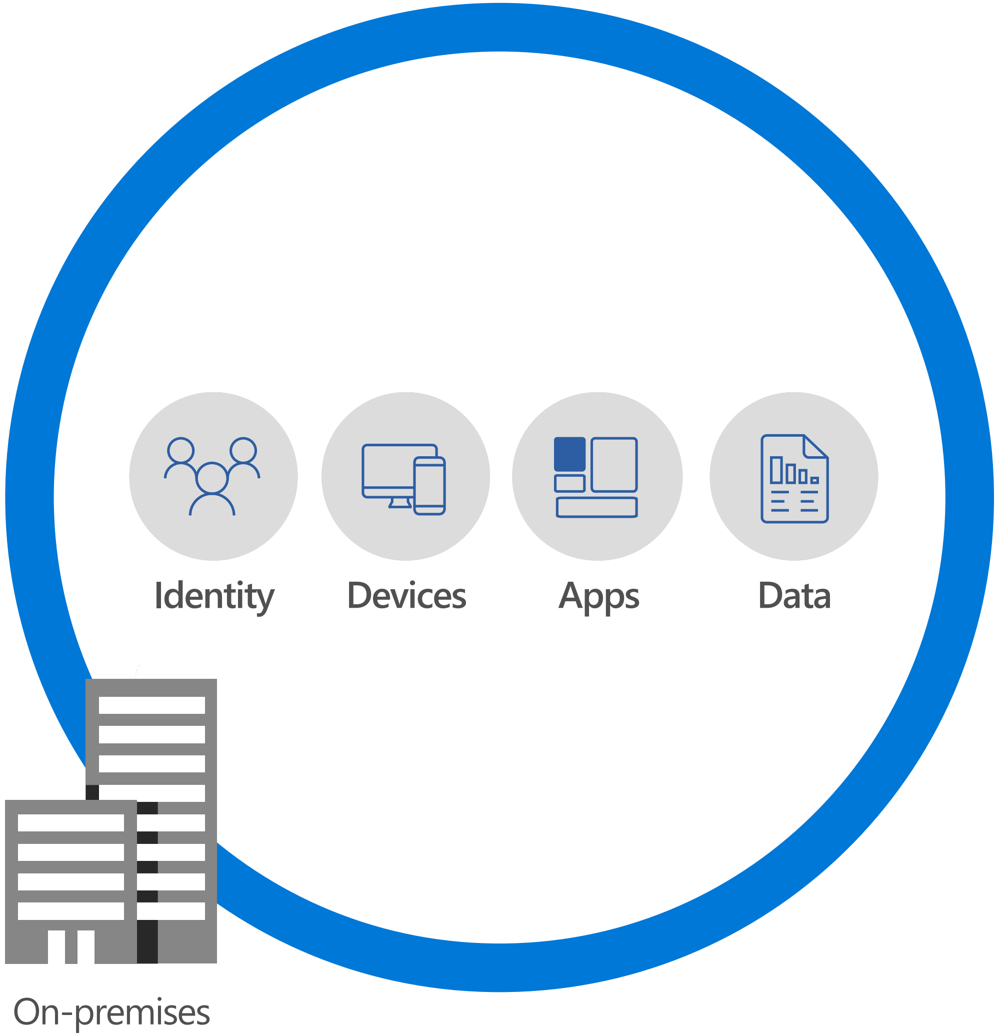
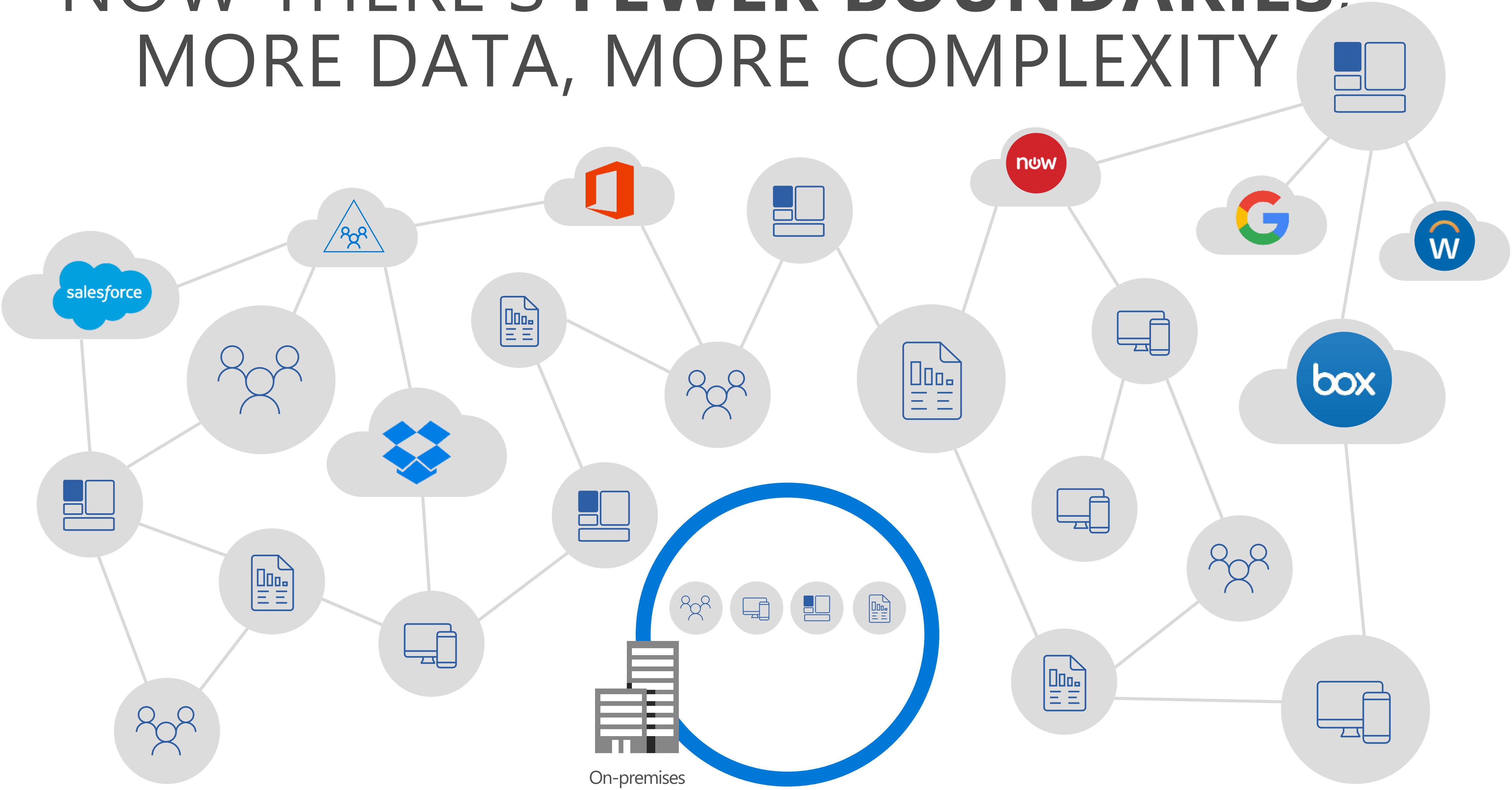
Microsoft

Security for the productive enterprise

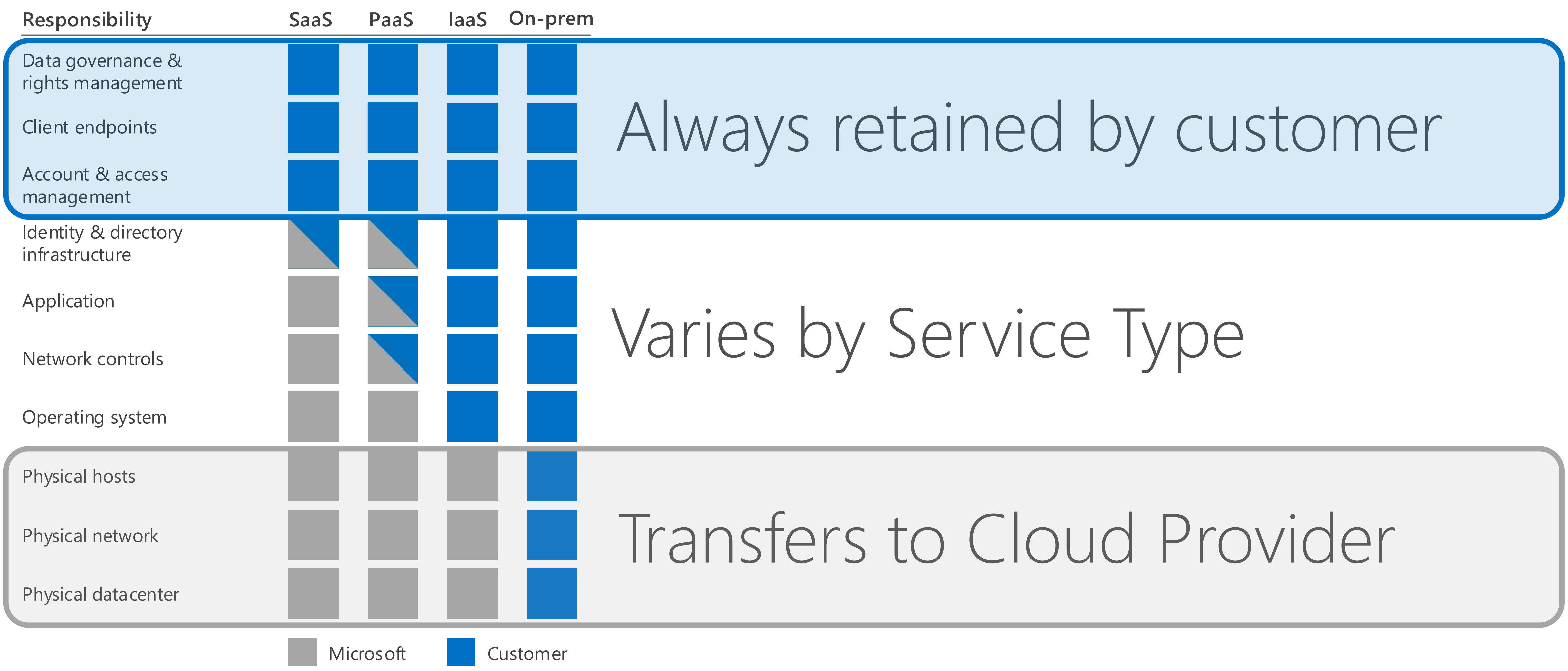
The security perimeter has changed



NOW THERE'S **FEWER BOUNDARIES**, MORE DATA, MORE COMPLEXITY



Cloud Redefines Responsibility Zones



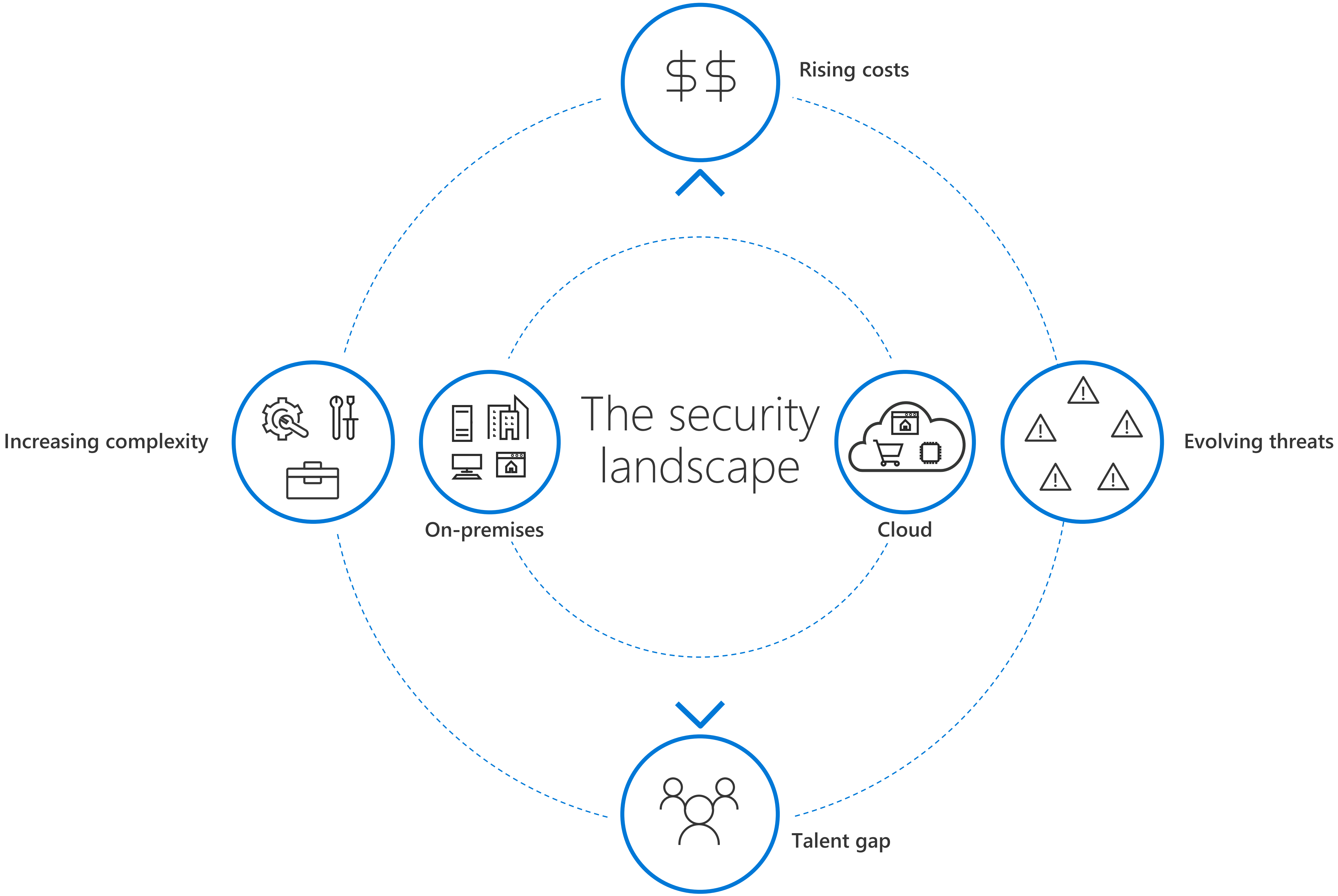
Responsibility	SaaS	PaaS	IaaS	On-prem
Data governance & rights management	🟦	🟦	🟦	🟦
Client endpoints	🟦	🟦	🟦	🟦
Account & access management	🟦	🟦	🟦	🟦
Identity & directory infrastructure	⬜/🟦	⬜/🟦	🟦	🟦
Application	⬜	⬜/🟦	🟦	🟦
Network controls	⬜	⬜/🟦	🟦	🟦
Operating system	⬜	⬜	🟦	🟦
Physical hosts	⬜	⬜	⬜	🟦
Physical network	⬜	⬜	⬜	🟦
Physical datacenter	⬜	⬜	⬜	🟦

Always retained by customer

Varies by Service Type

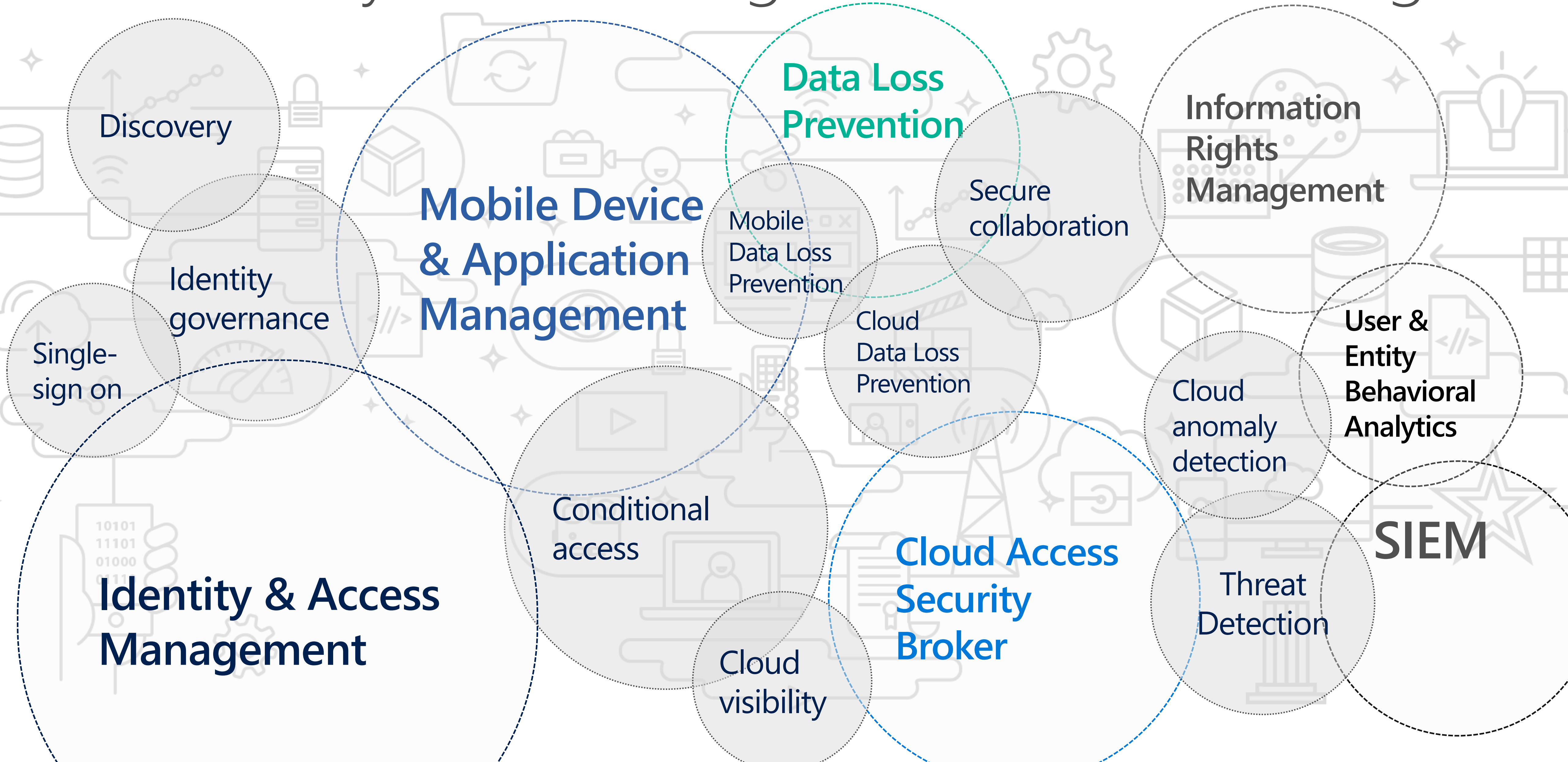
Transfers to Cloud Provider

⬜ Microsoft 🟦 Customer



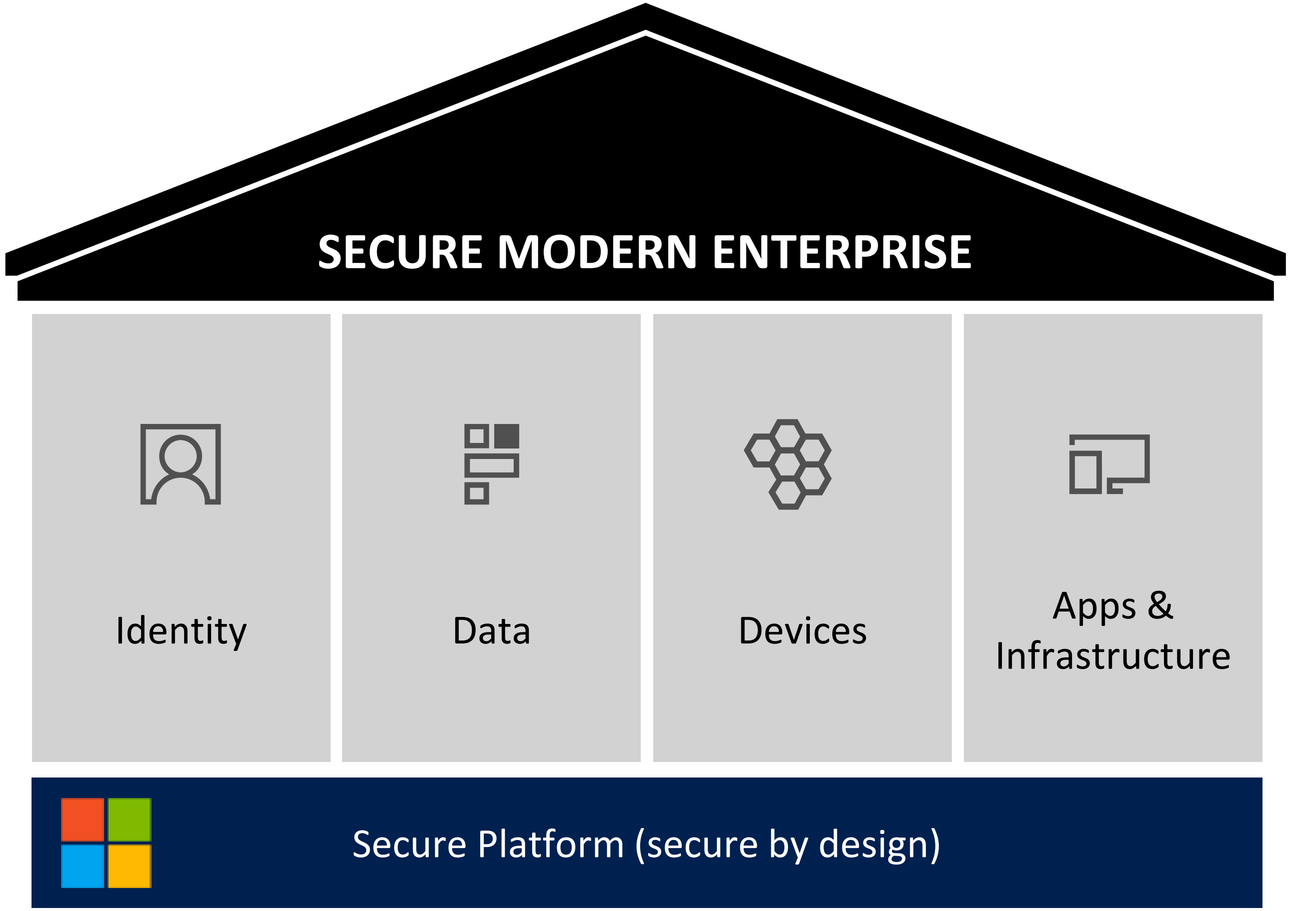
Rising costs
Increasing complexity
On-premises
The security landscape
Cloud
Evolving threats
Talent gap

The security market is segmented and confusing


Discovery
Identity governance
Single-sign on
Mobile Device & Application Management
Data Loss Prevention
Mobile Data Loss Prevention
Secure collaboration
Information Rights Management
Cloud Data Loss Prevention
User & Entity Behavioral Analytics
Cloud anomaly detection
Conditional access
Identity & Access Management
Cloud visibility
Cloud Access Security Broker
Threat Detection
SIEM

The secure modern enterprise

Aligned to business objectives and current threat environment



SECURE MODERN ENTERPRISE

Identity

Data

Devices

Apps & Infrastructure

Secure Platform (secure by design)

Identity

Embraces identity as primary security perimeter and protects identity systems, admins, and credentials as top priorities

Data

Aligns security investments with business priorities including identifying and securing communications, data, and applications

Devices

Accesses assets from trusted devices with hardware security assurances, great user experience, and advanced threat detection

Apps & Infrastructure

Operates on modern platform and uses cloud intelligence to detect and remediate both vulnerabilities and attacks

Identity & access management

Protect users' identities & control access to valuable resources based on user risk level

Azure Active Directory
Conditional Access
Windows Hello
Windows Credential Guard

Information protection

Ensure documents and emails are seen only by authorized people

Azure Information Protection
Office 365 Data Loss Prevention
Windows Information Protection
Microsoft Cloud App Security
Office 365 Advanced Security Mgmt.
Microsoft Intune

Threat protection

Protect against advanced threats and recover quickly when attacked

Advanced Threat Analytics
Windows Defender Advanced Threat Protection
Office 365 Advanced Threat Protection
Office 365 Threat Intelligence

Security management

Gain visibility and control over security tools

Azure Security Center
Office 365 Security Center
Windows Defender Security Center

5 teams
>400 eng.

> 20M
Protected users

>15K
Protected organizations

>1M
Protected servers

>50M
Items are labeled per month

>30M
Protected devices

Identity & access management

Protect users' identities & control access to valuable resources based on user risk level

Azure Active Directory
Conditional Access
Windows Hello
Windows Credential Guard

Information protection

Ensure documents and emails are seen only by authorized people

Azure Information Protection
Office 365 Data Loss Prevention
Windows Information Protection
Microsoft Cloud App Security
Office 365 Advanced Security Mgmt.
Microsoft Intune

Threat protection

Protect against advanced threats and recover quickly when attacked

Advanced Threat Analytics
Windows Defender Advanced Threat Protection
Office 365 Advanced Threat Protection
Office 365 Threat Intelligence
Azure Advanced Threat Protection

Security management

Gain visibility and control over security tools

Azure Security Center
Office 365 Security Center
Windows Defender Security Center

Microsoft

User-centric Security

ENFORCE CONDITIONAL ACCESS

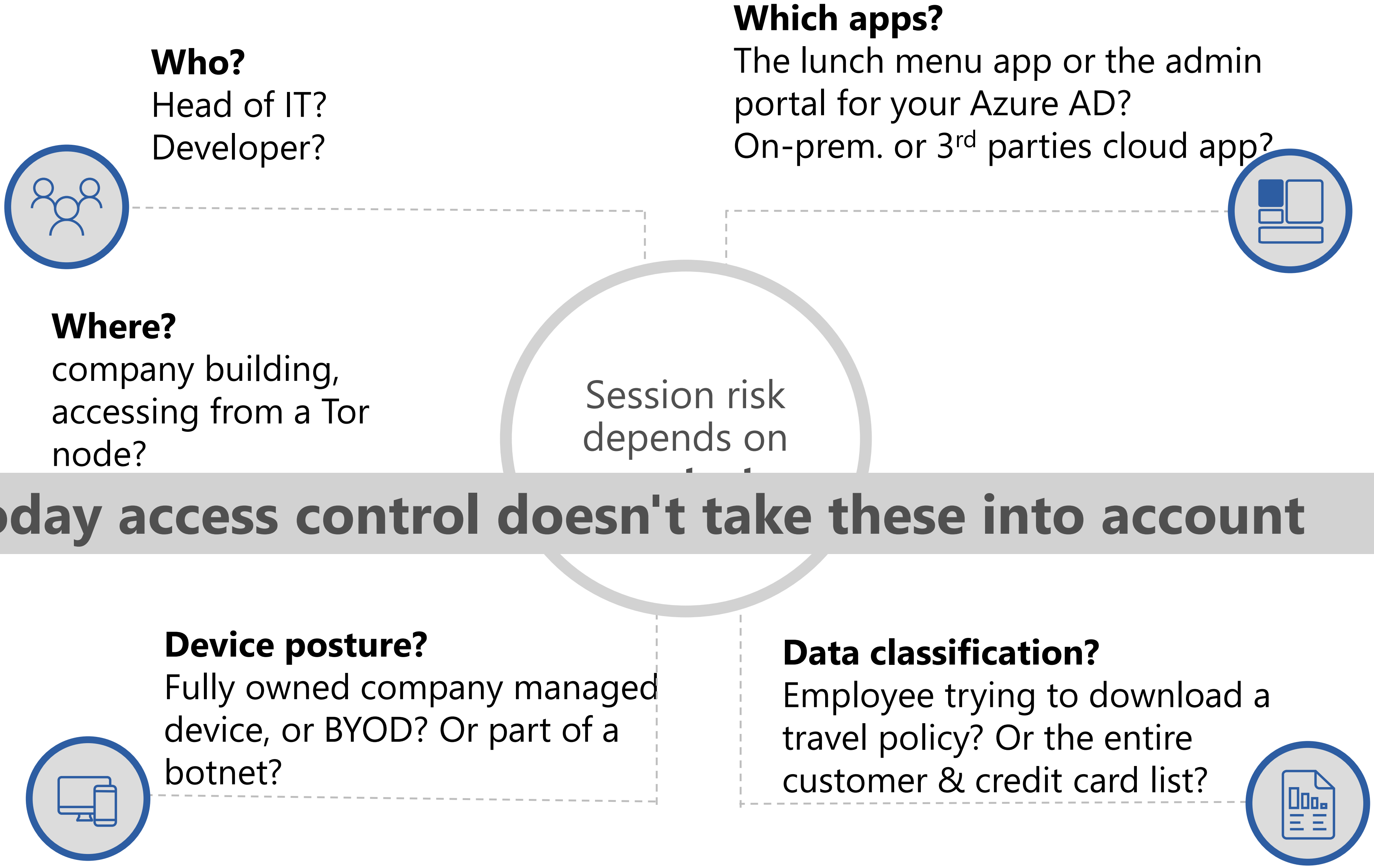
Common identity & context awareness

Strong Identity control

- Manage identities and access at scale **on-premises** and in the **cloud**
- Offers one common identity for secure access to all corporate resources with **single sign-on**
- Built in **MFA solution**

ENFORCE CONDITIONAL ACCESS

Why access should be context aware?



Who?
Head of IT?
Developer?

Which apps?
The lunch menu app or the admin portal for your Azure AD?
On-prem. or 3rd parties cloud app?

Where?
company building, accessing from a Tor node?

Session risk depends on

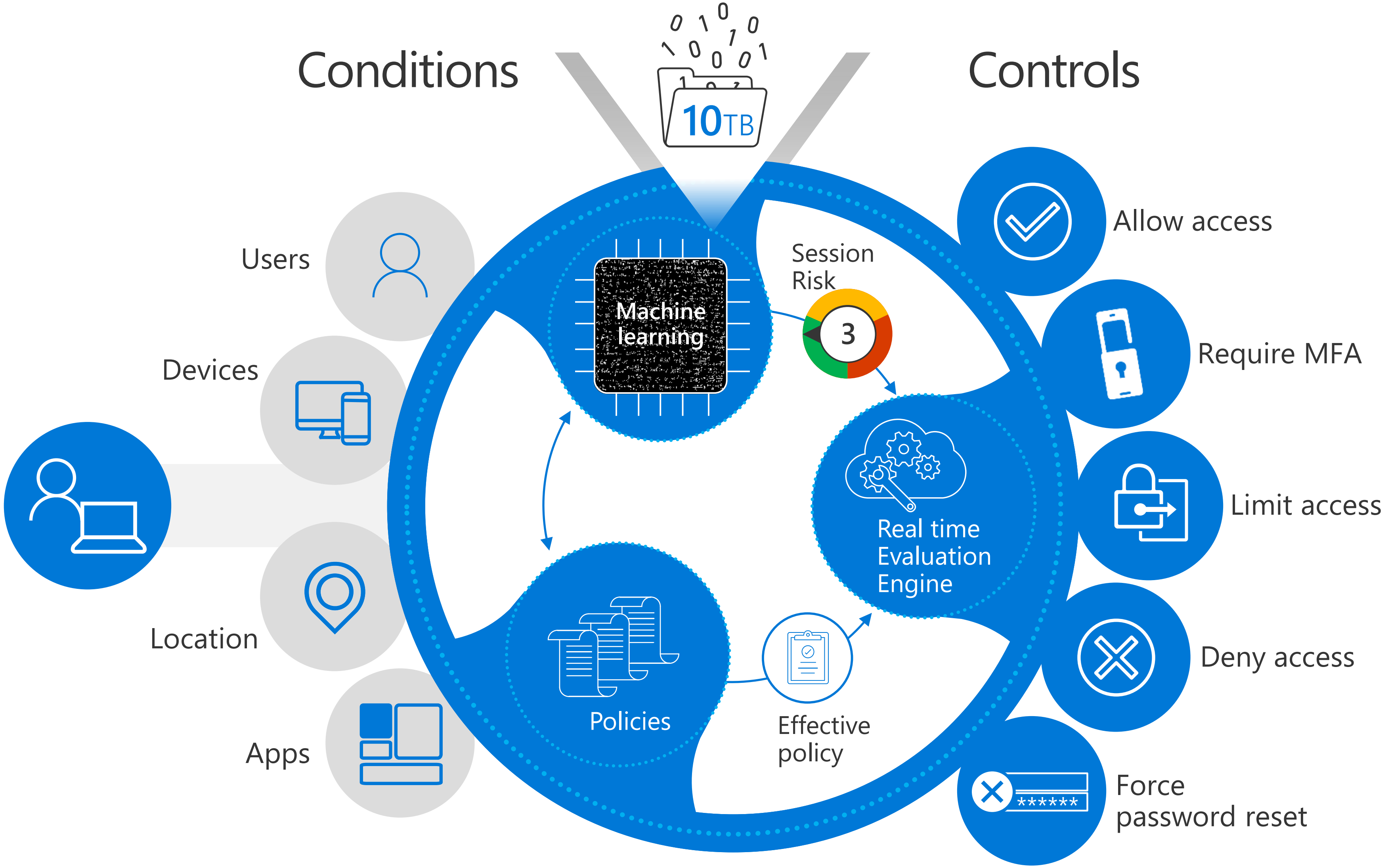
Device posture?
Fully owned company managed device, or BYOD? Or part of a botnet?

Data classification?
Employee trying to download a travel policy? Or the entire customer & credit card list?

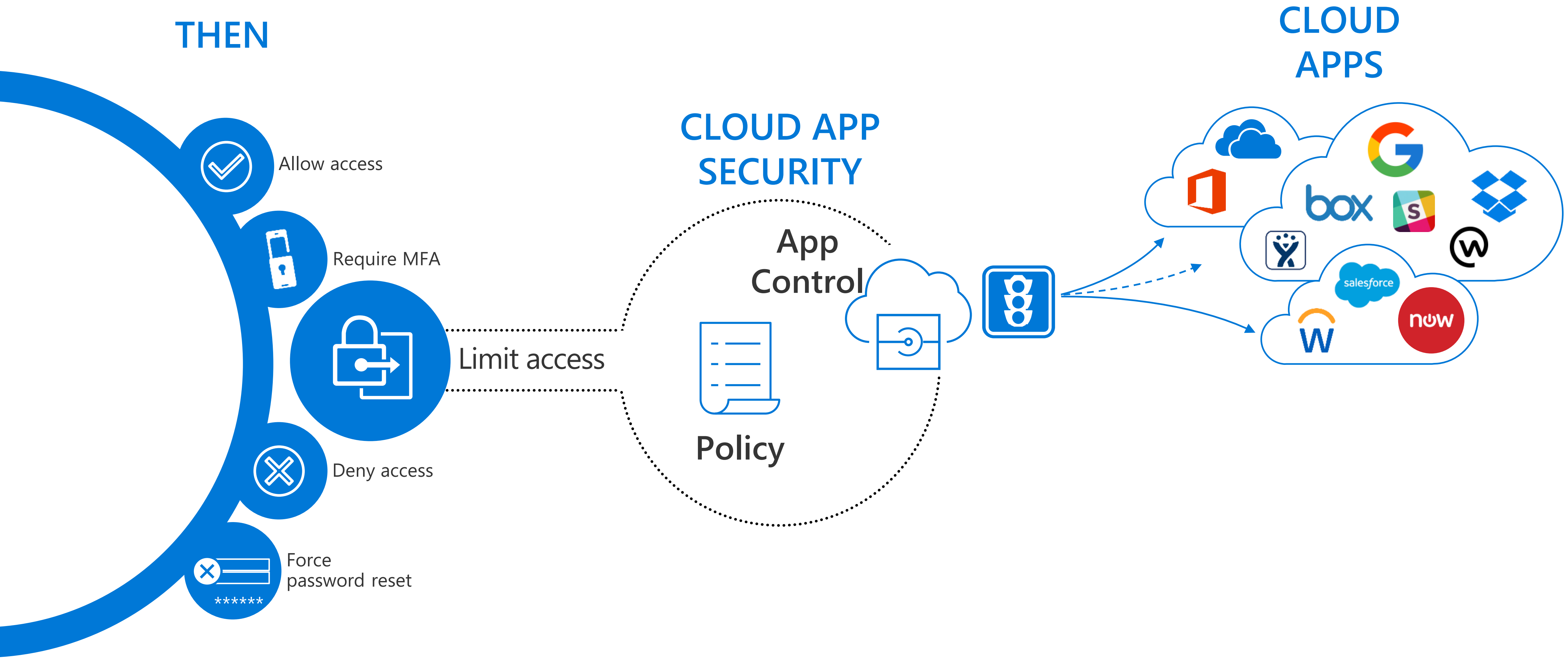
Today access control doesn't take these into account

ENFORCE
CONDITIONAL
ACCESS

Conditional Access



Introducing Conditional Access App Control



THEN

Allow access

Require MFA

Limit access

Deny access

Force password reset

CLOUD APP SECURITY

App Control

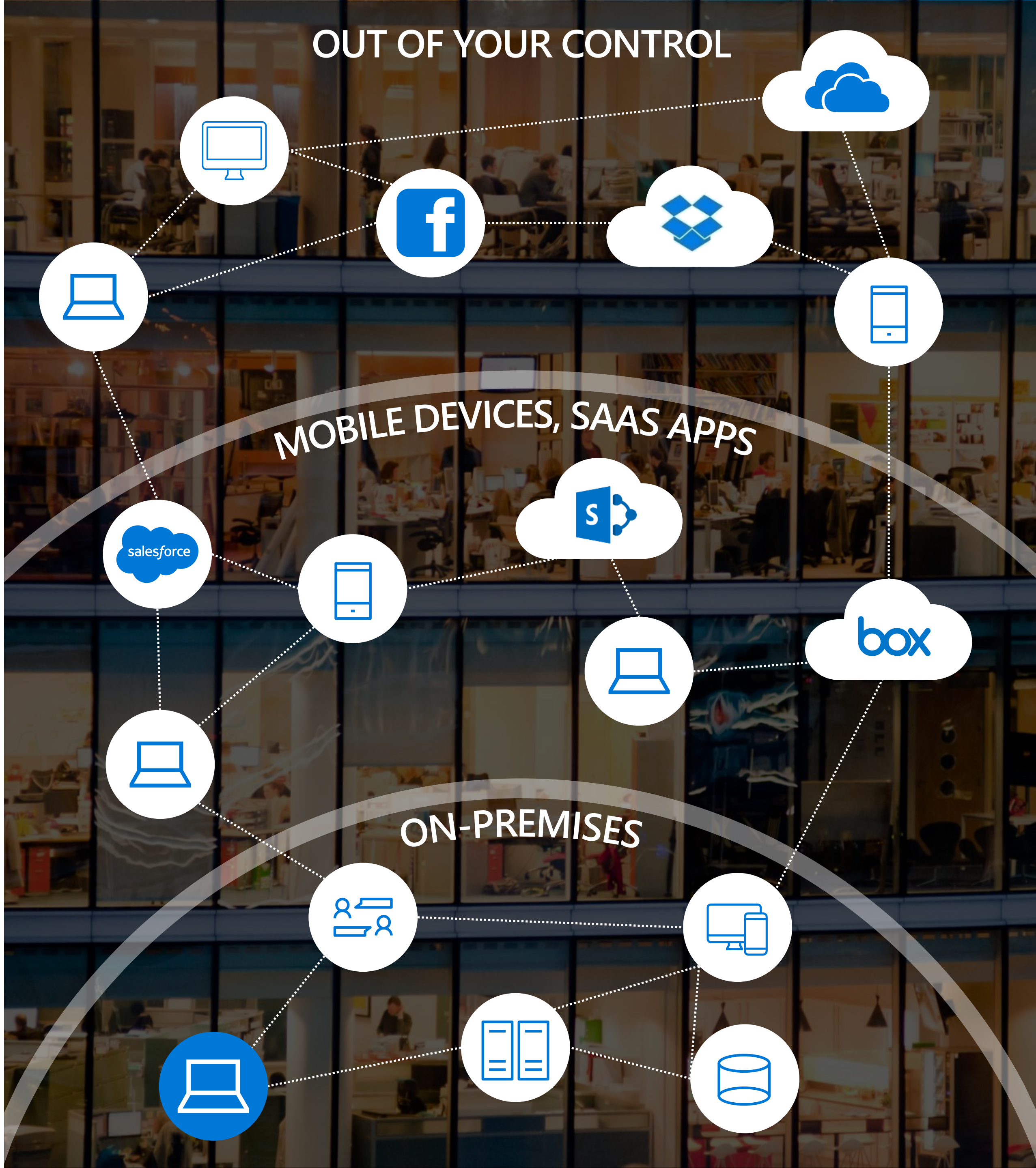
Policy

CLOUD APPS

PROTECT YOUR DATA ANYWHERE

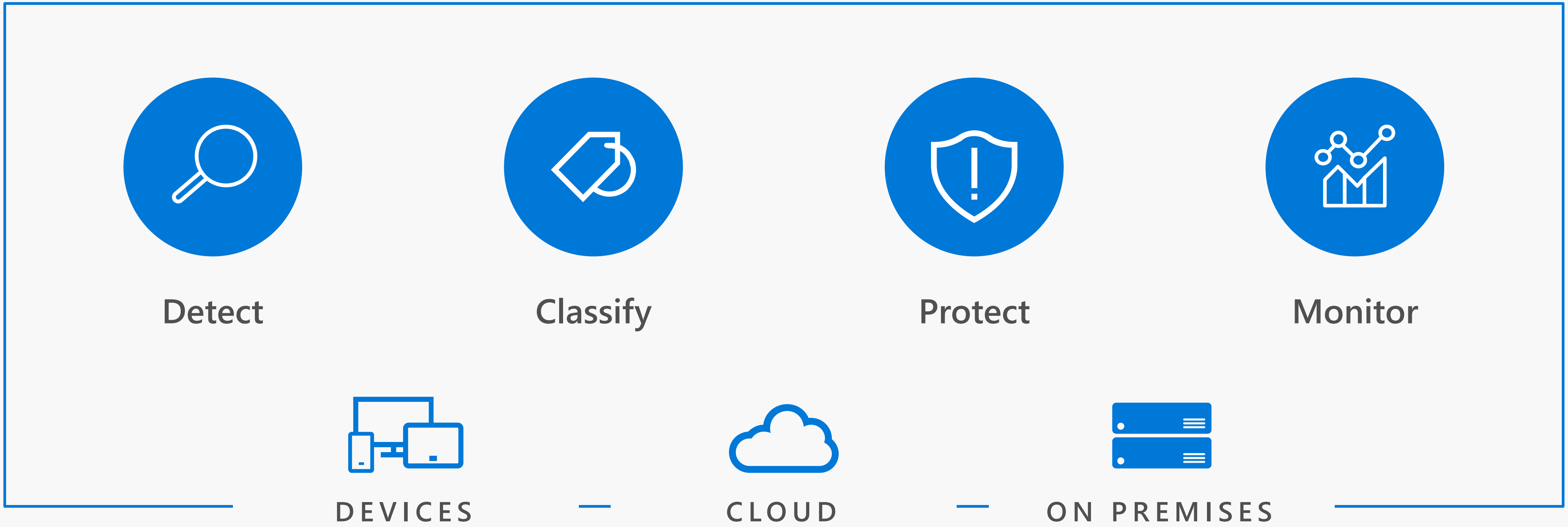
Unified Information Protection

How much control do you have over data?



MICROSOFT’S APPROACH TO **INFORMATION PROTECTION**

Comprehensive protection of sensitive data throughout the lifecycle – inside and outside the organization



Detect

Classify

Protect

Monitor

DEVICES

CLOUD

ON PREMISES

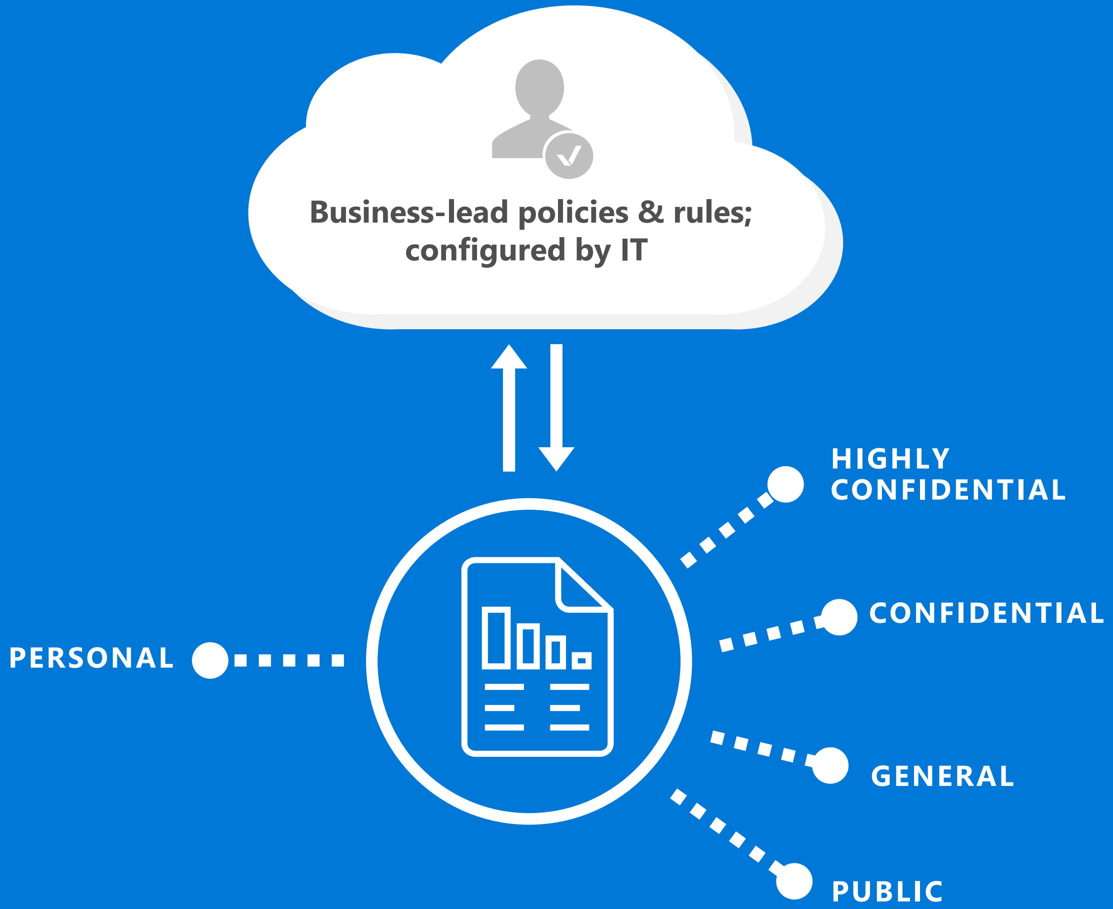
CLASSIFY ON **CREATION**

Automatic classification
Policies can be set by IT Admins for automatically applying classification and protection to data, right on creation

Recommended classification
Based on the content you're working on, you can be prompted with suggested classification

Manual reclassification
You can override a classification and optionally be required to provide a justification

User-specified classification
Users can choose to apply a sensitivity label to the email or file they are working on with a single click

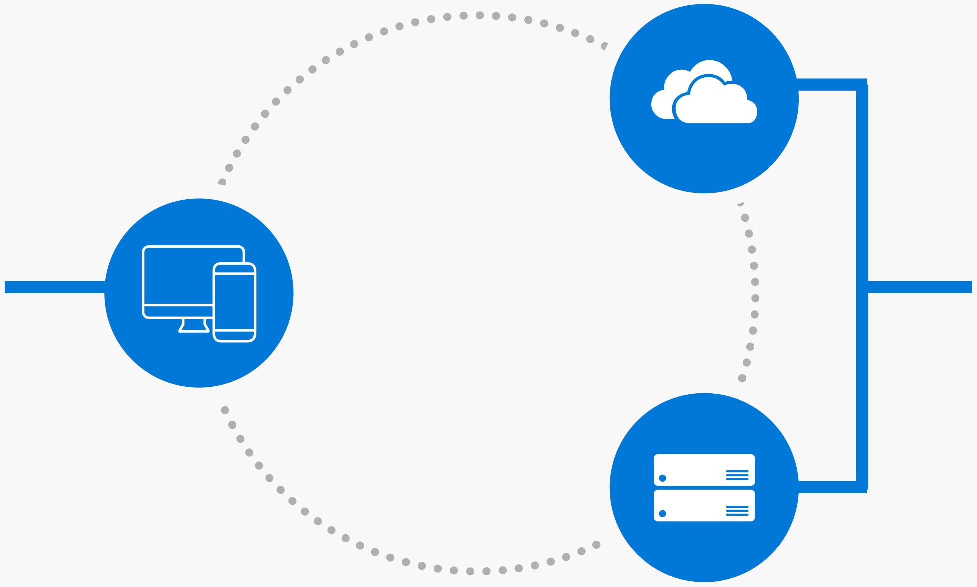


Business-lead policies & rules; configured by IT

PROTECT SENSITIVE DATA ACROSS YOUR ENVIRONMENT

Devices

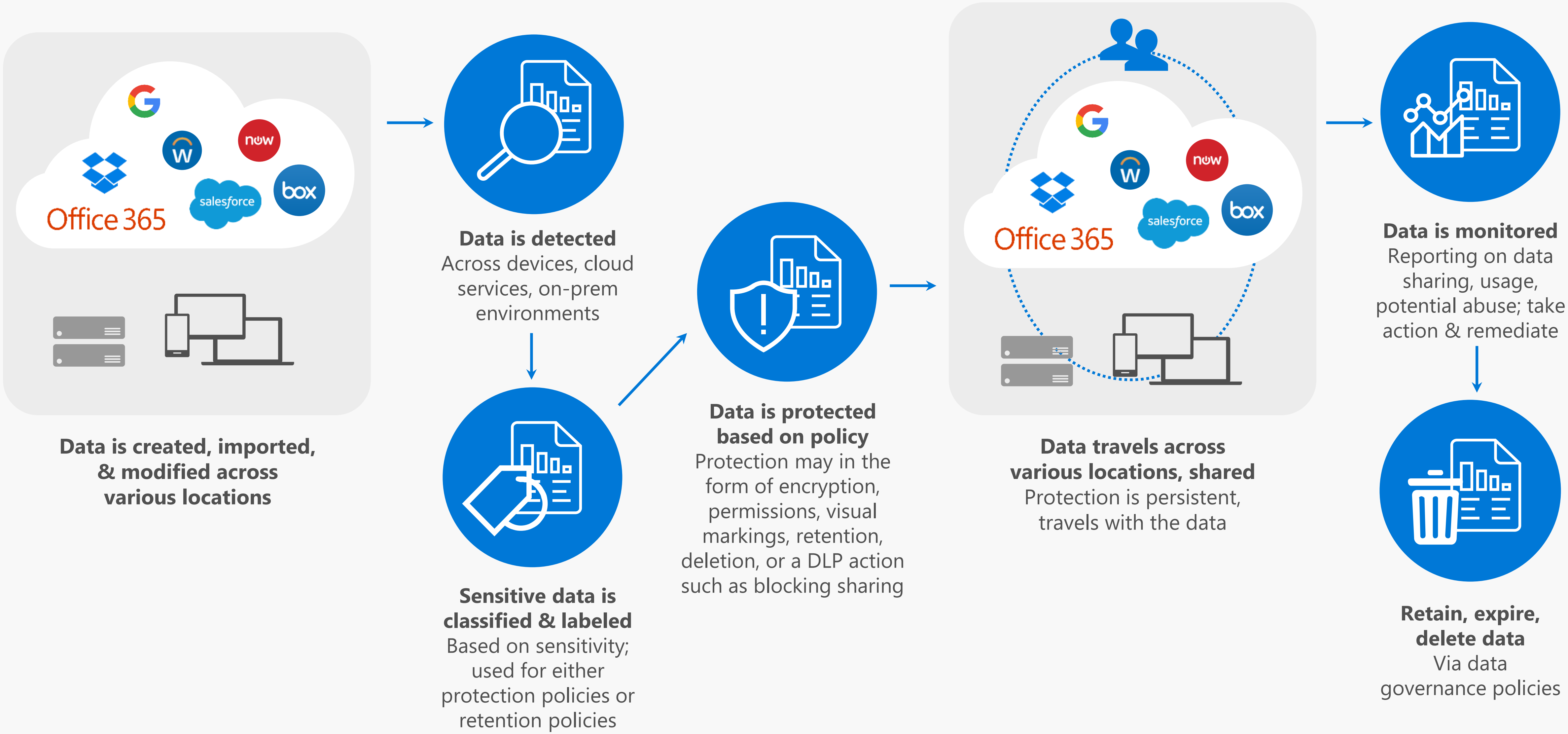
- Drive encryption
- Remote wipe
- Business data separation



Cloud & on-premises

- File encryption
- Email encryption and rights protection
- Permissions and rights-based restrictions
- DLP actions to prevent sharing
- Policy tips & notifications for end-users
- Visual markings in documents
- Control and protect data in cloud apps with granular policies and anomaly detection
- Data retention, expiration, deletion

THE LIFECYCLE OF A **SENSITIVE FILE**



Data is created, imported, & modified across various locations

Data is detected
Across devices, cloud services, on-prem environments

Sensitive data is classified & labeled
Based on sensitivity; used for either protection policies or retention policies

Data is protected based on policy
Protection may in the form of encryption, permissions, visual markings, retention, deletion, or a DLP action such as blocking sharing

Data travels across various locations, shared
Protection is persistent, travels with the data

Data is monitored
Reporting on data sharing, usage, potential abuse; take action & remediate

Retain, expire, delete data
Via data governance policies

AUTOMATE DETECTION & REMEDIATION

Intelligence, detection & remediation

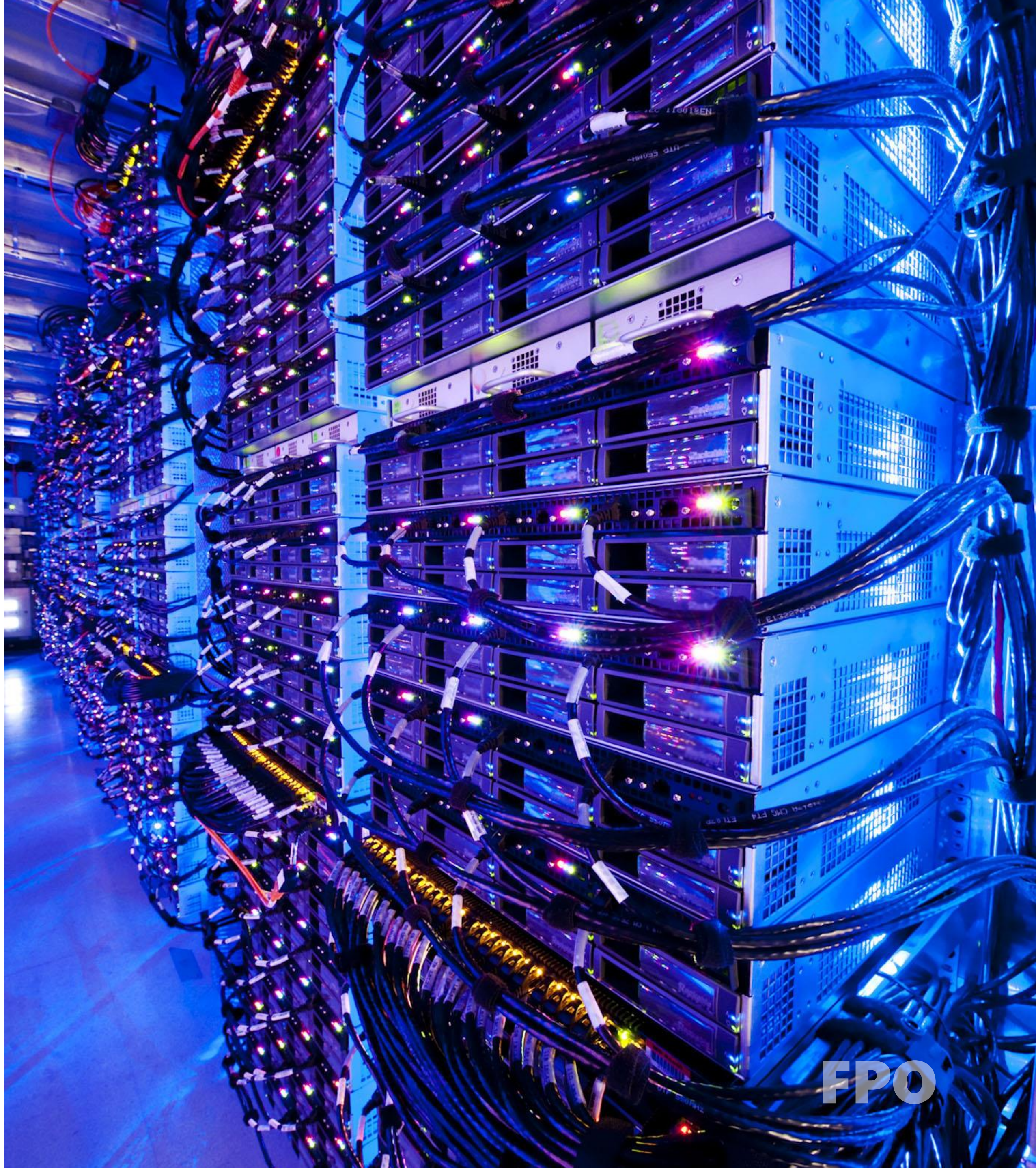
Detect & remediate attacks

91%

of cyberattacks and the resulting data breach begin with a spear phishing email

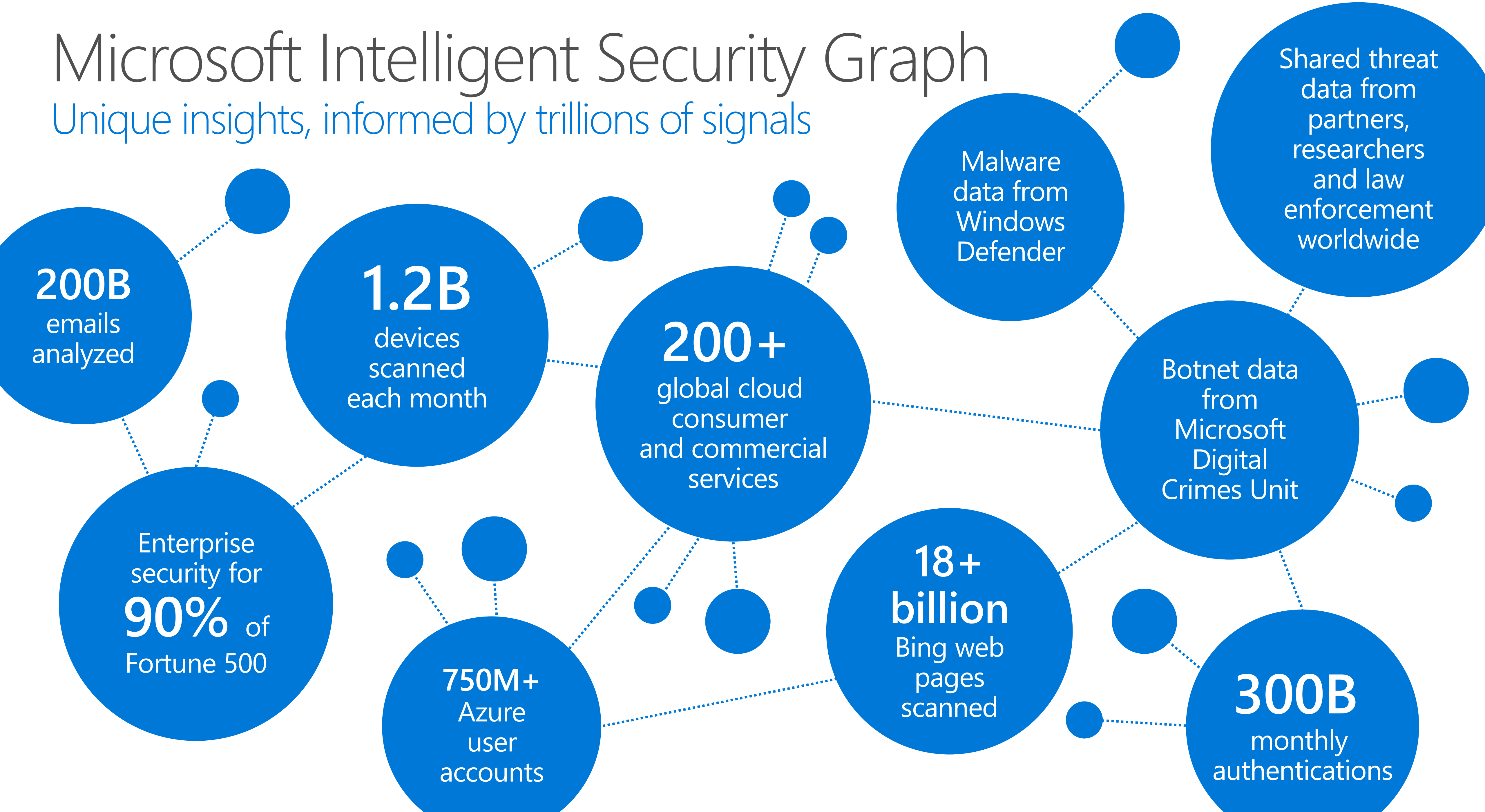
PhishMe 2016

How quickly are you able to detect attacks?



Microsoft Intelligent Security Graph

Unique insights, informed by trillions of signals



200B emails analyzed

1.2B devices scanned each month

200+ global cloud consumer and commercial services

Malware data from Windows Defender

Shared threat data from partners, researchers and law enforcement worldwide

Botnet data from Microsoft Digital Crimes Unit

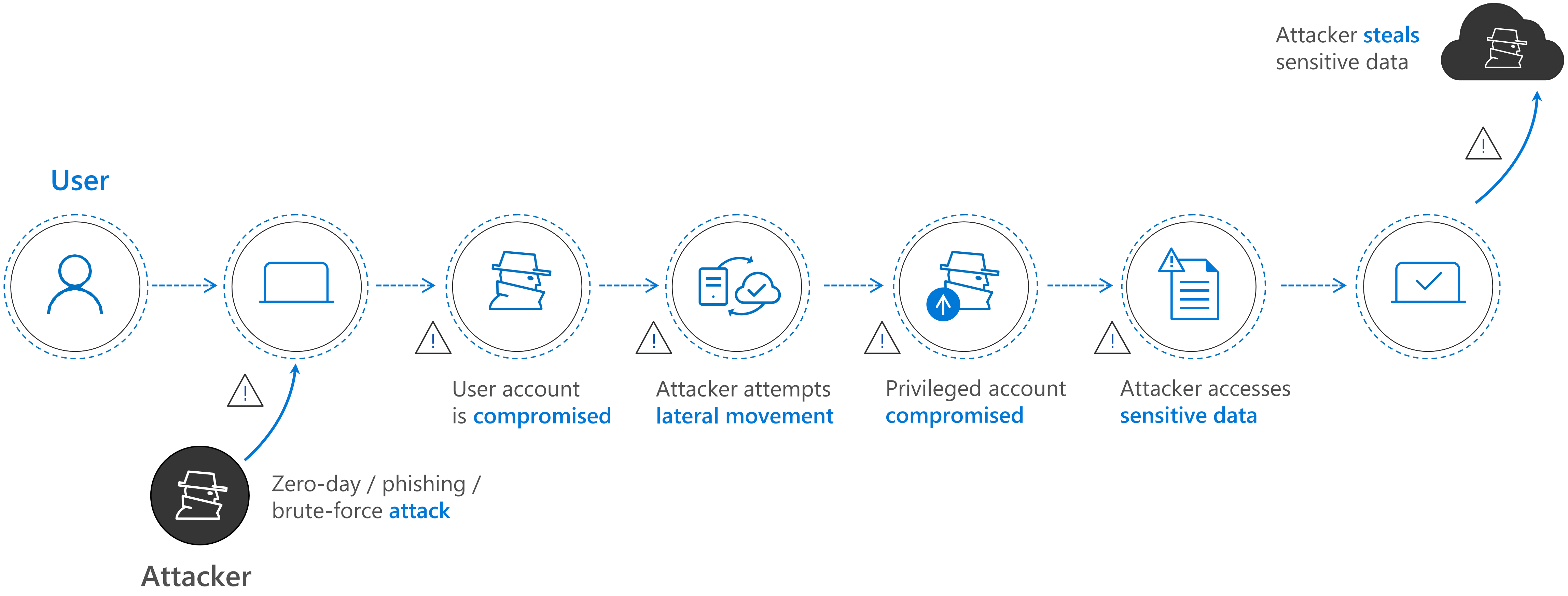
Enterprise security for **90%** of Fortune 500

750M+ Azure user accounts

18+ billion Bing web pages scanned

300B monthly authentications

The anatomy of an attack



Attacker **steals** sensitive data

User

User account is **compromised**

Attacker attempts **lateral movement**

Privileged account **compromised**

Attacker accesses **sensitive data**

Zero-day / phishing / brute-force **attack**

Attacker

⚠ Anomalous user behavior

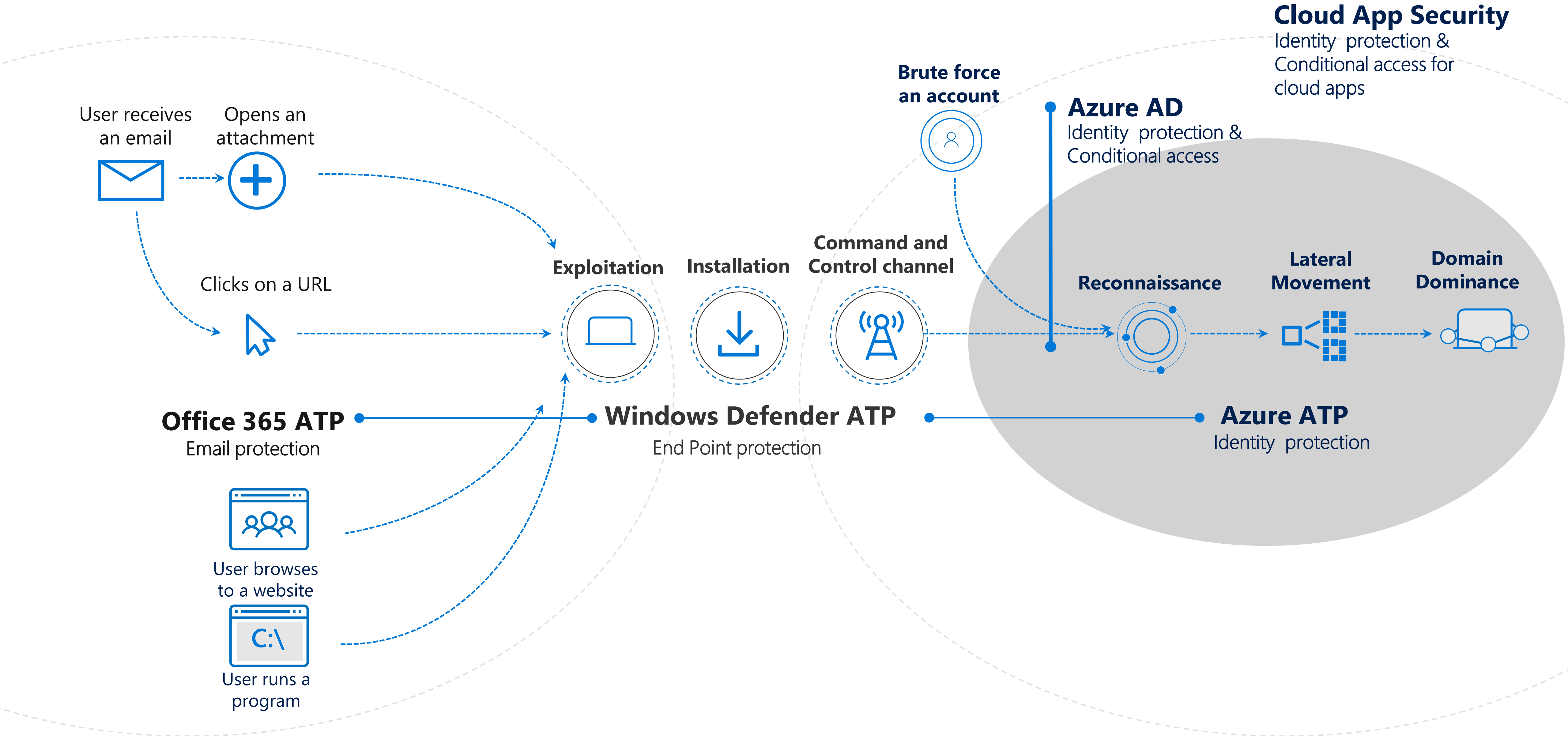
Unfamiliar sign-in location

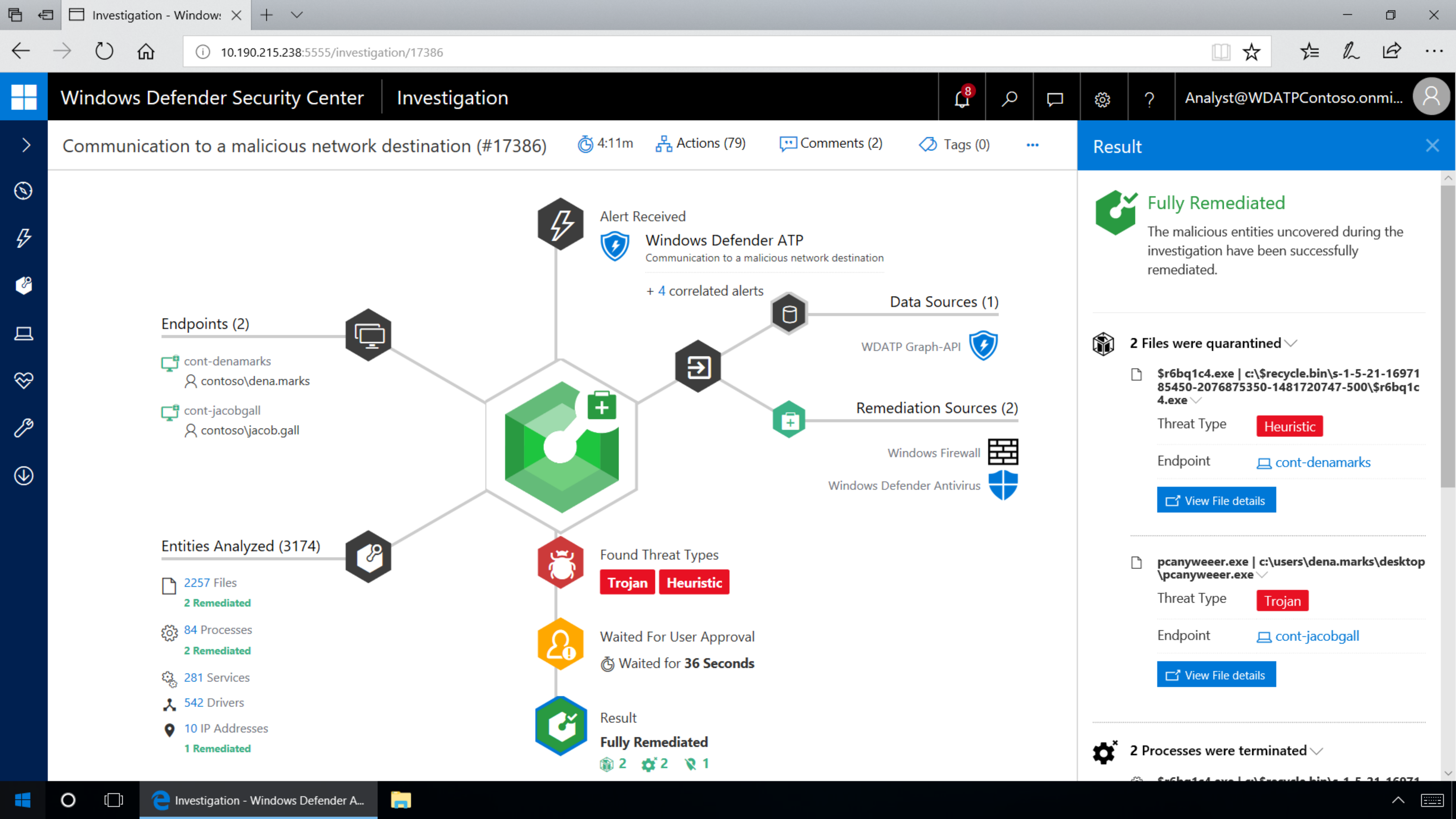
⚠ Lateral movement attacks

Escalation of privileges

Account impersonation

Maximize detection coverage throughout the attack stages




Investigation - Window:
10.190.215.238:5555/investigation/17386
Windows Defender Security Center
Investigation
8
Analyst@WDATPContoso.onmi...
Investigation - Windows Defender A...

Communication to a malicious network destination (#17386)

4:11m | Actions (79) | Comments (2) | Tags (0) | ···

Alert Received

Windows Defender ATP

Communication to a malicious network destination

+ 4 correlated alerts

Data Sources (1)

WDATP Graph-API

Endpoints (2)

cont-denamarks

contoso\dena.marks

cont-jacobgall

contoso\jacob.gall

Remediation Sources (2)

Windows Firewall

Windows Defender Antivirus

Entities Analyzed (3174)

2257 Files

2 Remediated

84 Processes

2 Remediated

281 Services

542 Drivers

10 IP Addresses

1 Remediated

Found Threat Types

Trojan Heuristic

Waited For User Approval

Waited for **36 Seconds**

Result

Fully Remediated

2 2 1

Result

Fully Remediated

The malicious entities uncovered during the investigation have been successfully remediated.

2 Files were quarantined

$r6bq1c4.exe | c:\$recycle.bin\s-1-5-21-1697185450-2076875350-1481720747-500\$r6bq1c4.exe

Threat Type	Heuristic
Endpoint	cont-denamarks

View File details

pcanyweeer.exe | c:\users\dena.marks\desktop\pcanyweeer.exe

Threat Type	Trojan
Endpoint	cont-jacobgall

View File details

2 Processes were terminated

$r6bq1c4.exe | c:\$recycle.bin\s-1-5-21-16971

Microsoft