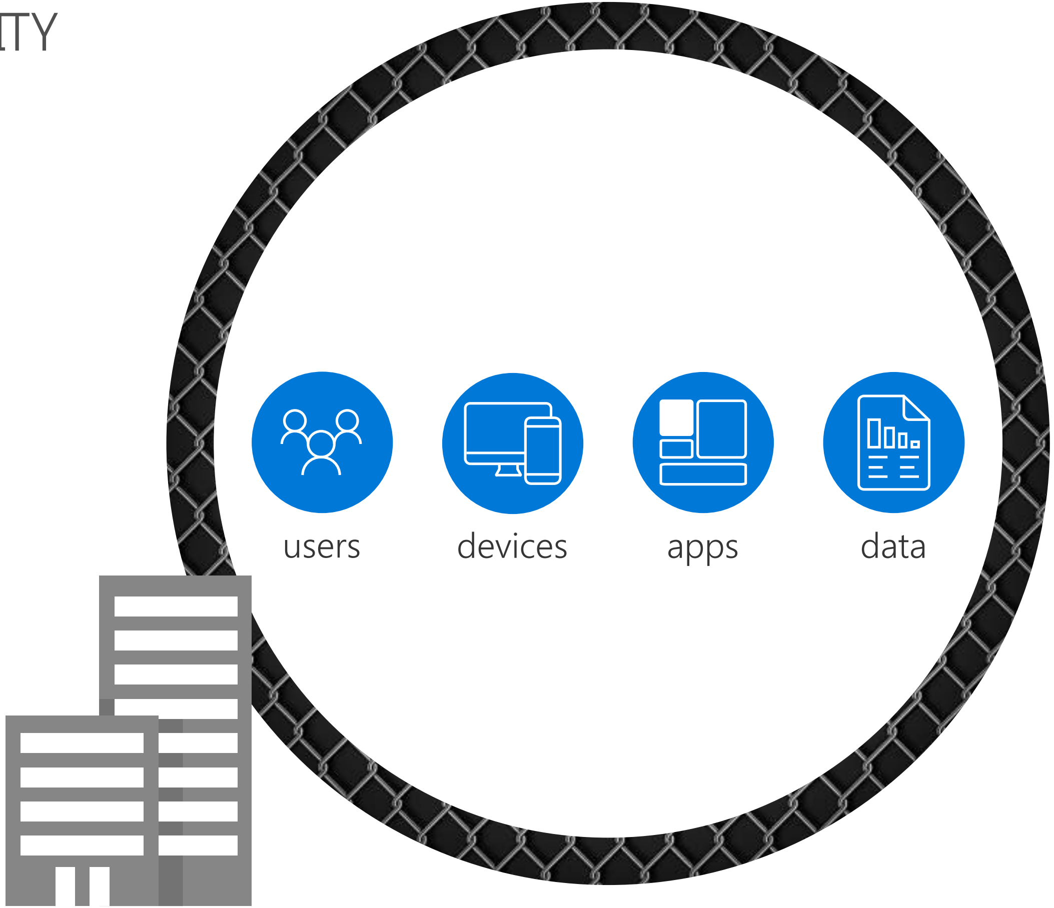
Microsoft

Identity Driven Security

Javier Dominguez
Identity and Information Protection Technical Specialist

THE WORLD BEFORE MOBILITY & CLOUD



users

devices

apps

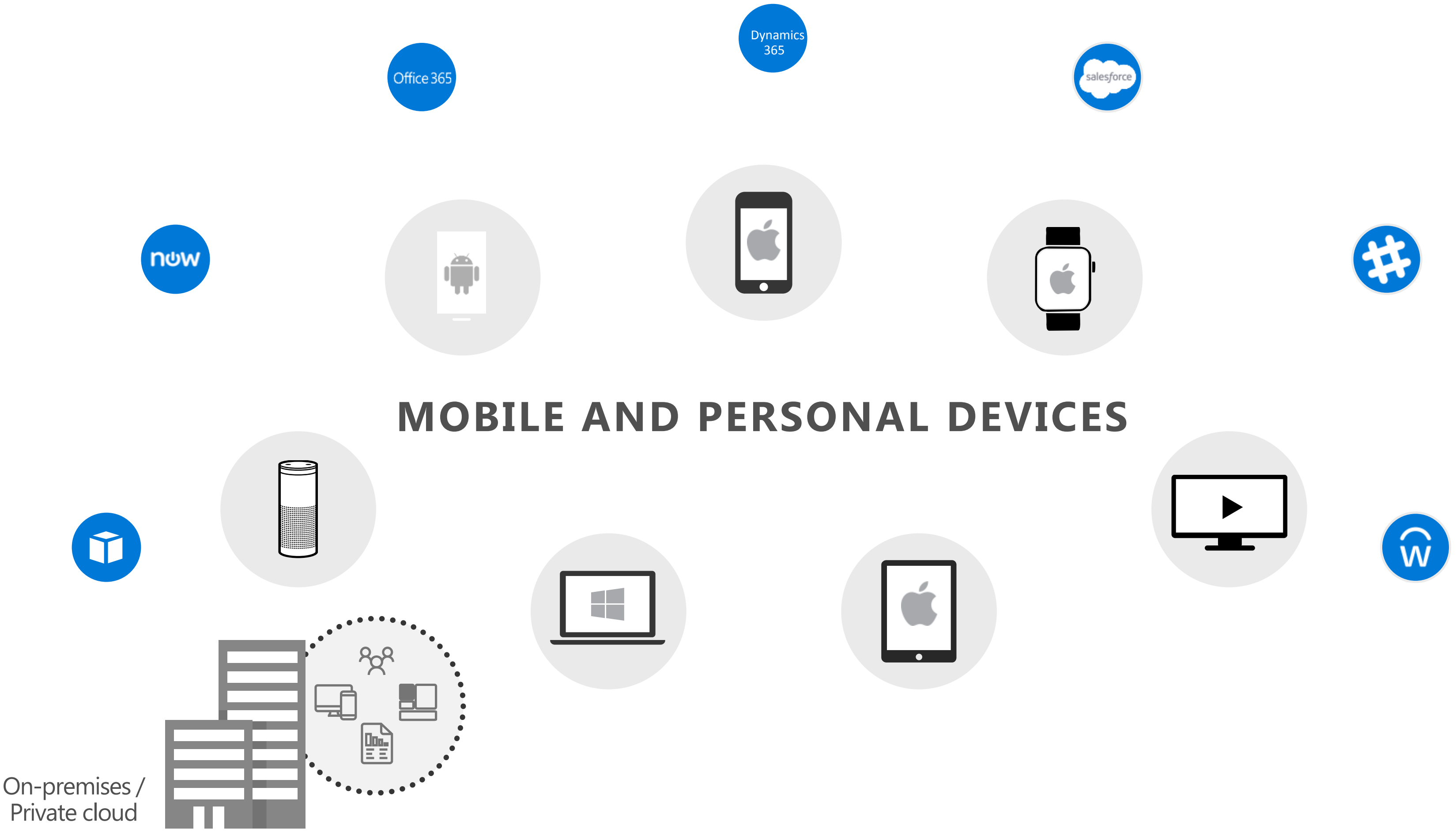
data

On-premises /
Private cloud

CLOUD APPS & SAAS SERVICES

now
Office 365
Dynamics 365
salesforce

On-premises /
Private cloud

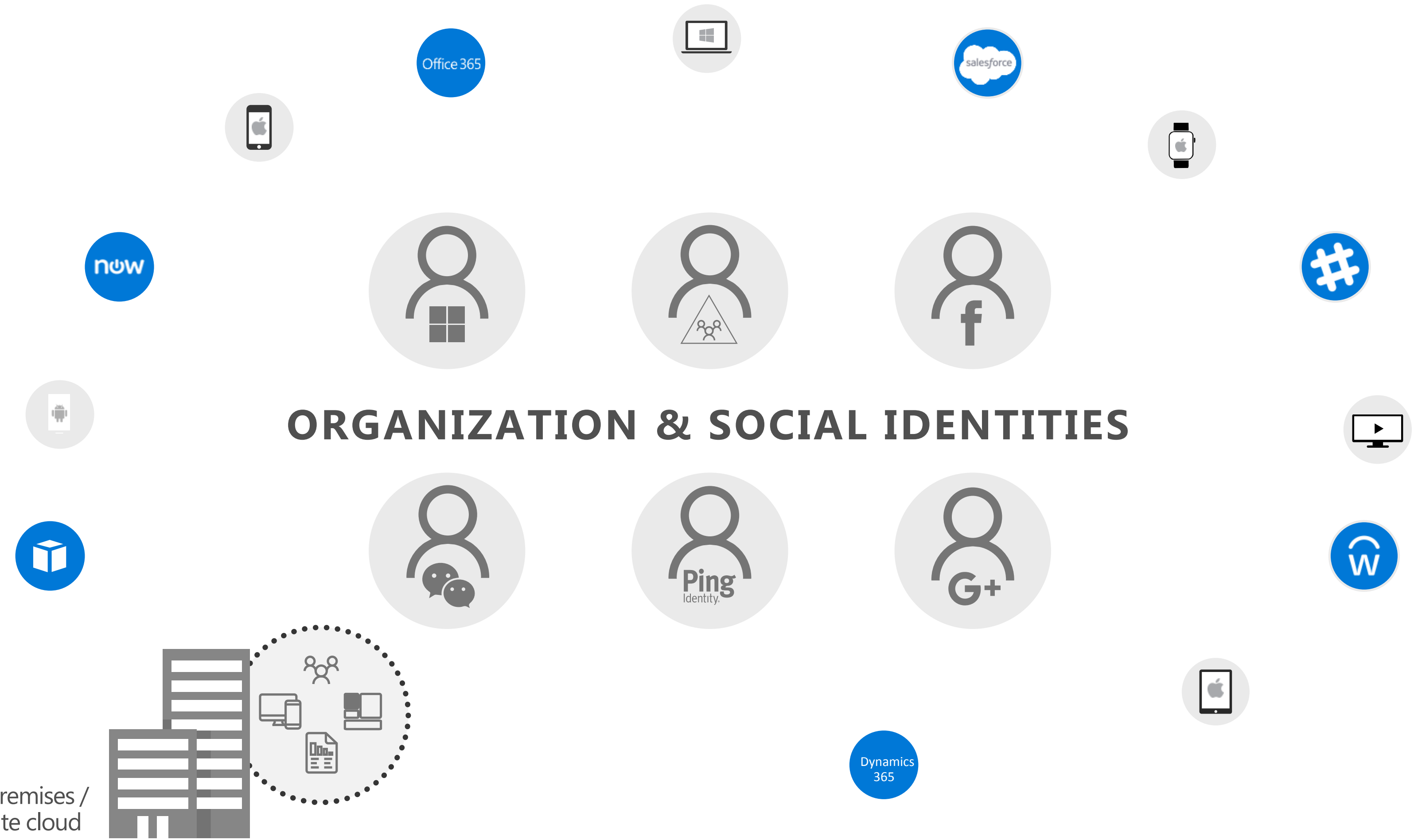


Office 365

Dynamics 365

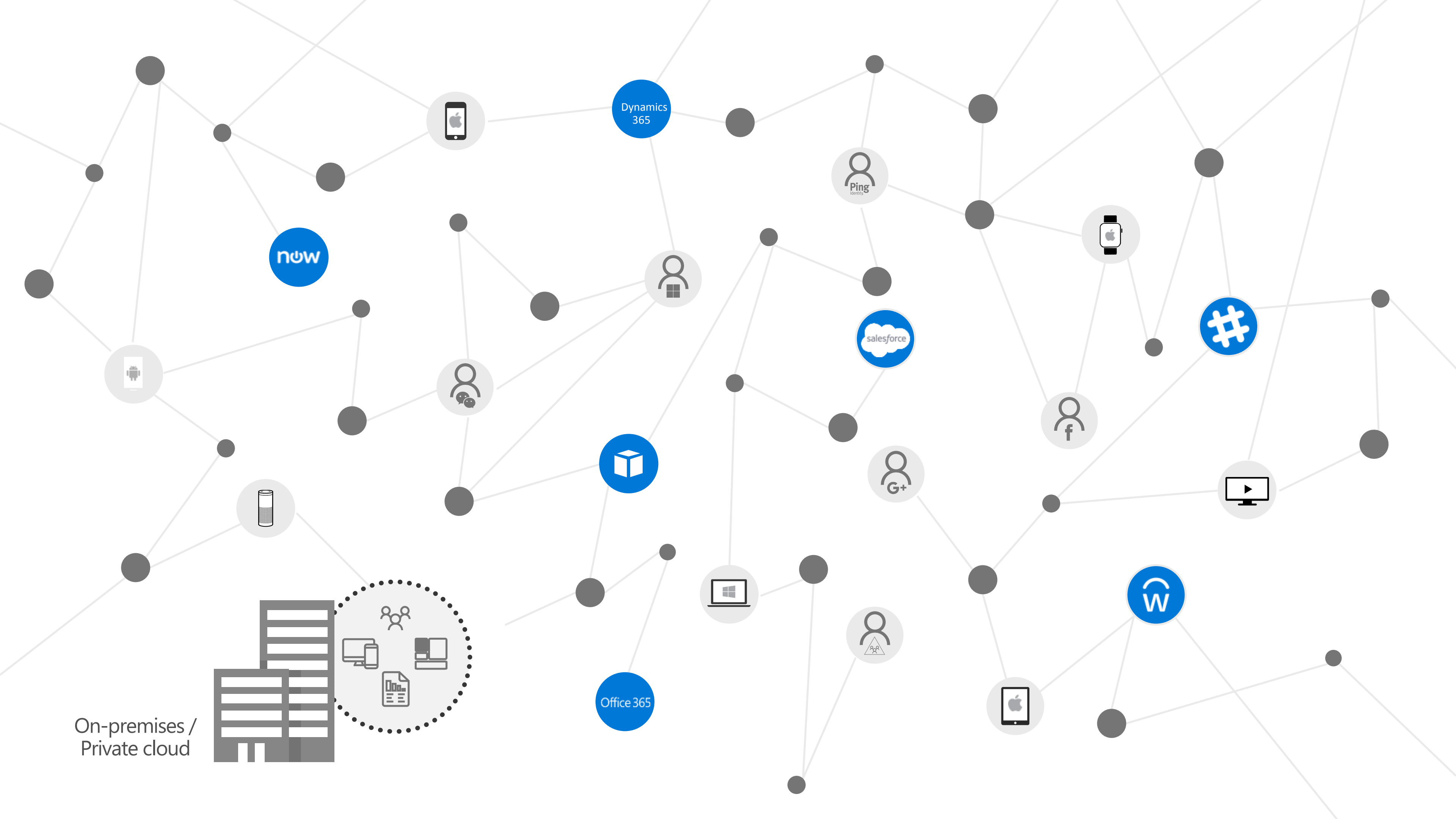
MOBILE AND PERSONAL DEVICES

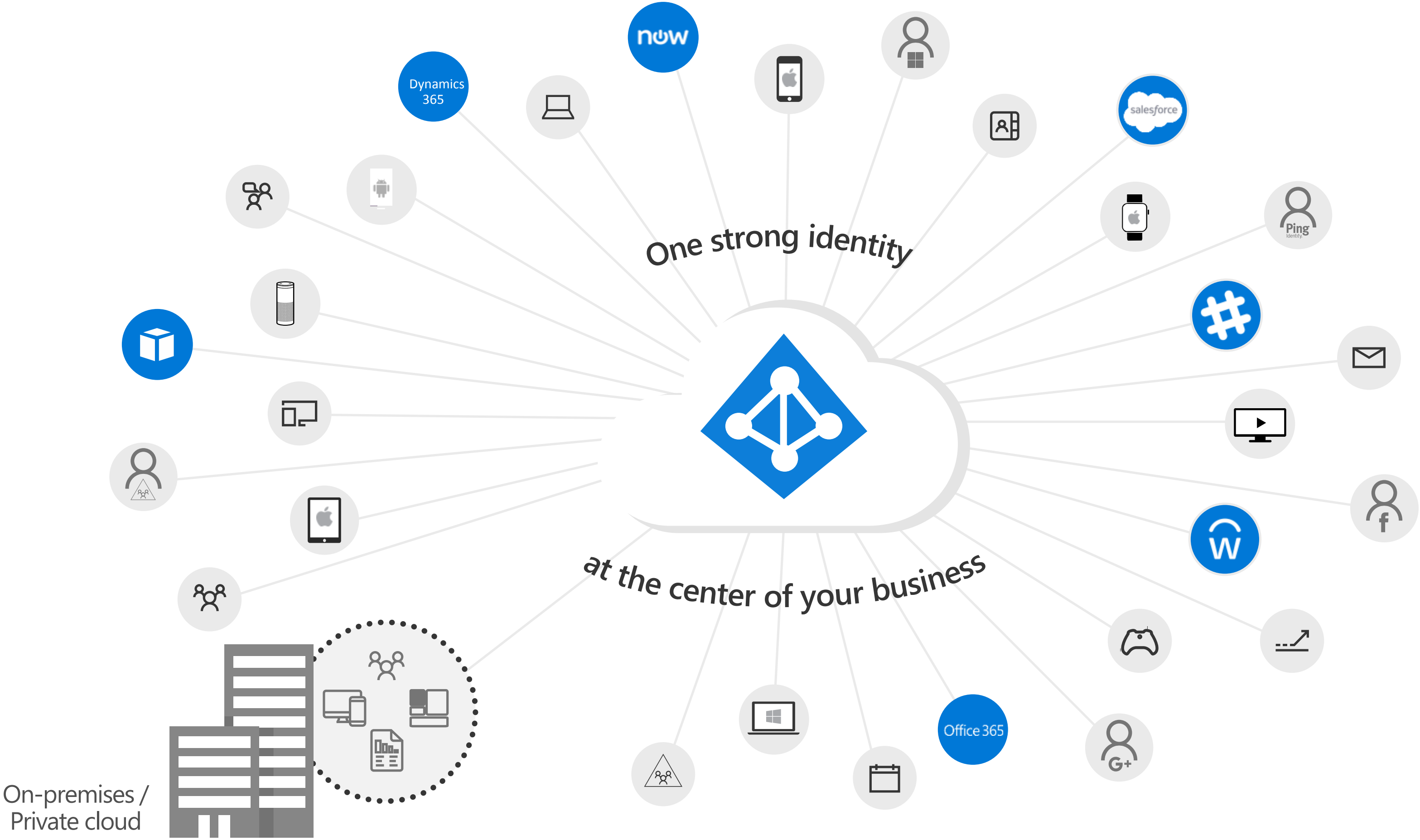
On-premises /
Private cloud



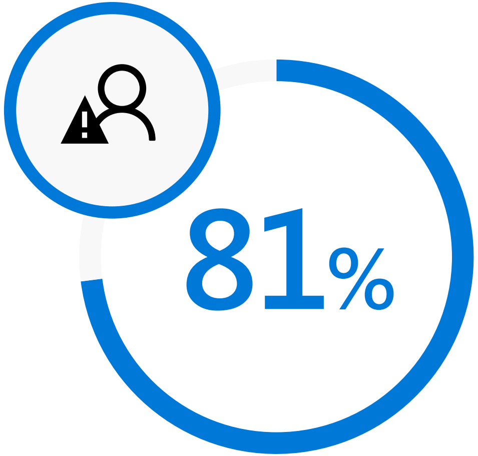
ORGANIZATION & SOCIAL IDENTITIES

On-premises /
Private cloud

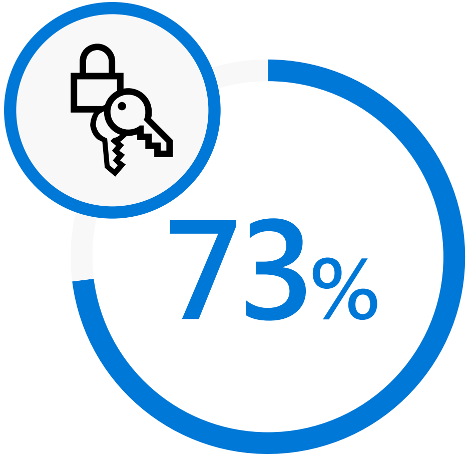

Dynamics 365
now
Ping Identity
salesforce
Office 365
On-premises / Private cloud


now
Dynamics 365
salesforce
Ping Identity
Office 365
One strong identity
at the center of your business
On-premises / Private cloud

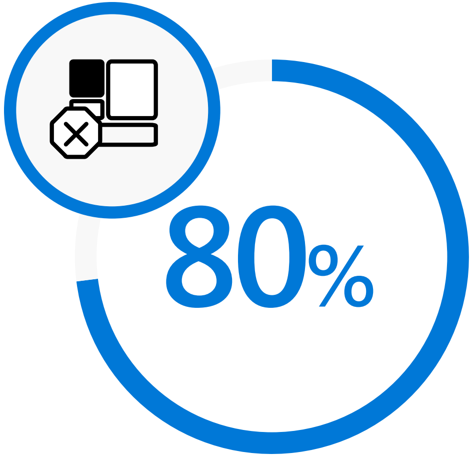
WHY IDENTITY IS IMPORTANT



of breaches are caused by credential theft



of passwords are duplicates



of employees use non-approved apps for work

IDENTITY & ACCESS MANAGEMENT

PROVE USERS ARE AUTHORIZED AND SECURE BEFORE GRANTING ACCESS TO APPS AND DATA

Protect at the front door

Simplify access to devices and apps

Safeguard your credentials

Traditional IT security tools have problems

Complexity

Initial setup, fine-tuning, and creating rules and thresholds/baselines can take a long time.

Prone to false positives

You receive too many reports in a day with several false positives that require valuable time you don’t have.

Designed to protect the perimeter

When user credentials are stolen and attackers are in the network, your current defenses provide limited protection.

Security data explosion

Useful Data

Web server logs

Windows Event logs, Linux syslog

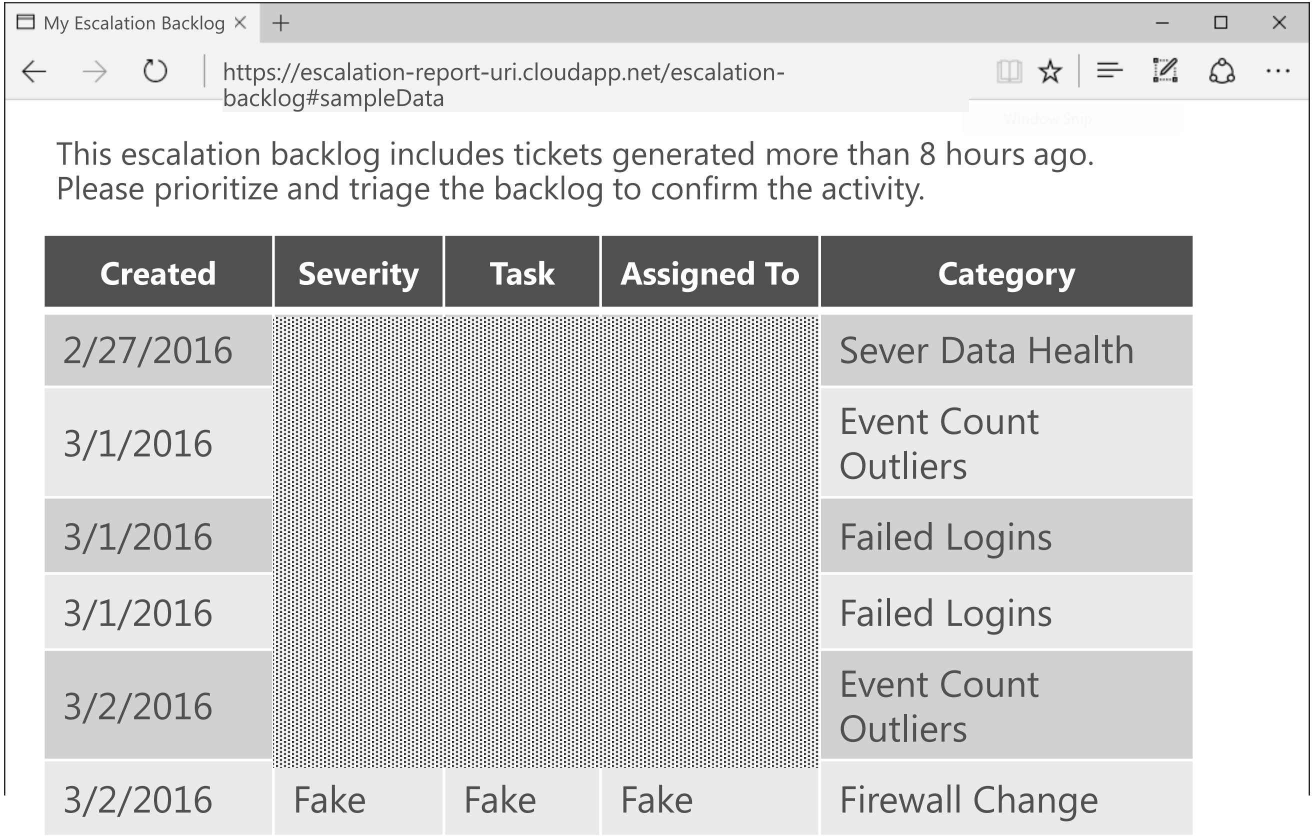
Network logs

SaaS servicesaudit information

Data center security token service

Cloud service logs

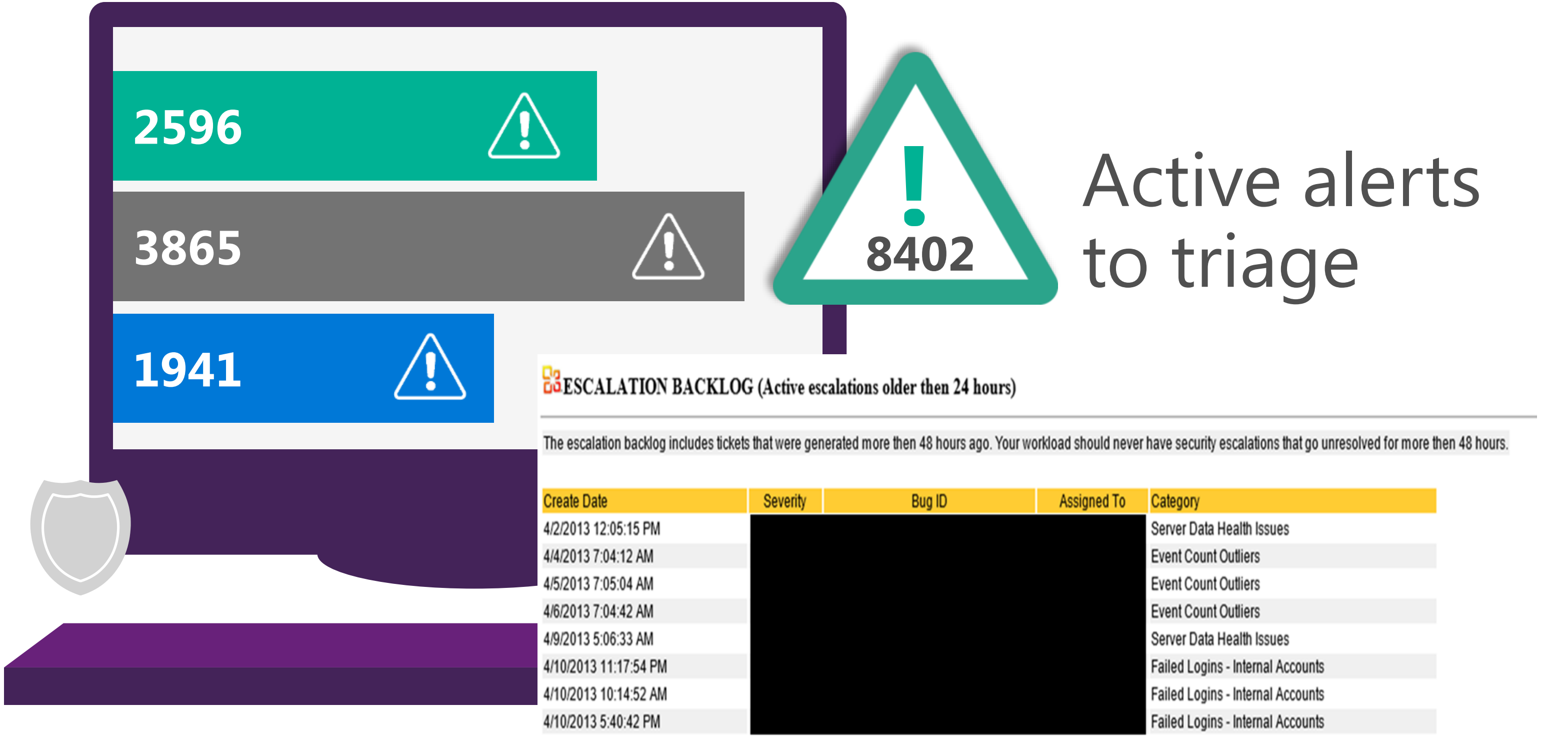
Weak independent alert streams


My Escalation Backlog
https://escalation-report-uri.cloudapp.net/escalation-backlog#sampleData
Window Snip

This escalation backlog includes tickets generated more than 8 hours ago.
Please prioritize and triage the backlog to confirm the activity.

Created	Severity	Task	Assigned To	Category
2/27/2016	[redacted]	[redacted]	[redacted]	Sever Data Health
3/1/2016	[redacted]	[redacted]	[redacted]	Event Count Outliers
3/1/2016	[redacted]	[redacted]	[redacted]	Failed Logins
3/1/2016	[redacted]	[redacted]	[redacted]	Failed Logins
3/2/2016	[redacted]	[redacted]	[redacted]	Event Count Outliers
3/2/2016	Fake	Fake	Fake	Firewall Change

Burden of triage



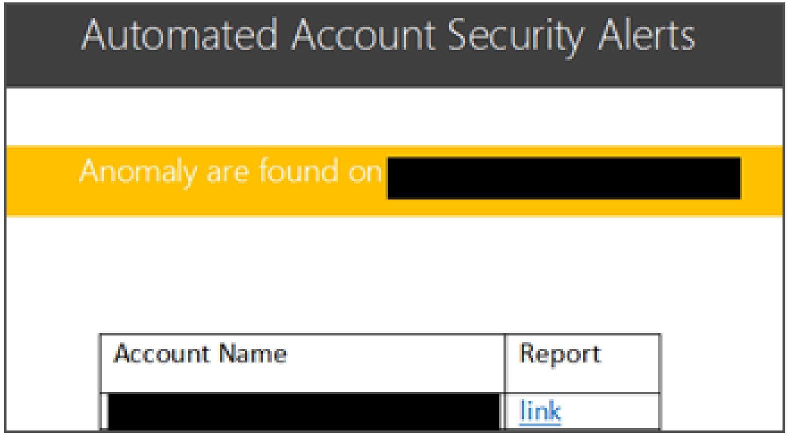
Active alerts to triage

ESCALATION BACKLOG (Active escalations older then 24 hours)

The escalation backlog includes tickets that were generated more then 48 hours ago. Your workload should never have security escalations that go unresolved for more then 48 hours.

Create Date	Severity	Bug ID	Assigned To	Category
4/2/2013 12:05:15 PM	[redacted]	[redacted]	[redacted]	Server Data Health Issues
4/4/2013 7:04:12 AM	[redacted]	[redacted]	[redacted]	Event Count Outliers
4/5/2013 7:05:04 AM	[redacted]	[redacted]	[redacted]	Event Count Outliers
4/6/2013 7:04:42 AM	[redacted]	[redacted]	[redacted]	Event Count Outliers
4/9/2013 5:06:33 AM	[redacted]	[redacted]	[redacted]	Server Data Health Issues
4/10/2013 11:17:54 PM	[redacted]	[redacted]	[redacted]	Failed Logins - Internal Accounts
4/10/2013 10:14:52 AM	[redacted]	[redacted]	[redacted]	Failed Logins - Internal Accounts
4/10/2013 5:40:42 PM	[redacted]	[redacted]	[redacted]	Failed Logins - Internal Accounts

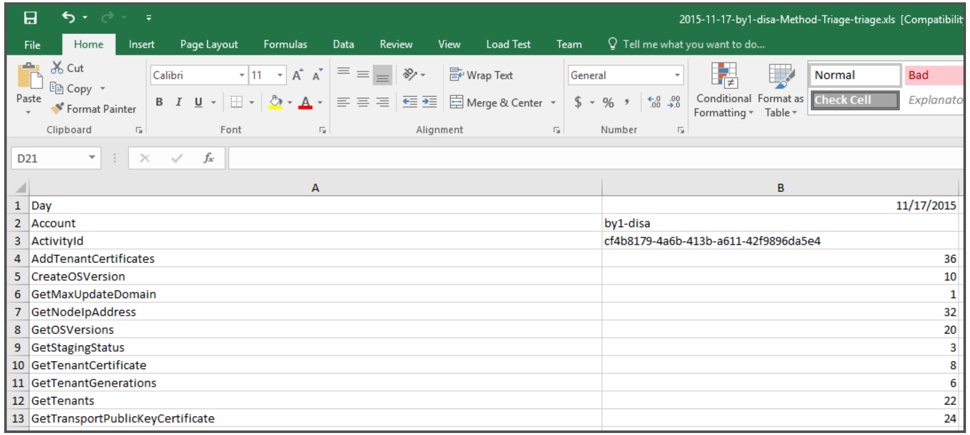
Interpretability of Alerts



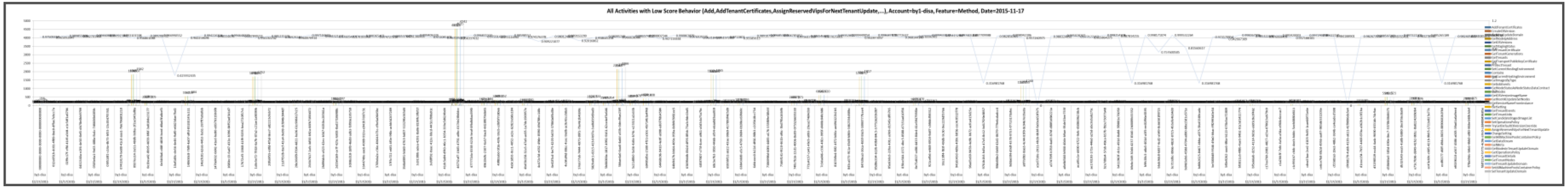
Automated Account Security Alerts

Anomaly are found on [redacted]

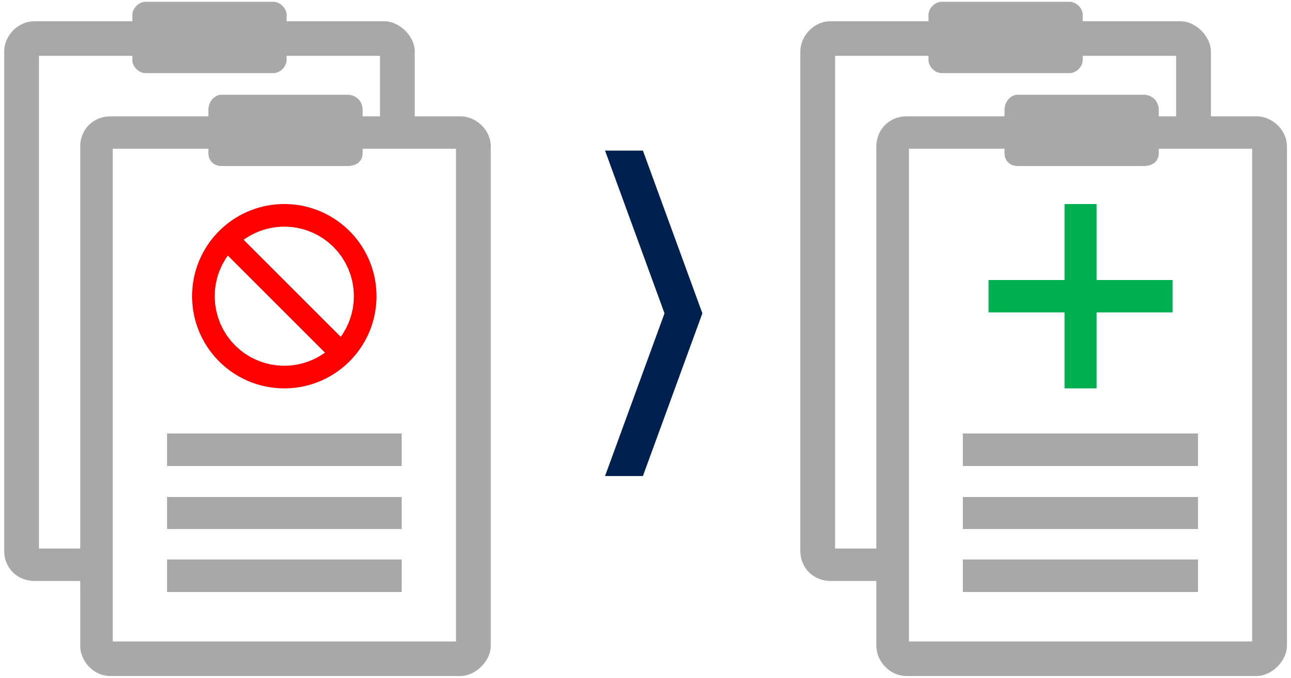
Account Name	Report
[redacted]	link



	A	B
1	Day	11/17/2015
2	Account	by1-disa
3	ActivityId	cf4b8179-4a6b-413b-a611-42f9896da5e4
4	AddTenantCertificates	36
5	CreateOSVersion	10
6	GetMaxUpdateDomain	1
7	GetNodeIpAddress	32
8	GetOSVersions	20
9	GetStagingStatus	3
10	GetTenantCertificate	8
11	GetTenantGenerations	6
12	GetTenants	22
13	GetTransportPublicKeyCertificate	24



Lack of Feedback



How Machine Learning can help

Reduce triage of burden by PRIORITIZING ALERTS

COMBINING INDEPENDENT ALERT STREAMS and providing informed scoring

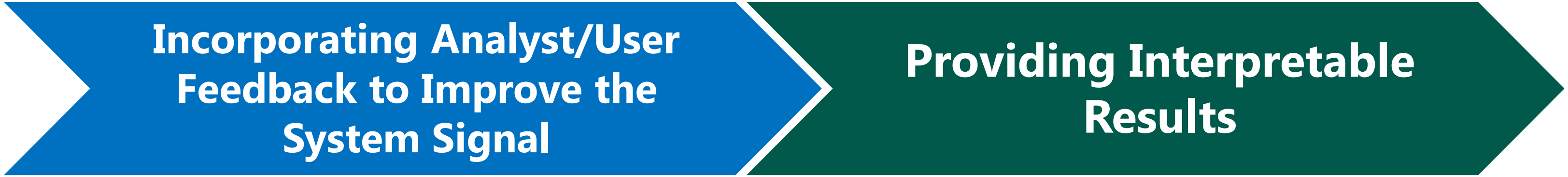
Account Name	Overall Triage Status
[redacted]	Triage-P1
[redacted]	Triage-P1
[redacted]	Triage-P1
[redacted]	Not-For-Ticketing
[redacted]	Not-For-Ticketing
[redacted]	Not-For-Ticketing
[redacted]	Not-For-Ticketing
[redacted]	Not-For-Ticketing
[redacted]	Not-For-Ticketing

Each alert combines multiple points:

- Is the sequence of API calls unusual for this account?
- Is the IP address unusual?
- Does the time of access look normal?

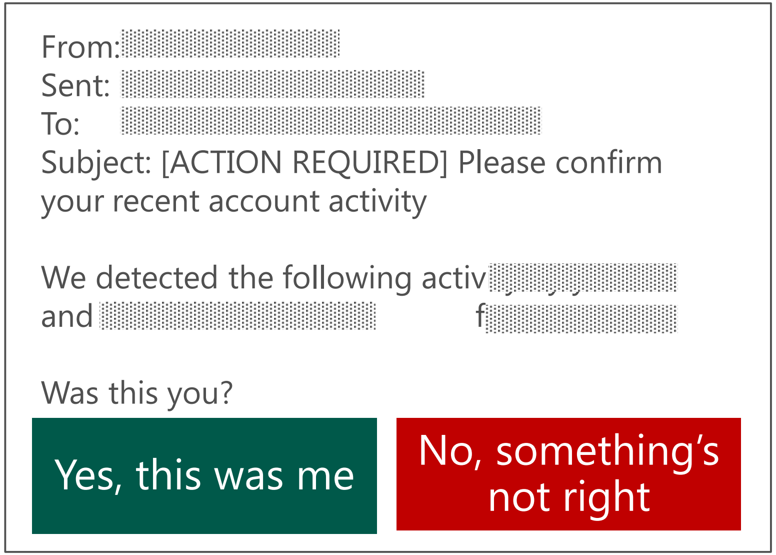
Typical Ops orgs anomaly detection, more 8 different weaker streams are combined

How Machine Learning can help



Incorporating Analyst/User Feedback to Improve the System Signal

Providing Interpretable Results



From: [redacted]
Sent: [redacted]
To: [redacted]
Subject: [ACTION REQUIRED] Please confirm your recent account activity

We detected the following activ[redacted] and [redacted] f[redacted]

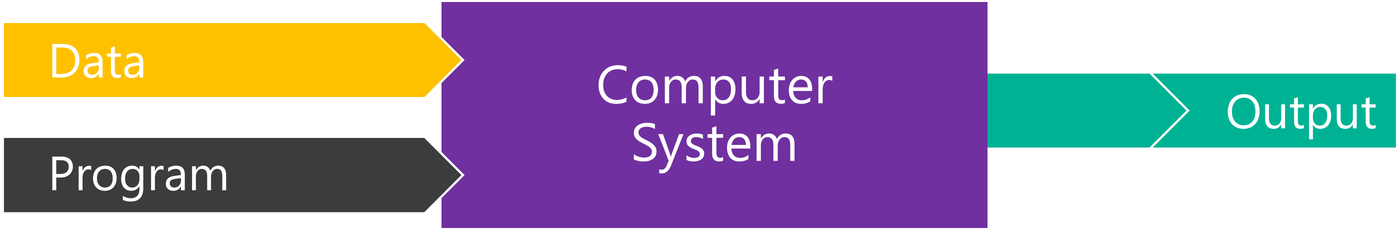
Was this you?

When we get an alert, we're informed exactly why the ML system feels it is anomalous. Not a black box.

Unusual UserAgent	Logins Eval	Unusual Location	Failed Login	Unusual IP	Unusual Activity	Overall Score
1	1	0	0	37	324	197106
0	0	0	0	0	64	134460
0	5	0	0	25	0	521308
5	3	0	0	0	0	33648
0	0	0	0	3048	0	129
0	2	0	1	3	0	94

How ML is different

Traditional Programming



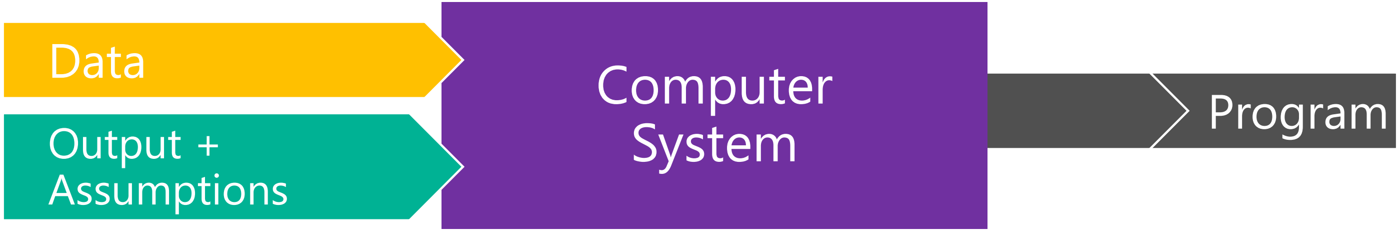
Data

Program

Computer System

Output

Machine Learning



Data

Output + Assumptions

Computer System

Program

Machine Learning for security is difficult

Lack of ground truth

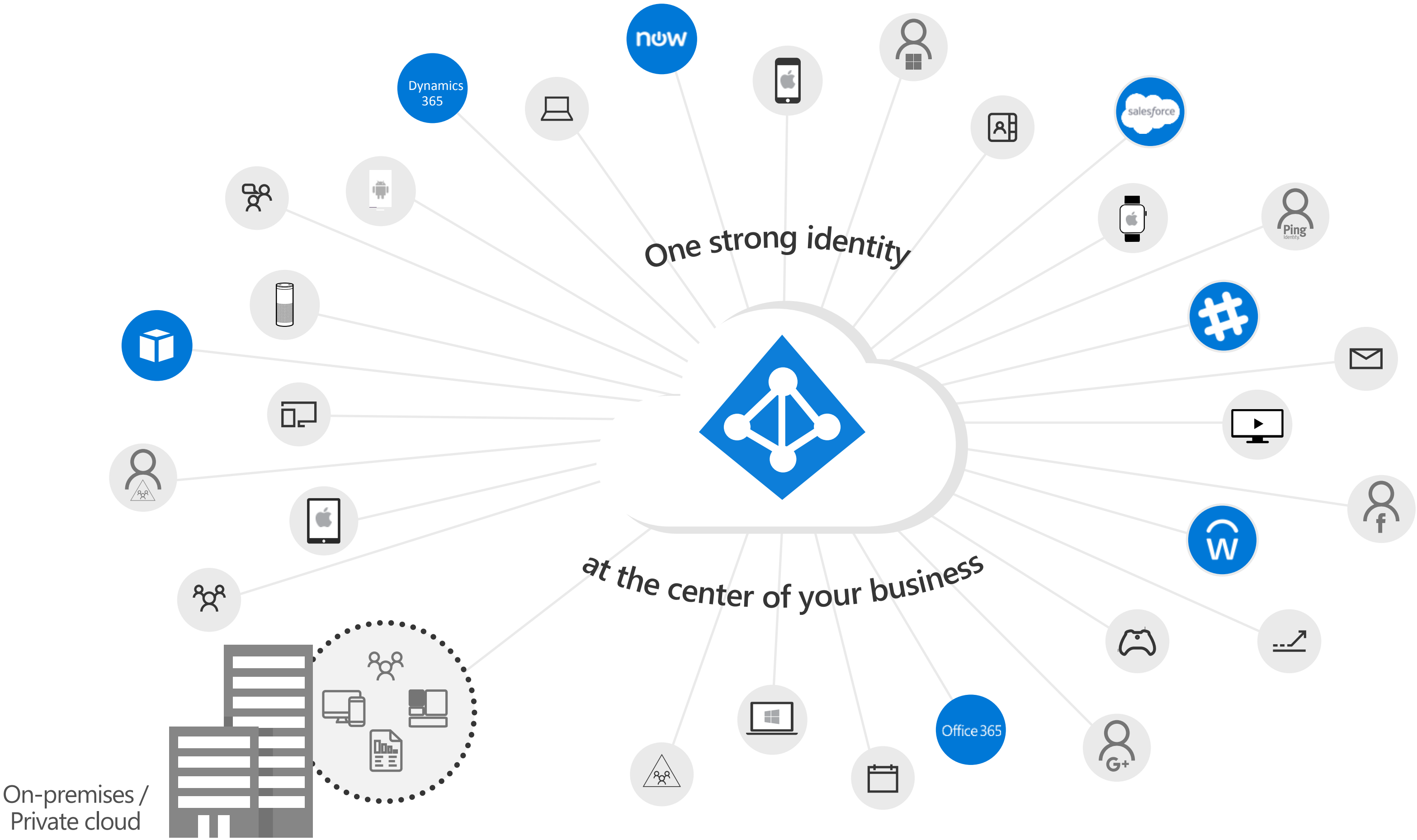
Data labeled as an attack is rare

Datasets are imbalanced

Disproportionate cost of false negative (missing an attack)

Constantly changing environment

Adversarial setting: deliberately avoiding detection


now
Dynamics 365
salesforce
Ping Identity
Office 365
One strong identity
at the center of your business
On-premises /
Private cloud

Advanced Threat Detection for Identities

Behavioral Analytics

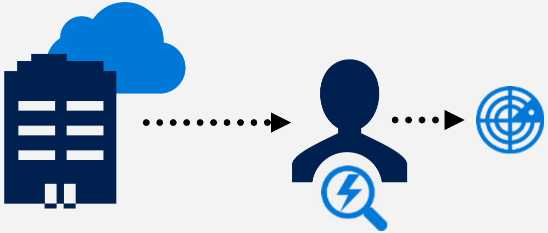
+

Detection of advanced attacks and security risks

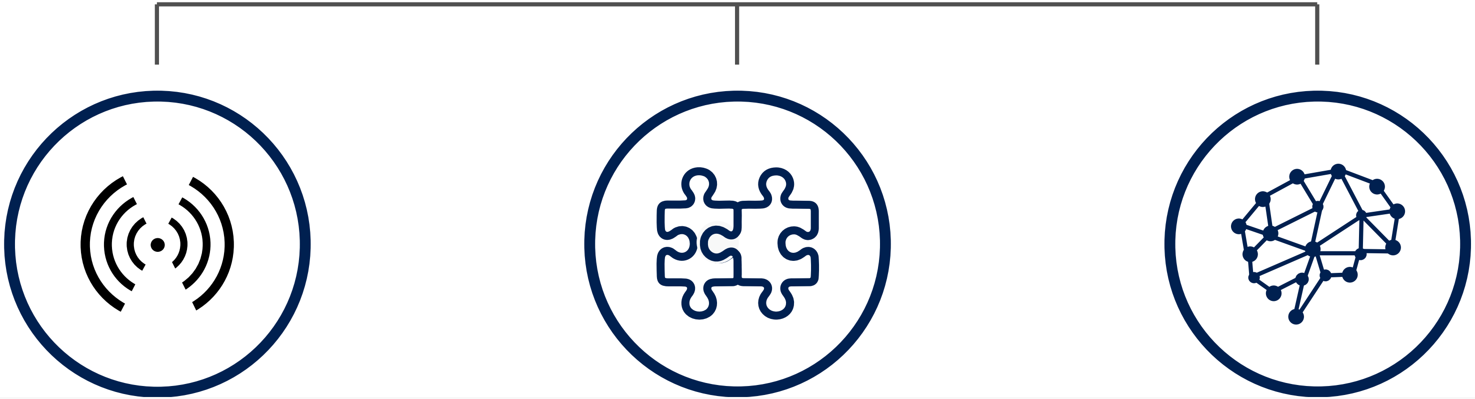
=

Advanced Threat Detection

POWERED BY MACHINE LEARNING



INTELLIGENT SECURITY GRAPH ENABLES



Signal Breadth

Integrated Intelligence

Machine Learning/AI

Microsoft Identity Security at Glance

Automatically detect/ deflect
1.5 million
attacks per day

Identify
30K
potentially compromised users per day

Bootnet data/ infected machines
from Microsoft DCU

Azure AD Directories
>9 M

More than
700 M
user accounts on Azure AD

>15 billion
authentications every day from consumer / commercial

Every day the Identity ML system processes
>10 TB of data

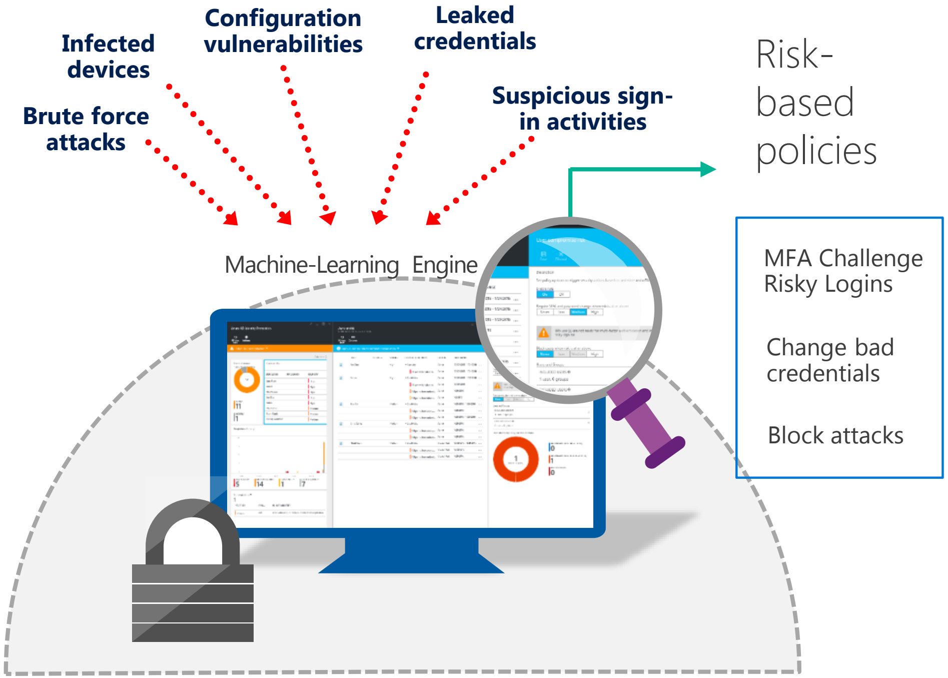
1.2 Billion
devices scanned each month

>42k
third-party applications used with Azure AD each month

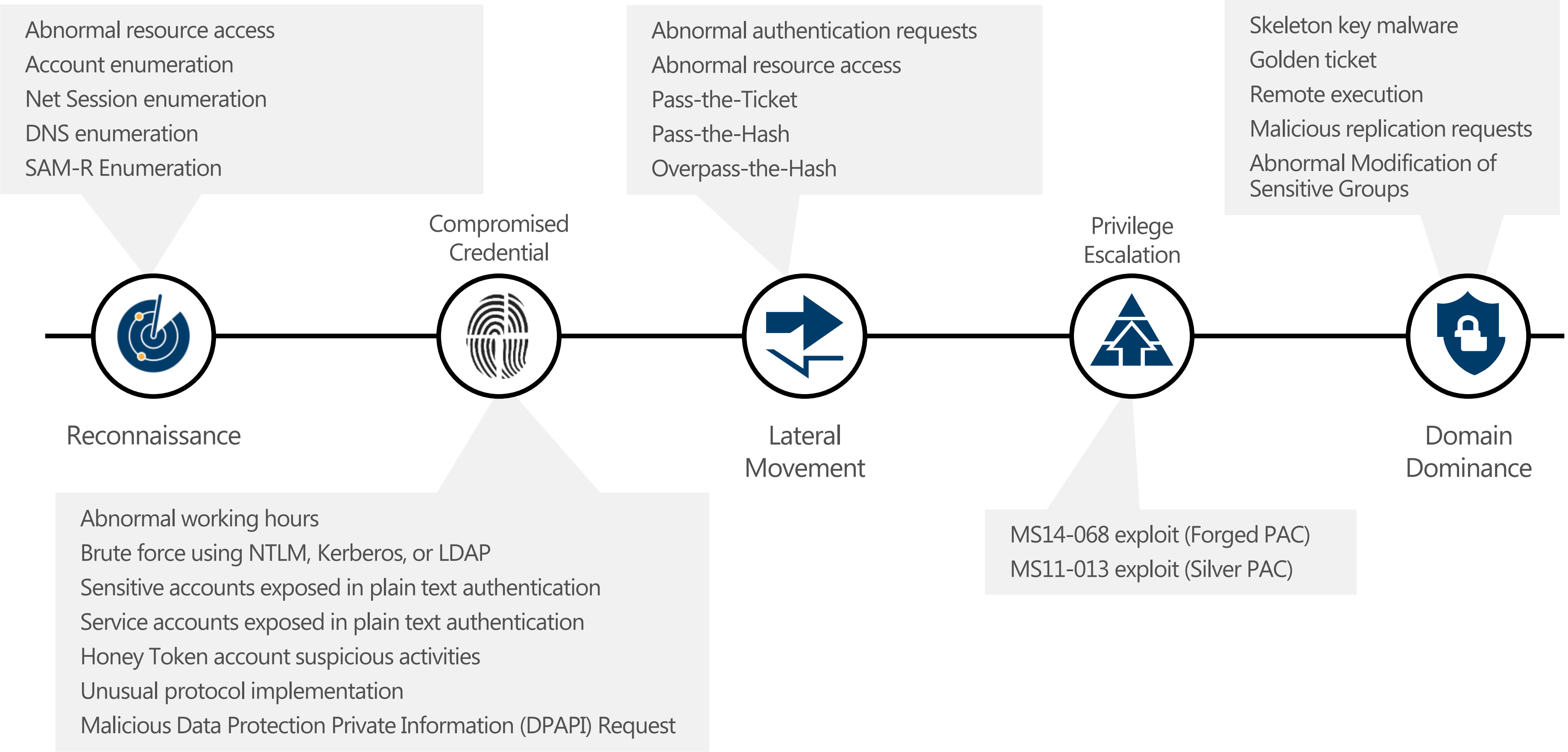
>18 billion Web Sites scanned

Cloud-powered protection

- Gain insights from a consolidated view of machine learning based threat detection
- Remediation recommendations
- Risk severity calculation
- Risk-based conditional access automatically protects against suspicious logins and compromised credentials



Detecting suspicious activities on prem



Abnormal resource access
Account enumeration
Net Session enumeration
DNS enumeration
SAM-R Enumeration

Reconnaissance

Compromised Credential

Abnormal working hours
Brute force using NTLM, Kerberos, or LDAP
Sensitive accounts exposed in plain text authentication
Service accounts exposed in plain text authentication
Honey Token account suspicious activities
Unusual protocol implementation
Malicious Data Protection Private Information (DPAPI) Request

Abnormal authentication requests
Abnormal resource access
Pass-the-Ticket
Pass-the-Hash
Overpass-the-Hash

Lateral Movement

Privilege Escalation

MS14-068 exploit (Forged PAC)
MS11-013 exploit (Silver PAC)

Skeleton key malware
Golden ticket
Remote execution
Malicious replication requests
Abnormal Modification of Sensitive Groups

Domain Dominance

Who is accessing? What is their role?
Is the account compromised?

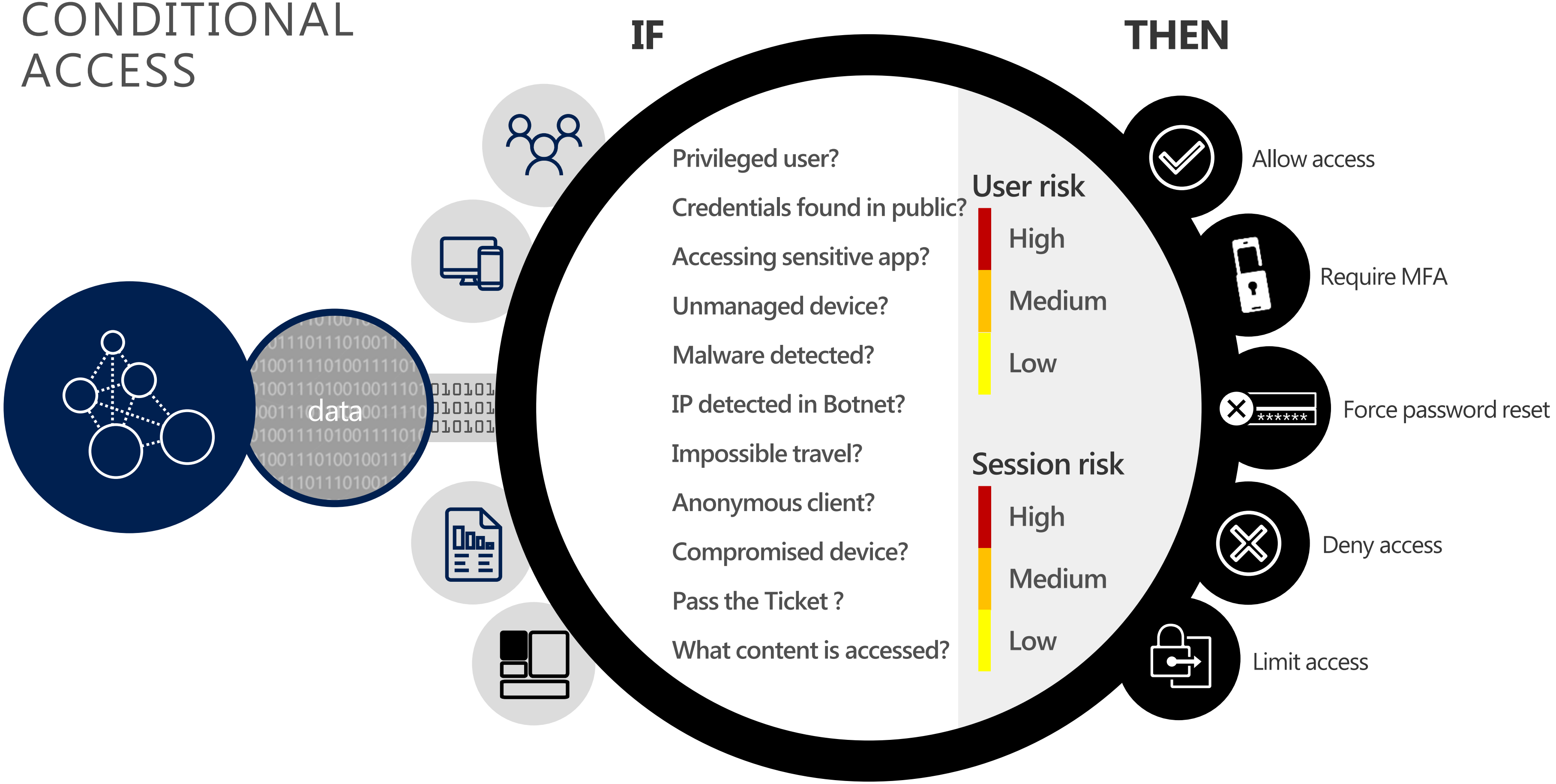
Where is the user based? From where is
the user signing in? Is the IP anonymous?

Which app is being accessed?
What is the business impact?

Is the device healthy? Is it managed?
Has it been in a botnet?

What data is being accessed?
Is it classified? Is it allowed off premises?

CONDITIONAL ACCESS



IF

- Privileged user?
- Credentials found in public?
- Accessing sensitive app?
- Unmanaged device?
- Malware detected?
- IP detected in Botnet?
- Impossible travel?
- Anonymous client?
- Compromised device?
- Pass the Ticket ?
- What content is accessed?

User risk
- 🟥 High
- 🟧 Medium
- 🟨 Low

Session risk
- 🟥 High
- 🟧 Medium
- 🟨 Low

THEN

- Allow access
- Require MFA
- Force password reset
- Deny access
- Limit access

HOW CAN YOU SIMPLIFY ACCESS TO **DEVICES & APPS?**

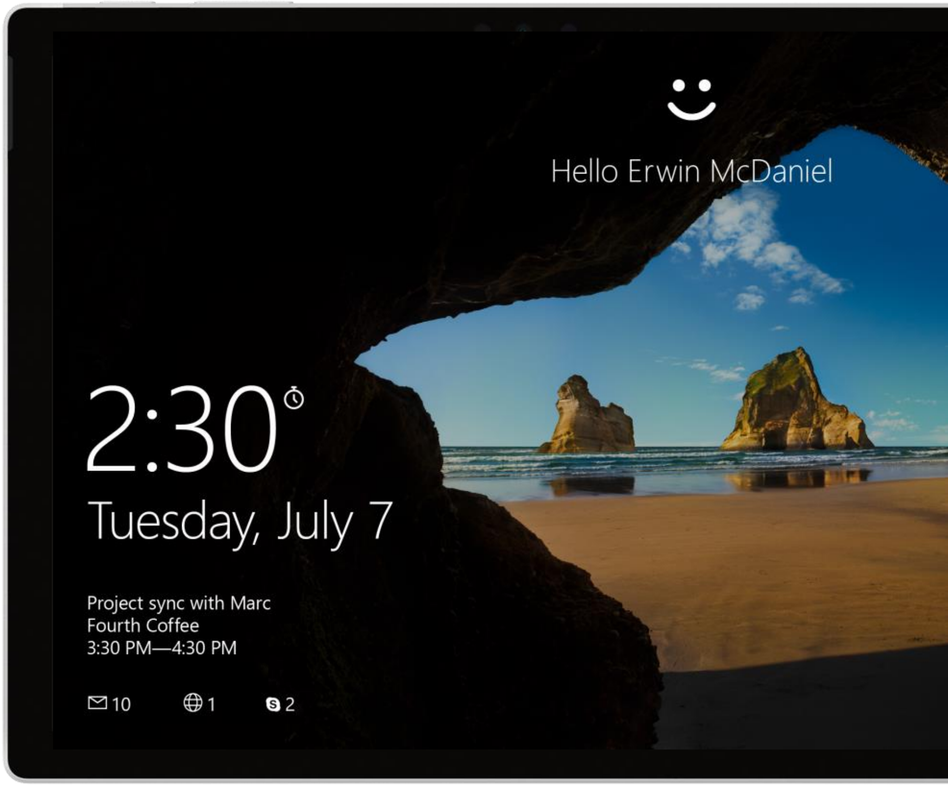
WINDOWS HELLO **FOR BUSINESS**

Passwordless strong authentication via multiple factors

- PC + PIN or Biometrics
- PC + Companion Device
- PC supported Biometrics: fingerprint & facial
- Companion Device can support other biometrics options (e.g.: EKG)

Supported on any Windows 10 device

>100 devices supporting biometrics



Hello Erwin McDaniel

2:30

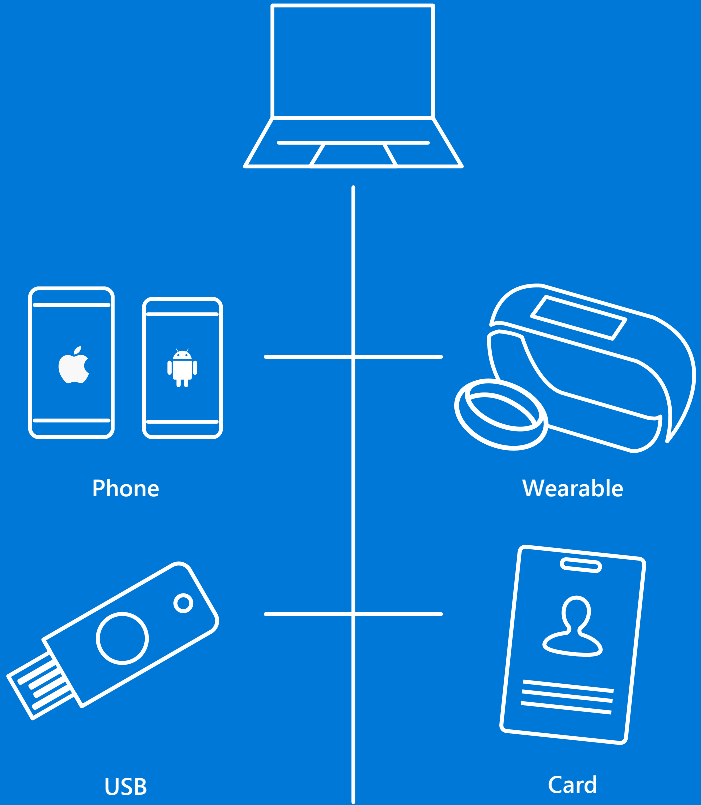
Tuesday, July 7

Project sync with Marc
Fourth Coffee
3:30 PM—4:30 PM

✉ 10 🌐 1 Ⓢ 2

MAKING WINDOWS HELLO **WORK FOR EVERY ENVIRONMENT**

Windows Hello Companion Device Framework



WHAT IS **FIDO?**

Security on premises and web

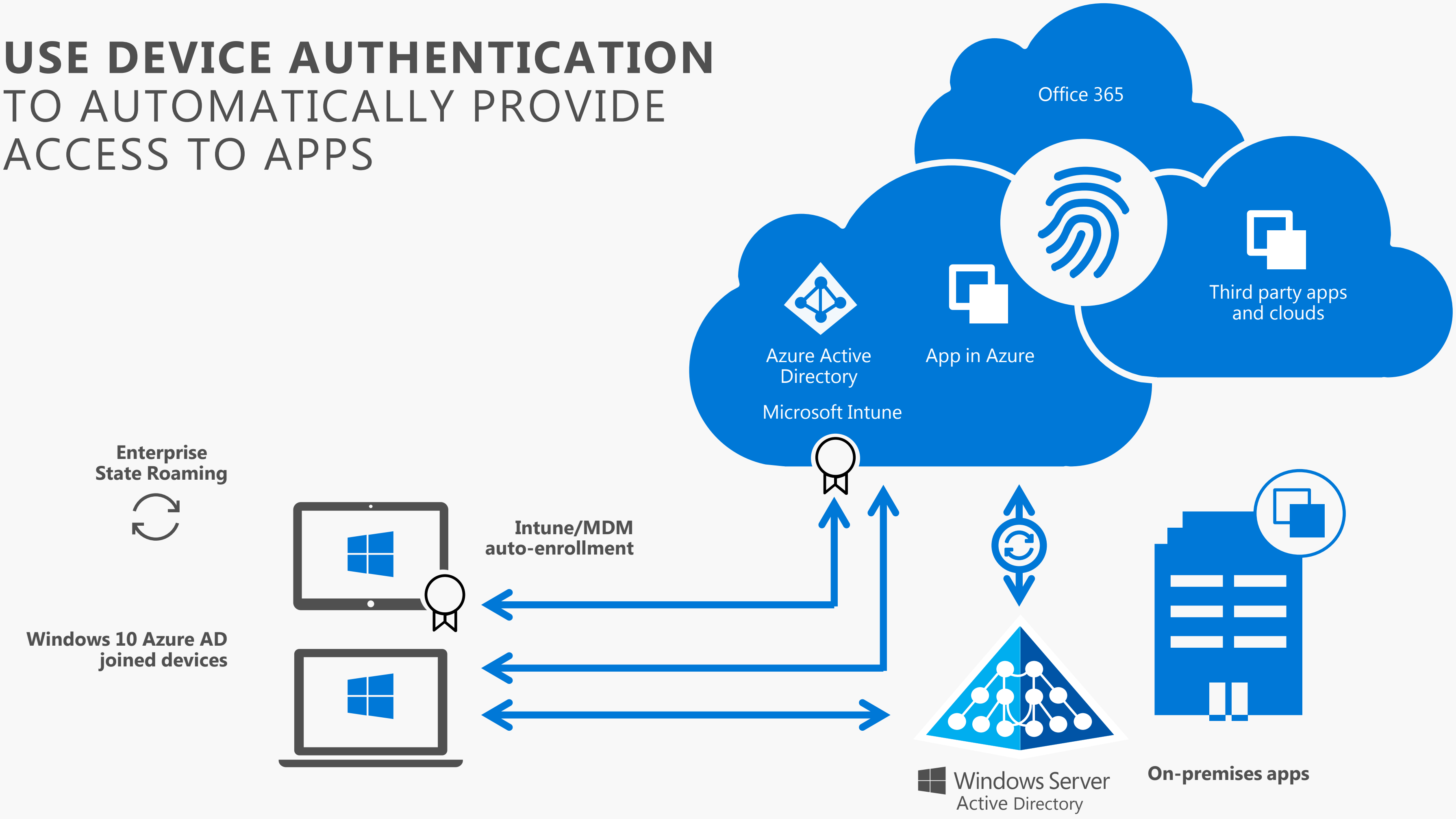
Secure mobile user credentials

Secure authentication

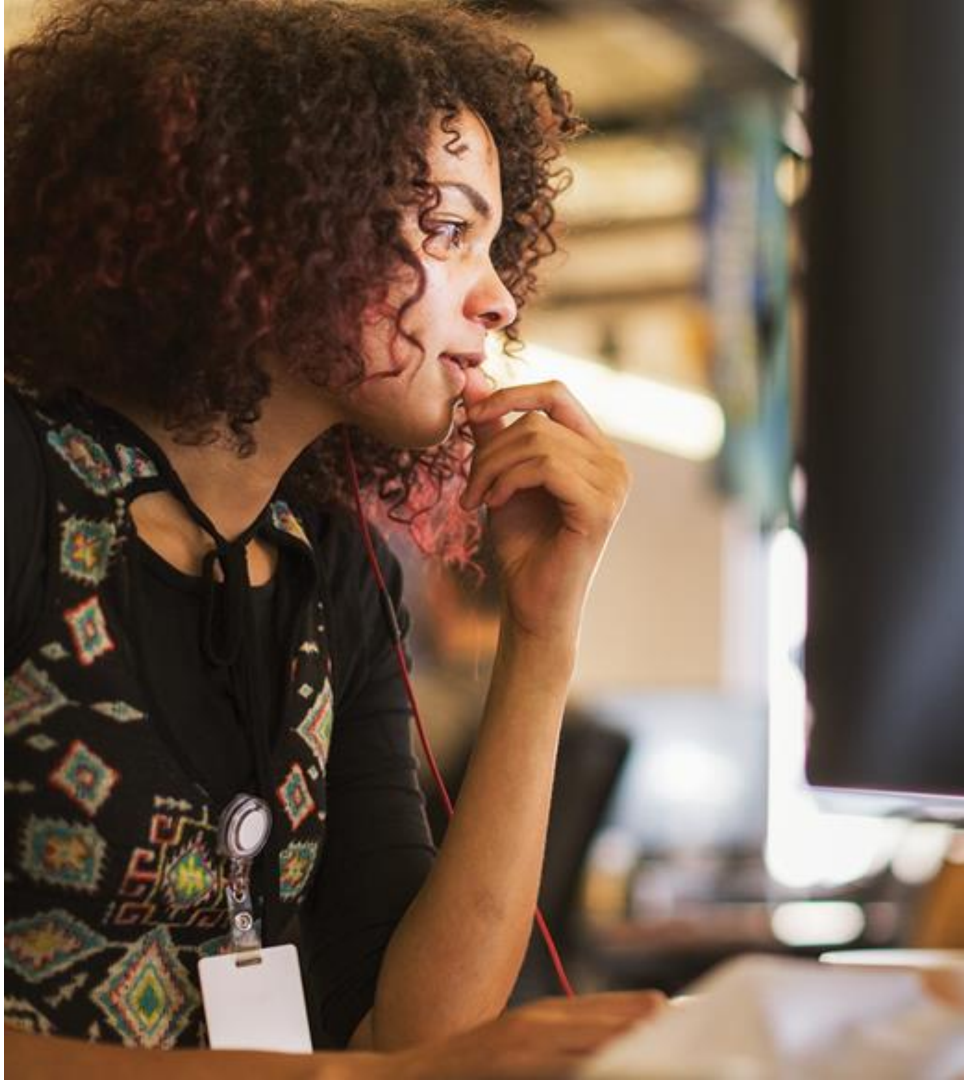
FIDO BOARD MEMBERS

Microsoft	Google	Nok Nok LABS	oberthur TECHNOLOGIES THE M COMPANY	Lenovo	aetna	Bank of America
PayPal	infineon	USAA	FINGERPRINTS	intel	ARM	yubico Trust the Net.
VASCO TRUST FOR THE DIGITAL WORLD	BCcard	RAON SECURE	mastercard	SAMSUNG	egis Technology	Synaptics
RSA	QUALCOMM	AMERICAN EXPRESS	gemalto security to be free	NTT docomo	NXP	ING
CrucialTec	VISA	Daon	FEITIAN WE BUILD SECURITY	Alibaba.com Global trade starts here.	LINE	

USE DEVICE AUTHENTICATION TO AUTOMATICALLY PROVIDE ACCESS TO APPS


Office 365
Azure Active Directory
App in Azure
Third party apps and clouds
Microsoft Intune
Enterprise State Roaming
Intune/MDM auto-enrollment
Windows 10 Azure AD joined devices
Windows Server Active Directory
On-premises apps

HOW DO YOU PROTECT USER & ADMINISTRATOR **CREDENTIALS?**



Can you protect credentials against Pass-the-Hash and other similar classes of attacks?

Can you restrict and monitor the use of privileged credentials?

How are the credentials stored in your devices?

HOW HELLO **PROTECTS CREDENTIALS**

Strong authentication via multiple factors

- Uses two factors for authentication (e.g.: PC + PIN or Biometric)
- Asymmetrical Keys (i.e: Private/Public)

User credentials protected by hardware

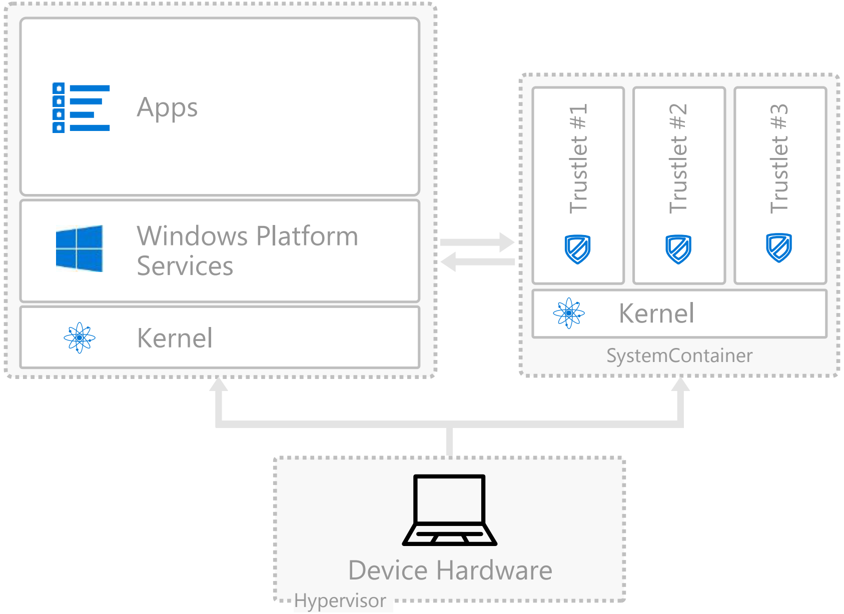
- Hardware generated credential (keys)
- Credential isolated and protected by hardware

Secure biometrics

- Hardened biometric implementation in Windows & hardware
- Anti-spoofing and brute-force protection

HOW WINDOWS PROTECTS **SINGLE SIGN-IN TOKENS**

- #1 go-to attack for hackers: Pass the Hash
- Used in nearly every major breach for lateral movement
- Credential Guard uses Windows Defender System Guard to hardware isolate authentication and authentication data away from system
- Fundamentally breaks derived credential theft even when OS is fully compromised

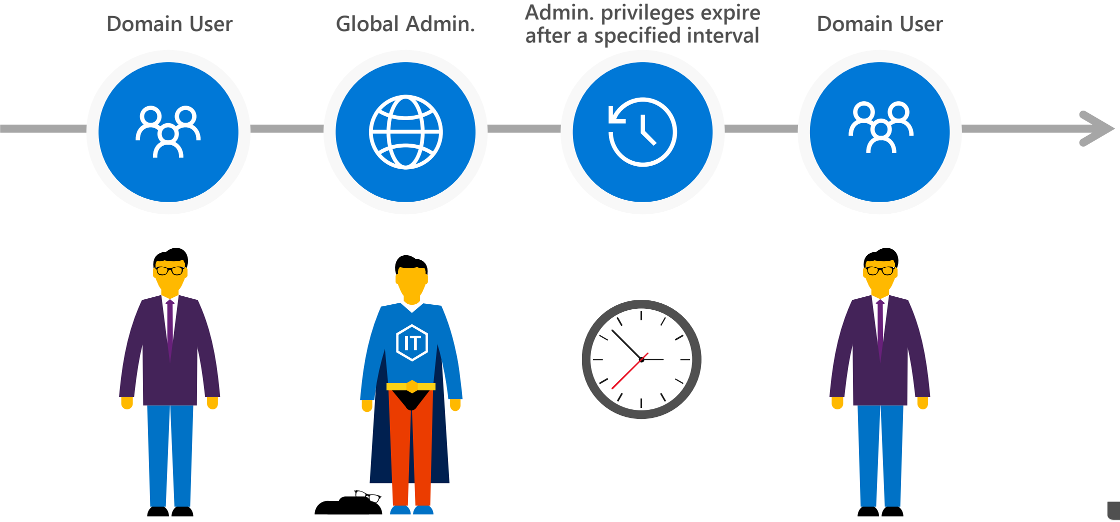


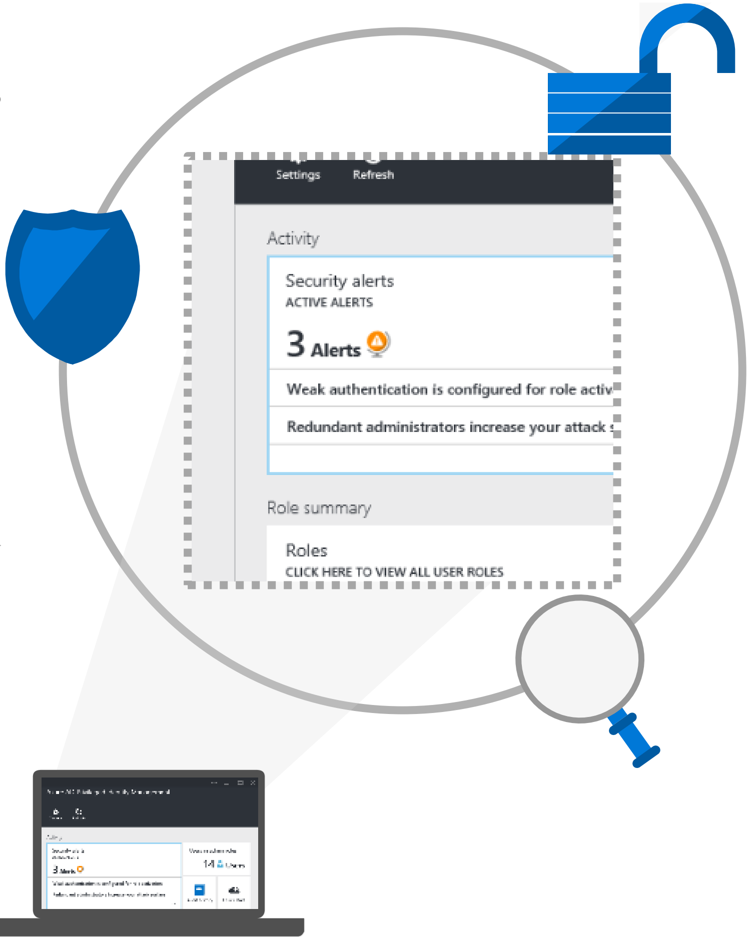
PROTECT **PRIVILEGED IDENTITIES**

Discover, restrict, and monitor privileged identities

Enforce on-demand, just-in-time administrative access when needed

Use Alert, Audit Reports and Access Review





Activity

Security alerts
ACTIVE ALERTS

3 Alerts

Weak authentication is configured for role activ

Redundant administrators increase your attack s

Role summary

Roles
CLICK HERE TO VIEW ALL USER ROLES

Thank You

Microsoft