Microsoft | 2017 Microsoft Cloud and Hosting Summit

Digital Transformation@work

Empowering Together

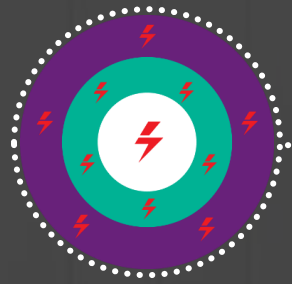
Digital Transformation @ work

Empowering Together

Identity-driven security

Nasos Kladakis,
Sr. Product Marketing Manager, @Akladakis
@AzureAD
Microsoft

New blind spots for IT



Cybercrimes

32% of businesses reported to be affected by cybercrimes

Data breaches

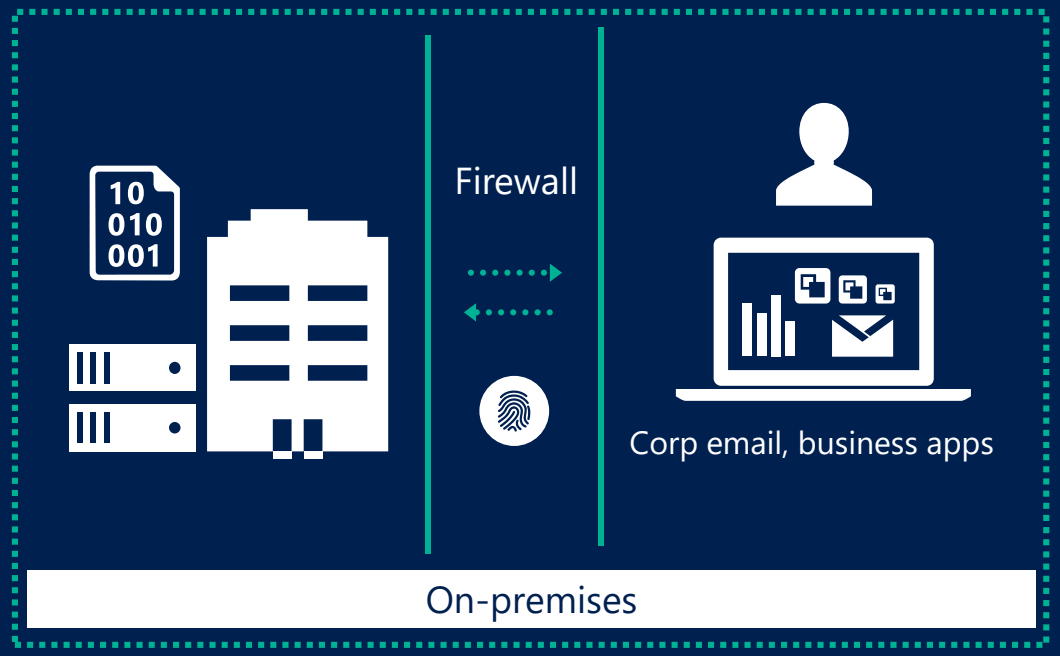
63% of confirmed data breaches involve weak, default, or stolen passwords

Shadow IT

>80% of employees admit using non-approved SaaS apps for work purposes

The security landscape has changed

LIFE **BEFORE CLOUD AND MOBILITY**

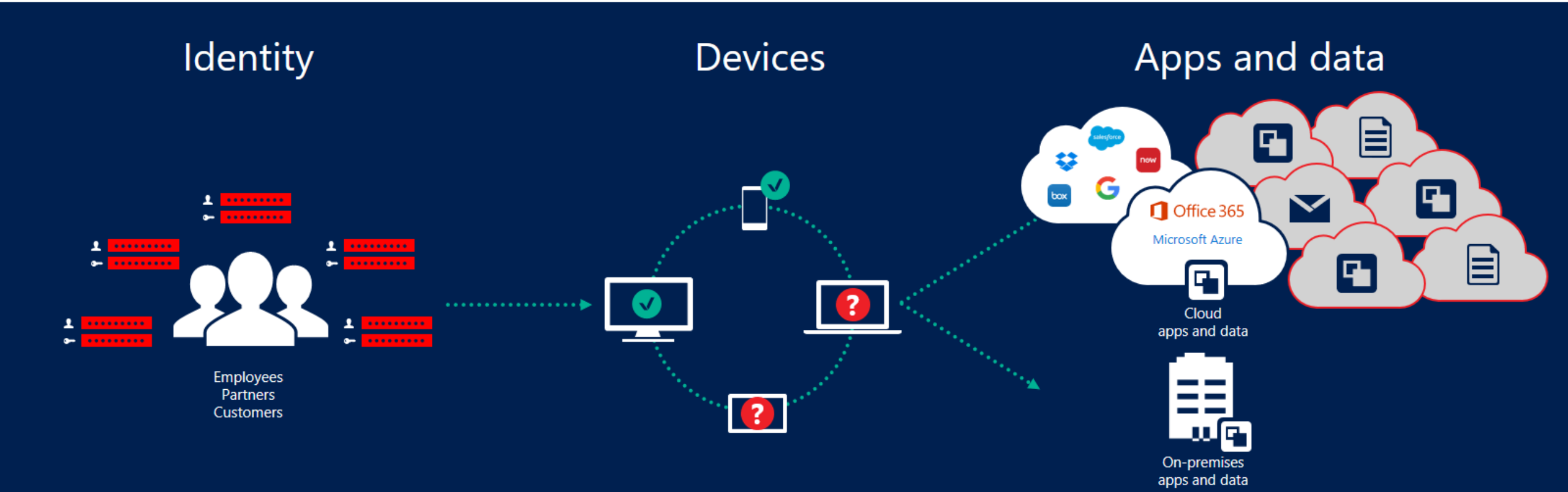


- Access via managed devices and networks
- Layers of defense protecting internal apps
- Known security perimeter

LIFE **AFTER CLOUD AND MOBILITY**

- Open access for users – any device, any network
- Unrestricted sharing methods – users decide how to share
- Cloud app ecosystem
- Limited visibility and control

Security landscape has changed



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

A need for holistic and innovative security

Transitioning to cloud and mobility

- End users making non-compliant choices
- Lack of visibility and control for cloud apps
- Controlling/securing critical data across devices

New attack landscape

- Credential theft
- Changes in attackers' techniques
- Costly recovery from advanced attacks

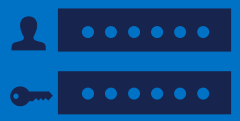
Traditional security solutions

- Complex
- Not up to the challenge
- False positives

Our approach to the security challenge

Holistic

Addresses security challenges across users (identities), devices, data, apps, and platforms—on-premises and in the cloud



Identity-driven

Offers one protected common identity for secure access to all corporate resources, on-premises and in the cloud, with risk-based conditional access

Innovative

Protects your data from new and changing cybersecurity attacks

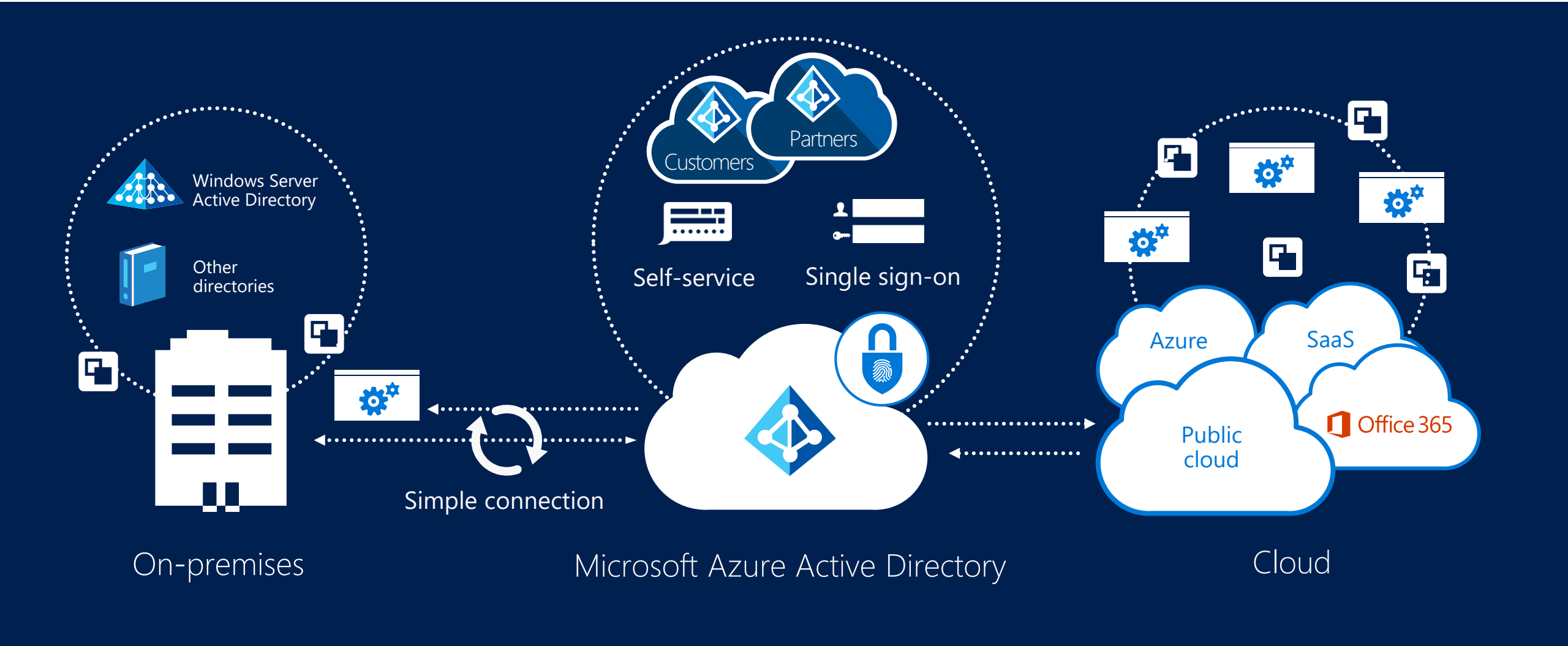
Intelligent

Enhances threat and anomaly detection with the Microsoft Intelligent Security Graph driven by a vast amount of datasets and machine learning in the cloud

Why Identity is significant?

Identity as the core of enterprise mobility

Azure Active Directory as the control plane



Identity is the new control plane

1000s of apps,
1 identity

Enable business
without borders

Manage access
at scale

Cloud-powered
protection

Azure Active Directory at the core of your business

Our approach to security challenge

Holistic. Innovative. Intelligent.

Protect at the front door

Safeguard your resources at the front door with innovative and advanced risk-based conditional accesses

Protect your data anywhere

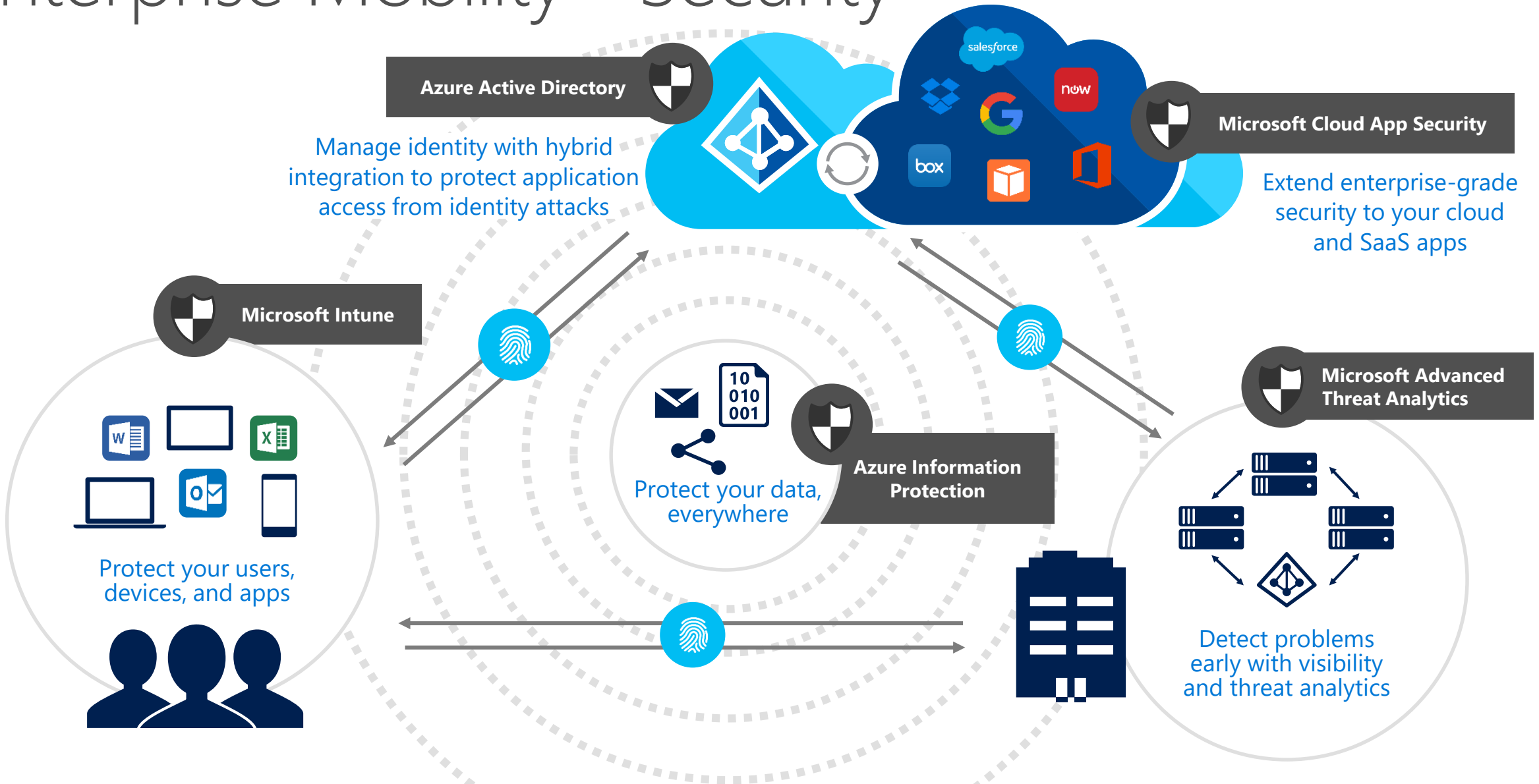
Discover and gain deeper visibility into user, device, and data activity on-premises and in the cloud.

Detect threats & remediate

Discover anomalies by on-going analytics. Uncover suspicious activity and pinpoint threats with deep visibility and ongoing behavioral analytics.

IDENTITY-DRIVEN SECURITY

Enterprise Mobility + Security



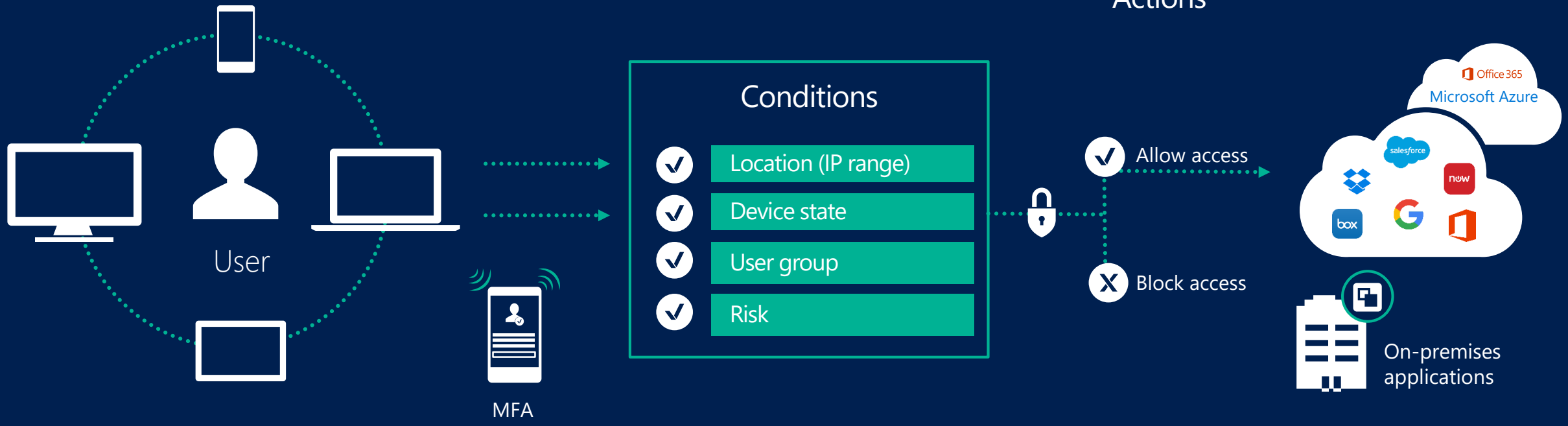
Identity-Driven Security

Protect at the front door

Protect your data anywhere

Detect attacks & remediate

Protect at the front door



How can I protect my organization at the front door?

Azure Active Directory Identity Protection

Risk-based conditional access

Privileged Identity Management

Azure Active Directory Identity Protection

Identity Protection at its best

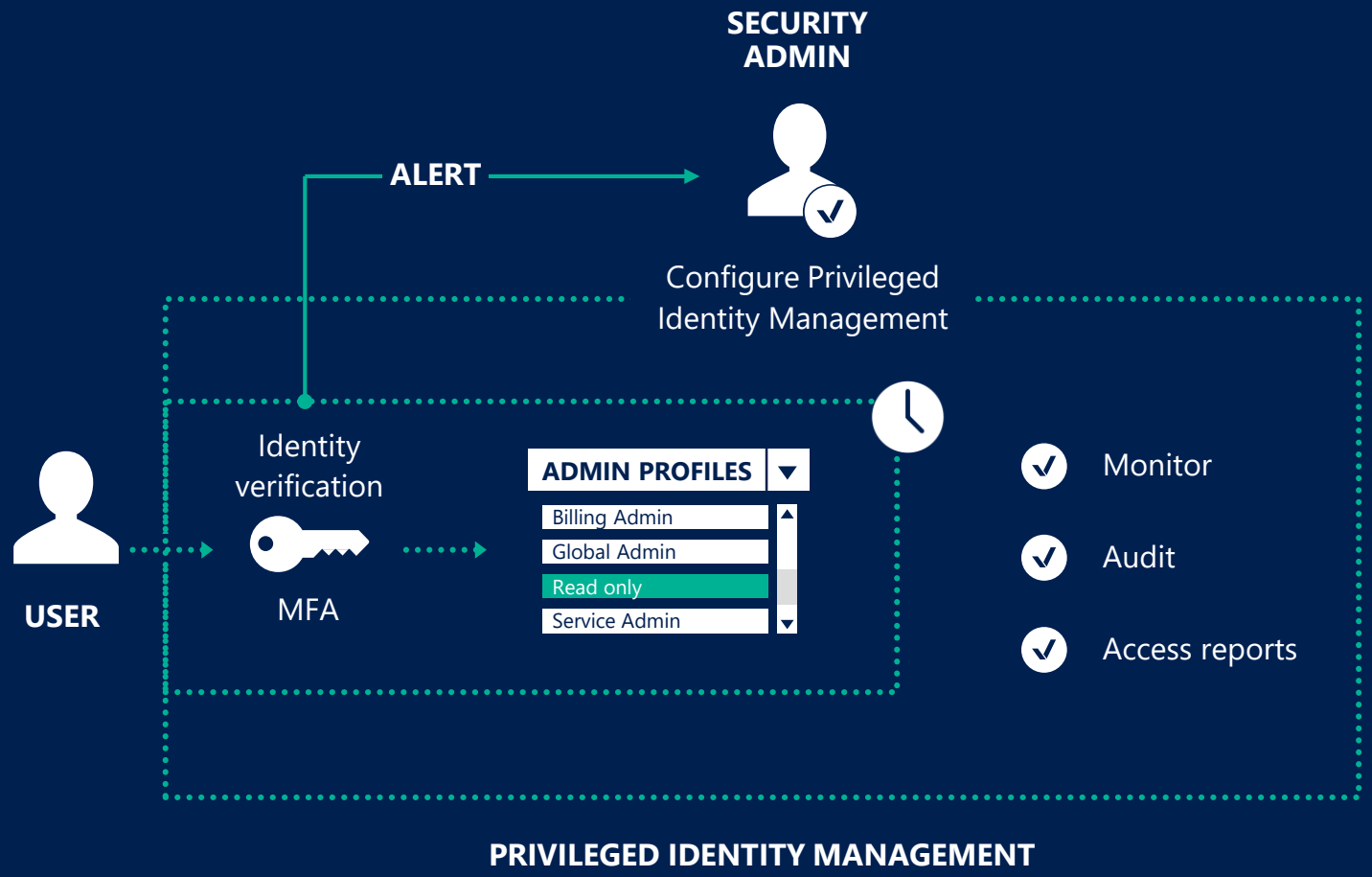
- Gain insights from a consolidated view of machine learning-based threat detection
- Remediation recommendations
- Risk severity calculation
- Risk-based conditional access automatically protects against suspicious logins and compromised credentials

PROTECT AT THE FRONT DOOR

Privileged identity management

Discover, restrict, and monitor privileged identities

- Users need to activate their privileges to perform a task
- MFA enforced during activation process
- Alerts inform administrators about out-of-band changes
- Users retain privileges for a pre-configured amount of time
- Security admins can discover all privileged identities, view audit reports, and review everyone who is eligible to activate via access reviews

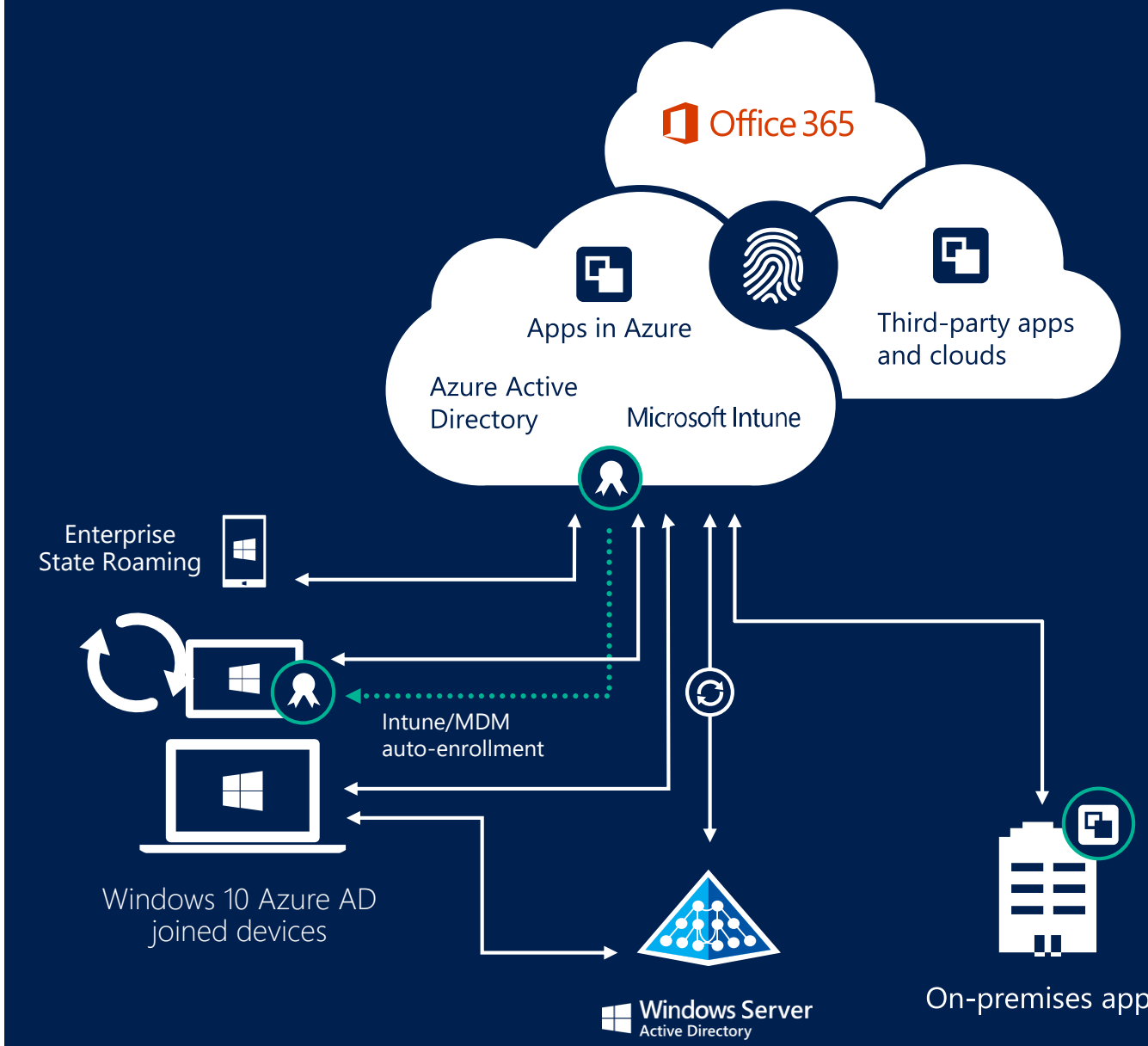


ENABLE BUSINESS WITHOUT BORDERS

Azure Active Directory Join for Windows 10

Azure Active Directory Join makes it possible to connect work-owned Windows 10 devices to your company's Azure Active Directory

- Enterprise-compliant services
- SSO from the desktop to cloud and on-premises applications with no VPN
- MDM auto-enrollment
- Support for hybrid environments



Demo

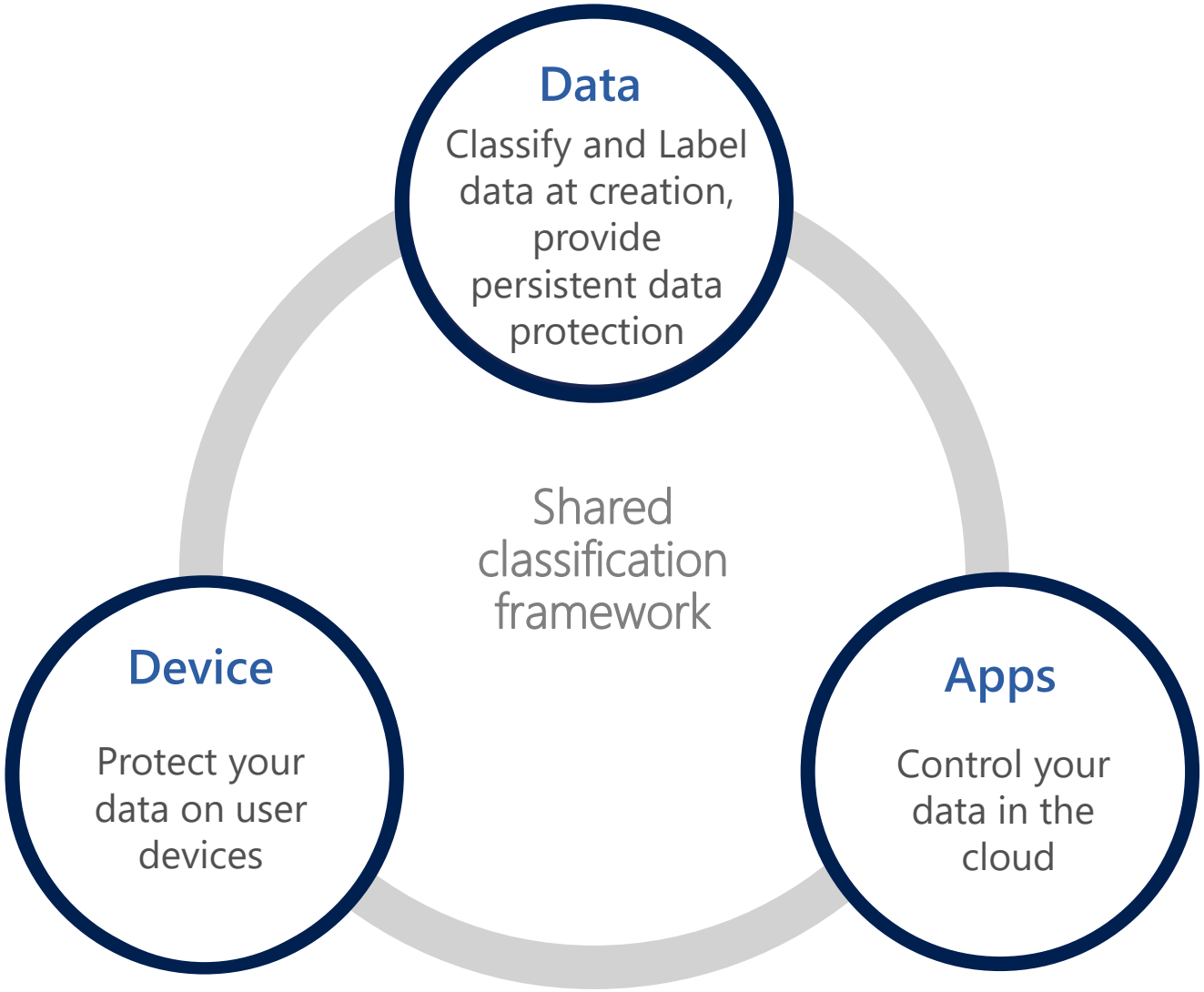
Identity-Driven Security

Protect at the front door

Protect your data anywhere

Detect attacks & remediate

Protect your data anywhere



Protect your data anywhere

How do I gain visibility and control of my cloud apps?

Cloud App Security

- Shadow IT Discovery
- Risk scoring
- Policies for data control

How do I prevent data leakage from my mobile apps?

Microsoft Intune

- DLP for Office 365 mobile apps
- Optional device management
- LOB app protection

How do I control data on-premises and in the cloud

Azure Information Protection

- Classify & Label
- Protect
- Monitor and Respond

Protect your data anywhere

Classification & labeling

Protect

Monitor & respond

Cloud App Security - Discovery

Shadow IT discovery

- Discover 13,000+ cloud apps in use—no agents required
- Identify all users, IP addresses, top apps, top users

Risk scoring

- Get an automated risk score driven by 60+ parameters
- See each app's risk assessment based on its security mechanisms and compliance regulations

Ongoing analytics

- Ongoing risk detection, powerful reporting, and analytics on users, usage patterns, upload/download traffic, and transactions
- Ongoing anomaly detection for discovered apps

PROTECT YOUR DATA ANYWHERE

Cloud App Security - Data control

Policy definition

- Set granular-control security policies for your approved apps
- Use out-of-the-box policies or customize your own

DLP and data sharing

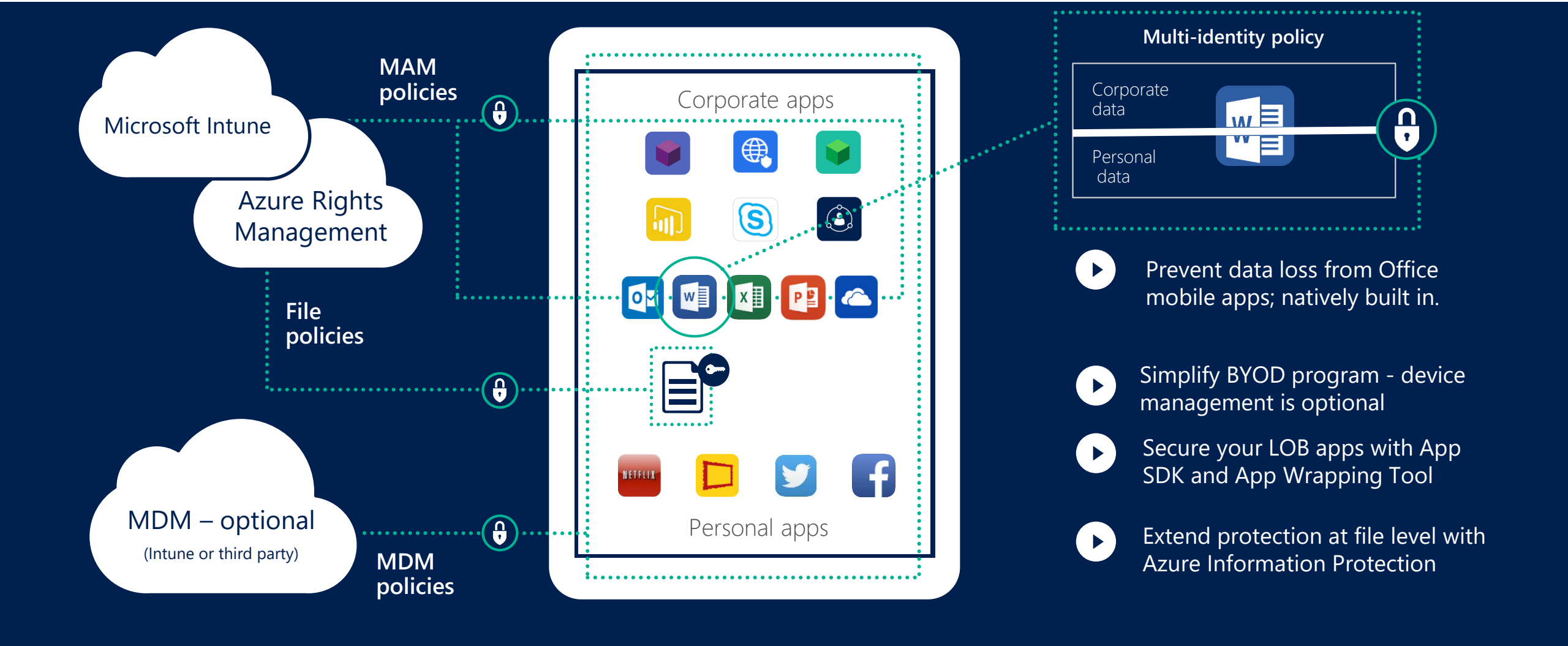
- Prevent data loss both inline and at rest
- Govern data in the cloud, such as files stored in cloud drives, attachments, or within cloud apps
- Use pre-defined templates or extend existing DLP policies

Policy enforcement

- Identify policy violations, investigate on a user, file, activity level
- Enforce actions such as quarantine and permissions removal
- Block sensitive transactions, limit sessions for unmanaged devices

PROTECT YOUR DATA ANYWHERE

Microsoft Intune: Mobile device and app management



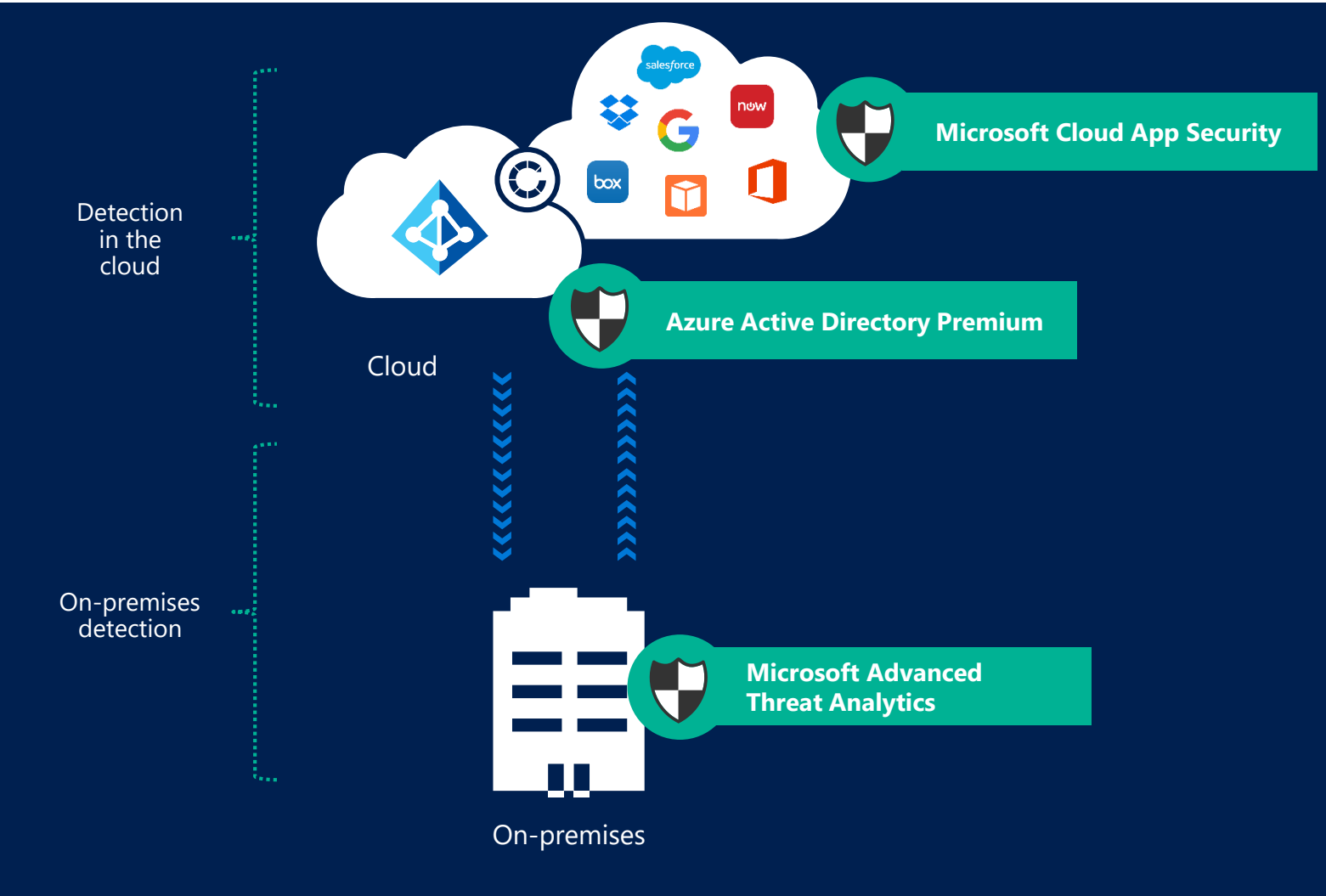
Identity-Driven Security

Protect at the front door

Protect your data anywhere

Detect attacks & remediate

Detect attacks and remediate



How do I detect attacks in the cloud?

Cloud App Security
(Application level)

- Behavioral analytics
- Anomaly detection

Azure Active Directory
(Identity level)

- Behavioral Analytics
- Security reporting and monitoring

How do I detect on-premises attacks?

Advanced Threat Analytics

- User and Entity Behavioral Analytics
- Abnormal behavior detection
- Known malicious attack and security vulnerabilities detection

DETECT ATTACKS AND REMEDIATE

Microsoft Advanced Threat Analytics

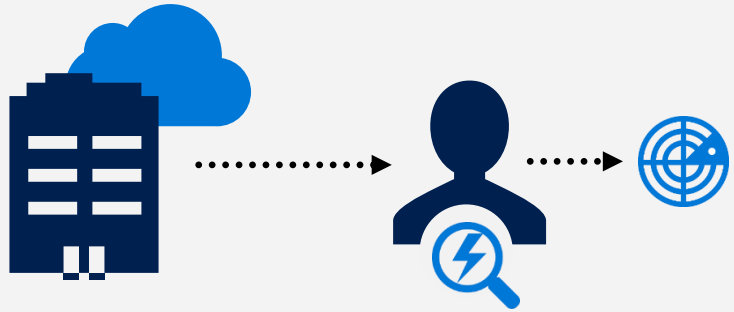
An on-premises platform to identify advanced security attacks and insider threats **before** they cause damage

Behavioral Analytics

Detection of advanced attacks and security risks

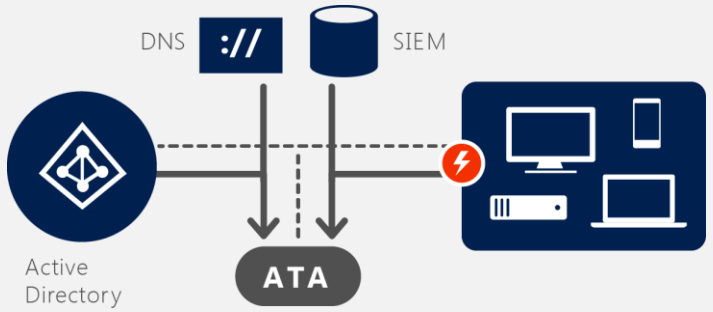
Advanced Threat Detection

Microsoft Advanced Threat Analytics brings the behavioral analytics concept to IT and the organization's users.



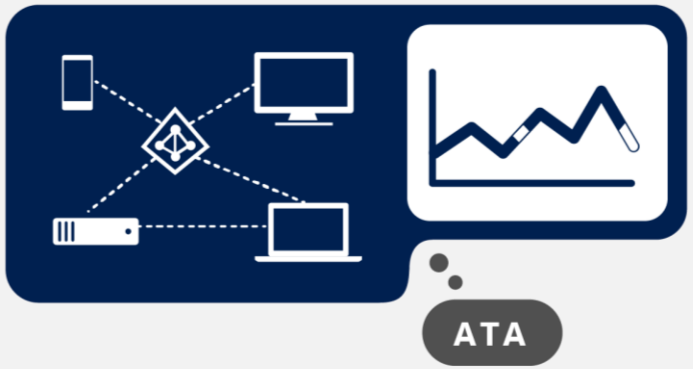
Microsoft Advanced Threat Analytics at work

1 Analyze



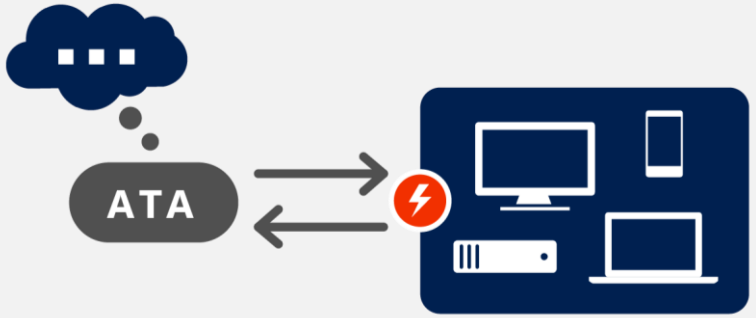
ATA analyzes all Active Directory-related traffic and collects relevant events from SIEM

2 Learn



ATA automatically learns all entities' behaviors

3 Detect



ATA builds the organizational security graph, detects abnormal behavior, protocol attacks, and weaknesses, and constructs an attack timeline

DETECT ATTACKS AND REMEDIATE

Threat prevention for your cloud apps with Cloud App Security

Behavioral analytics

- Identify anomalies in your cloud environment which may be indicative of a breach
- Leverage behavioral analytics (each user's interaction with SaaS apps) to assess risk in each transaction

Attack detection

- Identify and stop known attack pattern activities originating from risky sources with threat prevention enhanced with vast Microsoft threat intelligence
- **Coming soon:** send any file through real-time behavioral malware analysis

Identity-Driven Security

Protect at the front door

Protect your data anywhere

Detect attacks & remediate

Enhanced by Microsoft security intelligence

Microsoft Intelligent Security Graph

- Unique insights into the threat landscape
- Informed by trillions of signals from billions of sources
- Powered by inputs we receive across our endpoints, consumer services, commercial services, and on-premises technologies
- Anomaly detection that draws from our vast amount of threat intelligence, machine learning, security research, and development data