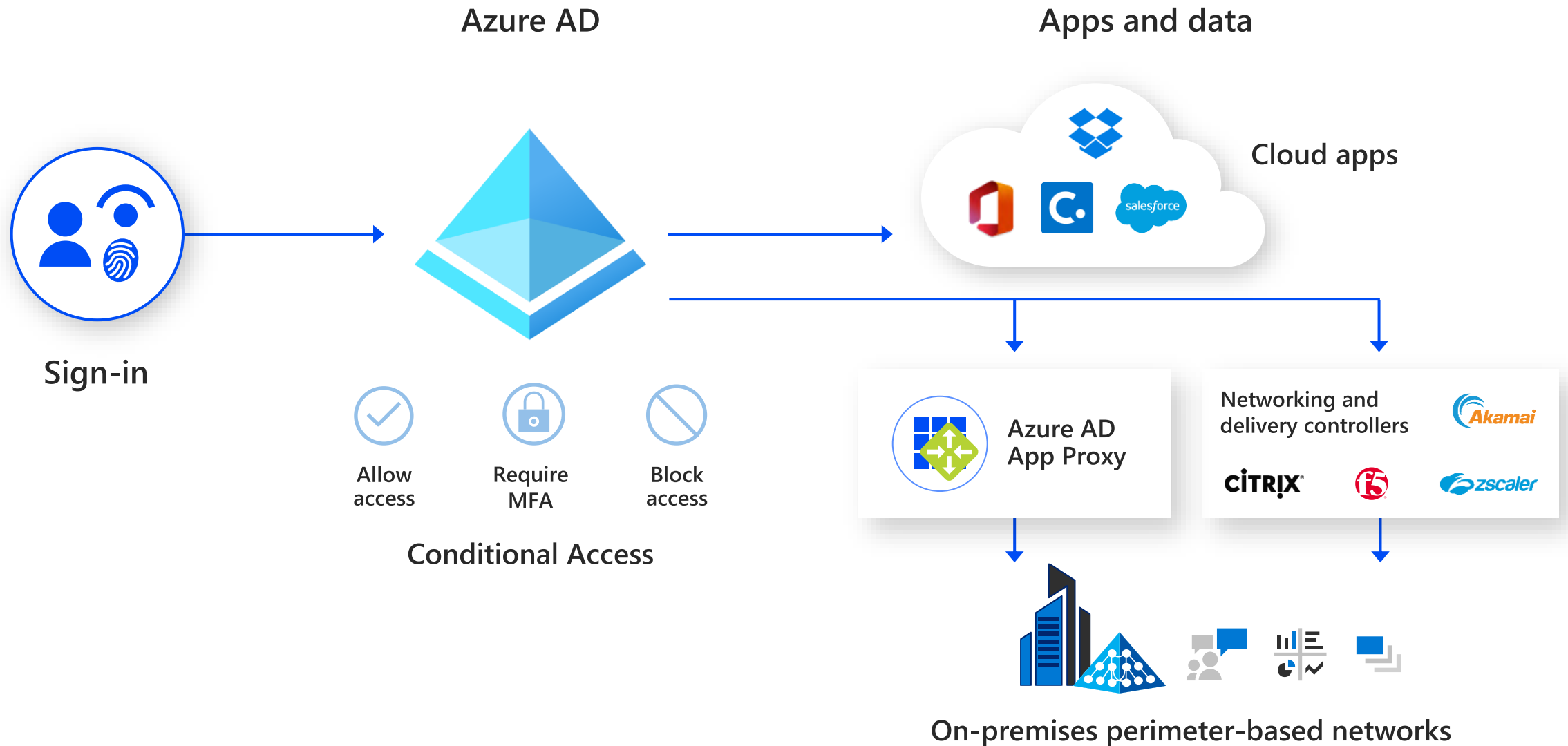


# Manage all your apps from one central location

- Gain a single consolidated view across all your applications



# Deliver consistent single sign-on experiences to legacy apps



Go beyond Microsoft Office—connect and secure *any* app to Azure AD

**2,000,000**  
active apps

**> 250m**

Azure AD  
monthly active  
users



# M365 E5 License: Where to start your licensing journey

DATA

Do you feel like organizations should have more urgency around Information Protection Solutions?



# GDPR challenges

Personal privacy rights

Must protect data

Mandatory data breach reporting

Big penalties for non-compliance



## Personal data

Any information related to an identified or identifiable natural person including direct and indirect identification.

Examples include:

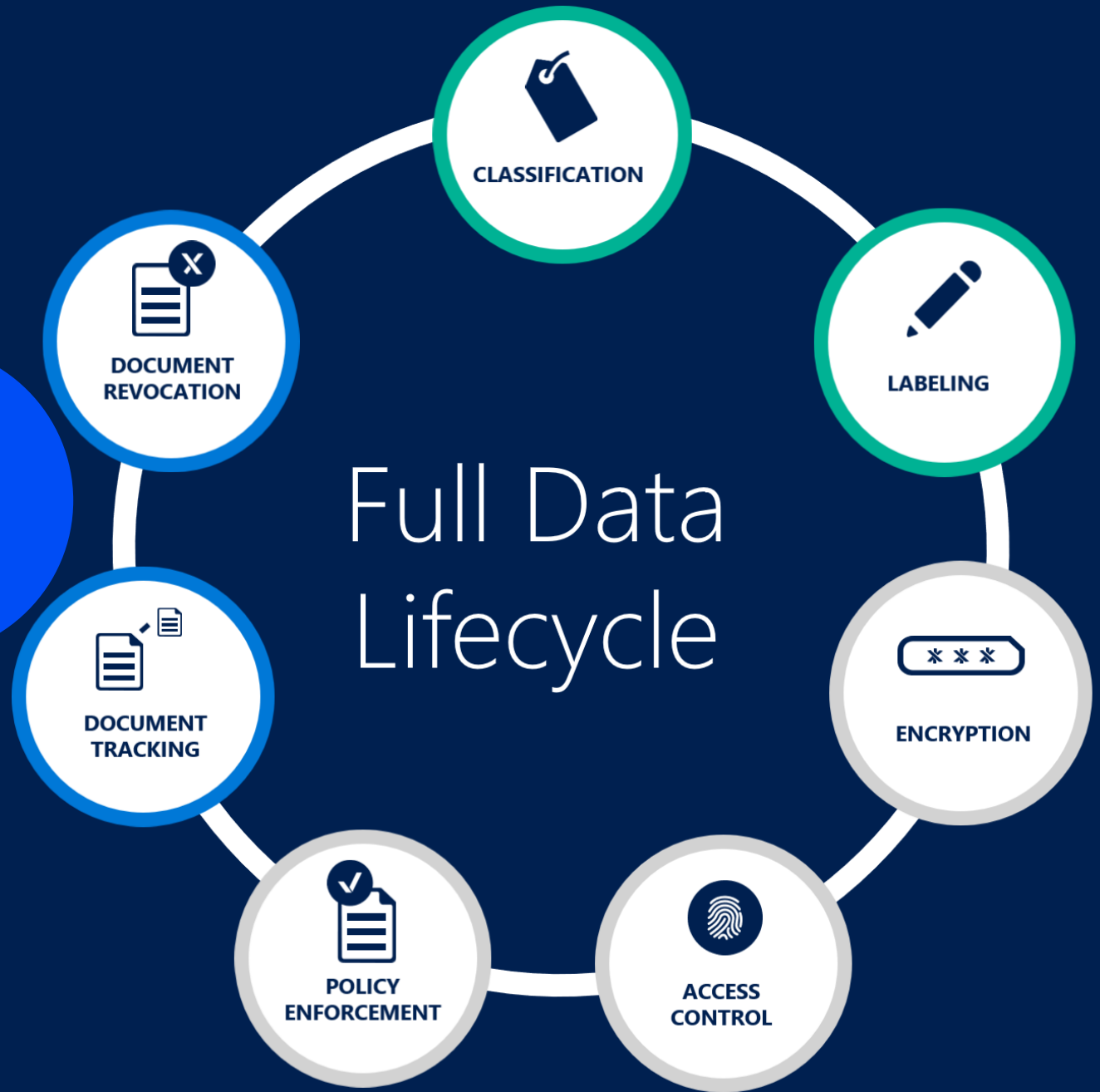
- Name
- Identification number (e.g., SSN)
- Location data (e.g., home address)
- Online identifier (e.g., e-mail address, screen names, IP addresses, device IDs)



## Sensitive personal data

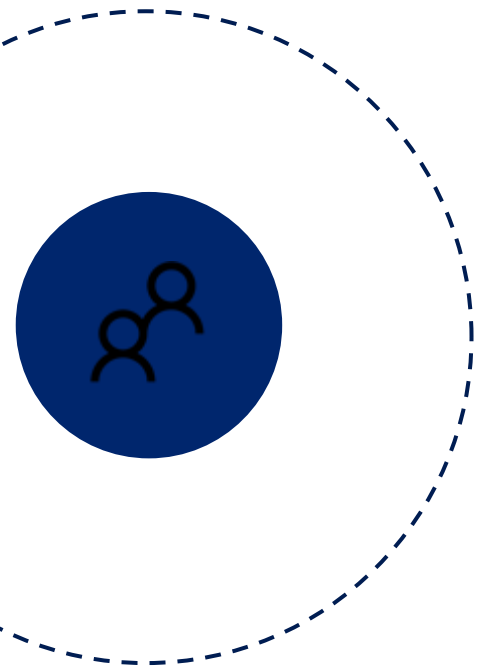
Personal data afforded enhanced protections:

- Genetic data (e.g., an individual's gene sequence)
- Biometric Data (e.g., fingerprints, facial recognition, retinal scans)
- Sub categories of personal data including:
  - Racial or ethnic origin
  - Political opinions, religious or philosophical beliefs
  - Trade union membership
  - Data concerning health
  - Data concerning a person's sex life or sexual orientation



What's this unified labeling thing? Microsoft Information Protection can be extended beyond the tenant perimeter?  
Help us catch up on this.

# The Data Lifecycle



Data is created



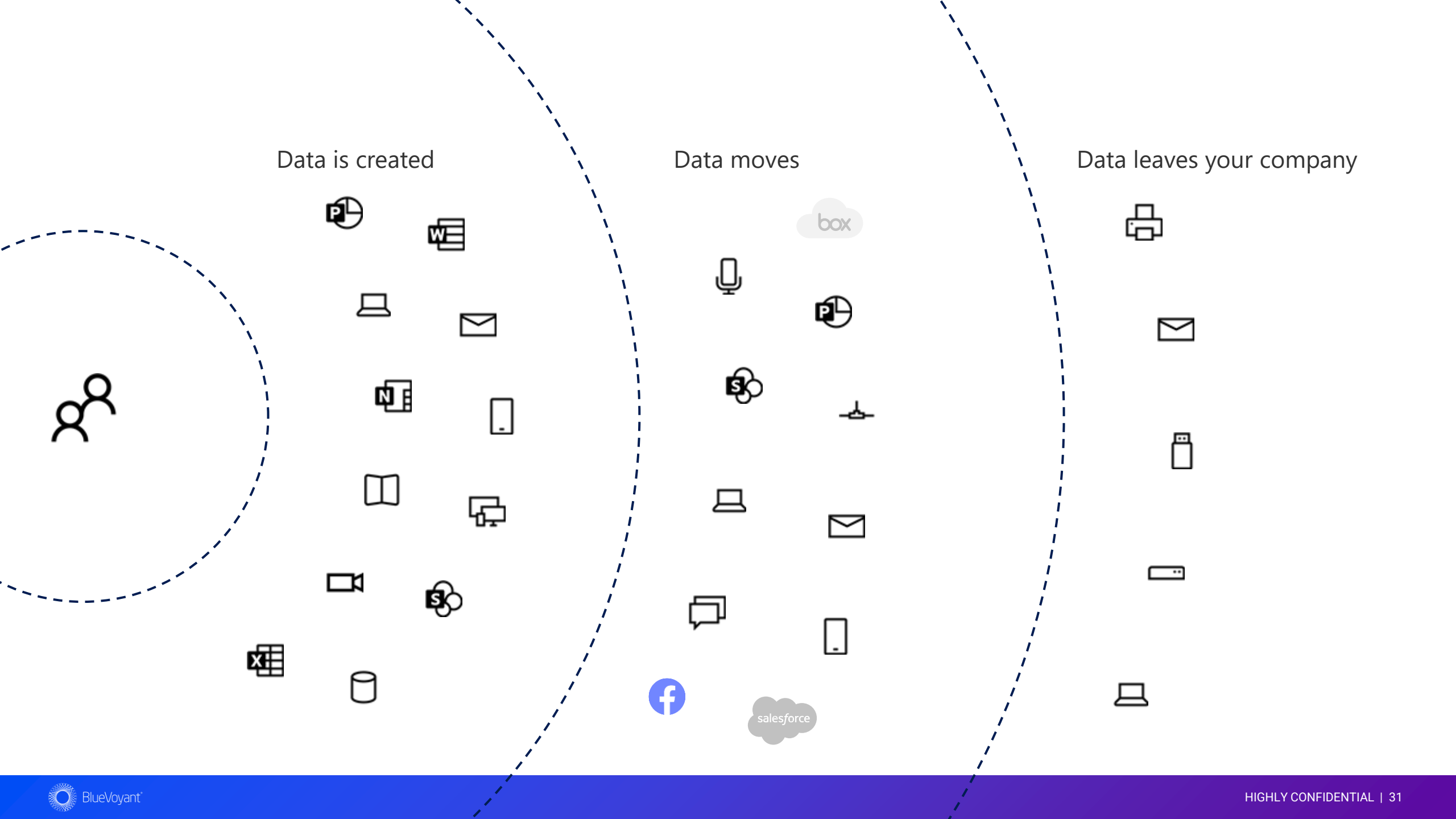


Data is created



Data moves





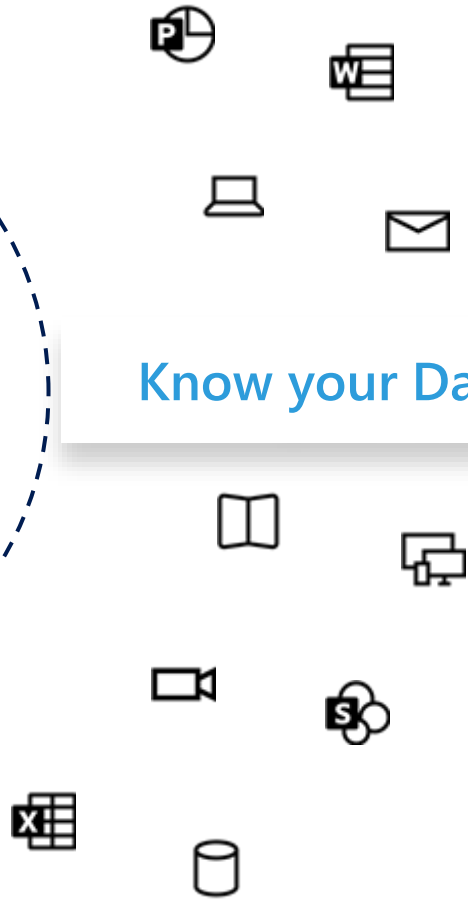
Data is created

Data moves

Data leaves your company

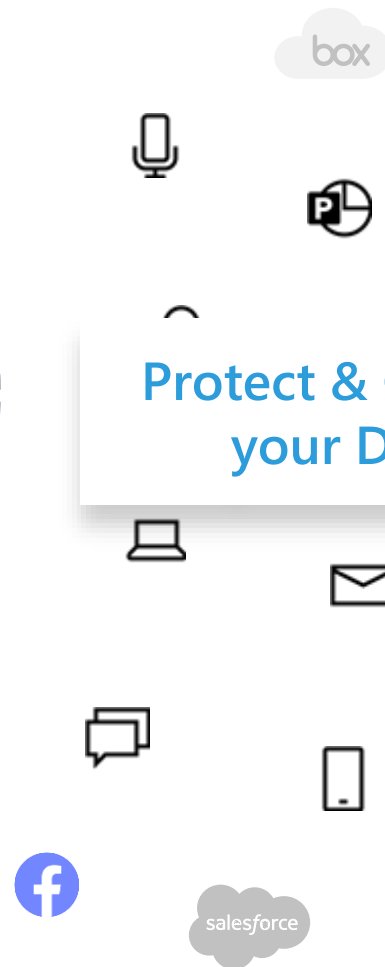


Data is created



**Know your Data**

Data moves



**Protect & Govern your Data**

Data leaves your company



**Prevent Data loss**



File **Message** Developer Help Tell me what you want to do

Ignore Delete Archive Reply Reply All Forward Meeting IM More

Junk

Protect

Done Mark as unread Include in beta Lists

Move Rules OneNote Actions

Assign Policy Mark Unread Categorize

Delete Respond Protection Quick Steps Move Tags

Sensitivity: ■ Confidential \ Recipients Only



Thu 07/05/2018 12:35

Enrique Saggese

Acquisition plans

To Enrique Saggese; esaggese@hotmail.com; john@contoso.com; Herbys68@gmail.com; esaggese@comcast.net

**Do Not Forward** - Recipients can read this message, but cannot forward, print, or copy content. The conversation owner has full permission to their message and all replies.  
Permission granted by: esaggese@microsoft.com

 Contoso Acquisition Plan.docx  
71 KB

Find attached the business acquisition plan we discussed.

The transaction should be complete by November 15<sup>th</sup>.

Regards,

**Enrique Saggese | Principal Program Manager – Customer Experience | Information Protection | Microsoft Corporation | Mobile +1 (425) 894 6696**

Azure Information Protection team Blog: <https://blogs.technet.microsoft.com/enterprisemobility/?product=azure-information-protection>

Visit the Azure Information Protection Web site to learn more! <https://www.microsoft.com/en-us/cloud-platform/azure-information-protection>

So we can apply our Information Protection Schemes outside of the Microsoft cloud. What about directing that same protection to on prem? Endpoints?



# Discover and classify sensitive information

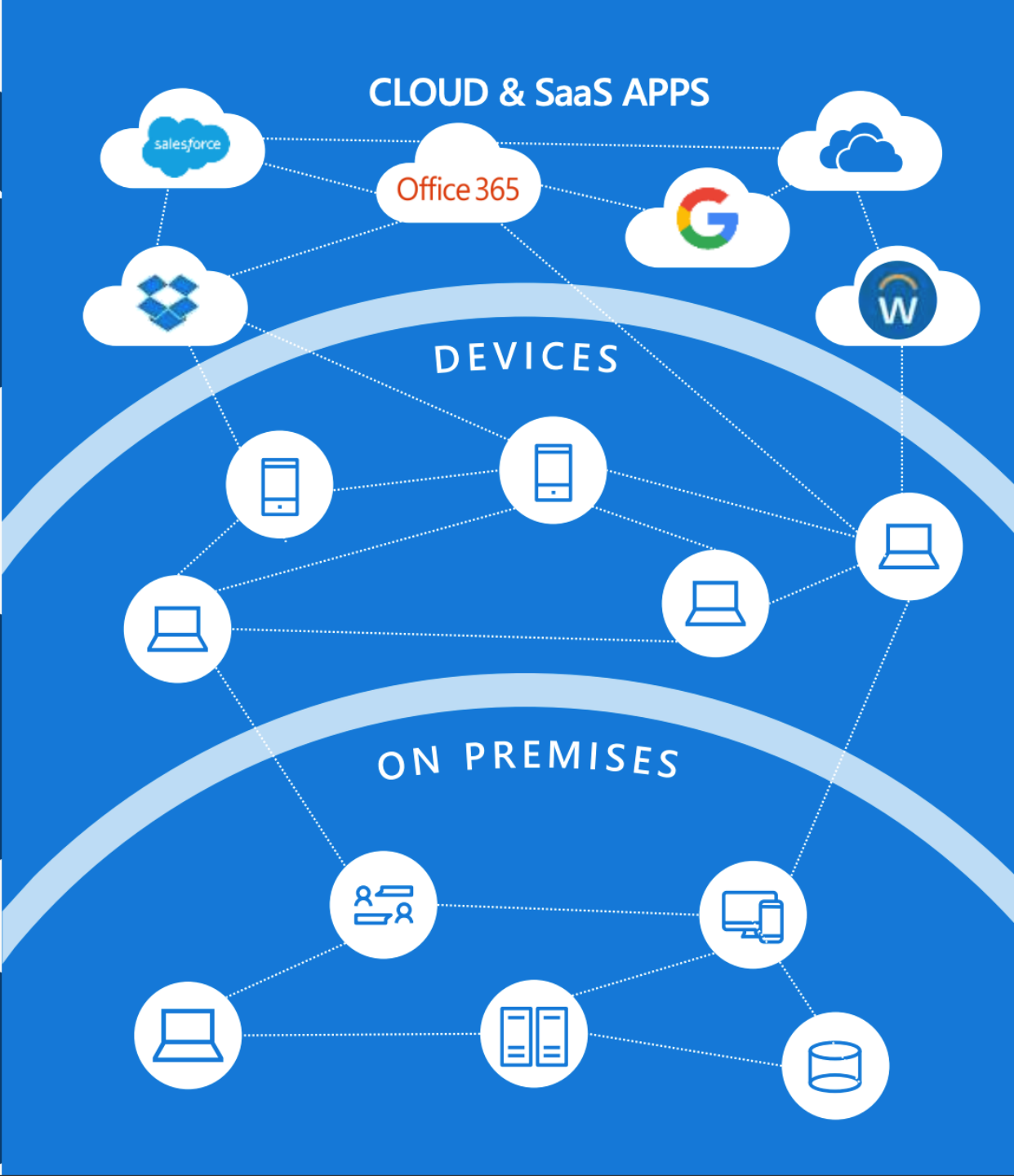
No matter where it's created, modified or shared



Office 365,  
Microsoft  
Cloud App  
Security

Office apps,  
Windows  
Information  
Protection

AIP  
scanner



# Azure Information Protection scanner capabilities



Scans **on-prem** repositories: file shares, NAS or any other CIFS based repositories, or SharePoint Server



Discover data in the scanned repositories and match it against AIP policy (detect sensitive info types, custom patterns and default label)



Labels and protects the discovered data per AIP policy



Create a report of discovered data, including the matched conditions for found patterns

Home > Azure Information Protection - Data discovery (Preview)

**Azure Information Protection - Data discovery (Preview)**

Search (Ctrl+F)

Log Analytics

Location type: Any

Apply

**Labels**

329

LOCATION TYPE	LOCATION
File repository	\\sislands\public\
Endpoint	W10-IW-CLIENT1
Endpoint	W10-IW-CLIENT2

General

Quick start

Dashboards

- Usage report (Preview)
- Activity logs (Preview)
- Data discovery (Preview)**

Classifications

- Labels
- Policies

Manage

- Configure analytics (Preview)
- Languages
- Protection activation

Windows Defender Security Center

jonathanw-pc

cont-jonathanw

Laptop North America

Machine details

Risk level: **High**

Domain: Contoso

OS: Windows 10 64-bit

Network activity

First seen: 09/15/2017 12:00

Last seen: 03/15/2018 13:30

Information protection

Data sensitivity: Confidential

See files in Azure Information Protection

Collect investigation package Run AV scan Restrict app execution Isolate machine Manage tags Action center

**Active alerts (6)**

High 0 Medium 0 Low 0 Info... 0

See all alerts

**Logged on users (12)**

Most frequent: Jonathan Wolcott

Least frequent: Eva Macias

See all users

**Secure score**

900 of 1000

2 security controls require attention

Manage score

Timeline Related alerts (6)

Search in machine timeline All event types All user accounts Display Export

03/15/2018 13:29

Dec 2017 Jan 2018 Feb 2018 Mar 2018 Apr 2018

Date/time	Event	Details	User
13:29:32	chrome.exe created document.pdf	explorer.exe > chrome.exe > document.pdf	Jonathan Wolcott

explorer.exe

explorer.exe

chrome.exe

chrome.exe

036c56034539719cecc1353bd641b6c2584411a0

C:\Program Files (x86)\Google\Chrome\Application\chrome.exe

"chrome.exe"

Document.pdf

b7dd479039a6885d77eef8020e59513f32983b5e

C:\Users\Jonathan\Downloads\Document.pdf

Confidential

Information Protection Integration with Microsoft Information Protection for sensitive data discovery and enforcement on endpoints

# Cloud Discovery

Continuous report Win10 Endpoint Users Timeframe Last 90 days

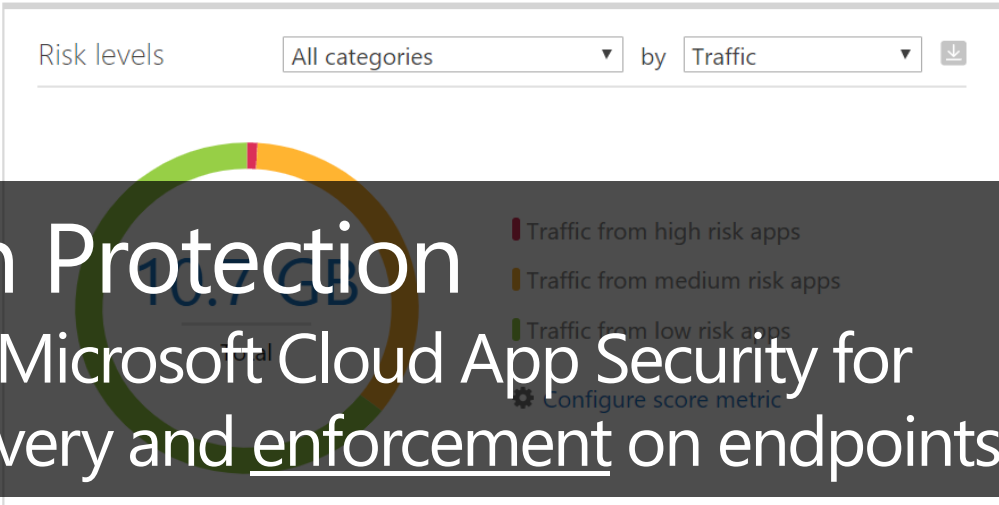
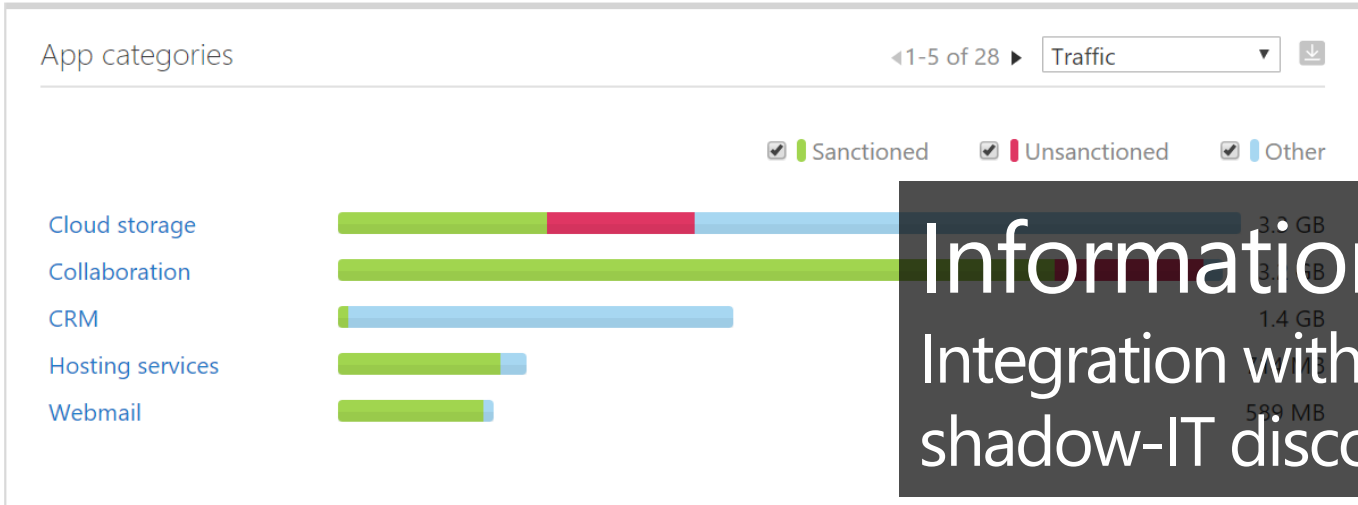
- Dashboard
- Discovered apps
- IP addresses
- Users
- Machines

Updated on Jul 18, 2018

Apps: 128 IP addresses: 2458 Users: 1113 Machines: 1113 Traffic: 10.7 GB ↑ 7.2 GB ↓ 3.5 GB

Cloud Discovery open alerts [+ Create policy](#)

48 Cloud Discovery alerts      0 Suspicious use alerts



**Information Protection**  
Integration with Microsoft Cloud App Security for shadow-IT discovery and enforcement on endpoints

### Discovered apps

Sanctioned    Unsanctioned    Other

App	Traffic
Microsoft Dynamics	1.4 GB
Microsoft SharePo...	1.3 GB
Microsoft Teams	909 MB
Amazon Web Serv...	648 MB

### Top entites

User	Total
CONTOSO/Bob	306 MB
CONTOSO/Chaya	44 MB
CONTOSO/Sloane	40 MB
CONTOSO/M/...	10 MB

Where are the central points that I can manage  
Information policy?

# Microsoft 365 Specialized Workspaces

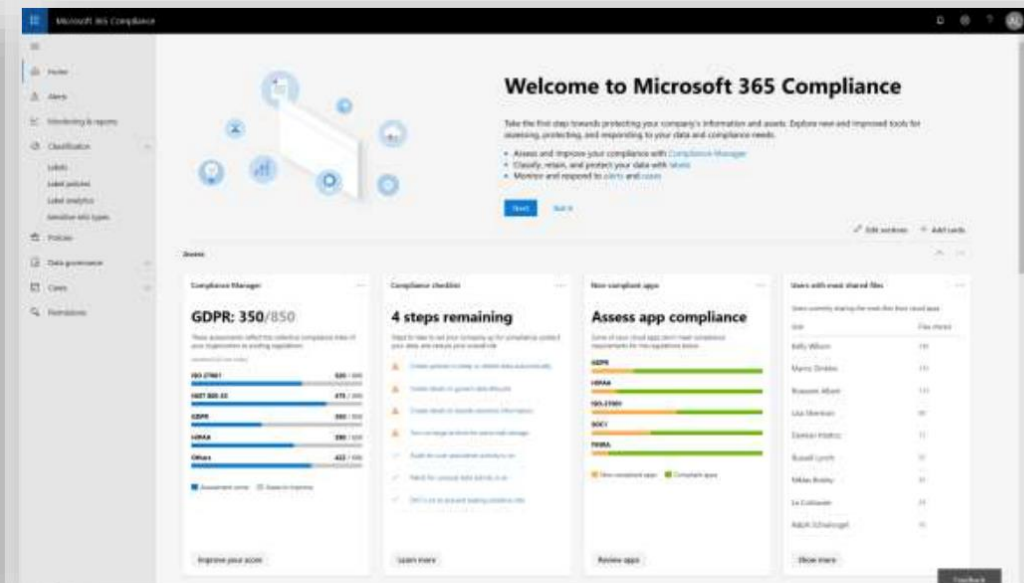
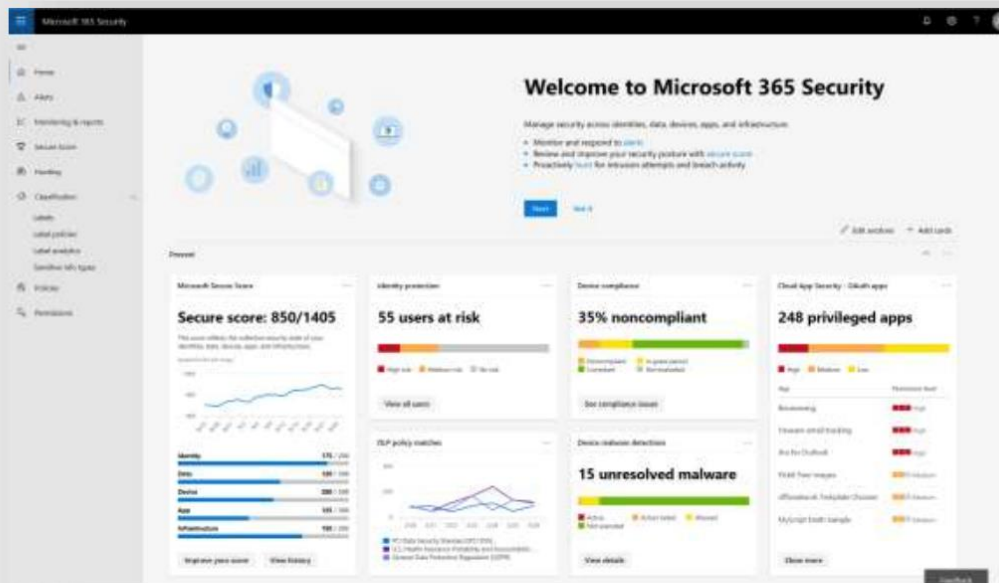
## Microsoft 365 Security Center

security.microsoft.com



## Microsoft 365 Compliance Center

compliance.microsoft.com

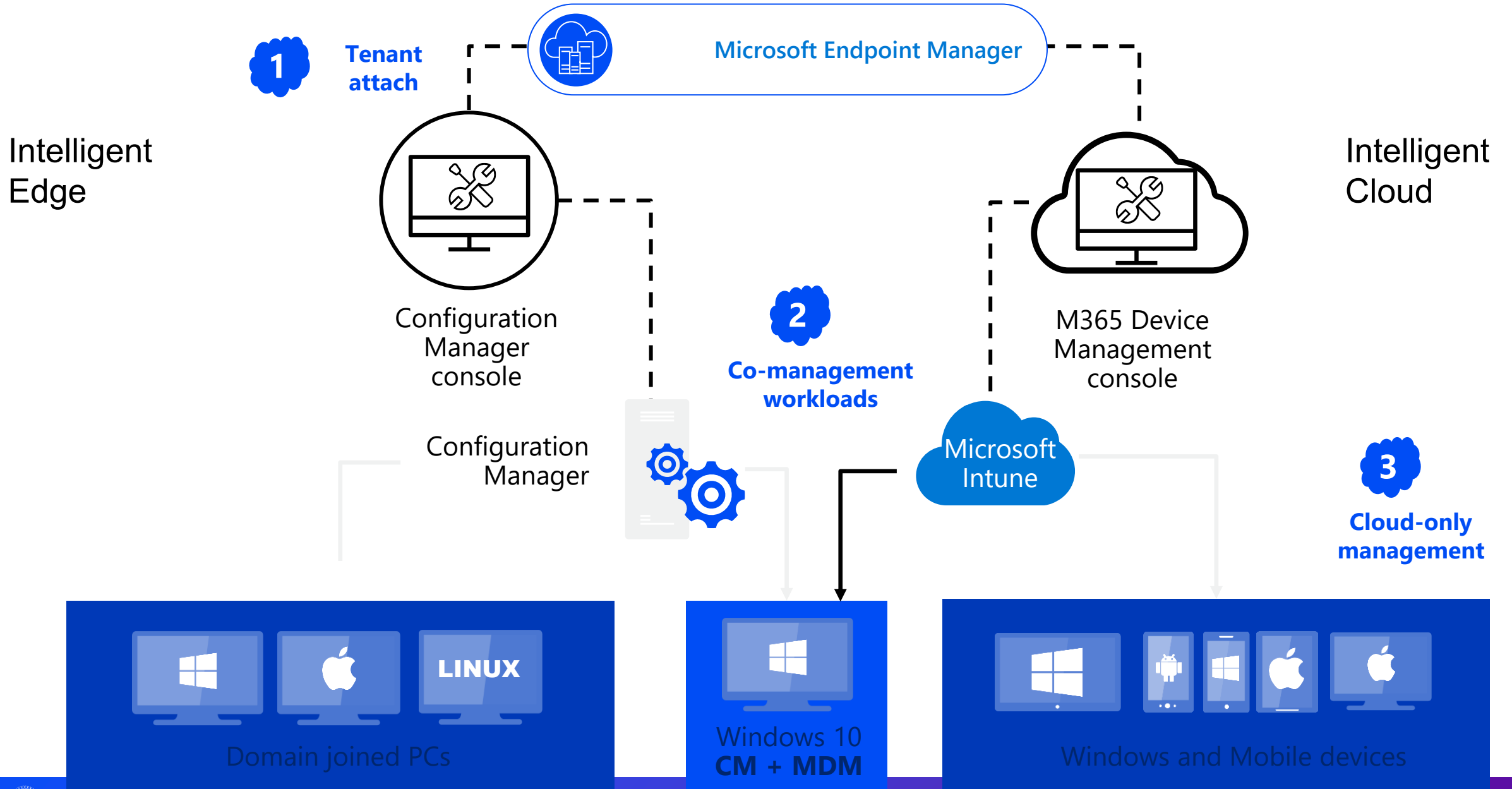




# M365 E5 License: Where to start your licensing journey

## DEVICES

What's the story with SCCM and Intune? Is SCCM here to stay?



Does Endpoint Manager play a role in the Zero Trust story?  
If so, how?

# Zero Trust Principles



## Verify Explicitly

Always authenticate and authorize based on all available data points, including user identity, location, device health, data classification, and anomalies.



## Least Privilege

Minimize user access with Just-In-Time and Just-Enough Access (JIT/JEA), risk-based adaptive policies, and data protection which protects data and productivity.








## Assume Breach

Minimize scope of breach damage and prevent lateral movement by segmenting access via network, user, devices and application awareness. Verify all sessions are encrypted end to end. Use analytics to get visibility and drive threat detection.

Talk to us about Imaging vs Management  
What's the story around Zero Touch provisioning?

# Zero touch provisioning

Streamlined and flexible provisioning of all your devices with Microsoft Endpoint Manager

-  Decrease costly image creation workload
-  Self-service provisioning directly by end users
-  Faster time to productivity
-  Out of the box security
-  Lower OPEX for staying current



Windows Autopilot



Apple Business Manager



Android Enterprise  
Zero Touch



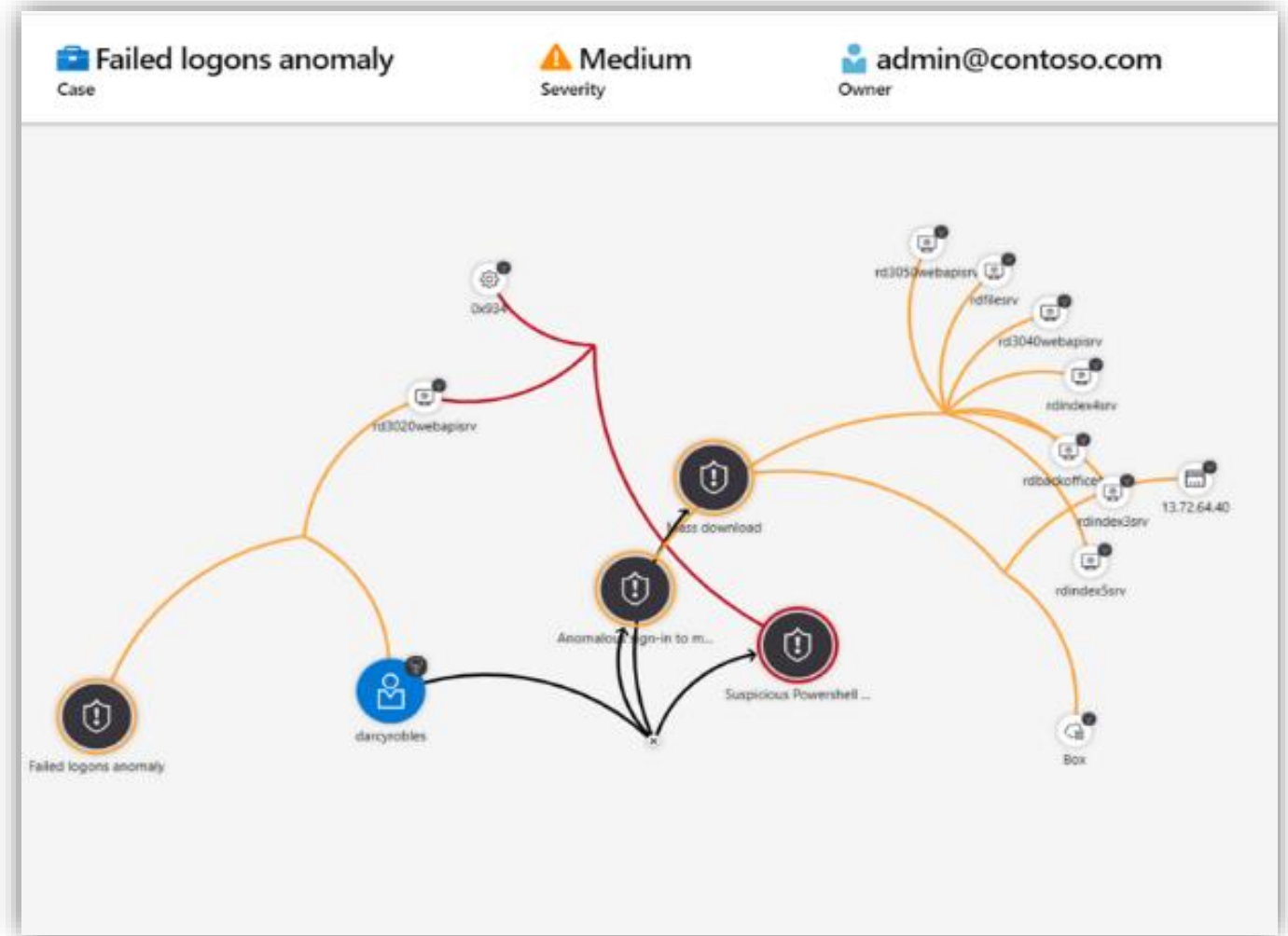
Samsung Knox  
Mobile Enrollment

We can't talk about Endpoints without covering Defender for Endpoint. What kind of adoption are we really seeing in all levels of the marketplace?



# Investigate threats with AI and hunt suspicious activities at scale

- Get prioritized alerts and **automated expert guidance**
- **Visualize** the entire attack and its impact
- Hunt for suspicious activities using **pre-built queries**



Prevention

### Microsoft Secure Score

**Secure score: 417 / 1000**

Microsoft Secure Score monitors the security state of your company's devices, data, identities, apps, and Azure resources.

Category	Score	Total
Devices	300	520
Data	40	230
Identity	36	100
Apps	21	150
Infrastructure	20	100

[Improve your security state](#) [View history](#)

### Device compliance

**68% devices compliant**

Of your 190k enrolled devices, 68% are compliant with the device compliance policies you created. Updated 6:20pm today

[View details in Device Management Admin Console](#)

### Device malware state

**85 unresolved threats**

Of detections by Windows Defender Antivirus in the last 24 hours: Updated 6:20pm today

[View details](#)

### Email protection overview

Malicious email content blocked by Office Advanced Threat Protection in the past 30 days. Updated 6:20pm today

**8067 Phishing blocked**  
**1272 Malware blocked**

[View details in Office 365 Security & Compliance Center](#)

### Identity protection overview

For accounts protected by Azure AD Identity Protection: Updated 6:20pm today

**55 Users flagged for risk**  
**88 Risky sign-in events** in 30 days  
**8 Global admins**

[View details in Azure AD Identity Protection](#)

### Top discovered app categories

**Cloud storage** 200GB  
**Collaboration** 191GB  
**CRM** 185GB  
**Webmail** 170GB

[View all in Cloud App Security](#)

### DLP policy matches

Updated 6:20am today

Legend: Policy 1 (Green), Policy 2 (Cyan), Policy 3 (Blue)

### Infrastructure protection overview

**185 protected resources**


Covered by your Azure Security Center subscription.

- 2 alerts
- 44 recommendations

Detection

### Active Incidents

27 active incidents Updated 6:20 pm today



■ High (4) ■ Medium (16) ■ Low (7)

Incident name	Severity	Last activity
Golden ticket compromise	High	June 18, 2018 11:12 AM
Phishing email campaign detected	High	June 18, 2018 11:10 AM
Suspicious PowerShell Activity	High	June 18, 2018 11:07 AM
Phishing email campaign detected	High	June 18, 2018 10:56 AM
Insider threat identified – sensitive data	Medium	June 18, 2018 10:52 AM
Potential Dofoil activity – malicious C2	Medium	June 18, 2018 10:50 AM
Windows Defender AV detected an active 'Azden' malware	Medium	June 18, 2018 11:12 AM
Windows Defender AV detected 'Reimage' unwanted software	Medium	June 18, 2018 11:11 AM

[Show more](#)

### Identity protection

Users with threat detections

Updated 6:20 pm today

User	Alerts
Jesse Wallin	56
Robin Goolsby	45
Eva Macias	32
Jonathan Wolcott	27
Rex Fredrickson	16
Donovan Eagle	15
Jess Passmore	8
Antoine Hindman	4
Wayne Wallin	2

[Show more](#)

### Device protection

34 devices at risk / 1,254

Updated 6:20 pm today

Device	Risk score
RDP_SRV_10	High
RDP_SRV_5	High
FIN_SRV_HQ	High
DC_SRV_US	High
cont-evamacias	High
cont-jonathanwolcott	High
cont-jesswallin	Medium
RDP_SRV_25	Medium
RDP_SRV_25	Medium

[See more](#)

### Email protection

12 email accounts at risk / 1,022

Updated 6:20 pm today

Email account	User
---------------	------

### Device threat analytics

Assess your defenses against high-profile threats

Updated 6:20 pm today

Get interactive reports on Windows Defender ATP about emerging threats

Spectre and Meltdown	23 active/132
Advanced Trojan Outbreak	16 active/182
NotPetya	13 active/254
Black Energy	13 active/142

### Threat News

- "BadKitten" - New threat in town**  
Check organization vulnerability
- Start hunting!**  
GitHub shared new query

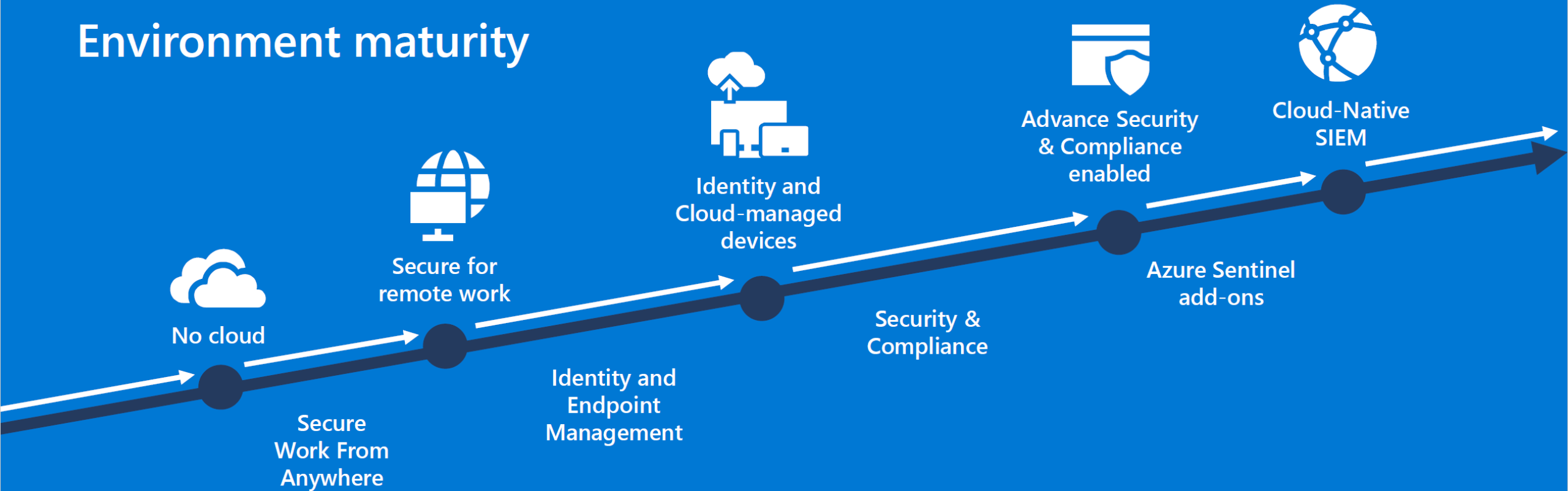
# M365 E5 License: Where to start your licensing journey

## NEXT STEPS

Join us for the next webinar on Azure Sentinel first week of June!

# Where are you at on your timeline?

## Environment maturity



# BlueVoyant Modern SOC and Microsoft

BlueVoyant's Modern SOC provides enterprises a complete portfolio of Microsoft security focused services, including a customized deployment of Microsoft security tools, ongoing platform care & maintenance and 24/7 security operations as a service. BlueVoyant is uniting Managed Detection and Response (MDR) with Microsoft® Azure Sentinel and Microsoft's® XDR solution.



Reach out to your Cadre rep and **schedule a 60 minute** cloud maturity assessment or reach us at [info@cadre.net](mailto:info@cadre.net)



With BlueVoyant's Microsoft security consulting and deployment services, you don't need to be an expert to take your security and compliance posture to the next level. Our Accelerator services are designed to get you up and running quickly and to maximize your investment in Microsoft Azure Sentinel and 365 Defender security technologies.

## How do I get started?

# Microsoft Security Accelerators from BlueVoyant

Pick one or both of our Accelerator services below. We will perform detailed analysis of your environment(s) and provide actionable security insights. What's included: A detailed assessment of your risks, guidance on how best to leverage Microsoft-powered solutions and/or deployment & configuration assistance based on your unique situation.

### AZURE SENTINEL ACCELERATOR



- Deploy Azure Sentinel in your Azure subscription
- Assist with the installation of Azure Syslog/CEF collector
- Onboard all Microsoft native data sources

### 365 DEFENDER ACCELERATOR



- Deploy:
  - Defender for Endpoint
  - Defender for Identities
  - Defender for Office 365
  - Microsoft Cloud App Security