inetum.
realdolmen
Positive digital flow

Welkom

Zero Trust, de nieuwe norm in cybersecurityland uitgelegd

Met dank aan:

aruba
a Hewlett Packard
Enterprise company

AvePoint®

COMMVAULT®

FORTINET®

Microsoft

SAMSUNG

tenable®

inetum realdolmen

Positive digital flow

Zero Trust

De nieuwe norm in cybersecurityland

Koen Tamsyn

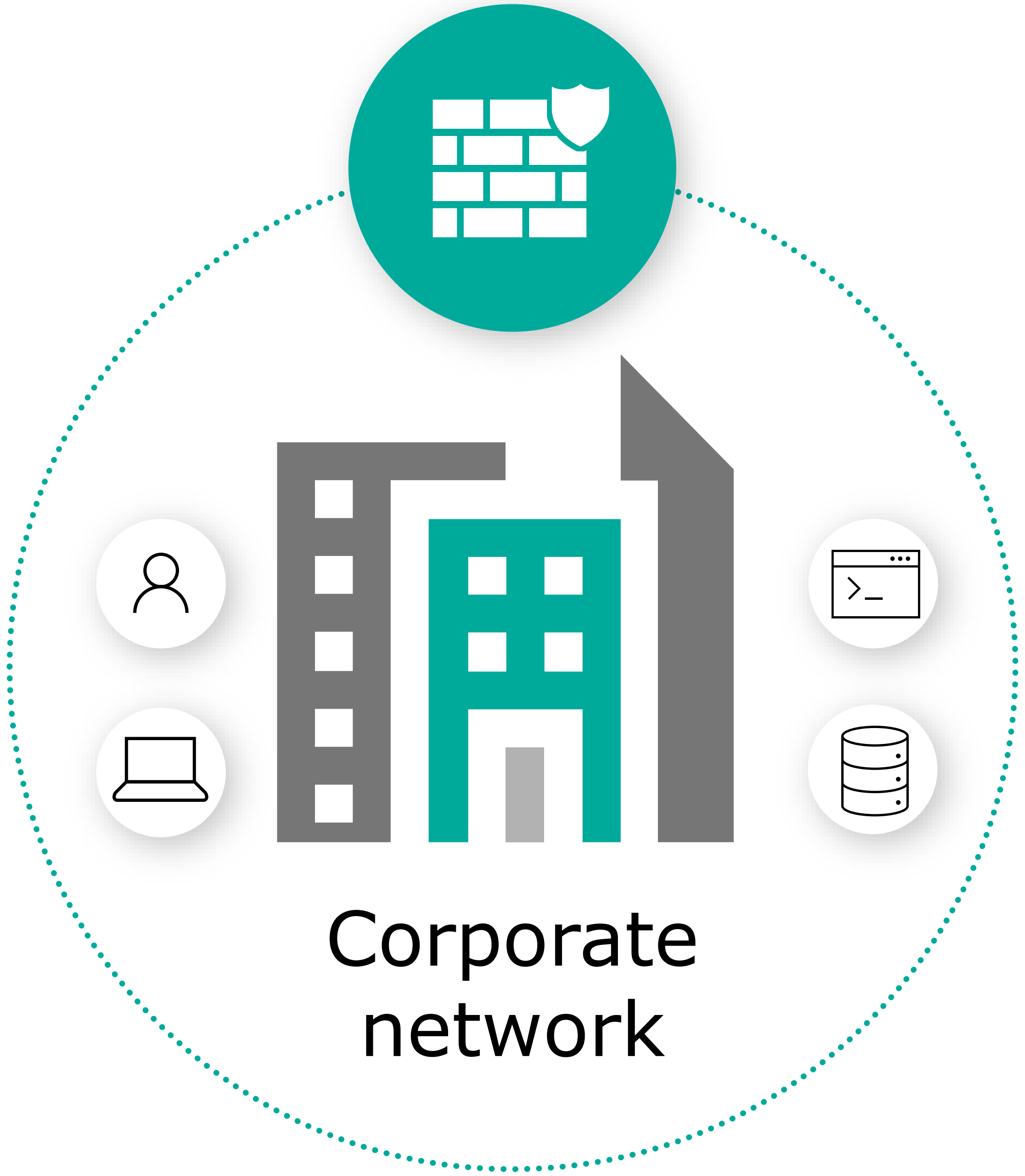
**Cybersecurity Architect
& Solution Manager**

CISSP® | Certified Information Systems Security Professional

koen.tamsyn@inetum-realdolmen.world

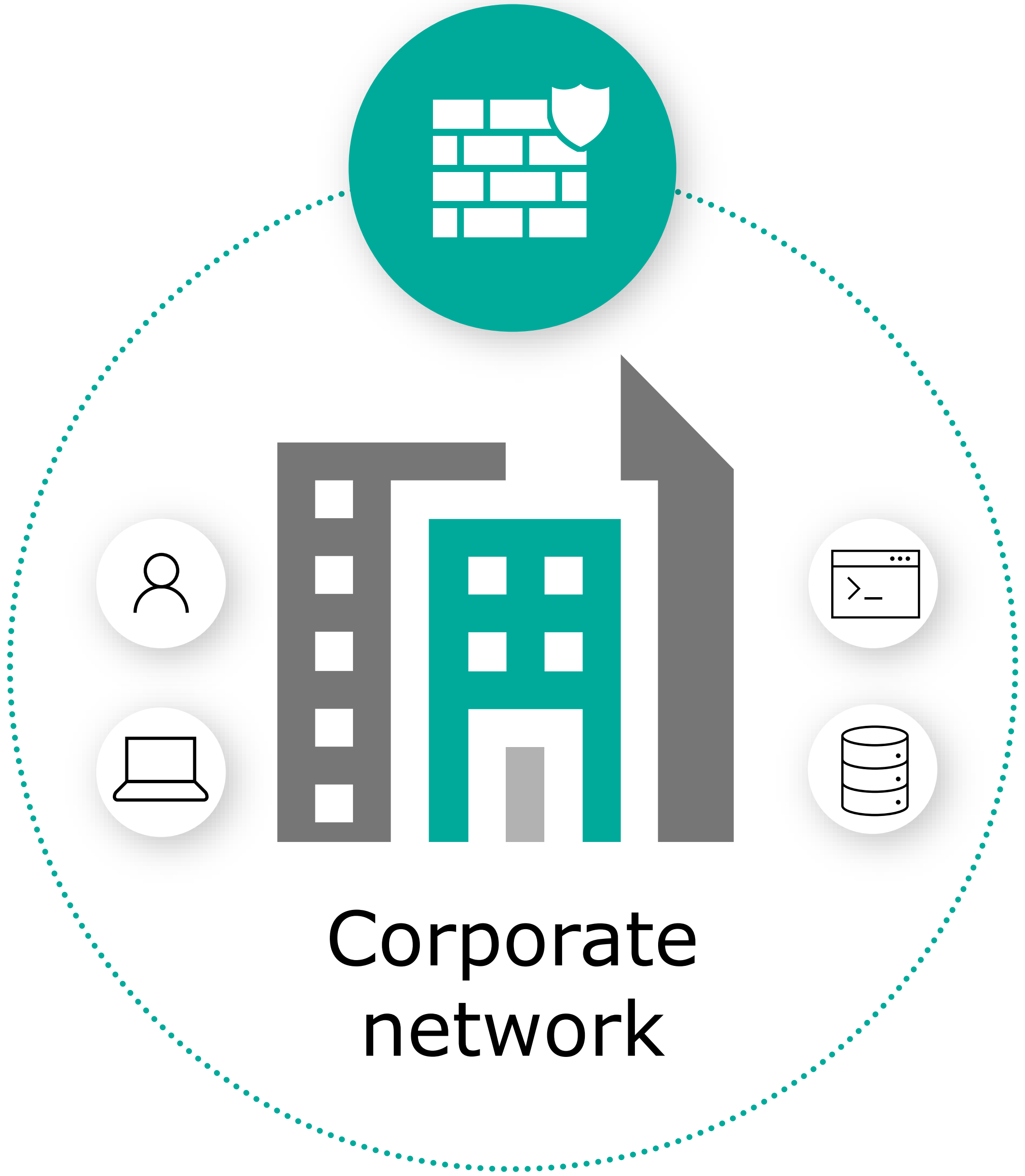
02/801.53.97 of Teams

Traditional Model

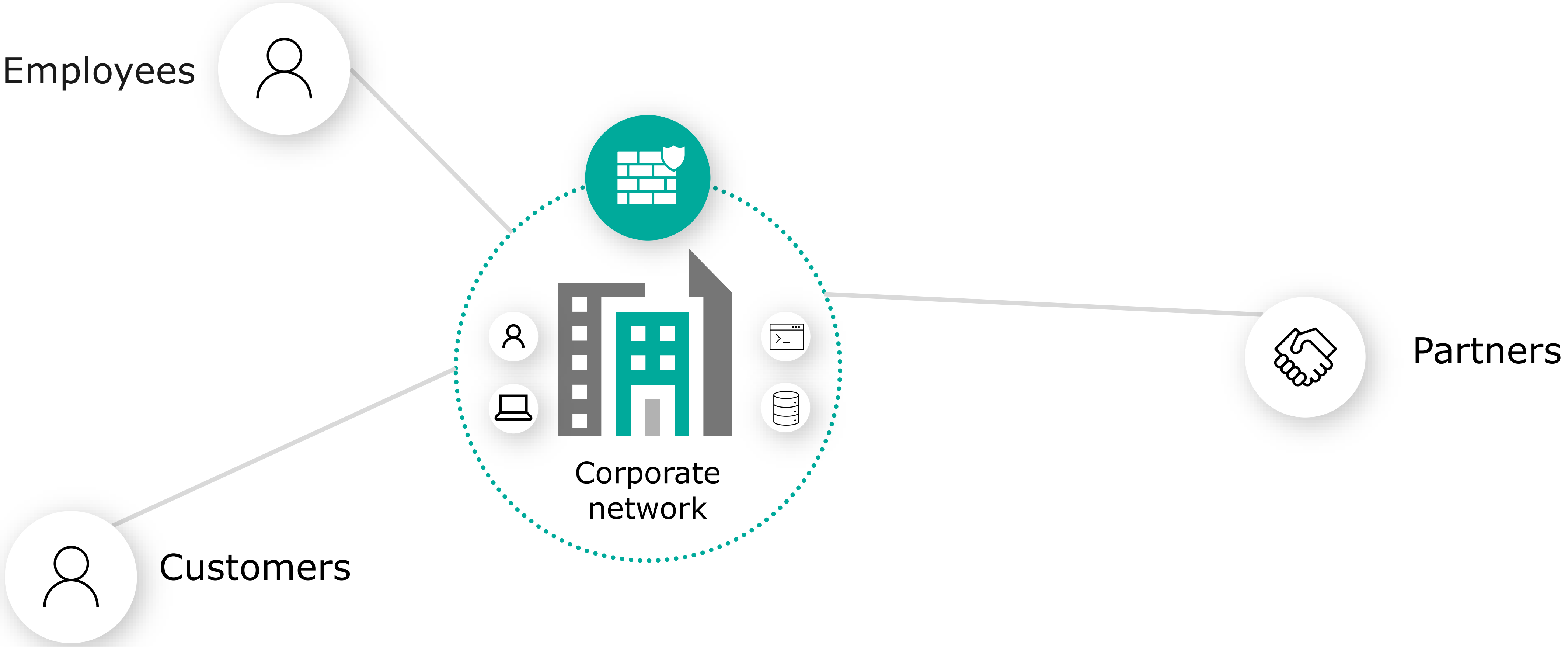


Users, devices, apps, and data protected behind a firewall

Traditional Model

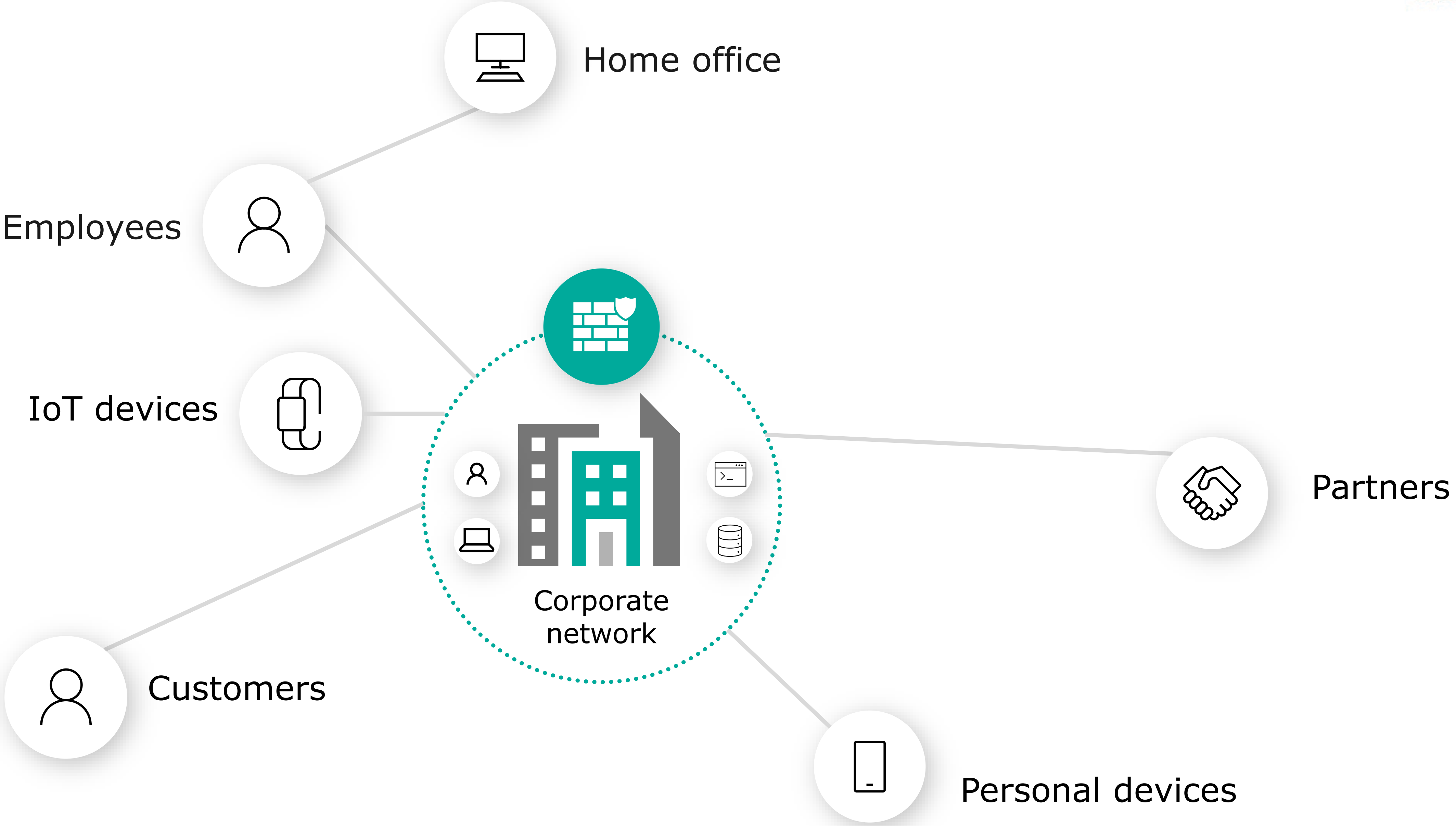


Traditional Model



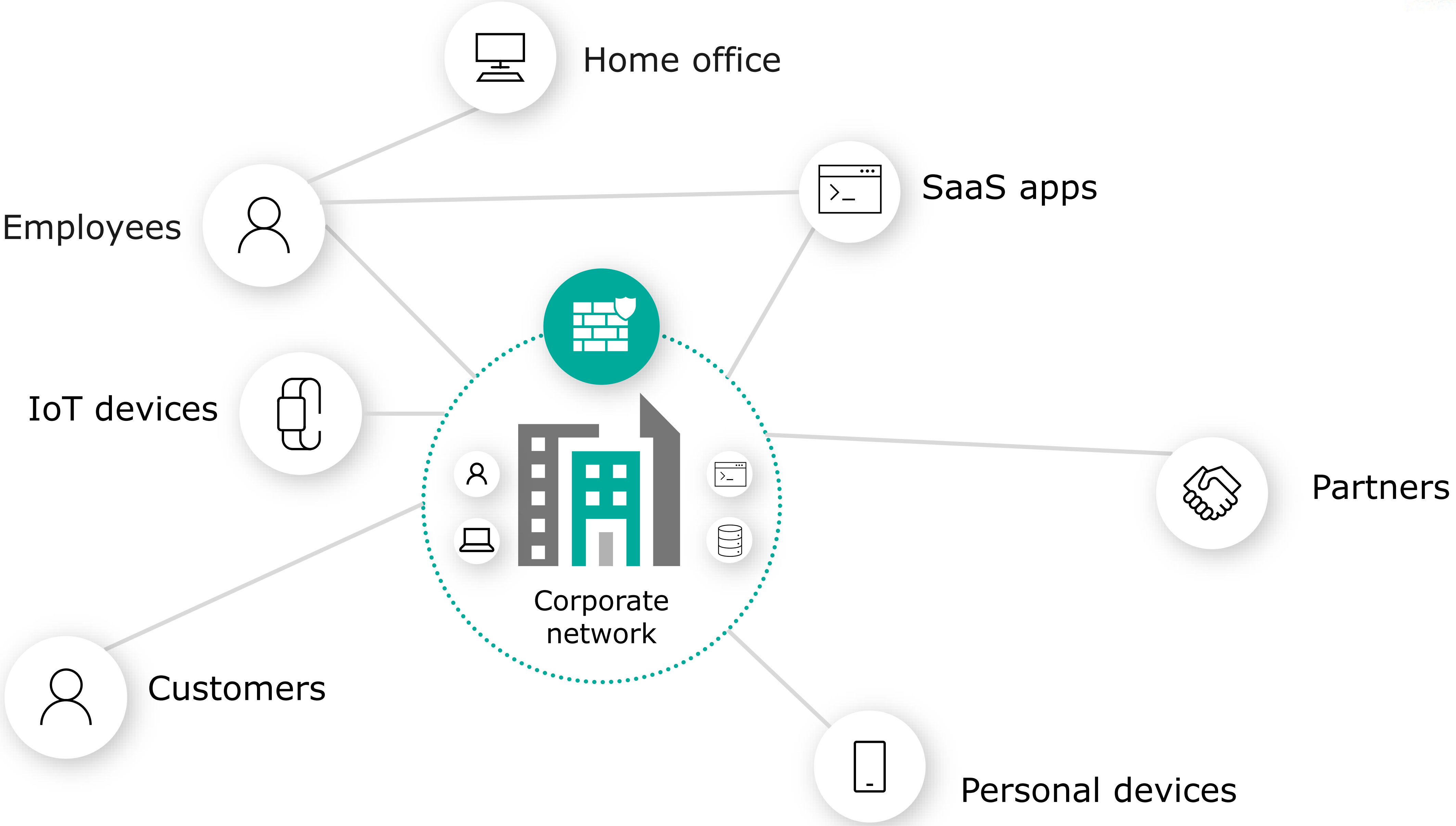
~~Users are employees~~ ❯ Employees, partners, customers, bots

Traditional Model



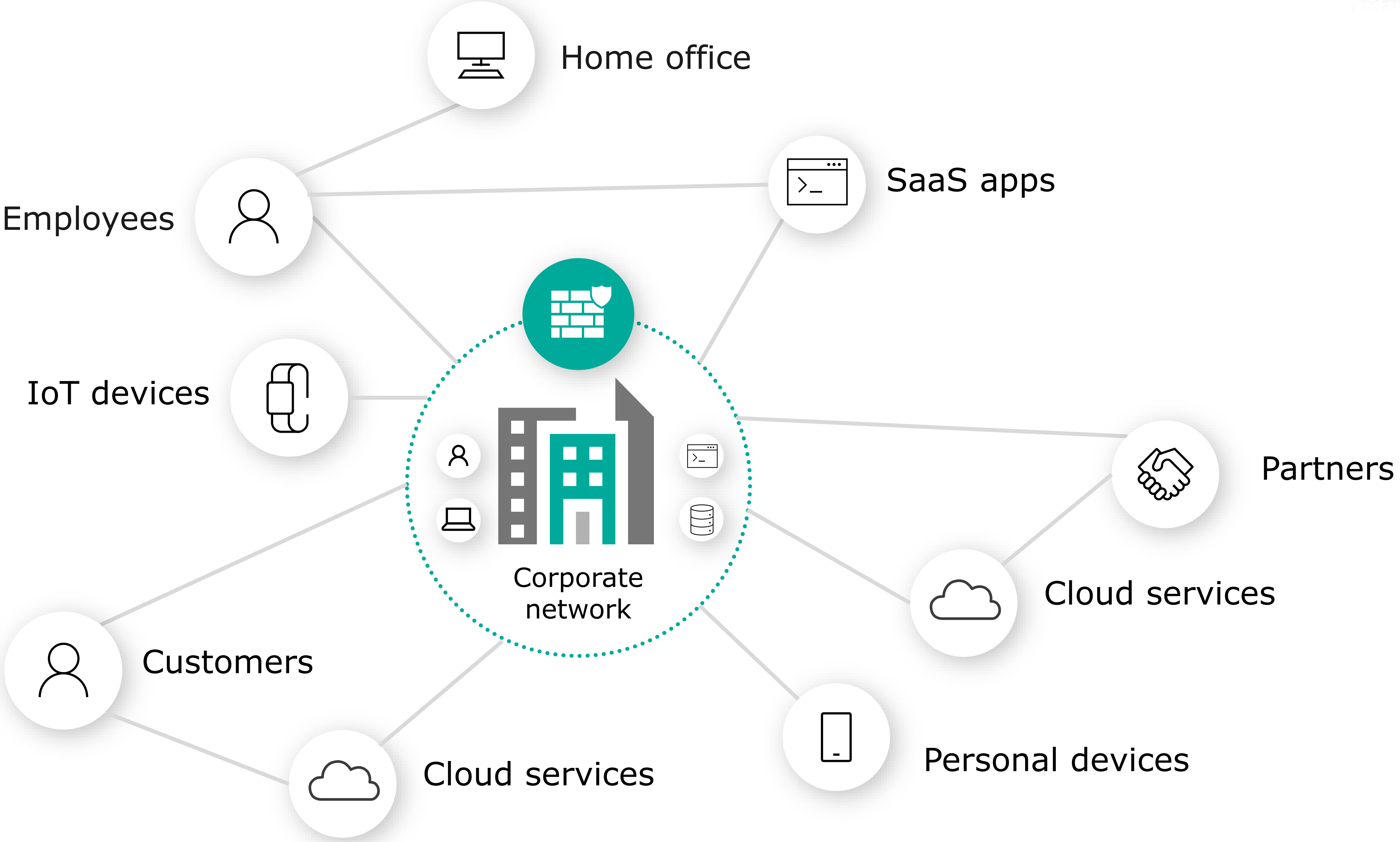
~~Corporate managed devices~~ Bring your own device and IoT

Traditional Model



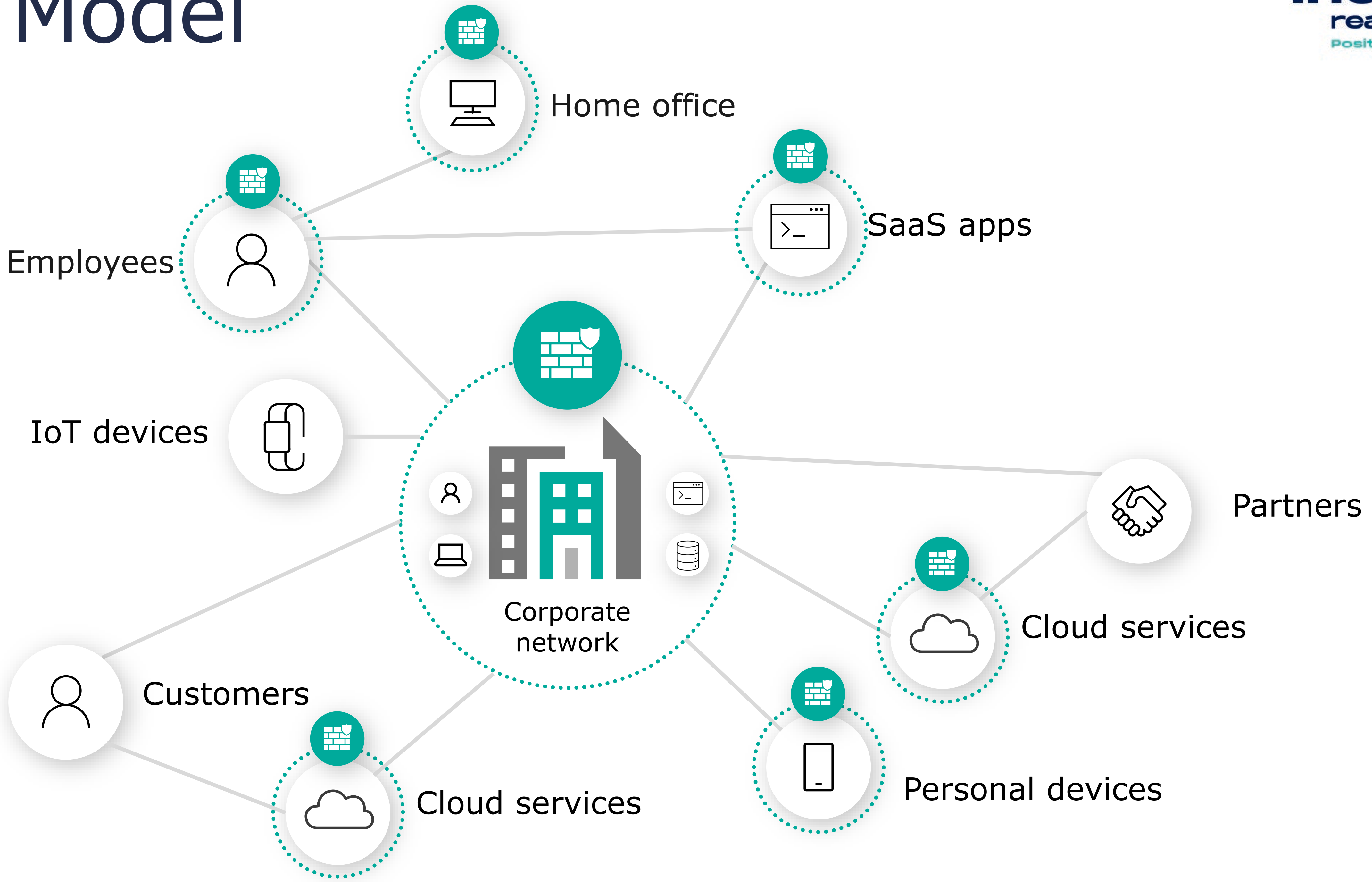
~~On-premises applications~~ Explosion of cloud applications

Traditional Model



~~Monolithic applications~~ Microservices and API’s

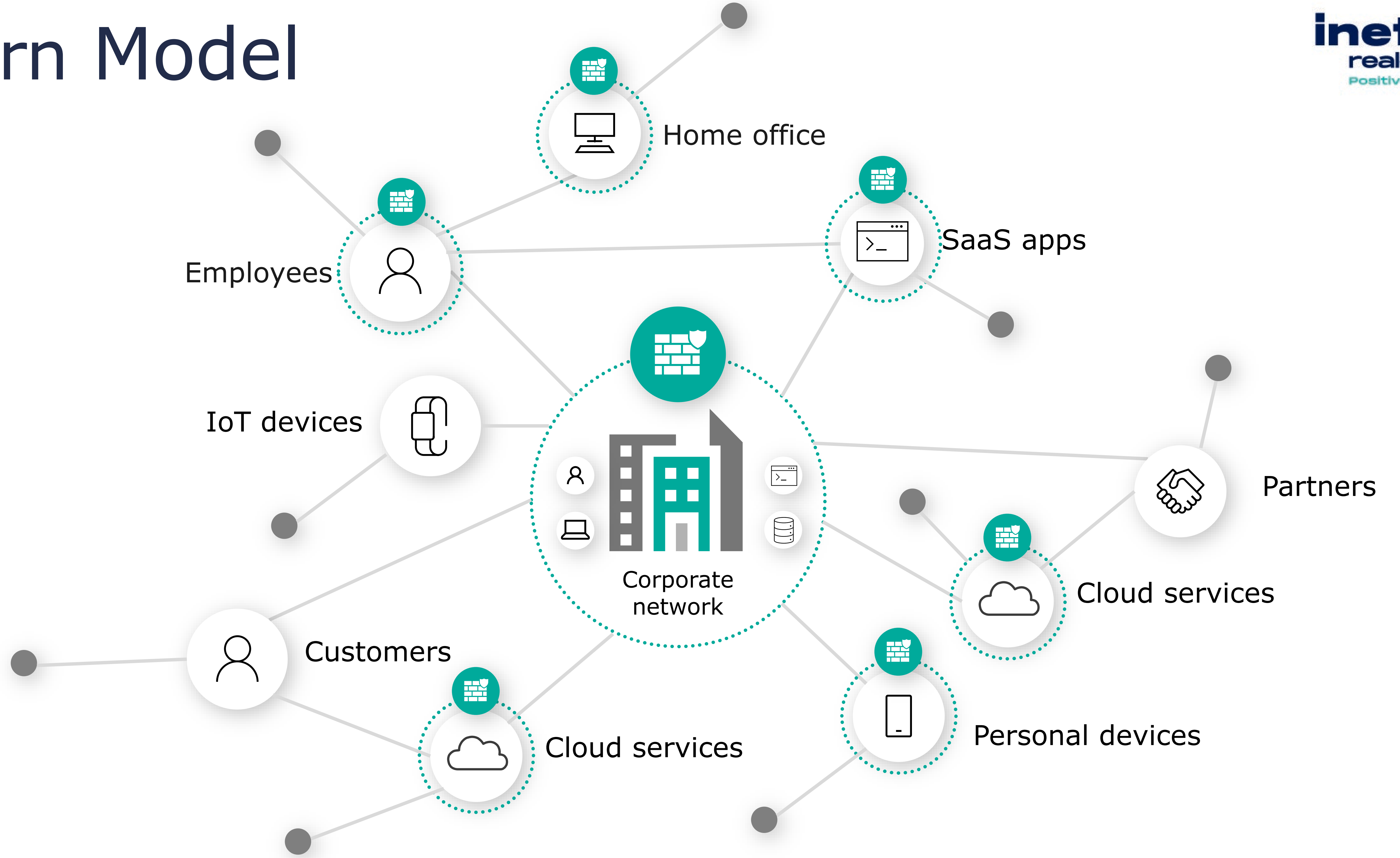
Traditional Model



~~Corp network and firewall~~ Expanding perimeters

Modern Model

inetum. realdolmen
Positive digital flow



~~Local packet tracking and logs~~ ❯ Explosion of signals

Zero Trust

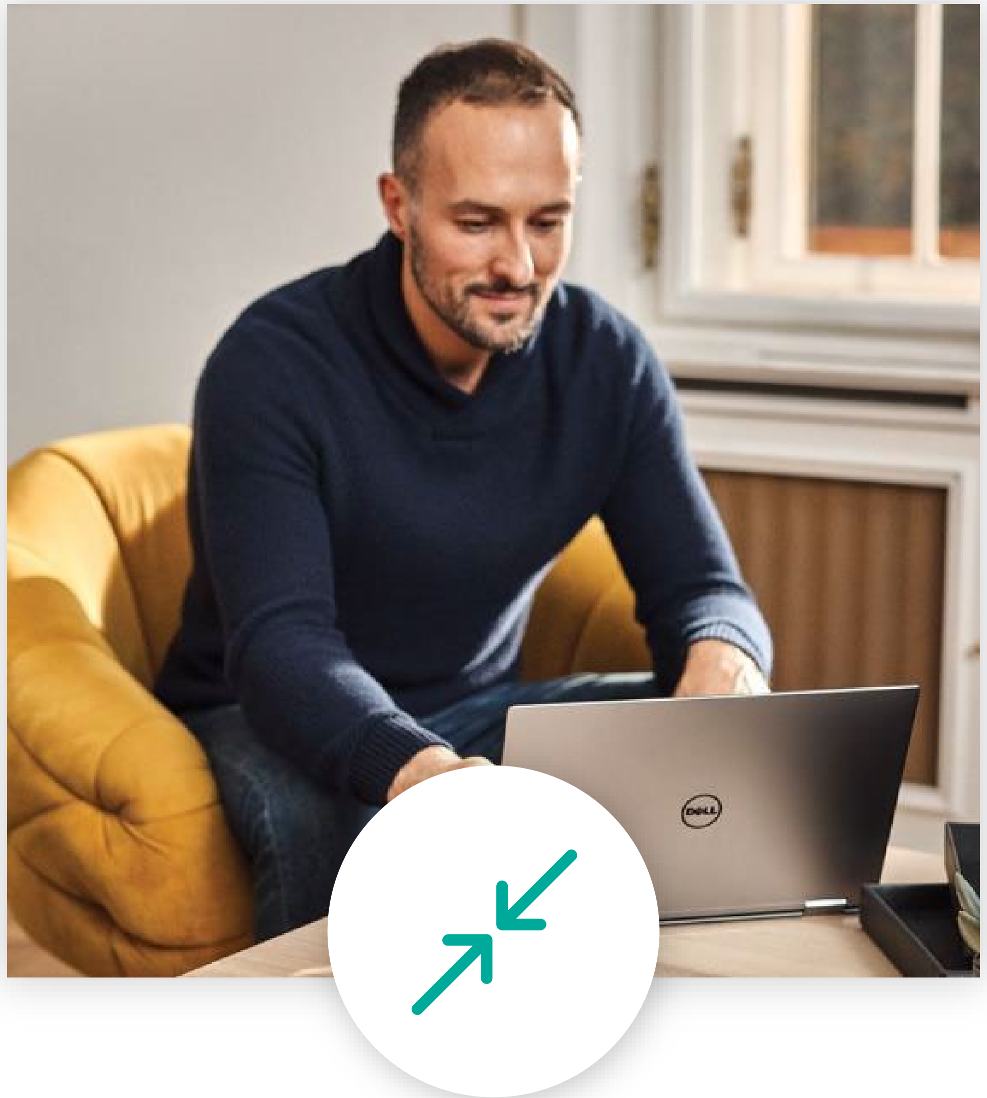
“A proactive approach to security
that uses a variety of adaptive controls and
continuous verification to prevent and respond to
threats more quickly and efficiently”

Not Zero Trust

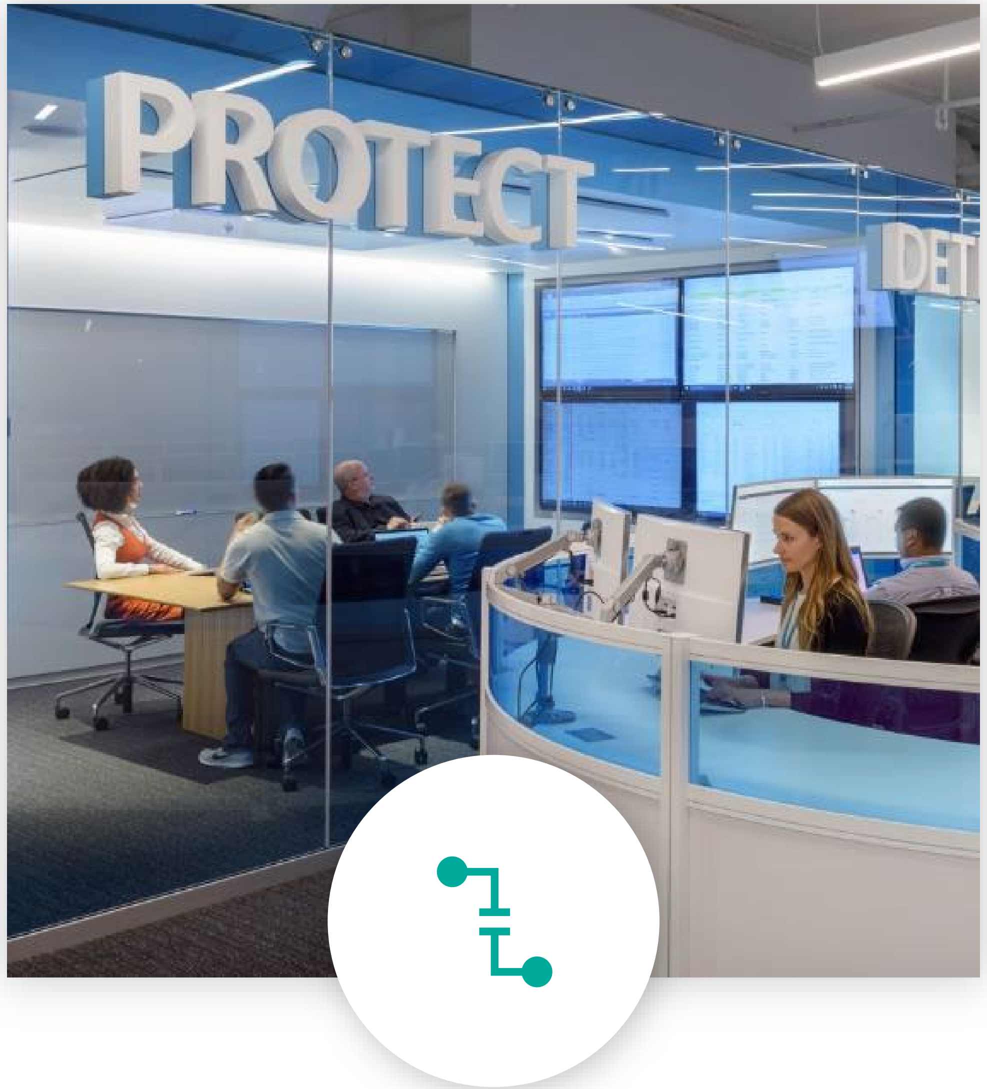
“A single technology, product or service. Nor is it a
one-time task or a one-size-fits-all solution that
can be purchased, installed and completed once
and for all”

A new reality needs new principles

Verify explicitly

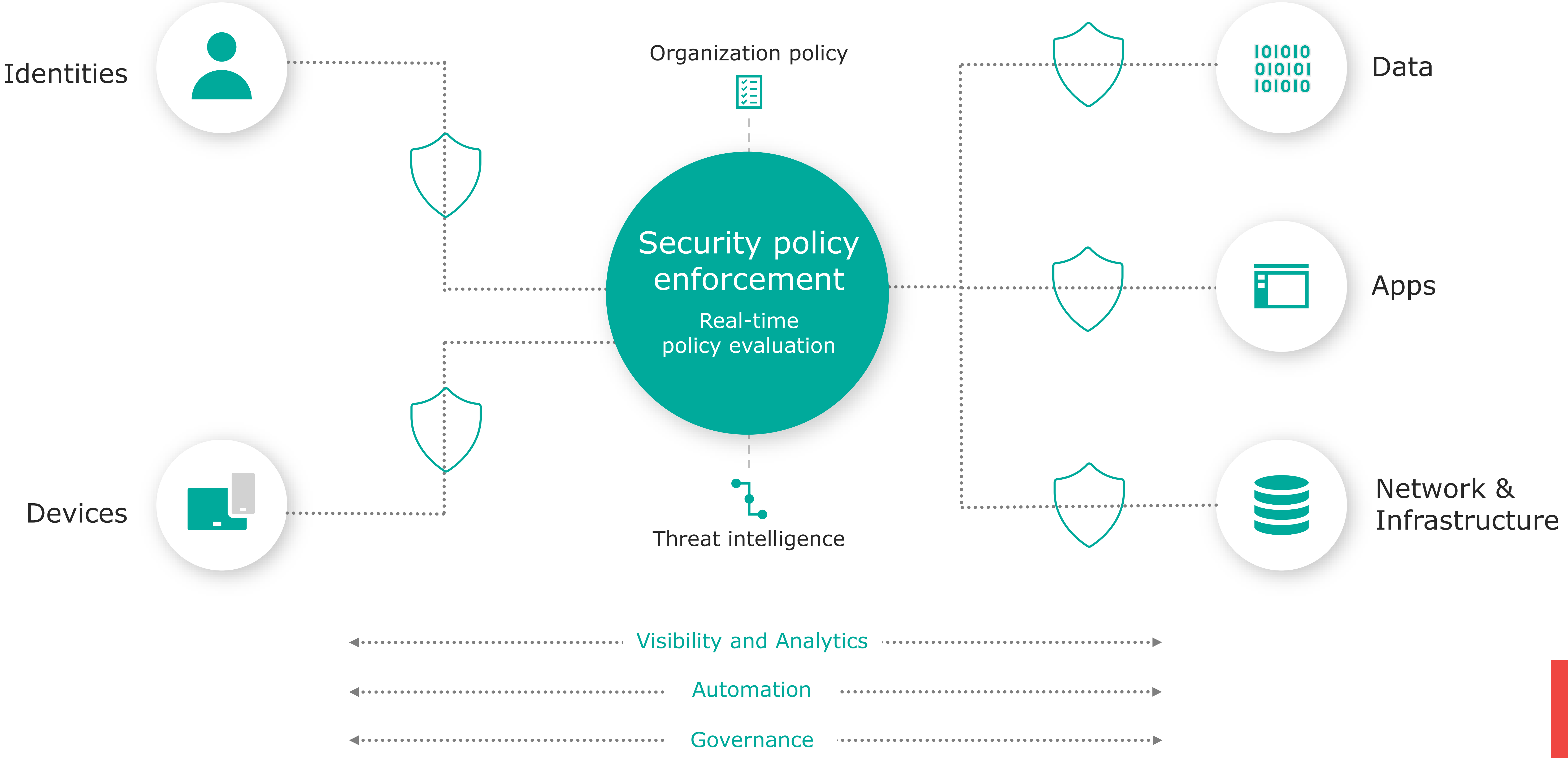


Use least privilege access



Assume breach

Zero Trust Architecture



Identities

Verify and secure every identity with strong authentication

Verify and secure every identity with strong authentication

Connect all of your users and applications

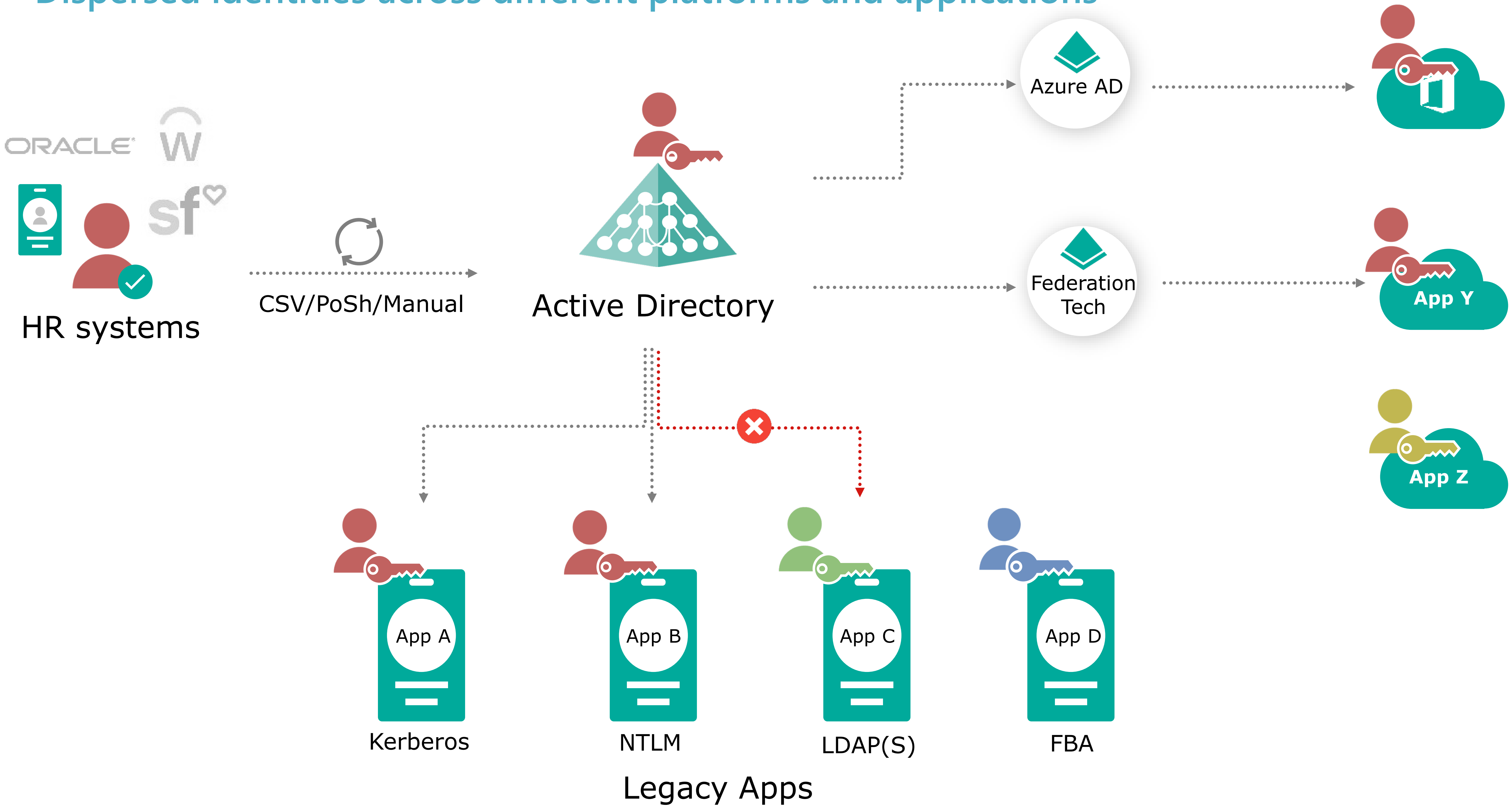
Verify identities with Multi-factor authentication (MFA)

Control access with smart policies and risk assessments

Enforce least privilege access with strong governance

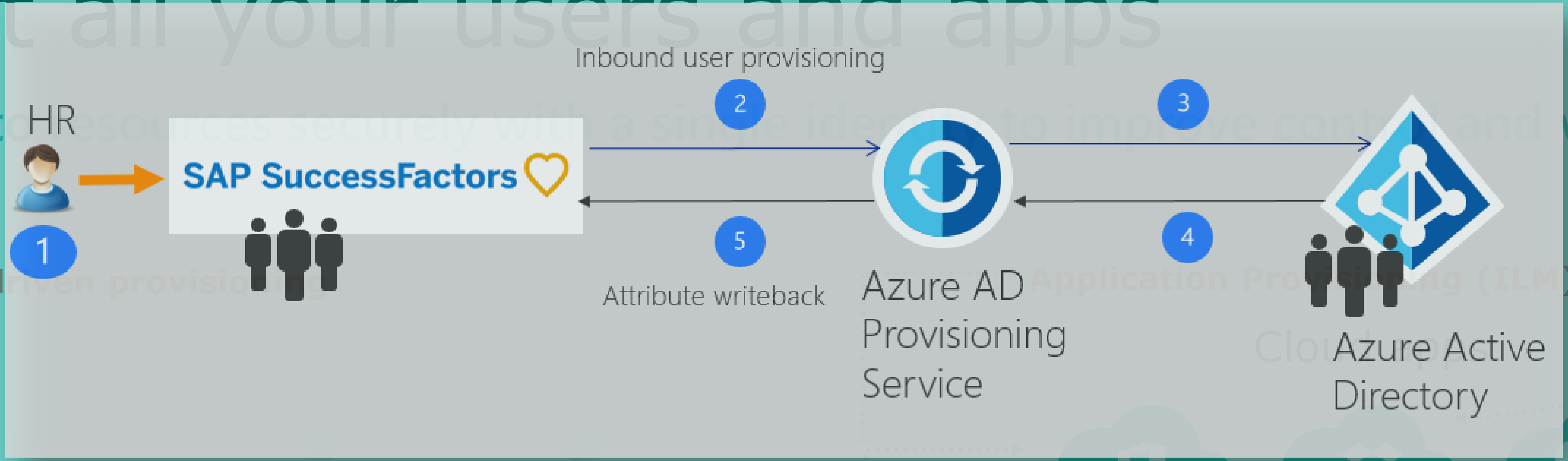
Traditional approach

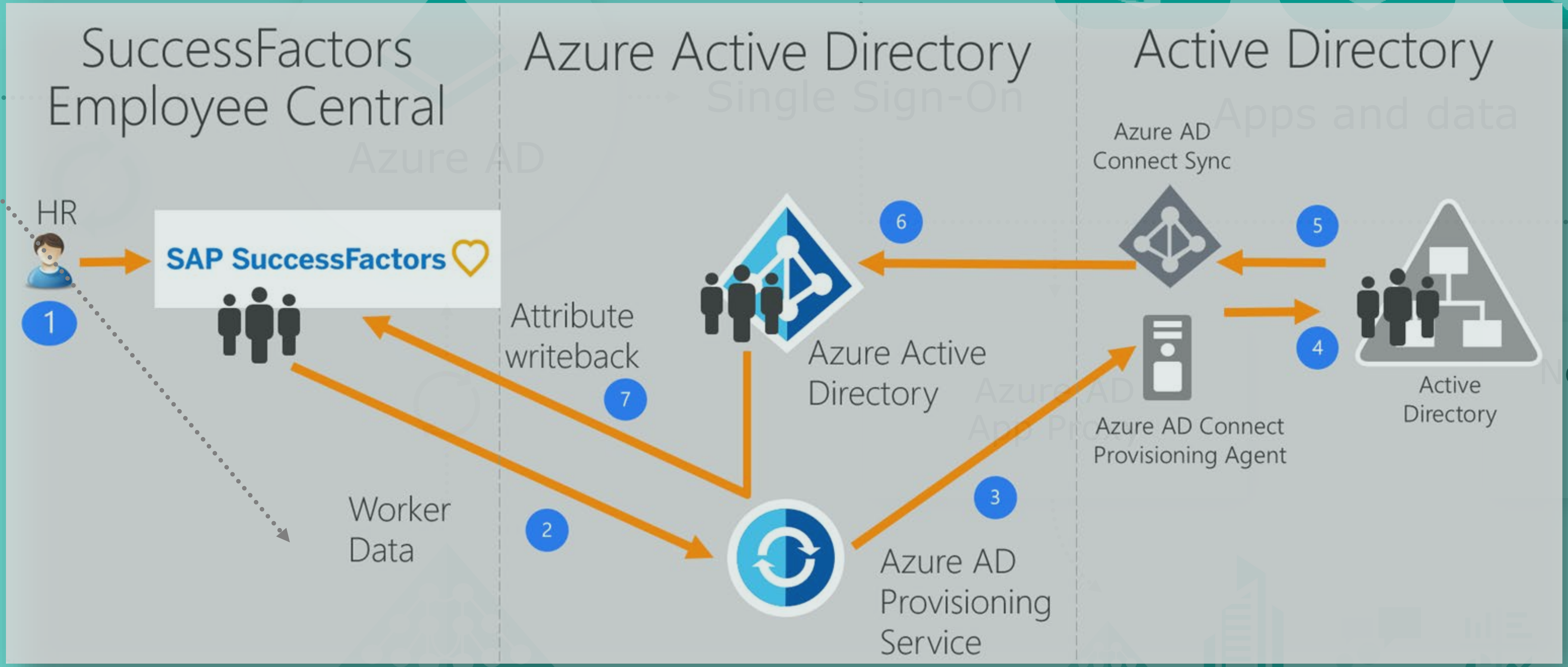
Dispersed identities across different platforms and applications



Connect all your users and apps

Enable access to resources securely with a single identity to improve control and visibility





HR-driven provisioning

Application Provisioning (ILM)

ORACLE

HR systems

AAD Provisioning Service

Cloud

Azure AD Single Sign-On

Apps and data

Azure AD

Azure AD App Proxy

Networking and delivery controllers

Active Directory

On-premises perimeter-based networks

Unified Identities, the benefits

inetum. realdolmen Positive digital flow

USER PERSPECTIVE

- ✓ Single credential to manage
- ✓ Productivity gain
- ✓ (Seamless) SSO across all applications, across company borders
- ✓ Self Service (Apps, Groups, Passwords, Privileges)

MANAGEMENT PERSPECTIVE

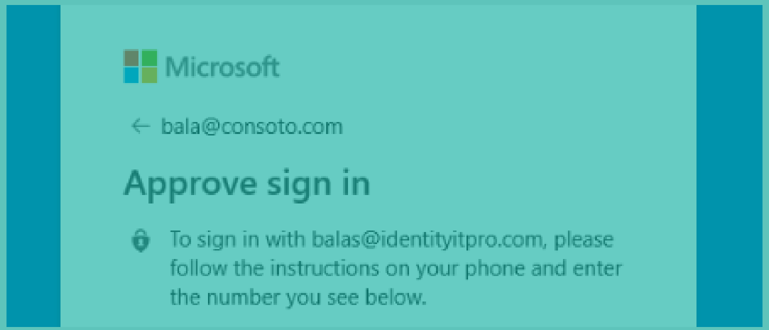
- ✓ Greater visibility and control
- ✓ Automated User Lifecycle Management
- ✓ Improvement of legacy app security
- ✓ Simplification of management
- ✓ Uniformly leverage security features

Multifactor Authentication

Bad ● Password (Only)	Good ● Password +	Better ● Password +	Best | Passwordless ●
123456	SMS	Authenticator (Push notifications)	Windows Hello
qwerty	Voice	Software Tokens OTP	Authenticator (Phone Sign-in)
password		Hardware Tokens OTP (Preview)	FIDO2 security key
Iloveyou			
Password1			

Verify identities with Multi-Factor Authentication

inetum.
realdolmen
Positive digital flow

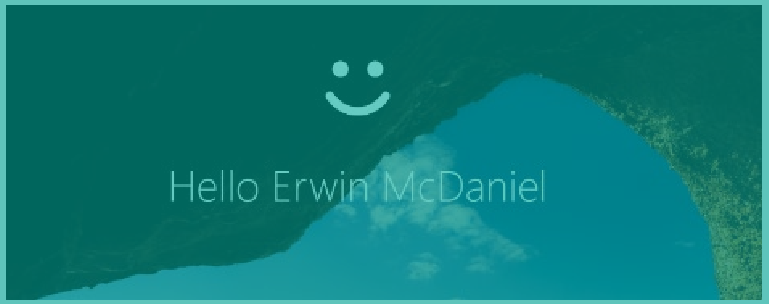


Microsoft

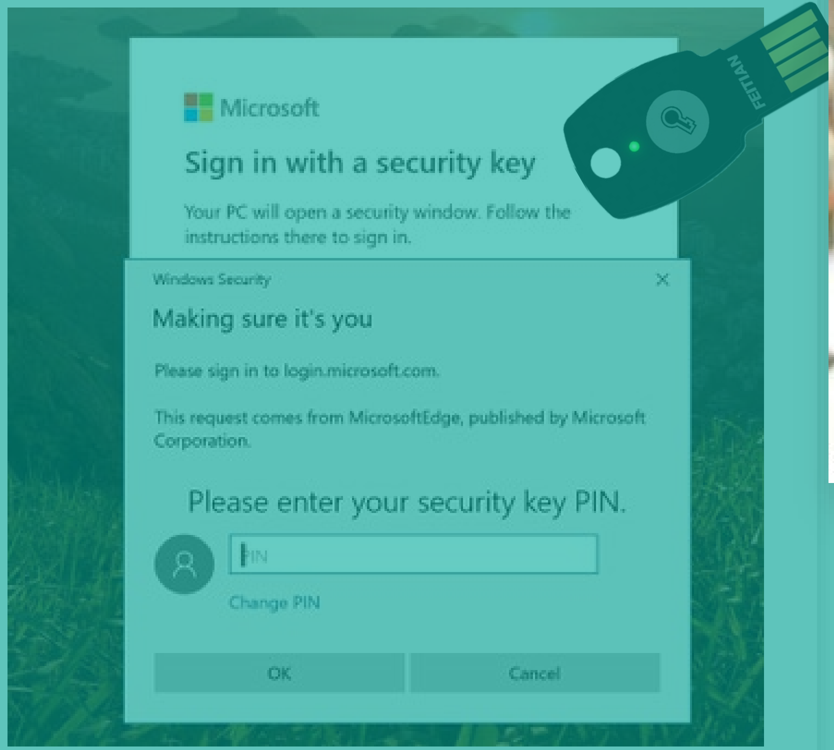
← bala@consoto.com

Approve sign in

To sign in with balas@identityitpro.com, please follow the instructions on your phone and enter the number you see below.



Hello Erwin McDaniel



Microsoft

Sign in with a security key

Your PC will open a security window. Follow the instructions there to sign in.

Windows Security

Making sure it's you

Please sign in to login.microsoft.com.

This request comes from MicrosoftEdge, published by Microsoft Corporation.

Please enter your security key PIN.

PIN

Change PIN

Passwordless authentication

Software Platform Hardware

Passwords

Low Security

Some Stats…

73 percent of passwords are duplicates

Multi-factor authentication prevents **99.9%** of identity attacks

54 percent of users leverage five or fewer passwords for all of their online accounts

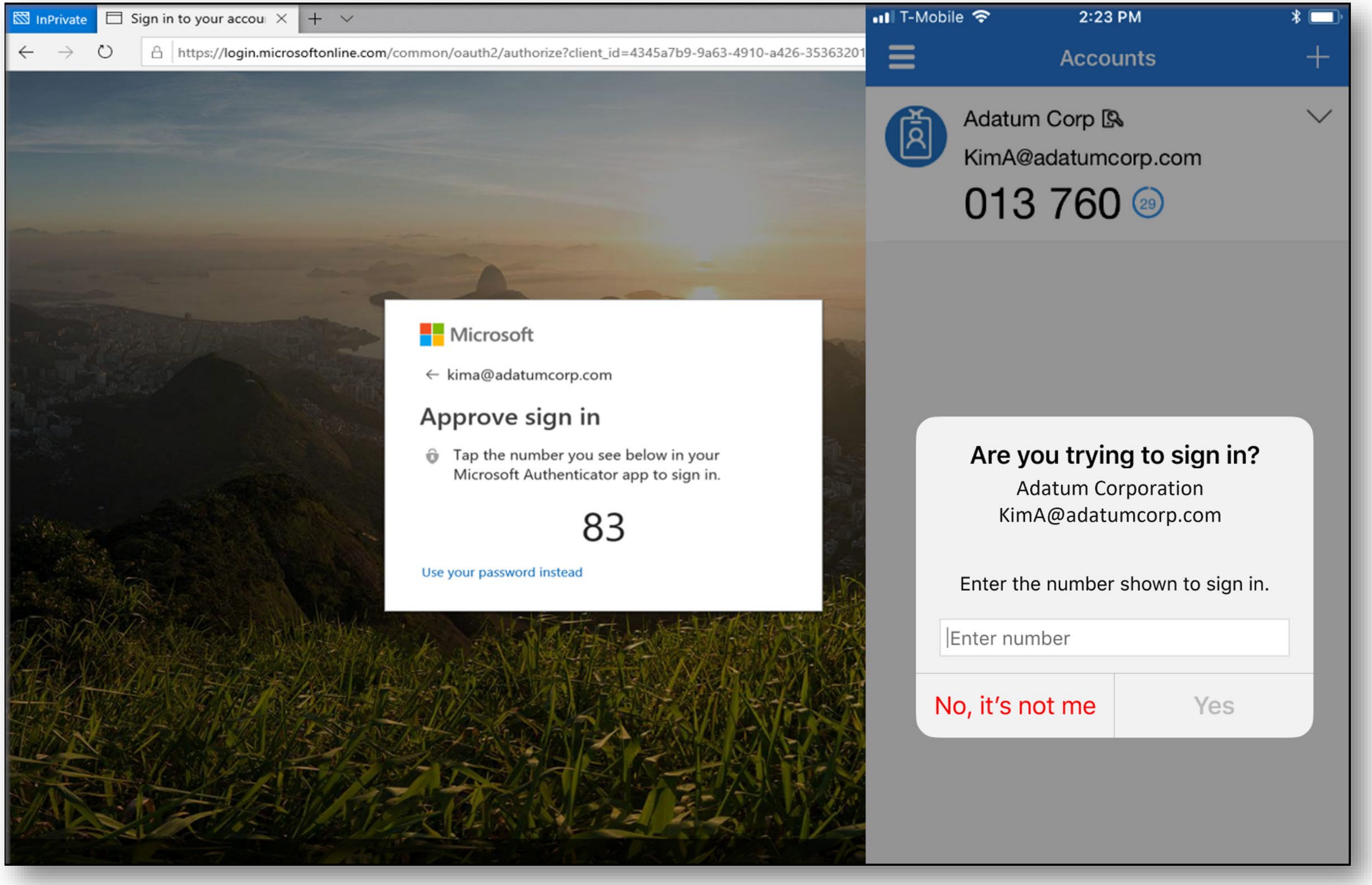
Just **11 percent** of orgs use MFA, overall

81% of data Breaches have been the result of weak or stolen passwords

Mobile push notifications are the most common authentication method

Authenticator Advanced Features (Generally Available)

Number matching & Additional Context – prevent accidental approvals



https://login.microsoftonline.com/common/oauth2/authorize?client_id=4345a7b9-9a63-4910-a426-35363201

Microsoft

kima@adatumcorp.com

Approve sign in

Tap the number you see below in your Microsoft Authenticator app to sign in.

83

Adatum Corp

KimA@adatumcorp.com

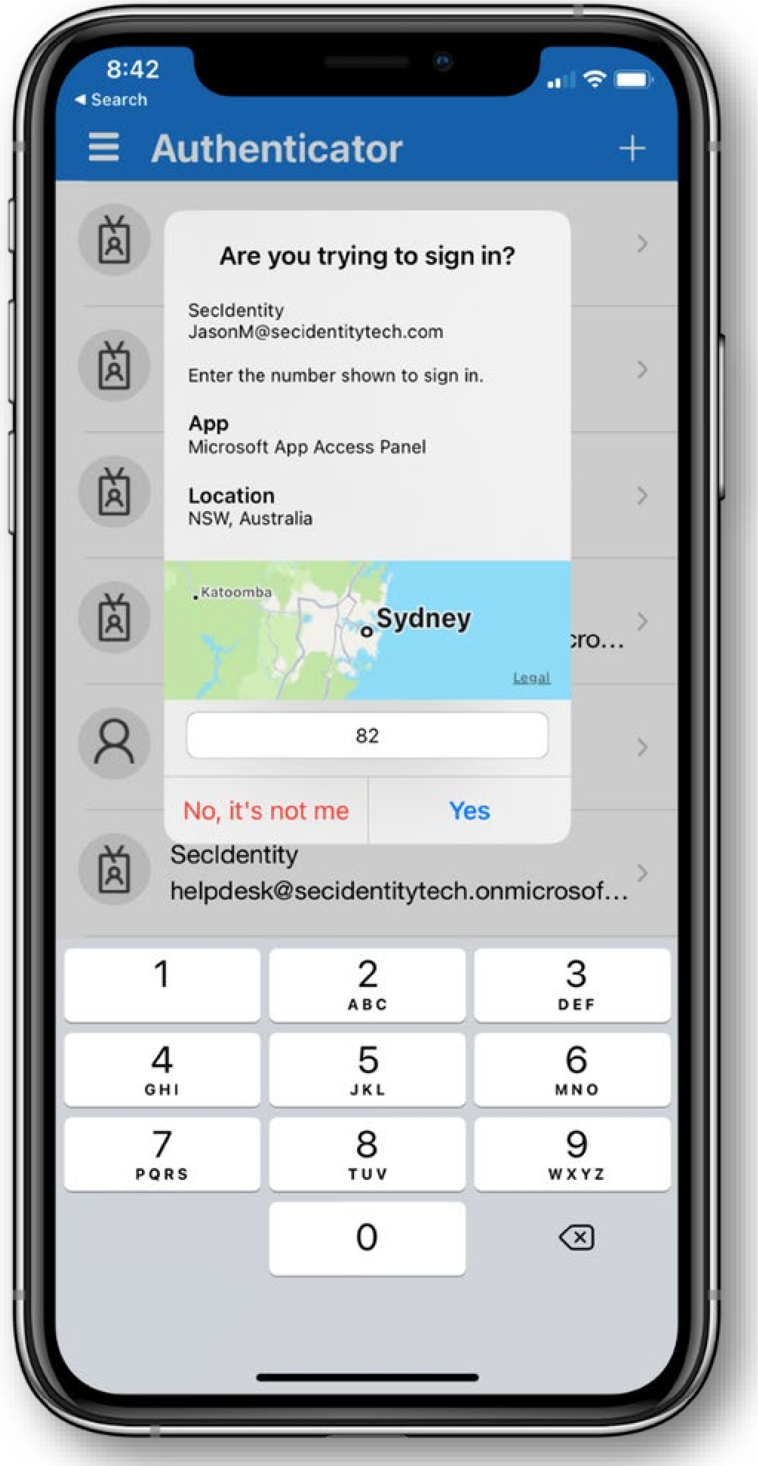
013 760

Are you trying to sign in?

Adatum Corporation

KimA@adatumcorp.com

Enter the number shown to sign in.



Are you trying to sign in?

SecIdentity
JasonM@secidentitytech.com

Enter the number shown to sign in.

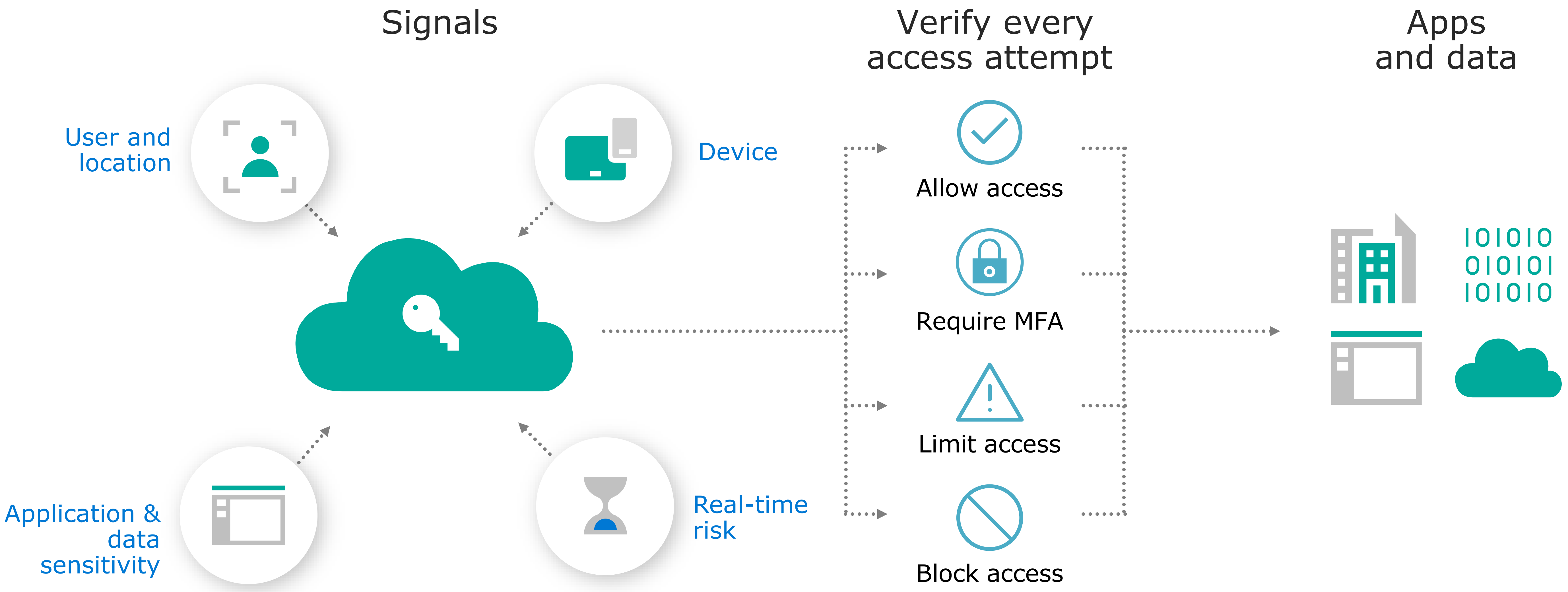
App
Microsoft App Access Panel

Location
NSW, Australia

82

SecIdentity
helpdesk@secidentitytech.onmicrosof...

Control access with smart policies and risk assessments



Signals

Verify every access attempt

Apps and data

Conditional Access Authentication Strength (Preview)

Authenication methodes availability under certain conditions

- Require specific authentication methods to access a **sensitive resource**
- Require a specific authentication method when a user **takes a sensitive action** within an application
- Require more secure authentication methods for **users at high risk.**
- Require specific authentication methods from **guest users** who access a resource tenant

Authentication method combo	MFA strength	Passwordless MFA strength	Phishing-resistant MFA strength
FIDO2 security key	☑	☑	☑
Windows Hello for Business	☑	☑	☑
Certificate-based authentication (Multi-Factor)	☑	☑	☑
Microsoft Authenticator (Phone Sign-in)	☑	☑	
Temporary Access Pass (One-time use AND Multi-use)	☑		
Password + something you have[1]	☑		
Federated single-factor + something you have[1]	☑		
Federated Multi-Factor	☑		

Enforce least privilege access with strong governance

salesforce
W
101010
010101
101010

Identity lifecycle

User onboarded

Access lifecycle

Oversight with
access reviews

Admin rights

Privileged identity
management

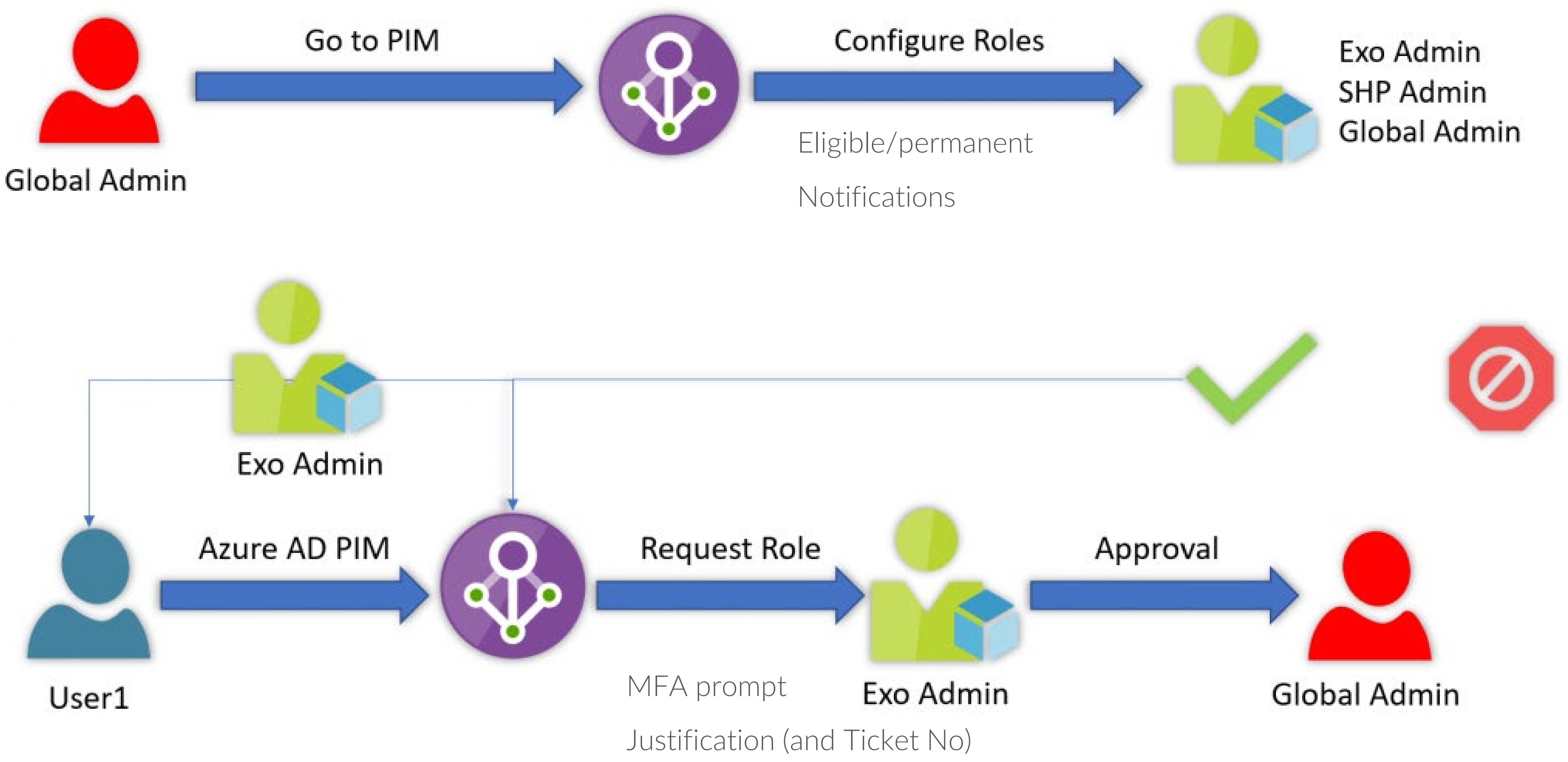
End of lifecycle

Access rights
automatically removed

Privileged Identity Management

Manage, control and monitor access to important resources

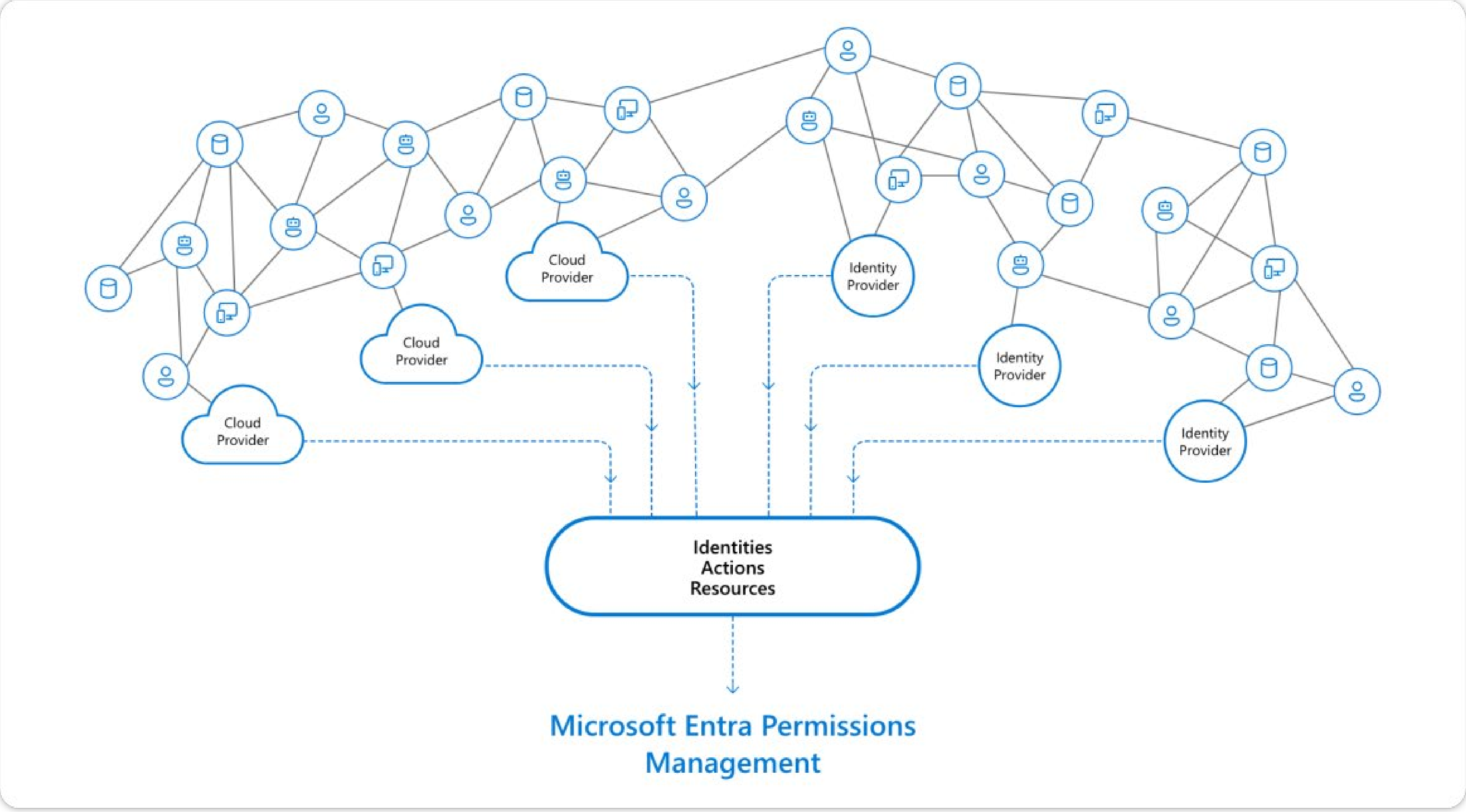
- ✓ Time-bound Privileged Access (JIT)
- ✓ Approval Flow possibilities
- ✓ Leverage MFA to validate requestor
- ✓ Auditing / Discovery & Insights
- ✓ Leverage Access Reviews
- ✓ M365 roles and Azure resources
- ✓ Privilege Access Groups (Preview)
- ✓ Azure AD Premium 2 License (MAU!)



Entra Permissions Management (CloudKnox)

Discover, remediate, and monitor permission risks for any identity or resource.

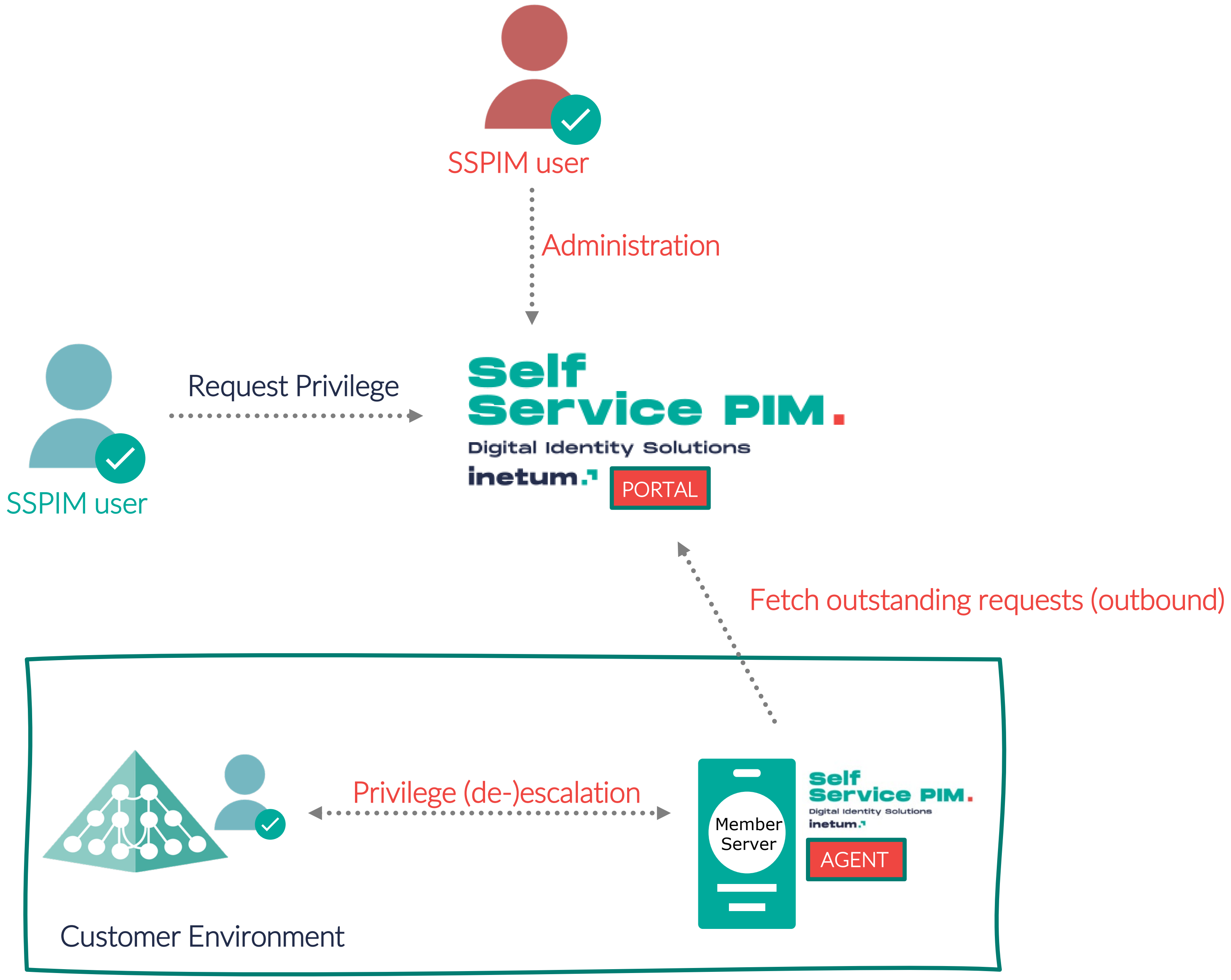
- ✓ CIEM - Cloud Infrastructure Entitlement Management
- ✓ Visualize and reduce high-risk permissions
- ✓ Multicloud: Azure, AWS, GCP
- ✓ Continuous monitoring
- ✓ Permission Creep Index
- ✓ Automated deletion of unused permissions
- ✓ Permissions on demand (JIT)



Self Service PIM

Privileged Identity Management for Active Directory Domain Services

- ✓ Just in Time access to AD privileges
- ✓ Cloud based solution
- ✓ Software-as-a-Service
- ✓ Agent-based processing (only on-prem component
- ✓ Audit trail and scheduled reports
- ✓ Azure AD as the Identity Control Plane
- ✓ Multi-domain support
- ✓ We are eating our own dog food



Zero Trust Roadmap Identities

TRADITIONAL

- 🔓 Several identity providers are in use,
- 🔓 No SSO is present between cloud and on-premises apps
- 🔓 Visibility into identity risk is very limited

ADVANCED

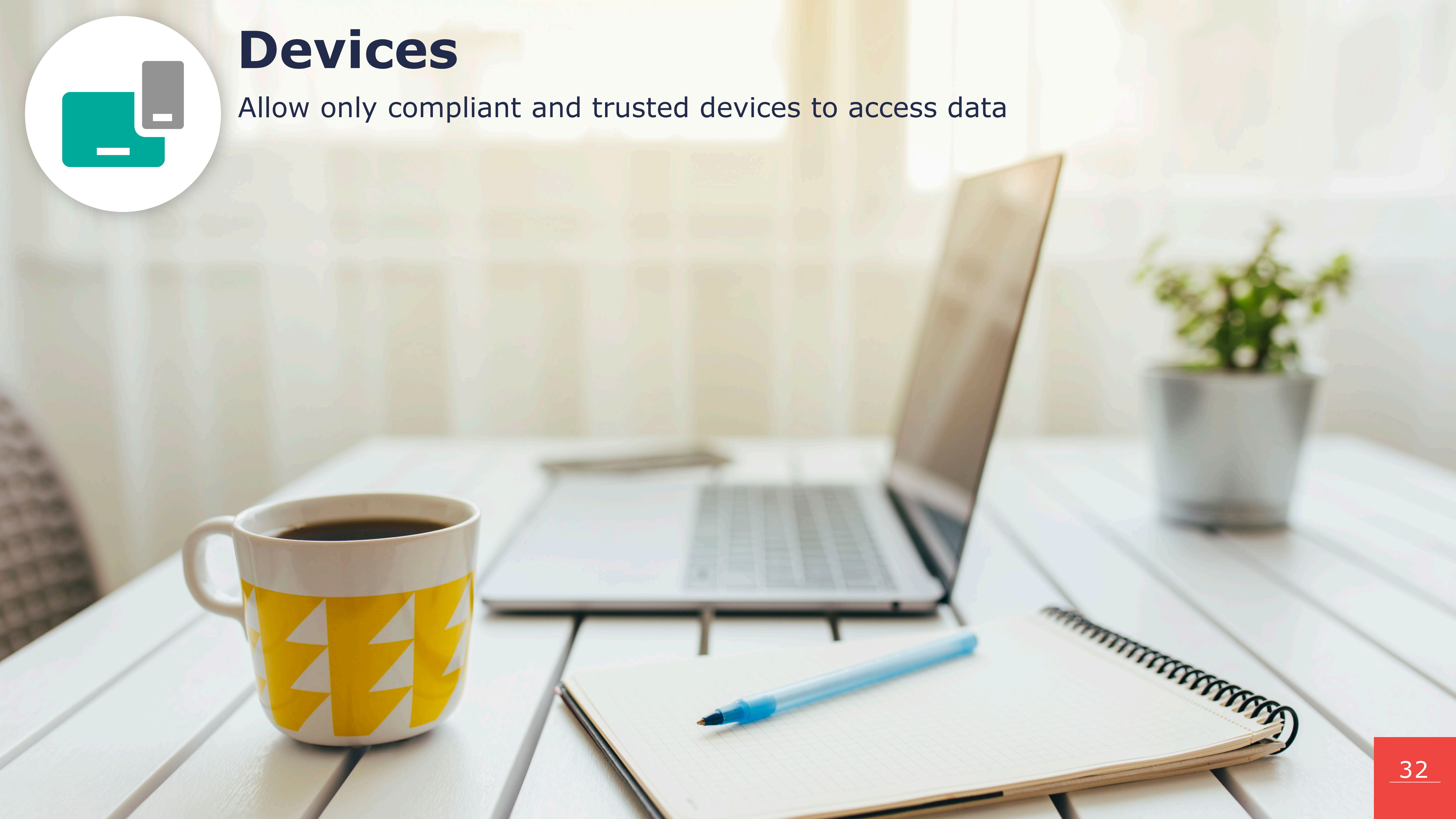
- 🔒 Cloud identity federates with on-premises systems
- 🔒 Basic conditional access policies implemented
- 🔒 Visibility into identity risk with analytics
- 🔒 Enforce basic MFA

OPTIMAL

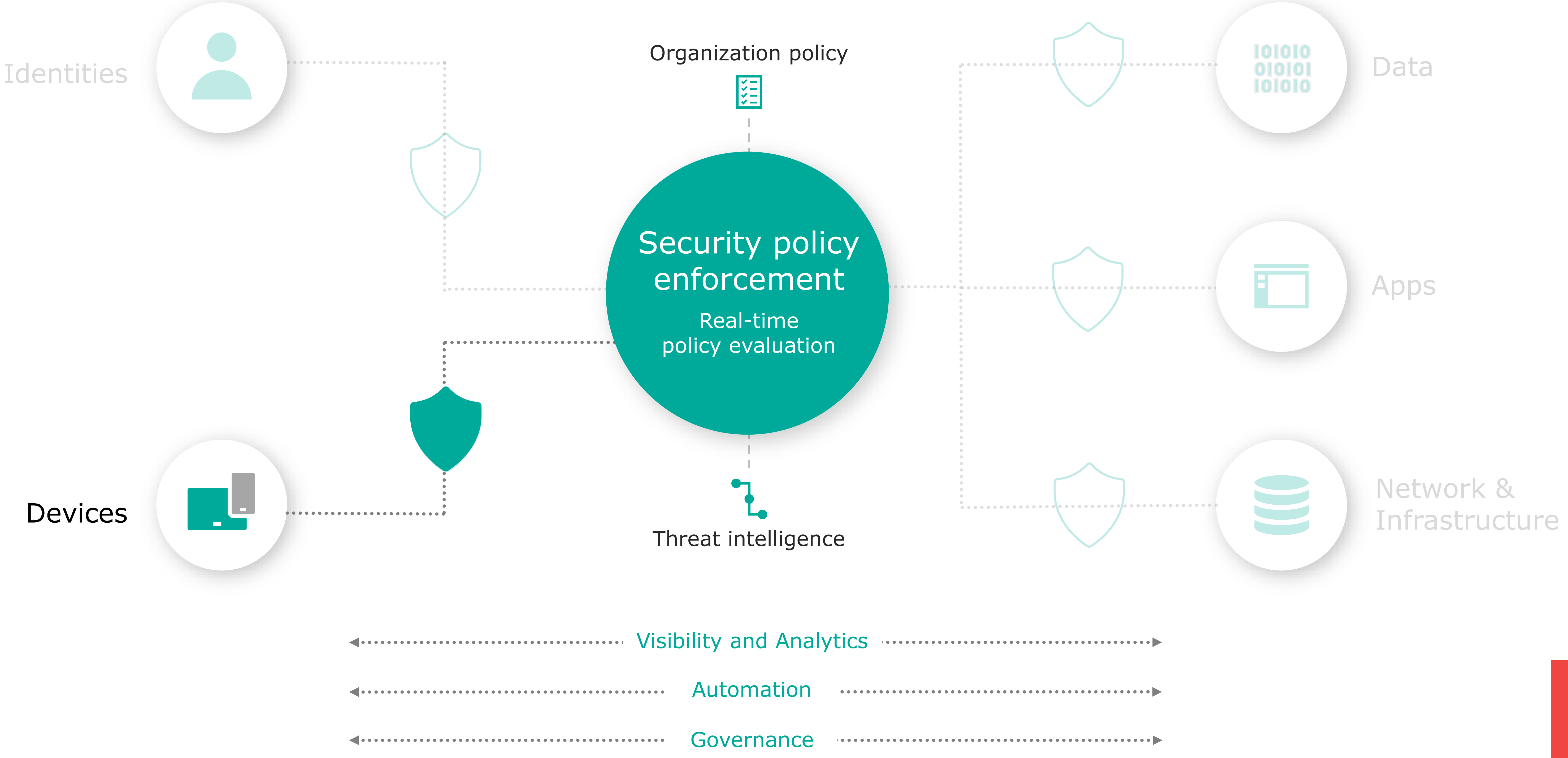
- 🔒 Password less authentication is enabled
- 🔒 Phishing-proof MFA is enforced
- 🔒 User behavior is analyzed in real time to determine risk
- 🔒 Enforce least privilege access with strong governance

Devices

Allow only compliant and trusted devices to access data



Zero Trust Architecture



Allow only compliant and trusted apps and devices to access data

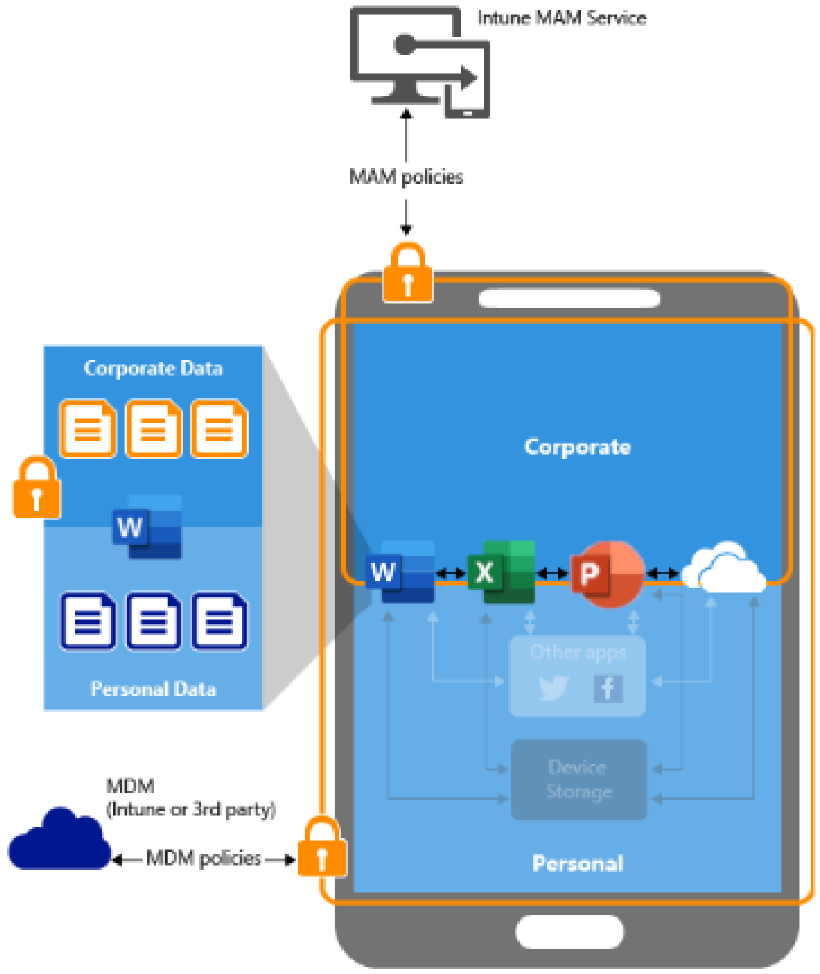
Visibility into device health and compliance

Restrict access from vulnerable and compromised devices

Enforce security policies on mobile devices and applications

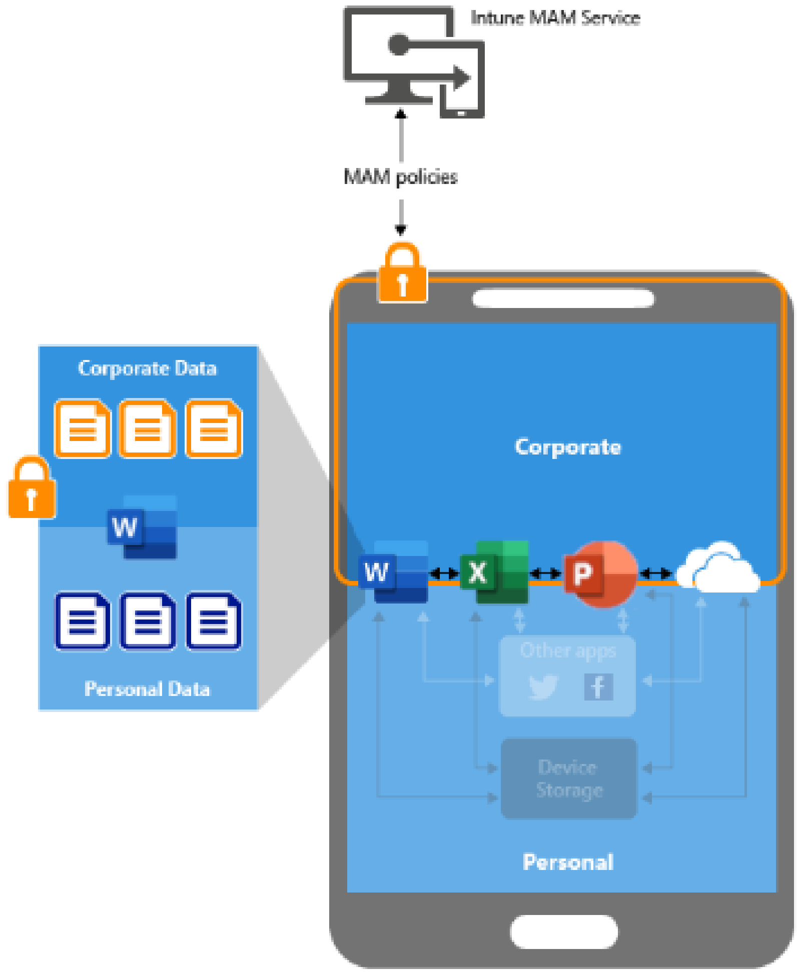
Compliancy – MDM & MAM / MAM

MDM & MAM



Corporate

MAM only



Personal

Compliance policies (MDM)

Device settings verification

Verification of various settings of a device, typically set in Endpoint Security Policies or Configuration Profiles.

Examples: require a PIN, data encryption, network connectivity etc.

OS Integrity

Root? Jailbreak?

Verification of device OS characteristics.

Examples: minimum/maximum OS version, integrity of device drivers, location, jailbreak detection etc.

Apps Integrity

Google Play Protect

Verification if apps installed on the device can be deemed secure.

Examples: presence of restricted apps or apps from unknown sources, etc.

Threat Level

Symantec. Check Point SOFTWARE TECHNOLOGIES LTD

Verification if a device is at certain threat level as assessed by Threat Defense solutions such as Microsoft Defender for Endpoint or Mobile Threat Defense solutions from partners, device vendor’s health attestation, etc.

AppProtection policies (MAM)

Device settings verification

Verification of some basic config of the device.

Examples: require a device Lock, safetynet, manufacturer...

OS Integrity

Verification of device OS characteristics.

Examples: minimum/maximum OS version, integrity of device drivers, jailbreak detection etc.

Apps

Approved Apps, Managed Apps

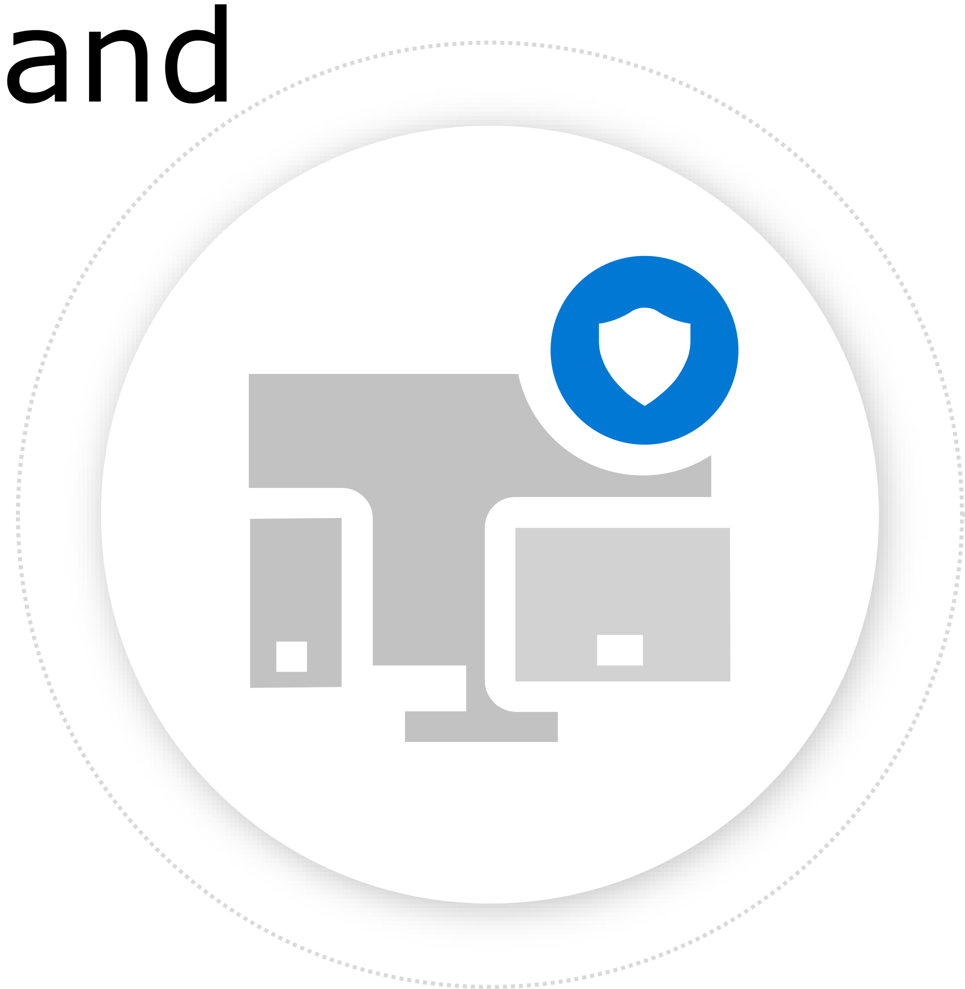
Examples: Only allow access from approved + Managed apps, control copy/paste, backup control, selective Wipe,

Threat Level

Verification if a device is at certain threat level as assessed by Threat Defense solutions such as Microsoft Defender for Endpoint or Mobile Threat Defense solutions from partners, device vendor’s health attestation, etc.

Visibility into device health and compliance

inetum realdolmen
Positive digital flow



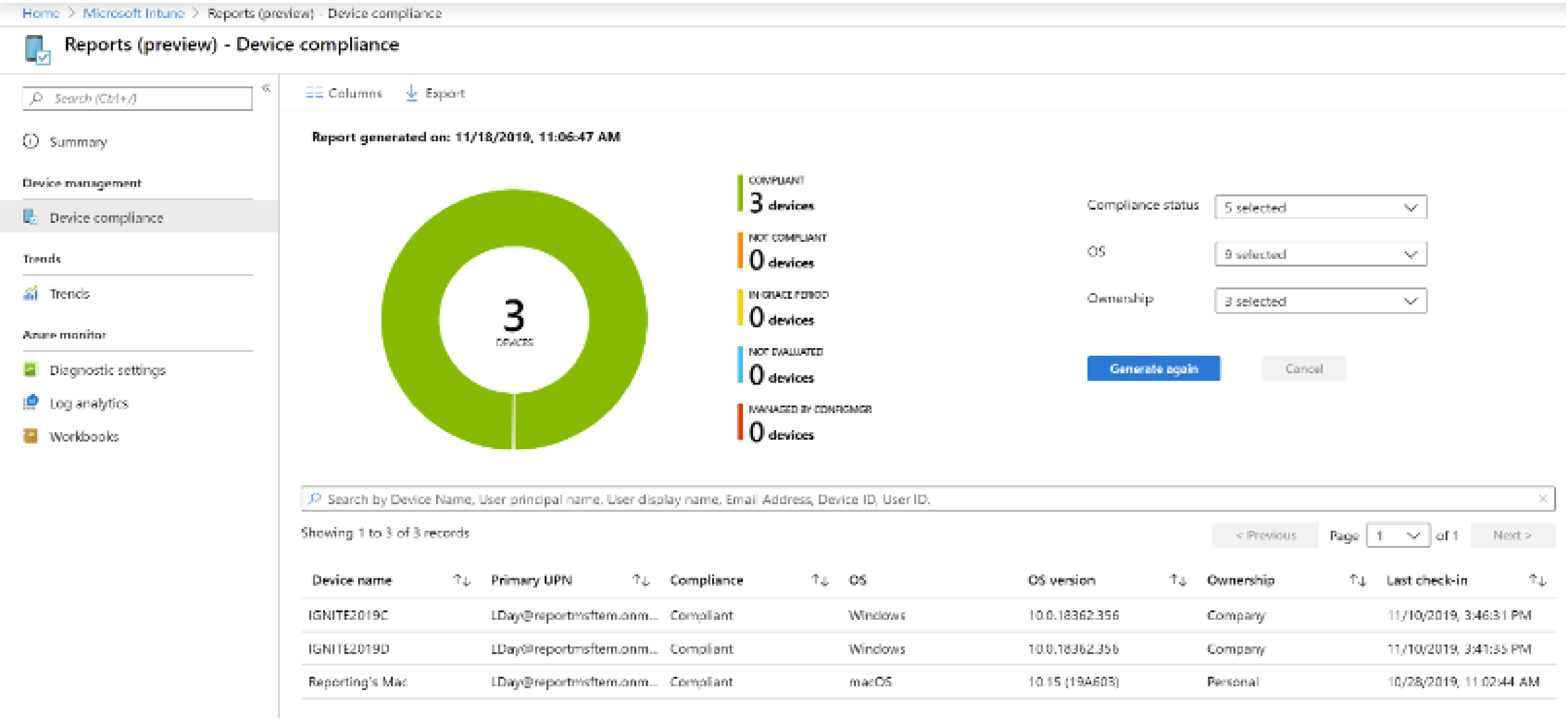
Device information detection:

- ⚠ Malicious Apps
- Device manipulation
- Network exploits
- Data privacy violations
- Device health
- Encryption
- OS version / jailbroken
- ✉ Email profile

Microsoft
Lookout
Symantec
ZIMPERIUM
pradeo
Google Play Protect
Check Point SOFTWARE TECHNOLOGIES LTD

Visibility

Corporate



Home > Microsoft Intune > Reports (preview) - Device compliance

Reports (preview) - Device compliance

Search (Ctrl+/)

Summary

Device management

Device compliance

Trends

Trends

Azure monitor

Diagnostic settings

Log analytics

Workbooks

Columns Export

Report generated on: 11/18/2019, 11:06:47 AM

COMPLIANT 3 devices

NOT COMPLIANT 0 devices

IN GRACE PERIOD 0 devices

NOT EVALUATED 0 devices

MANAGED BY CONFIGMGR 0 devices

Compliance status: 5 selected

OS: 9 selected

Ownership: 3 selected

Generate again Cancel

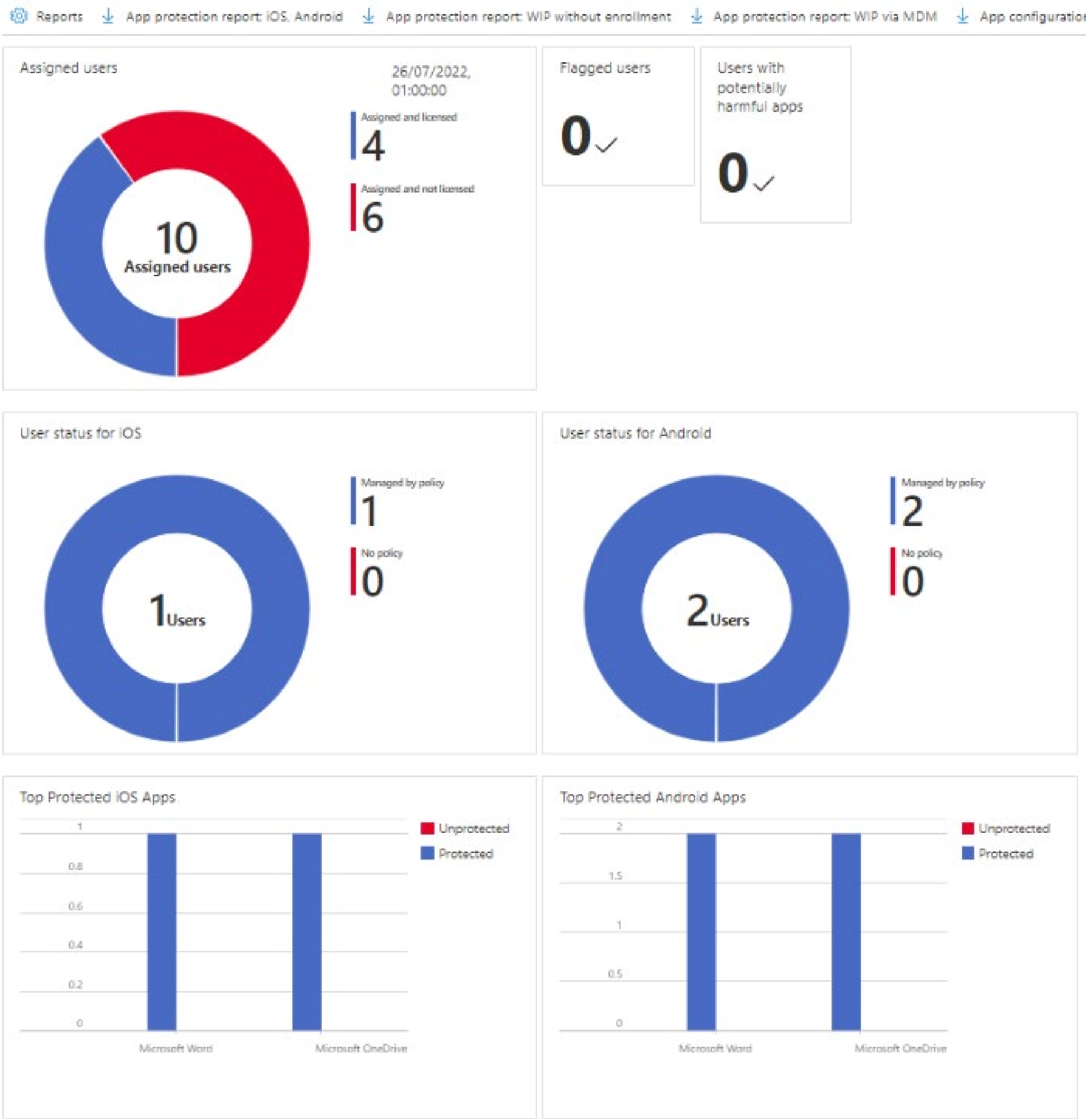
Search by Device Name, User principal name, User display name, Email Address, Device ID, User ID.

Showing 1 to 3 of 3 records

< Previous Page 1 of 1 Next >

Device name	Primary UPN	Compliance	OS	OS version	Ownership	Last check-in
IGNITE2019C	LDay@reportmsftem.onm...	Compliant	Windows	10.0.18362.356	Company	11/10/2019, 3:46:31 PM
IGNITE2019D	LDay@reportmsftem.onm...	Compliant	Windows	10.0.18362.356	Company	11/10/2019, 3:41:35 PM
Reporting's Mac	LDay@reportmsftem.onm...	Compliant	macOS	10.15 (19A603)	Personal	10/28/2019, 11:02:44 AM

Personal



Reports App protection report: iOS, Android App protection report: WIP without enrollment App protection report: WIP via MDM App configuratio

Assigned users

26/07/2022, 01:00:00

Assigned and licensed 4

Assigned and not licensed 6

Flagged users 0 ✓

Users with potentially harmful apps 0 ✓

User status for iOS

Managed by policy 1

No policy 0

User status for Android

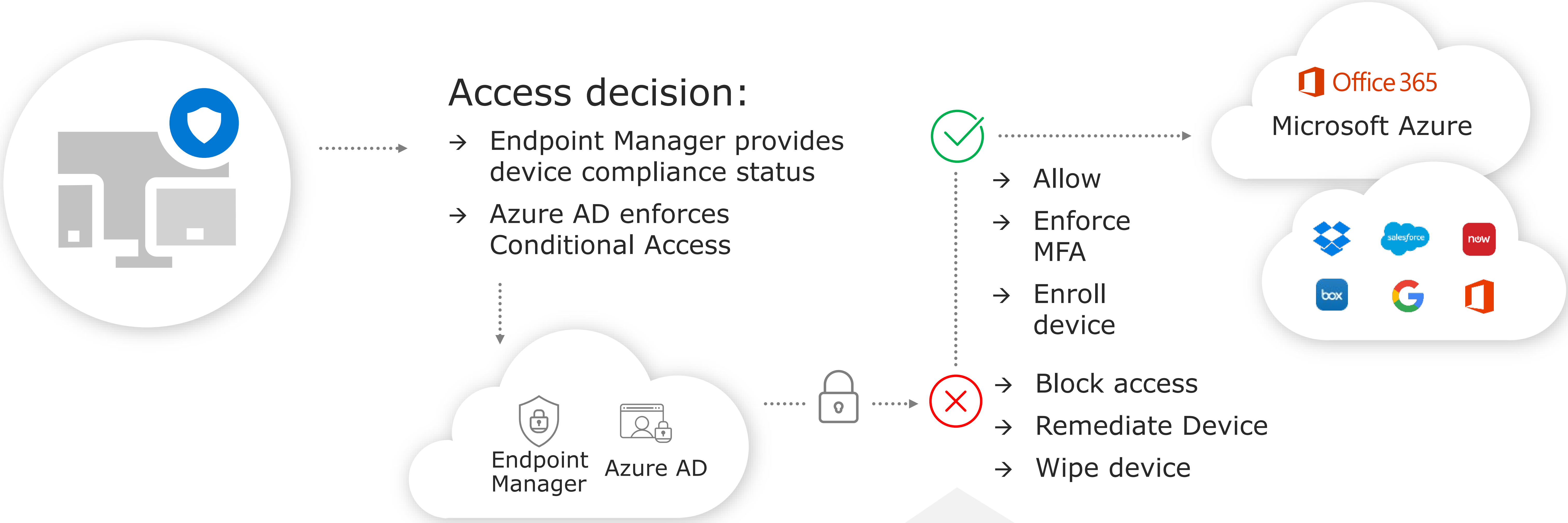
Managed by policy 2

No policy 0

Top Protected iOS Apps

Top Protected Android Apps

Restrict access from vulnerable and compromised devices



Access decision:

→ Endpoint Manager provides device compliance status

→ Azure AD enforces Conditional Access

→ Allow

→ Enforce MFA

→ Enroll device

→ Block access

→ Remediate Device

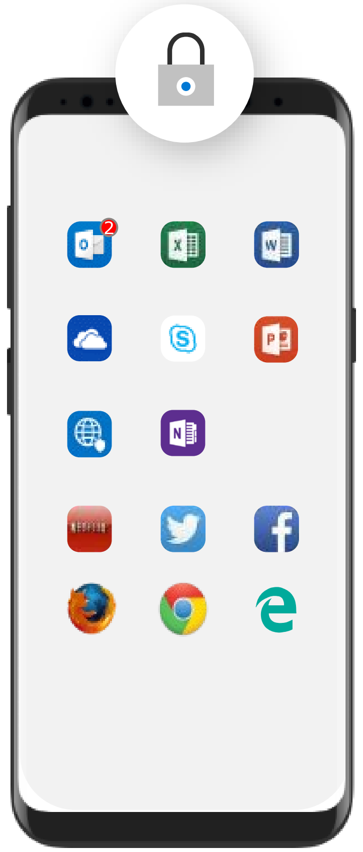
→ Wipe device

Users on unmanaged and insecure devices can be blocked or managed

Zero Trust compliance for mobile devices and apps

Mobile **Device** Management (MDM+[MAM])

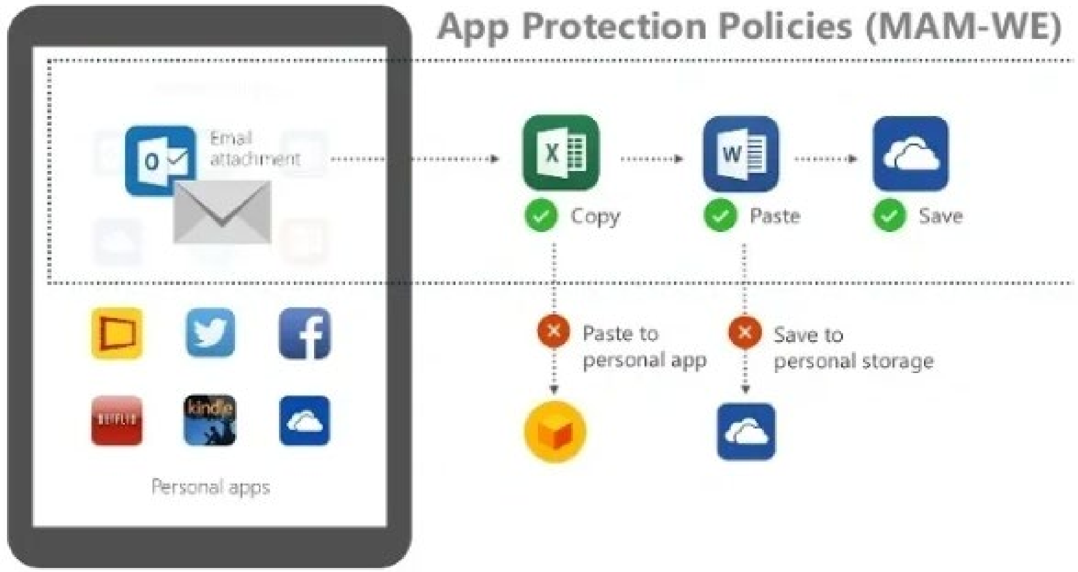
Conditional Access: Restrict access to managed and compliant devices



- Enroll devices for management
- Configure & update apps
- Report & measure device compliance
- Provision settings, certs, profiles
- Secure & Remove corporate data from devices

Mobile **Application** Management (MAM)

Conditional Access: Restrict which apps can be used to access email or files



- Provide mobile apps to users
- Configure apps
- Report app usage
- Secure & remove corporate data within mobile apps

Zero Trust Roadmap Devices

TRADITIONAL

- Devices are domain joined and managed with GPO’s
- Devices are required to be on a corporate network to access data
- No overview and inventory of devices

ADVANCED

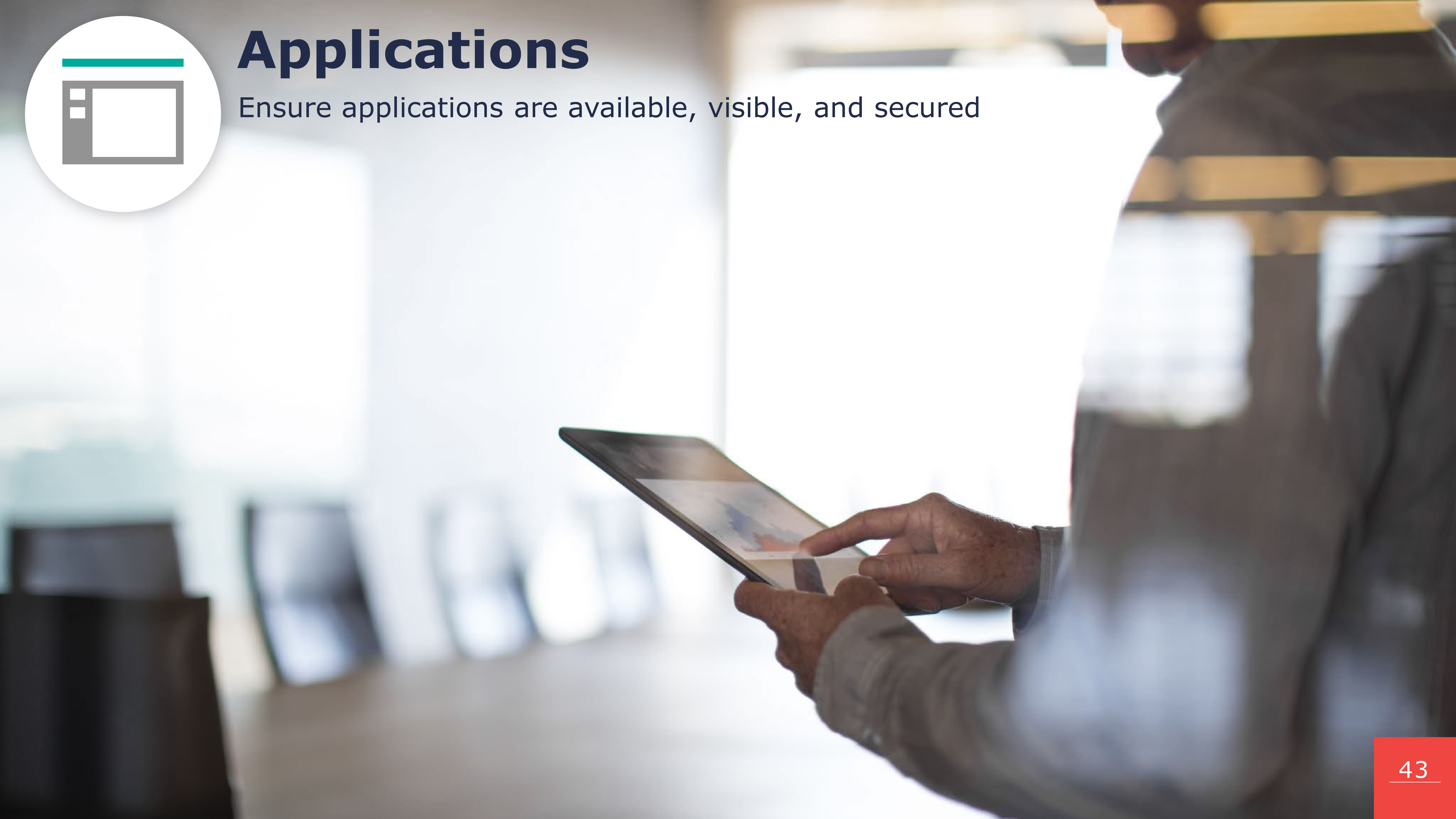
- Devices are registered with a cloud identity provider
- Access only granted to cloud managed or compliant devices
- DLP policies are enforced for BYOD
- Basic asset management and inventory in place

OPTIMAL

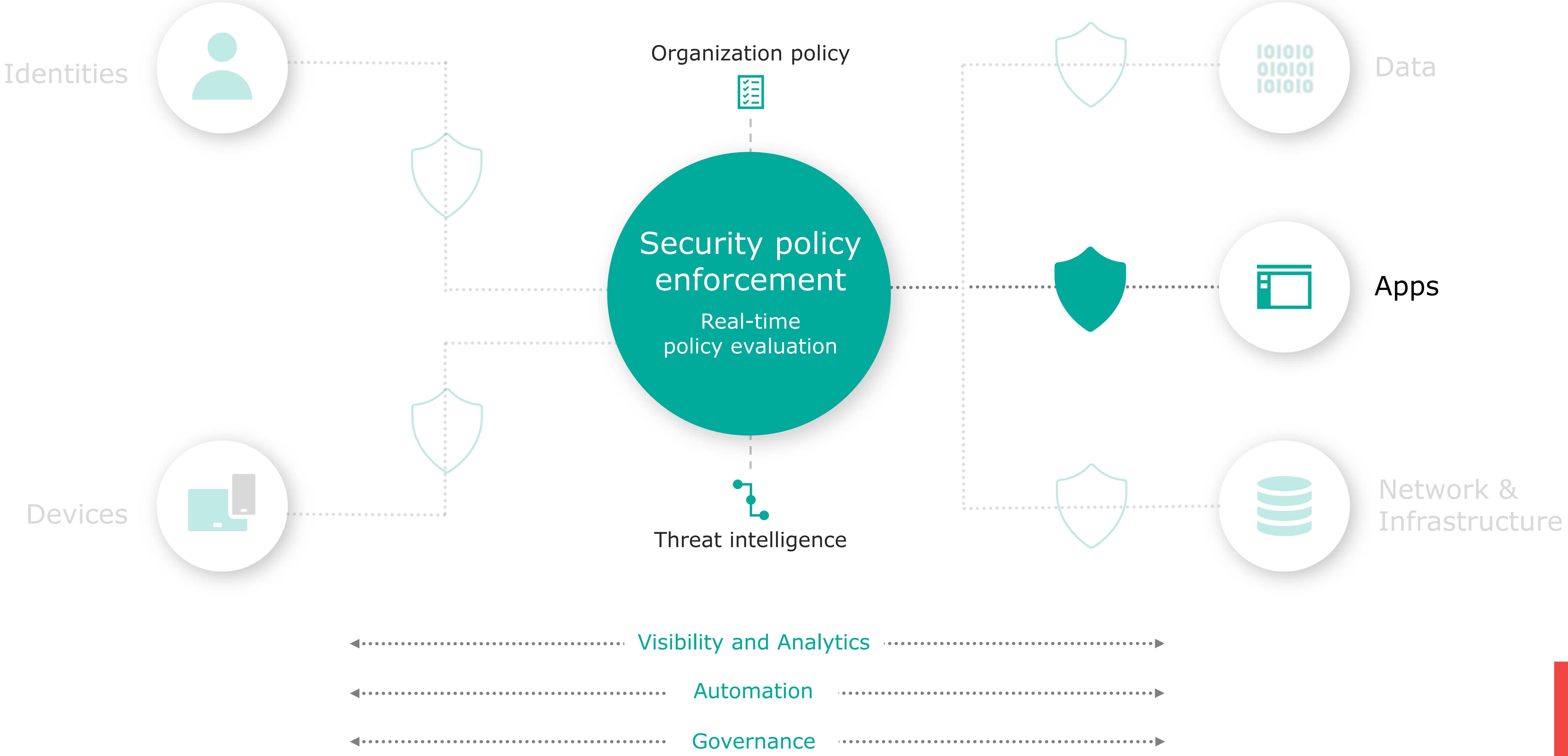
- Endpoint threat protection is used to monitor device risk
- Access control is gated on device risk
- Continuous risk-based asset management and inventory in place

Applications

Ensure applications are available, visible, and secured



Zero Trust Architecture



Ensure applications are available, visible and secured

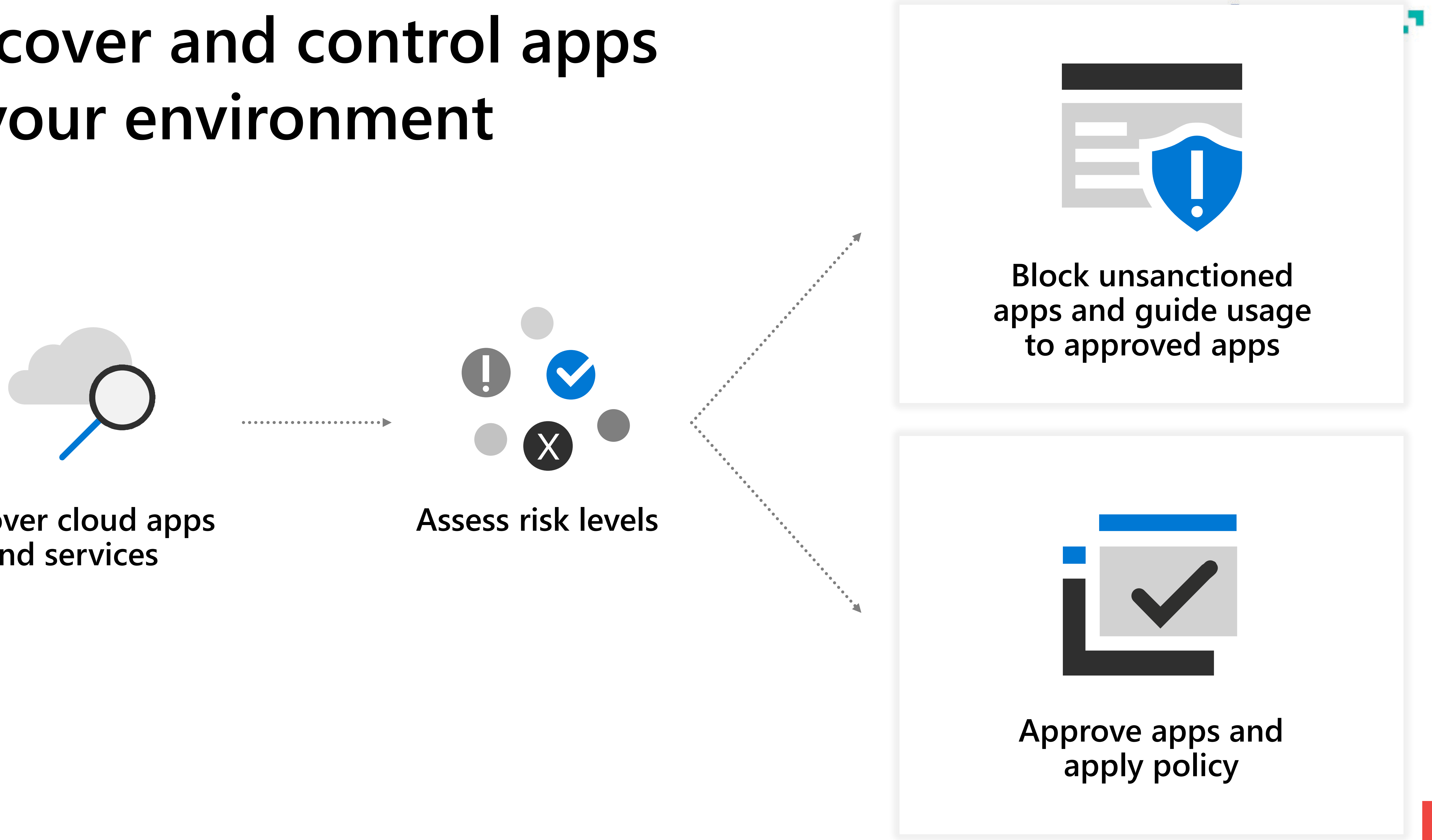
Discover and control apps in your environment

Extend policy enforcement into the session

Protect sensitive data in cloud apps

Protect apps from risks and threats across multi-cloud environments

Discover and control apps in your environment



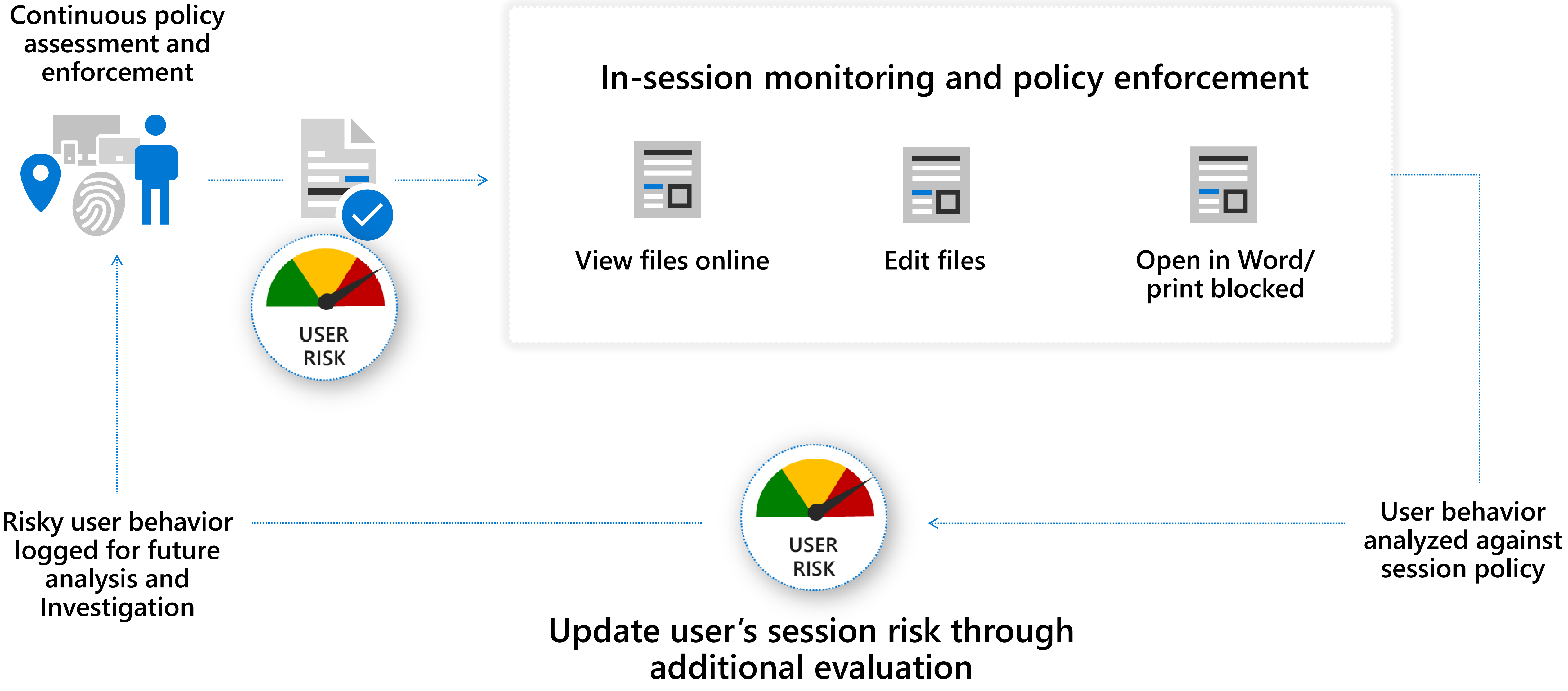
Discover cloud apps and services

Assess risk levels

Block unsanctioned apps and guide usage to approved apps

Approve apps and apply policy

Extend policy enforcement into the session



Continuous policy assessment and enforcement

In-session monitoring and policy enforcement

- View files online
- Edit files
- Open in Word/ print blocked

User behavior analyzed against session policy

Update user's session risk through additional evaluation

Risky user behavior logged for future analysis and Investigation

Protect sensitive data

Discover sensitive data exposure in your apps

- Visibility into application-based file sharing, collaborators and classification labels
- Report out on data exposure and compliance risks of applications

Classify, label and protect data across cloud apps

- Govern data in the cloud with granular DLP policies for applications
- Classify and label data to automatically protect, encrypt and restrict access to sensitive files across applications

Monitor, investigate and remediate data risks

- Generate alerts on policy violations and trigger automatic governance actions across applications
- Investigate incident, quarantine files, remove permissions and notify users across applications

Zero Trust Roadmap Applications

TRADITIONAL

- On-premises apps are accessed through physical networks or VPN
- Some critical cloud apps are accessible to users
- No overview of shadow IT

ADVANCED

- On-premise apps are internet-facing and cloud apps are configured with SSO
- Gain visibility into the activities in your applications by connecting them via APIs
- Discover and control the use of shadow IT
- Critical apps are monitored for abnormal activities

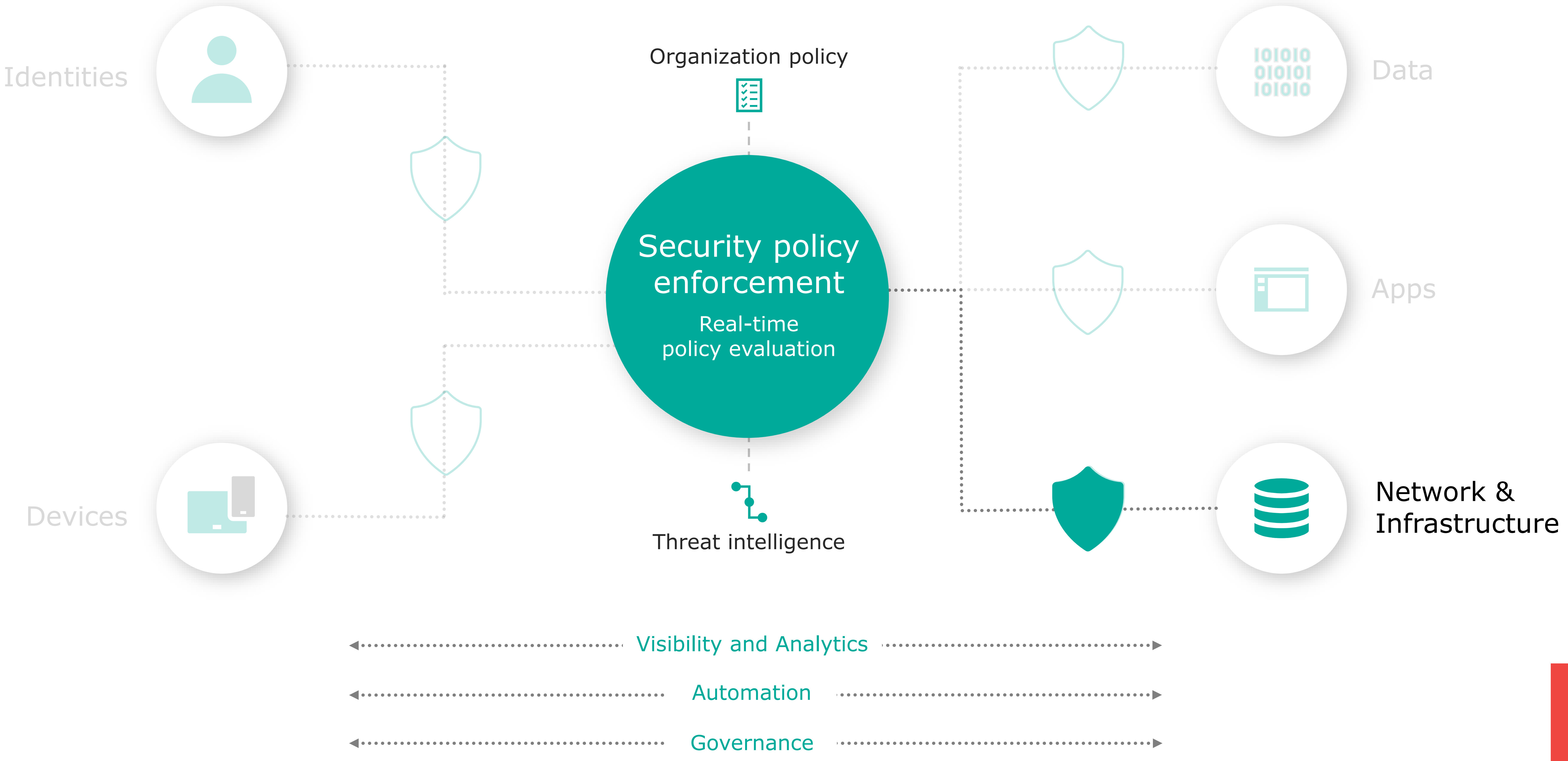
OPTIMAL

- All apps are available using least privilege access with continuous verification
- Dynamic control is in place for all apps with in-session monitoring and response
- Assess the security posture of your cloud environments

Network & Infrastructure

Move beyond traditional network & infrastructure security approaches

Zero Trust Architecture



Move beyond traditional network security approaches

Segment networks, implement NAC (Network Access Control) and a comprehensive security framework

Use real-time threat protection to detect and respond to threats

Protect data with end-to-end encryption

Segmentation

- Basic network segmentation (Macro segmentation)

- Micro segmentation
  - Datacenter
  - Campus

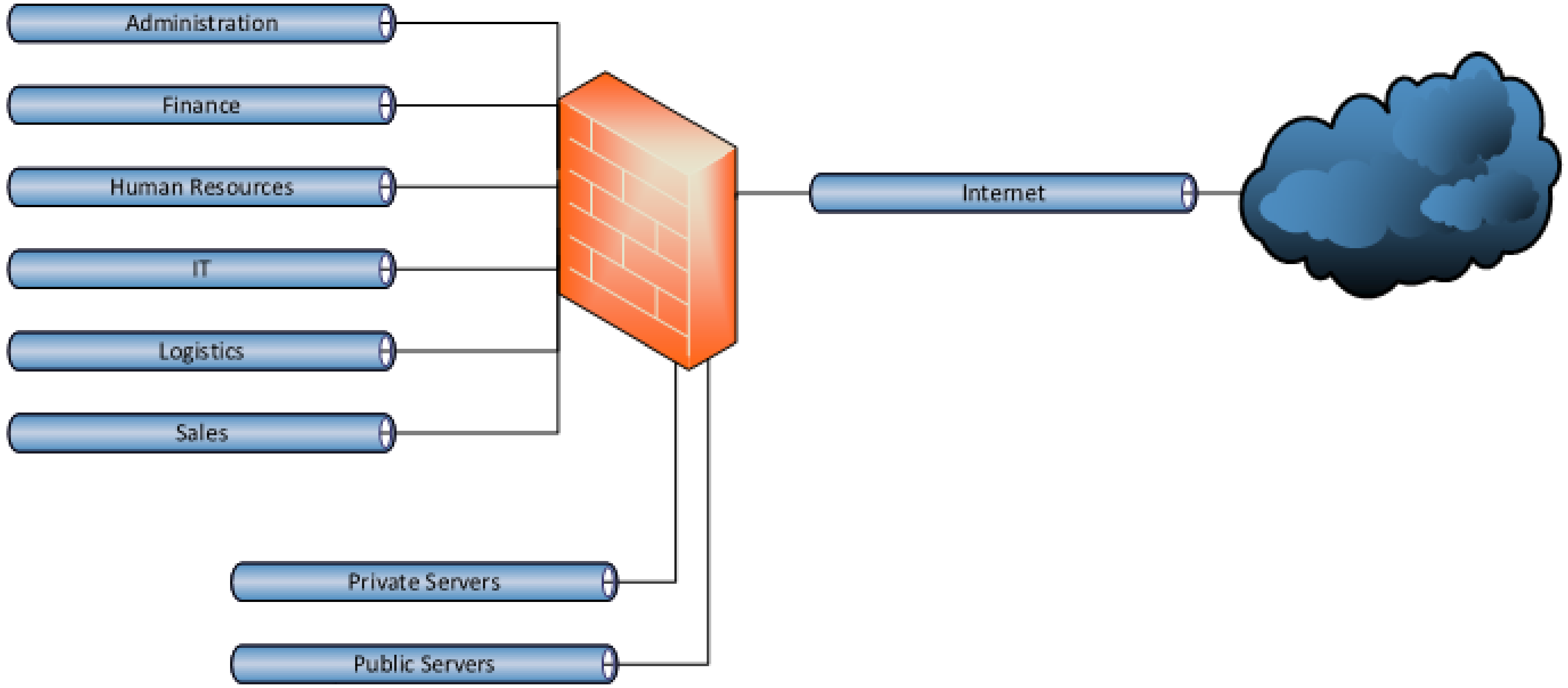
- Network access control

Macro Segmentation

- Vlan based

- Terminated on switch
  - Minimal Security
  - Not statefull
  - Lateral movement possible

- Terminated on firewall
  - Performance
  - Complex
  - Expensive



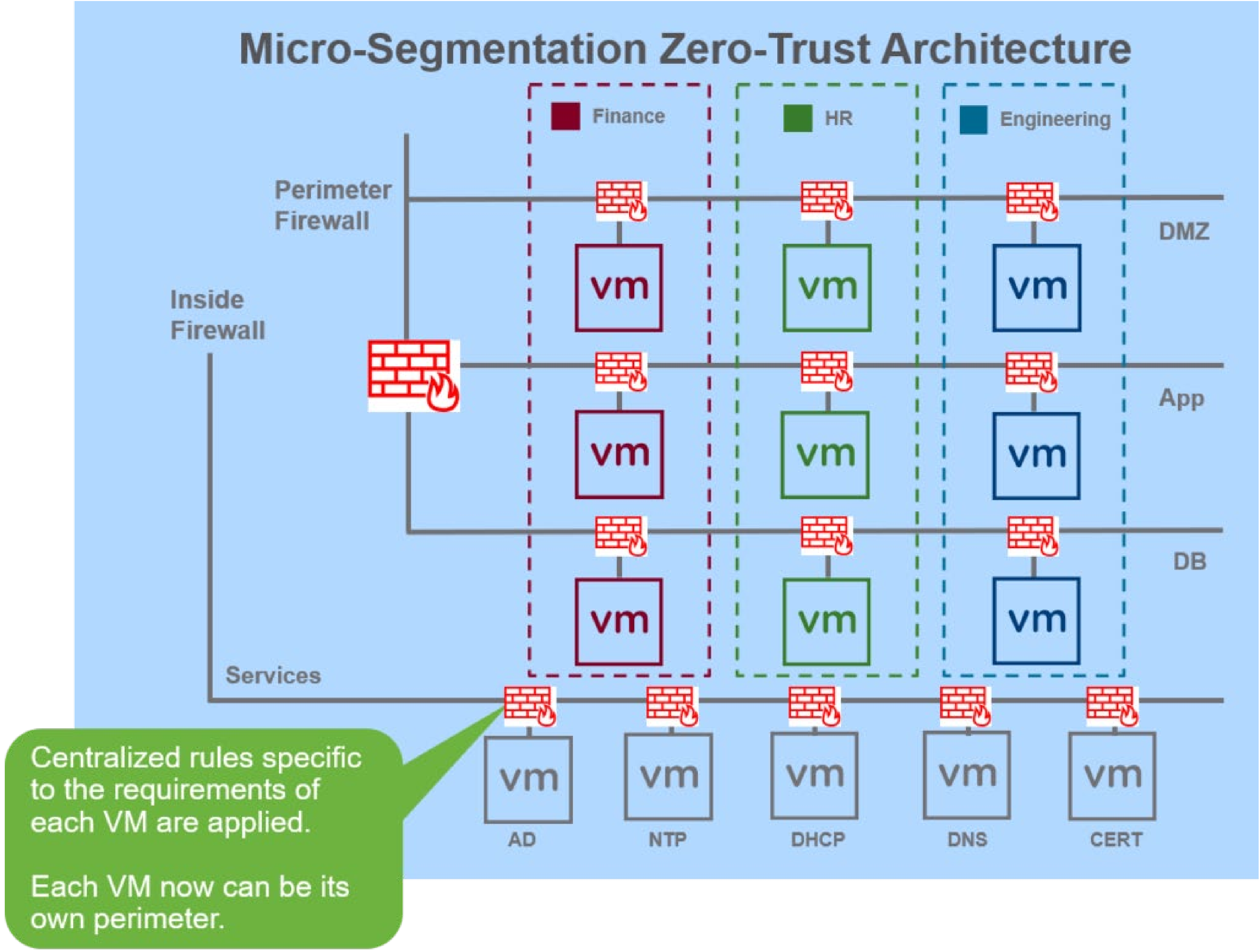
Micro Segmentation

Datacenter

- Virtual firewalls
  - Expensive
  - complex

- Distributed firewalls
  - Hypervisor based
  - Expensive
  - Only for VM's
  - Close to the application
  - Flow visibility

- Distributed services switch
  - Close to the application
  - Flow visibility
  - Physical and virtual loads
  - ASIC



Micro-Segmentation Zero-Trust Architecture

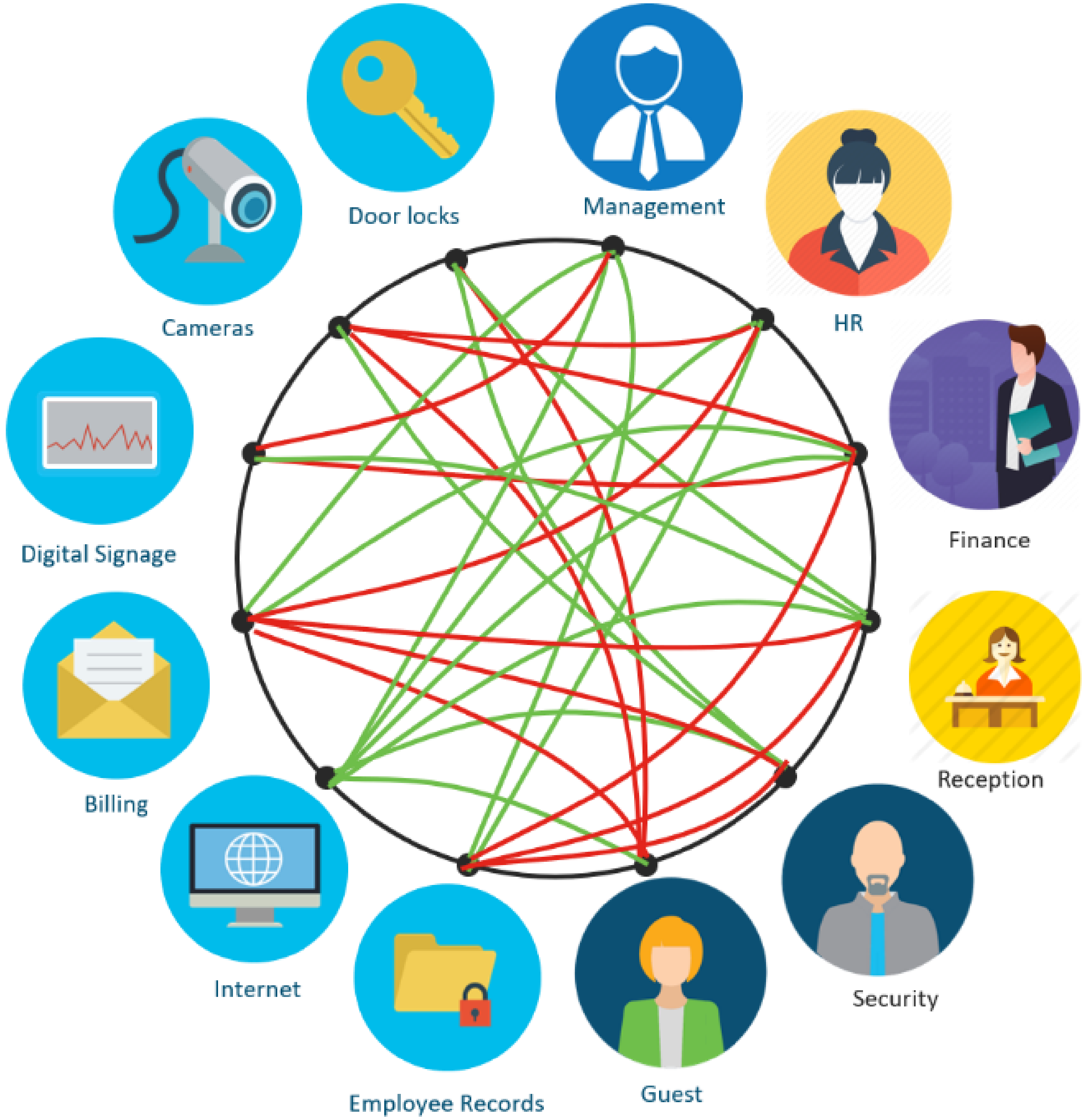
Centralized rules specific to the requirements of each VM are applied.

Each VM now can be its own perimeter.

Micro Segmentation

Campus

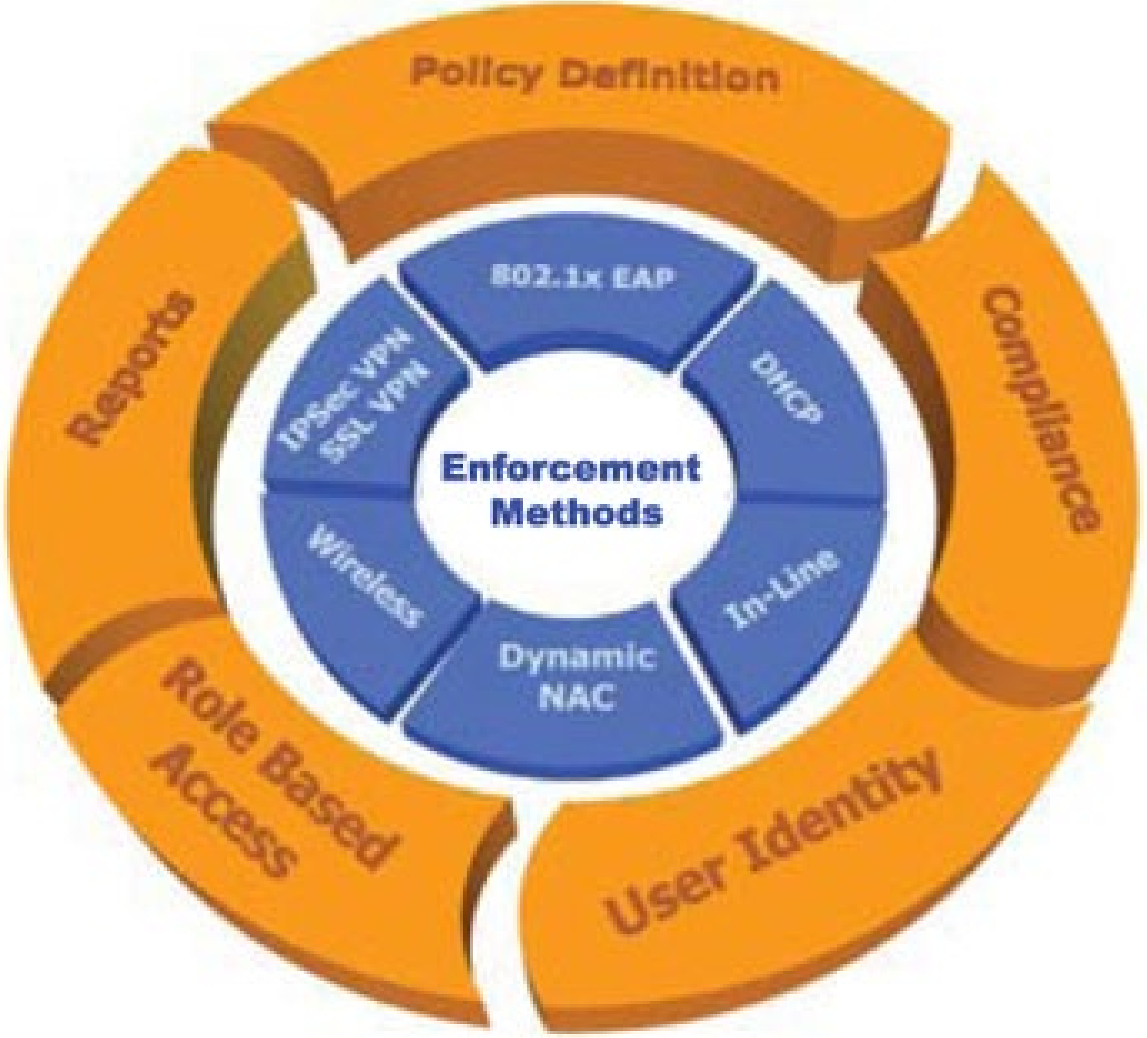
- VxLAN based
- Disconnect security from IP
- Role based
- Group based policies



NAC Network Access Control

Campus

- Authentication
- Role based access
- Dynamic segmentation
- Compliancy
- BYOD
- Guest

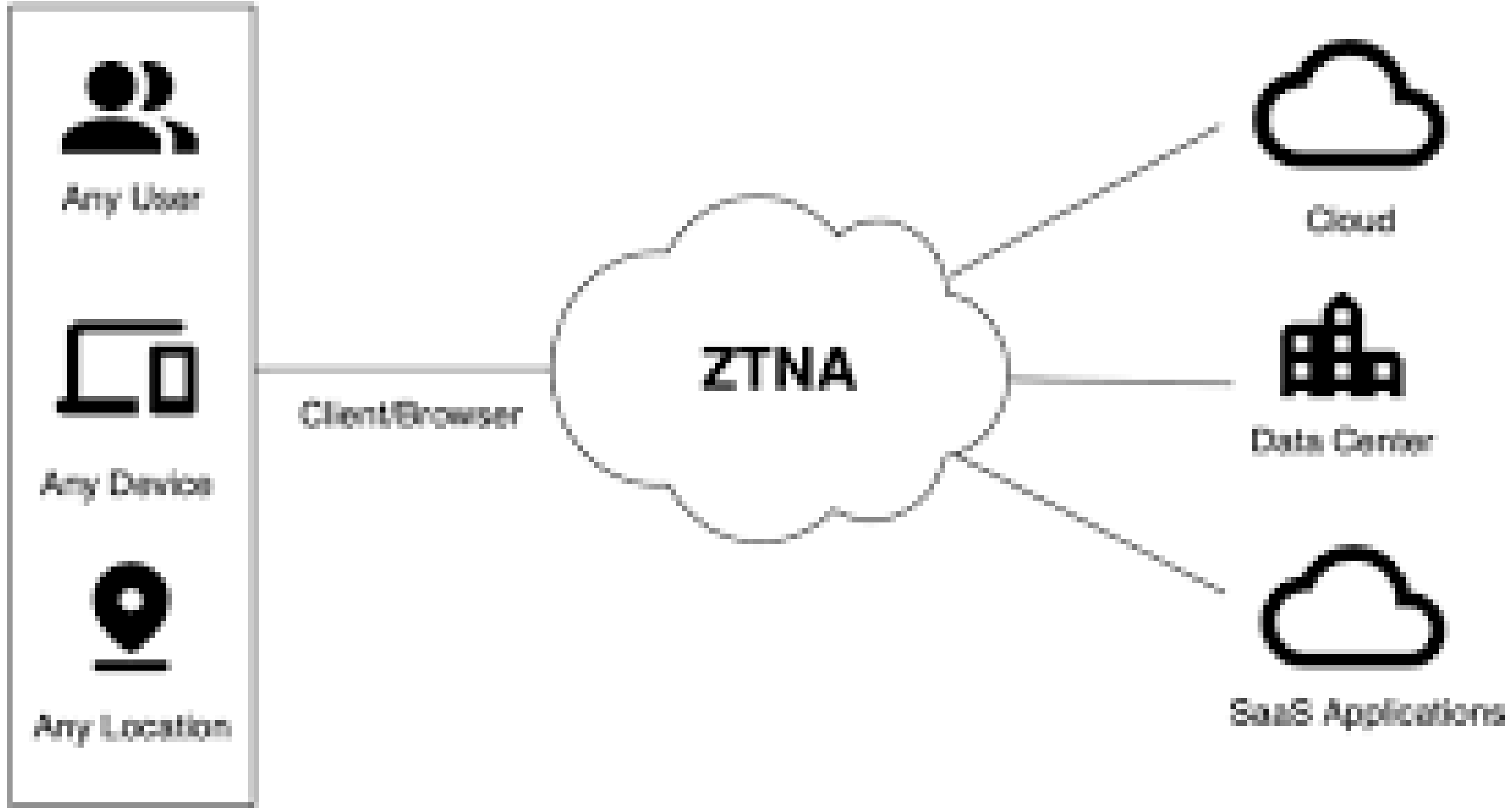


Zero Trust Network Access (ZTNA)

- Secure remote access

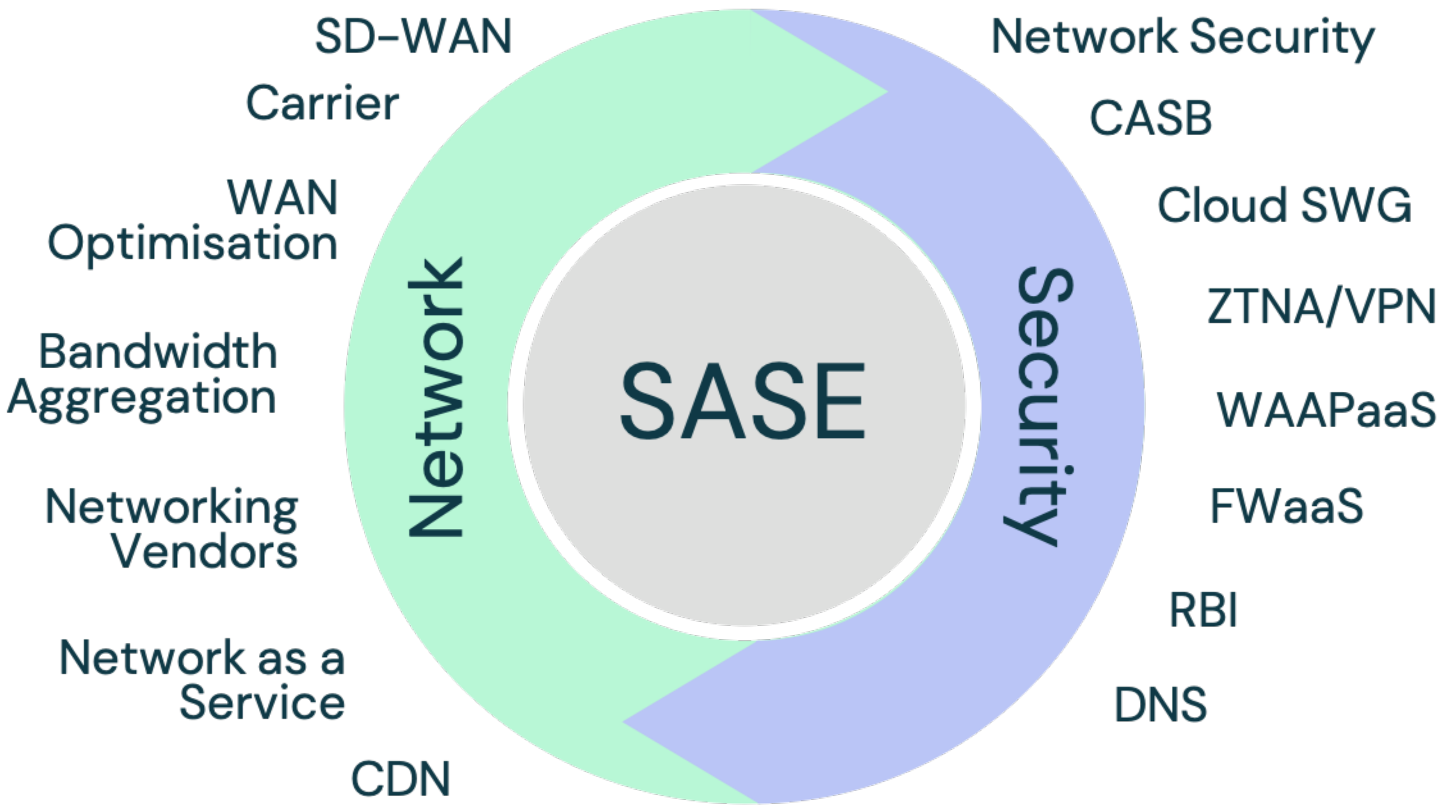
ZTNA VS VPN

- Access to application, services and data
- Default deny
- Prohibits lateral movement
- Part of SASE



SASE

- Cloud service
- Multicloud
- Combines network security and WAN
- Flexible



Advanced threat protection

- Known threats
- Unknown threats
- Cloud based intelligence
- AI/ML

Encryption

At rest

Encrypt VM disks, storage, and data

In transit

Encrypt data on the wire

Management of keys, secrets, and certificates backed by hardware security modules

Encryption

At Rest

- Storage encryption
- VM disk encryption
  - Hypervisor based
- Encrypt disks on clients

Encryption

On the wire

- Use TLS
  - Web Applications
  - Services
  - Databases
  - …
- Encryption on network devices
  - MACSEC
    - Client - switch
    - Switch – switch
    - Specific hardware

In VxLAN MACSEC can also be used from VTEP to VTEP

Zero Trust Roadmap Network & Infrastructure

inetum. realdolmen Positive digital flow

TRADITIONAL

- Few network security parameters and flat open network
- Minimal threat protection and static traffic filtering
- Unencrypted traffic

ADVANCED

- Basic network segmentation
- Cloud native filtering and threat protection
- Admin access to workloads requires Just-In-Time
- Workloads are monitored and alerted for abnormal behavior

OPTIMAL

- Micro segmentation of all networks
- ML-based threat protection and filtering
- All traffic is encrypted
- Unauthorized deployments of workloads are blocked

Data

Protect sensitive data wherever it lives or travels

Protect your sensitive data—wherever it lives or travels

Discover and classify your data based on sensitivity

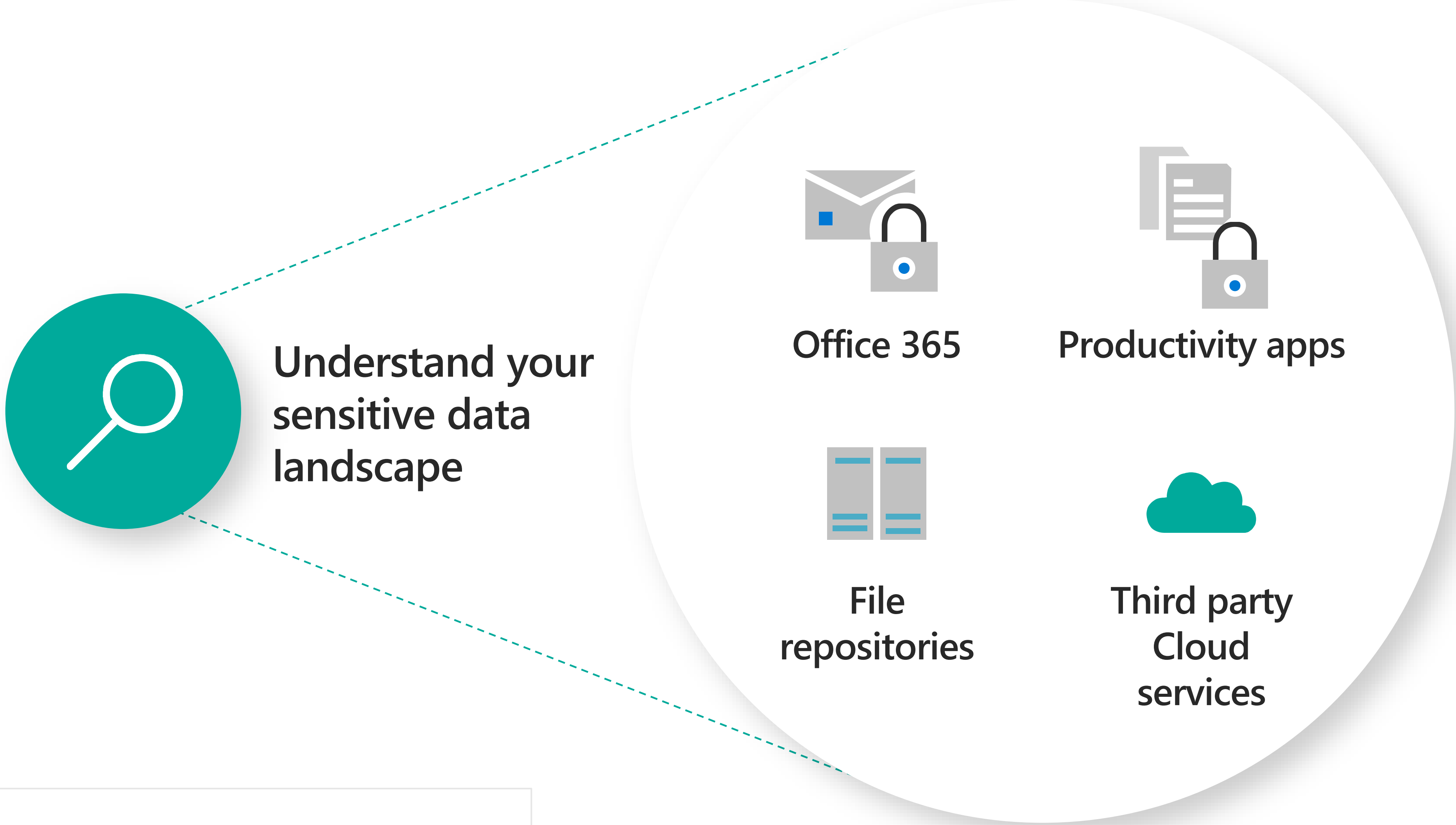
Apply real-time protection to your sensitive data

Gain visibility into sensitive data activity, policy violations, and risky sharing

Discover and classify your data

Understand your sensitive data exposure and define your protection policies

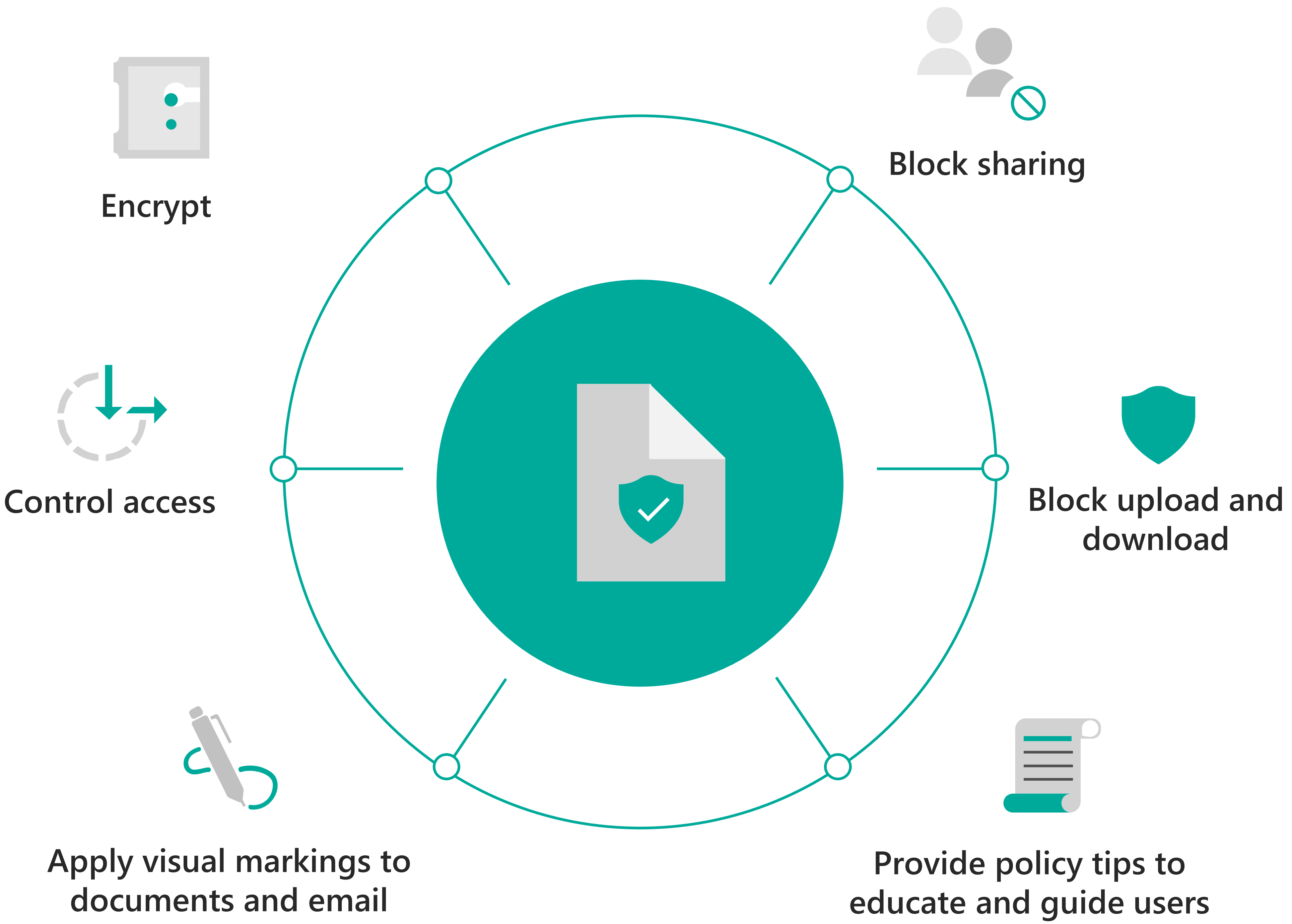
- → Define your policies for security and compliance requirements
- → Automatically inspect documents and emails across locations
- → Detect common data types such as financial, healthcare, PII—or customize your own


Understand your sensitive data landscape
Office 365
Productivity apps
File repositories
Third party Cloud services

163 zettabytes of data per year will be created by 2025

Apply comprehensive protection to data and files

Enforce the right protection actions based on data type, location, and sensitivity



Encrypt

Block sharing

Control access

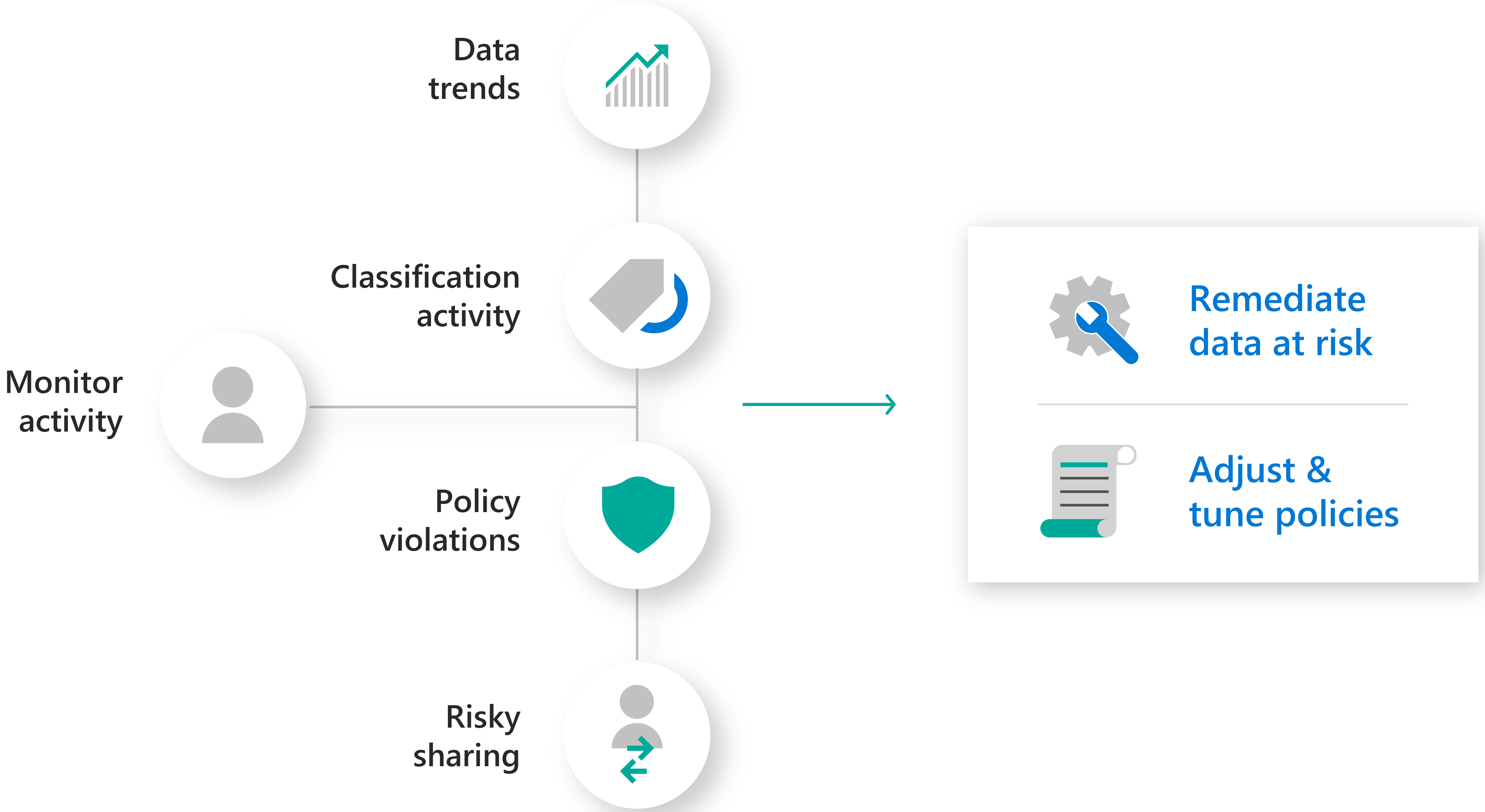
Block upload and download

Apply visual markings to documents and email

Provide policy tips to educate and guide users

Monitor and remediate

Gain visibility into sensitive data activity, policy violations, and risky sharing



Data trends

Classification activity

Monitor activity

Policy violations

Risky sharing

Remediate data at risk

Adjust & tune policies

Zero Trust Roadmap Data

TRADITIONAL

- Access is governed by perimeter control, not data sensitivity
- Sensitivity labels are applied manually, with inconsistent data classification
- Data is unencrypted

ADVANCED

- Access decisions are governed by sensitivity labels
- Data is classified and labeled via keyword methods
- Data is encrypted

OPTIMAL

- Data classification is augmented by smart machine learning models
- Access decisions are governed by a cloud security policy engine
- Prevent data leakage through DLP policies based on sensitivity labels and content inspection