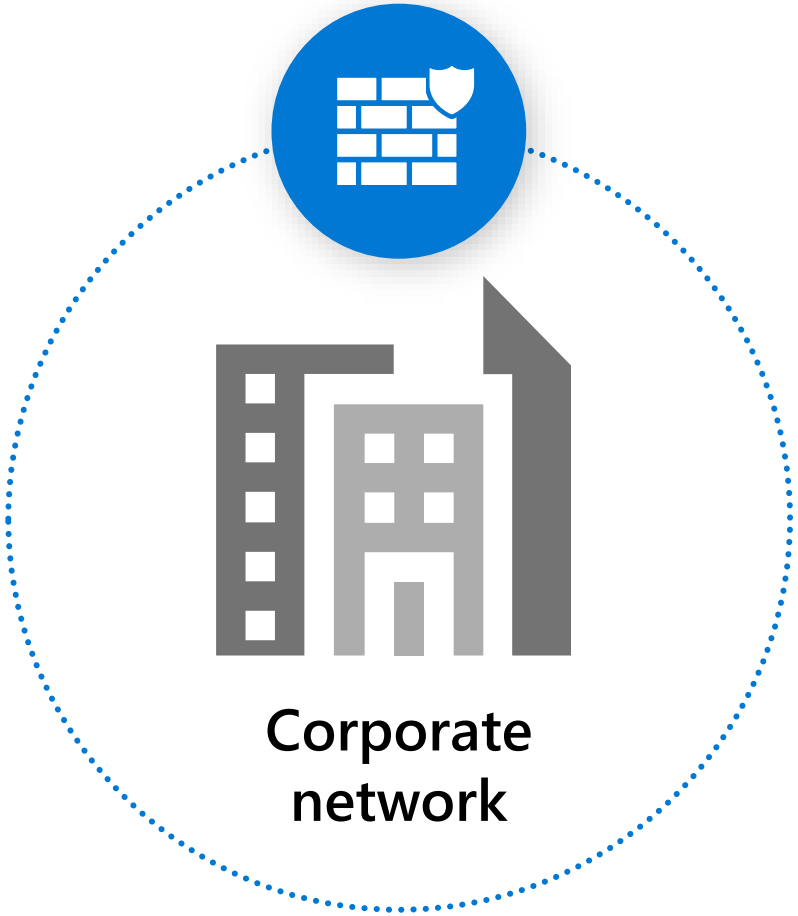
Modern security with a Zero Trust end-to-end strategy

James Ringold
Chief Security Advisor

John Rex
Director – Security, Compliance, and Identity

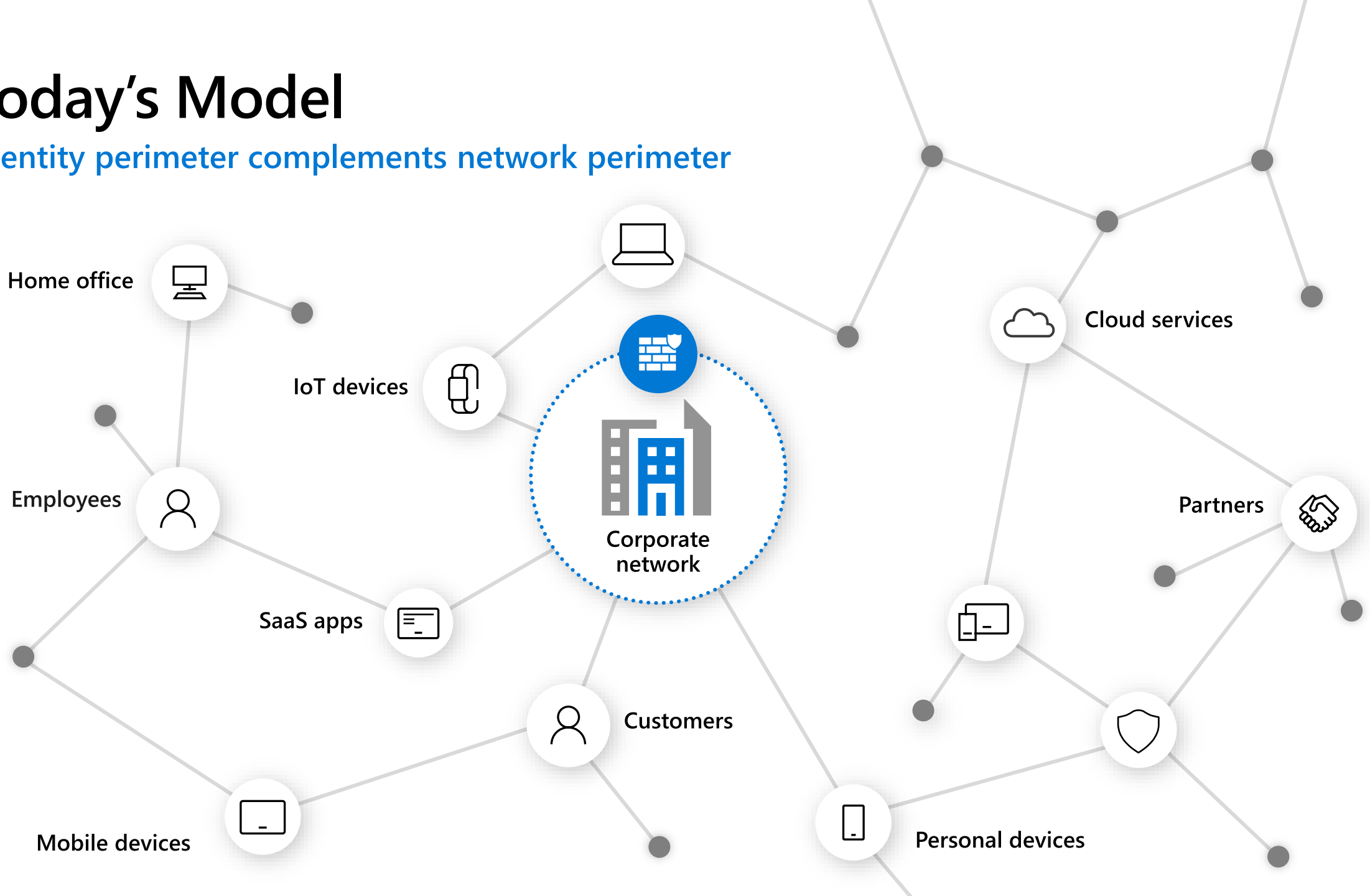
Traditional Model



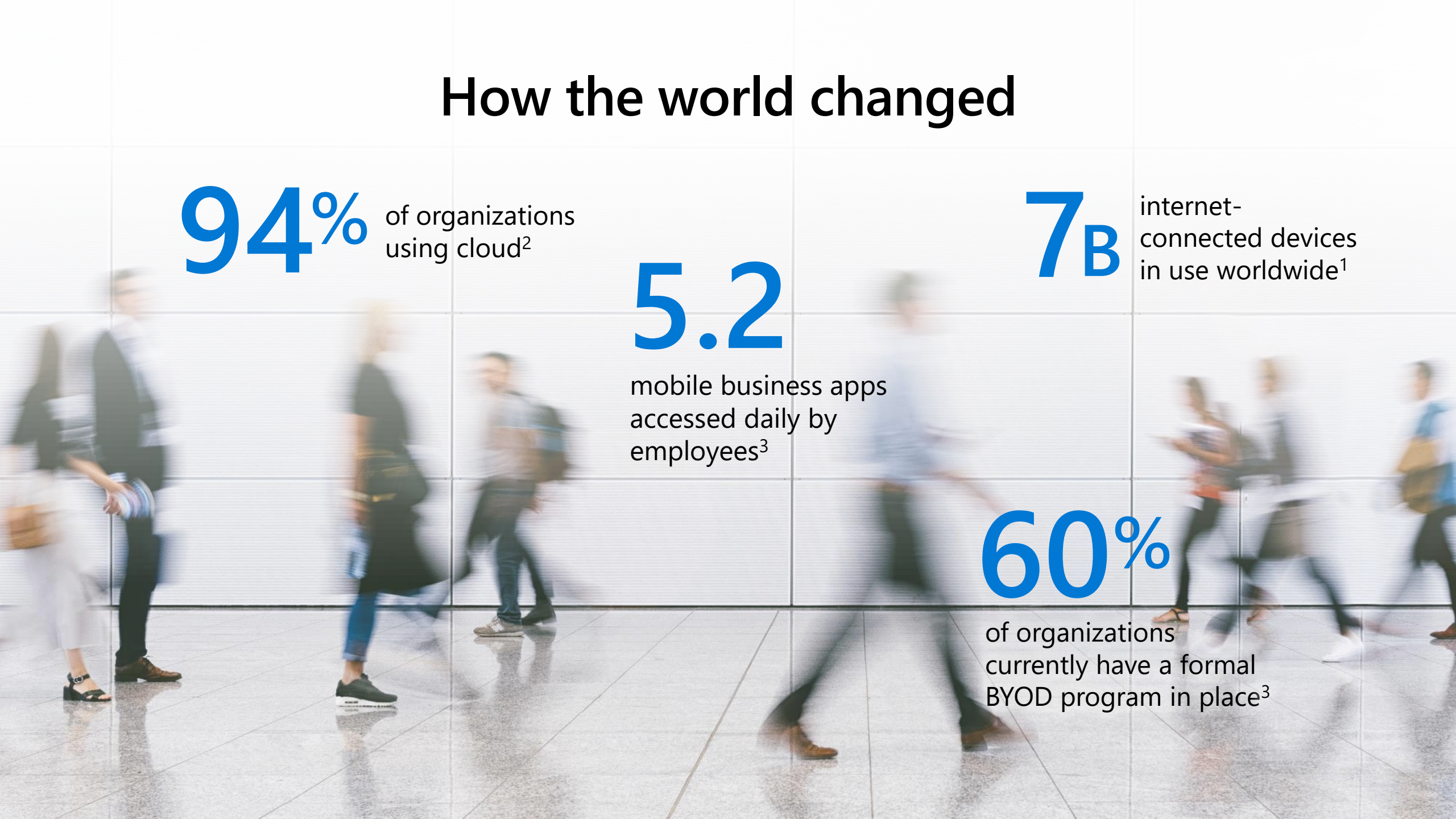
Users, devices, apps, and data protected behind a DMZ/firewall

Today's Model

Identity perimeter complements network perimeter



How the world changed



94% of organizations using cloud[2]

5.2 mobile business apps accessed daily by employees[3]

7B internet-connected devices in use worldwide[1]

60% of organizations currently have a formal BYOD program in place[3]

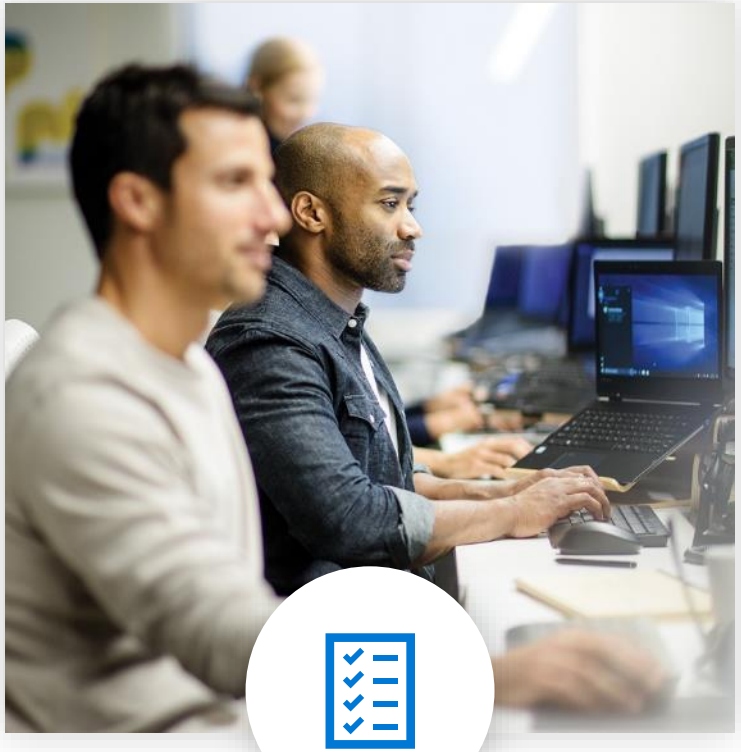
Old World vs. New World

~~Users are employees~~		Employees, partners, customers, bots
~~Corporate managed devices~~		Bring your own devices and IoT
~~On-premises apps~~		Explosion of cloud apps
~~Monolithic apps~~		Composite apps & public restful APIs
~~Corp network and firewall~~		Expanding Perimeters
~~Local packet tracking and logs~~		Explosion of signal

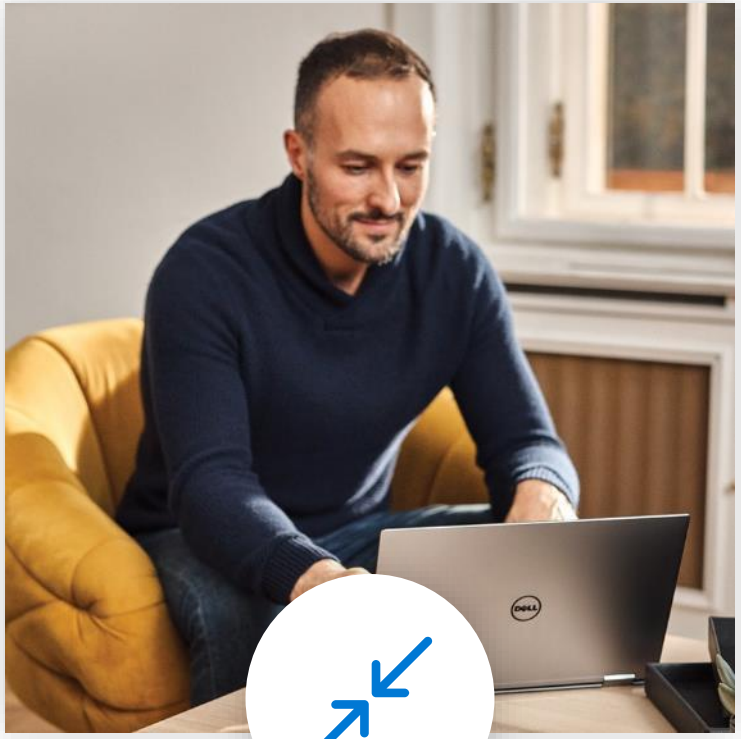
Zero Trust

An integrated approach to securing access with adaptive controls and continuous verification across your entire digital estate

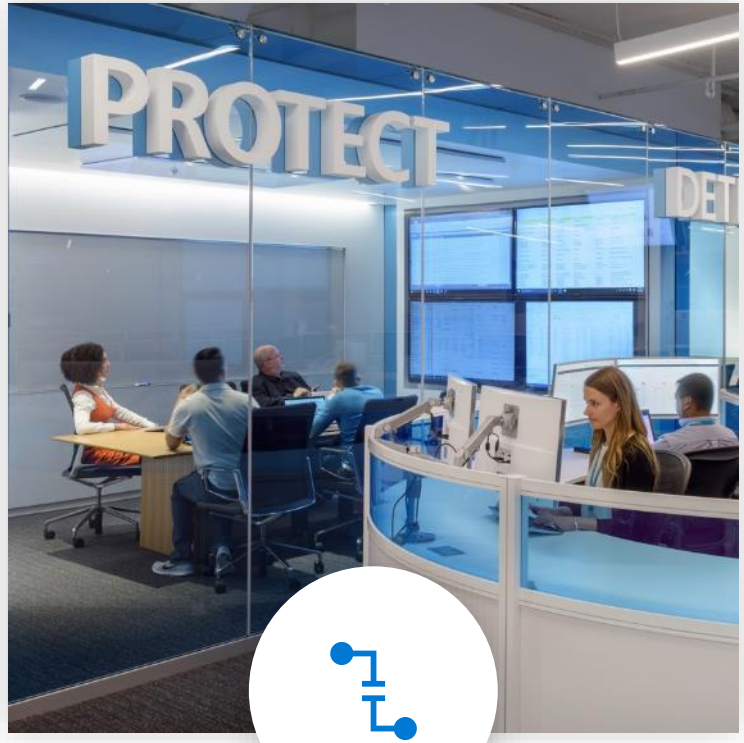
A new reality needs new principles



Verify explicitly

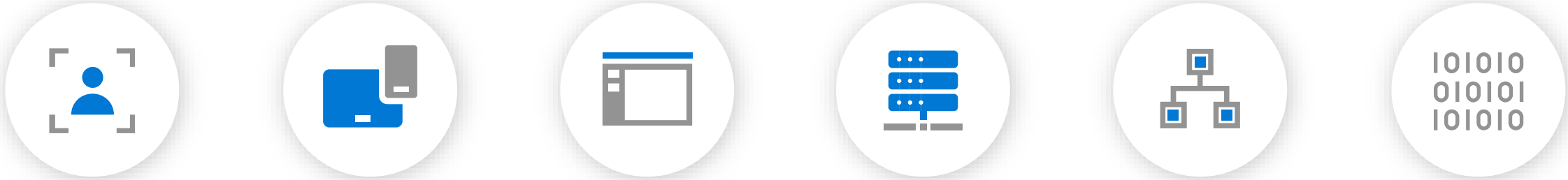


Use least privilege access



Assume breach

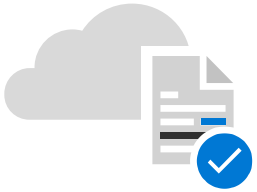
Zero Trust across the digital estate



Verify and secure every identity with strong authentication

Connect all of your users and applications

Verify identities with Multi-factor authentication (MFA)

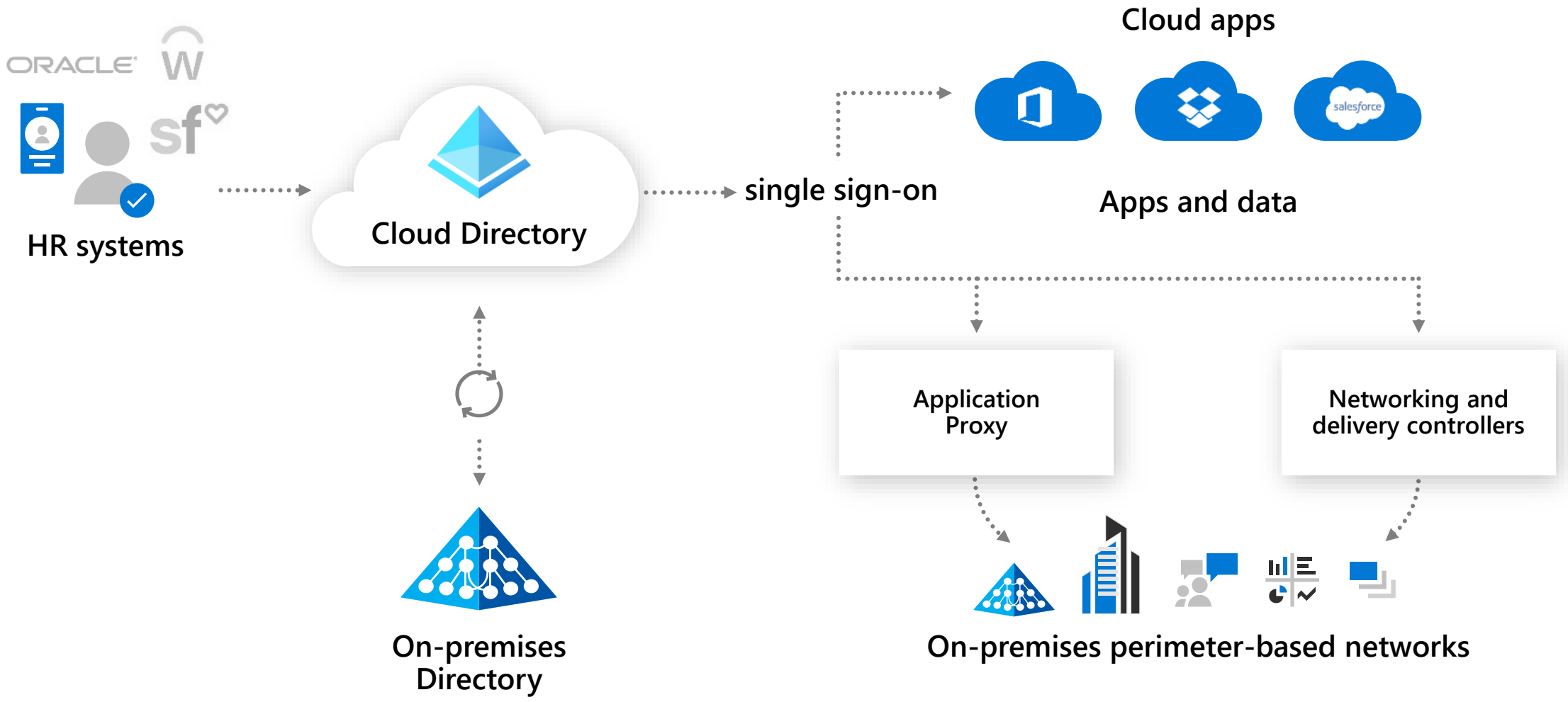


Control access with smart policies and risk assessments

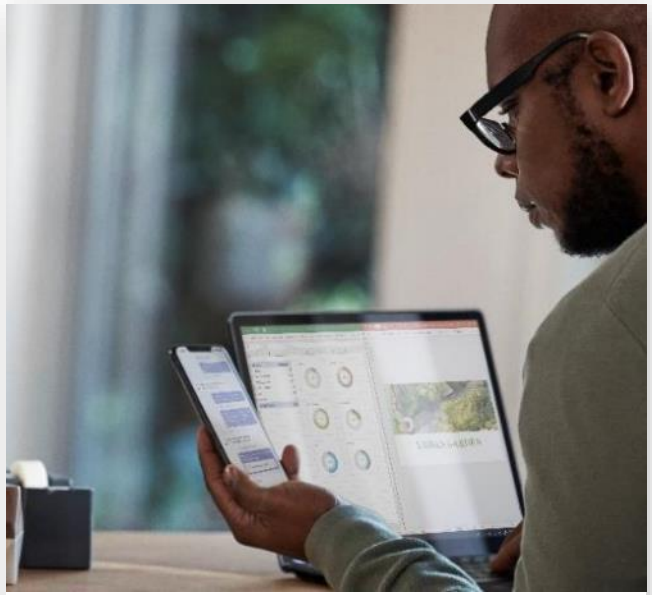
Enforce least privilege access with strong governance

Connect all your users and apps

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



Verify identities with Multi-Factor Authentication (MFA)



Support a broad range of multi-factor authentication options

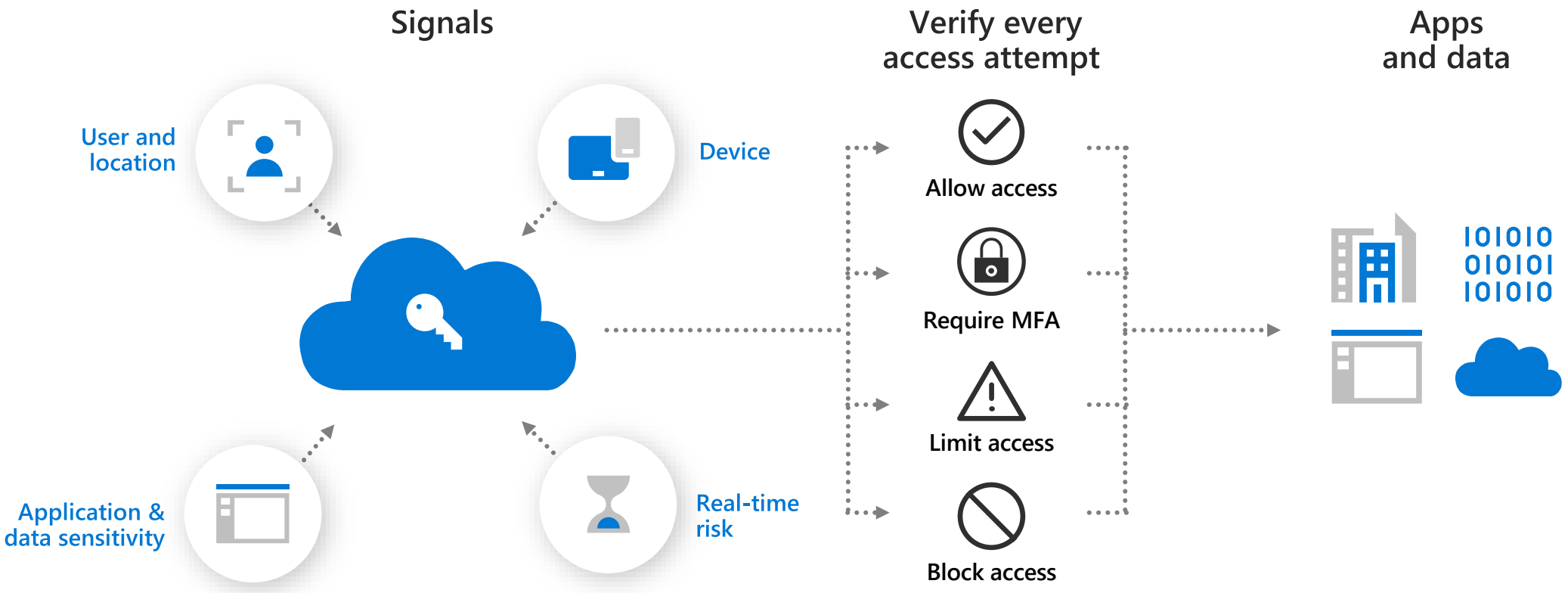
Including passwordless technology

- Authenticator Apps
- Facial Recognition
- FIDO2 security key
- Biometrics

- Push notification
- Soft Tokens OTP
- Hard Tokens OTP
- SMS, voice

Multi-factor authentication prevents 99.9% of identity attacks

Control access with smart policies and risk assessments



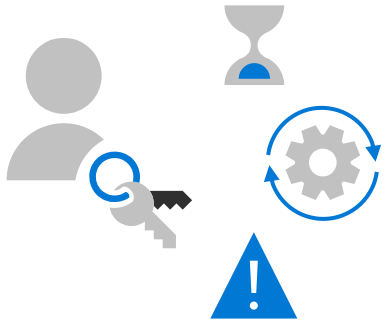
Enforce least privilege access with strong governance

Identity lifecycle

User onboarded

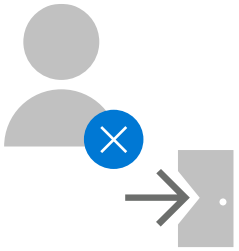
Access lifecycle

Oversight with access reviews



Admin rights

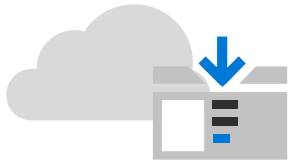
Privileged identity management



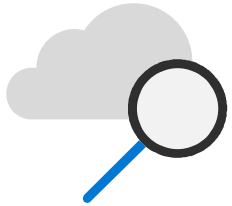
End of lifecycle

Access rights automatically removed

Allow only compliant and trusted apps and devices to access data



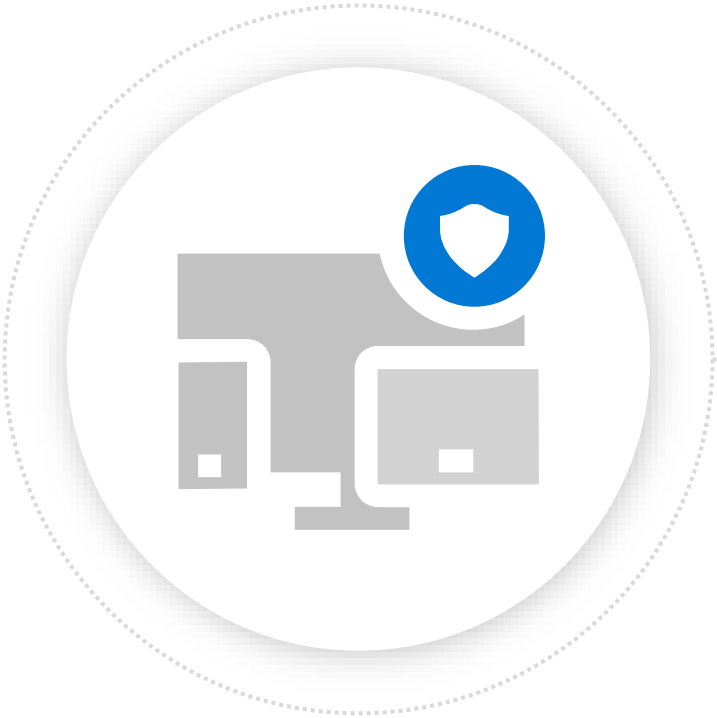
Visibility into device health and compliance



Restrict access from vulnerable and compromised devices

Enforce security policies on mobile devices and applications

Visibility into device health and compliance



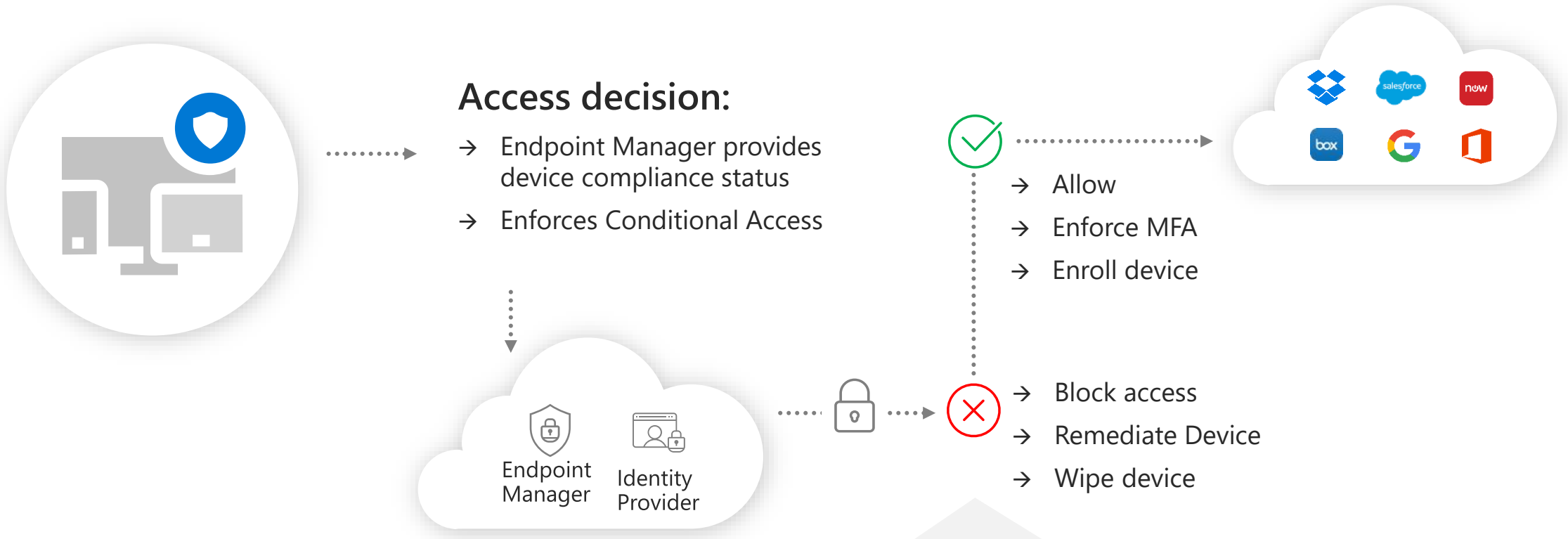
Device information detection:

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

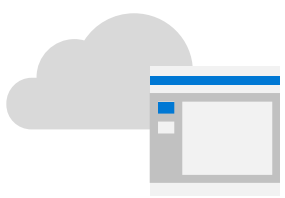
Endpoint protection and posture assessment across devices and types

Support for mobile and traditional computing platforms

Restrict access from vulnerable and compromised devices



Ensure applications are available, visible and secured



Discover and control apps in your environment

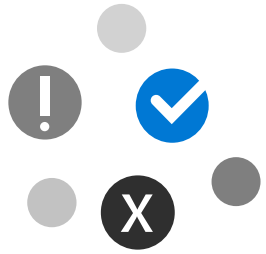
Extend policy enforcement into the session

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

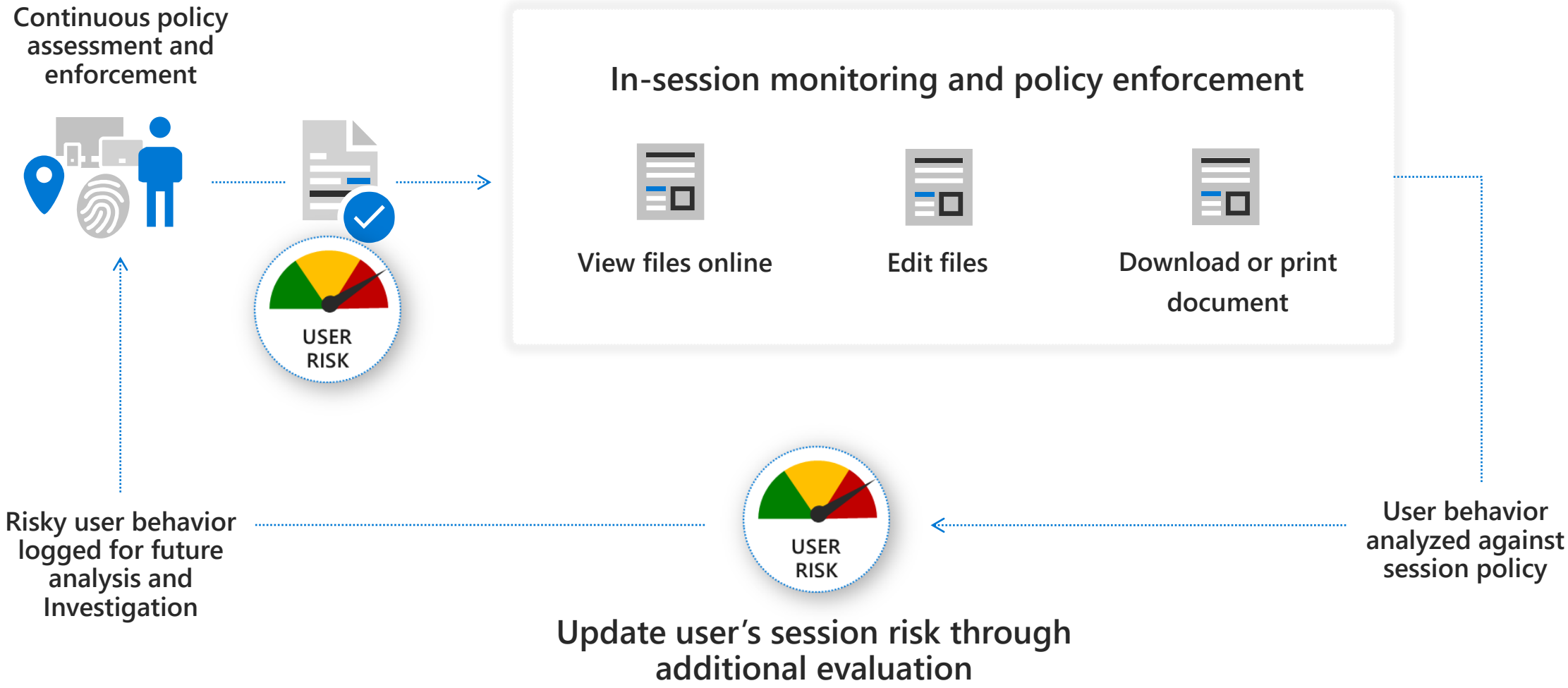


Assess risk levels

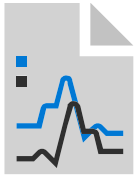
Block unsanctioned apps and guide usage to approved apps

Approve apps and apply policy

Extend policy enforcement into the session

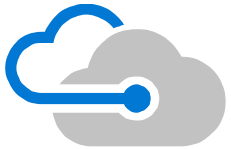


Protect sensitive data in cloud apps



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



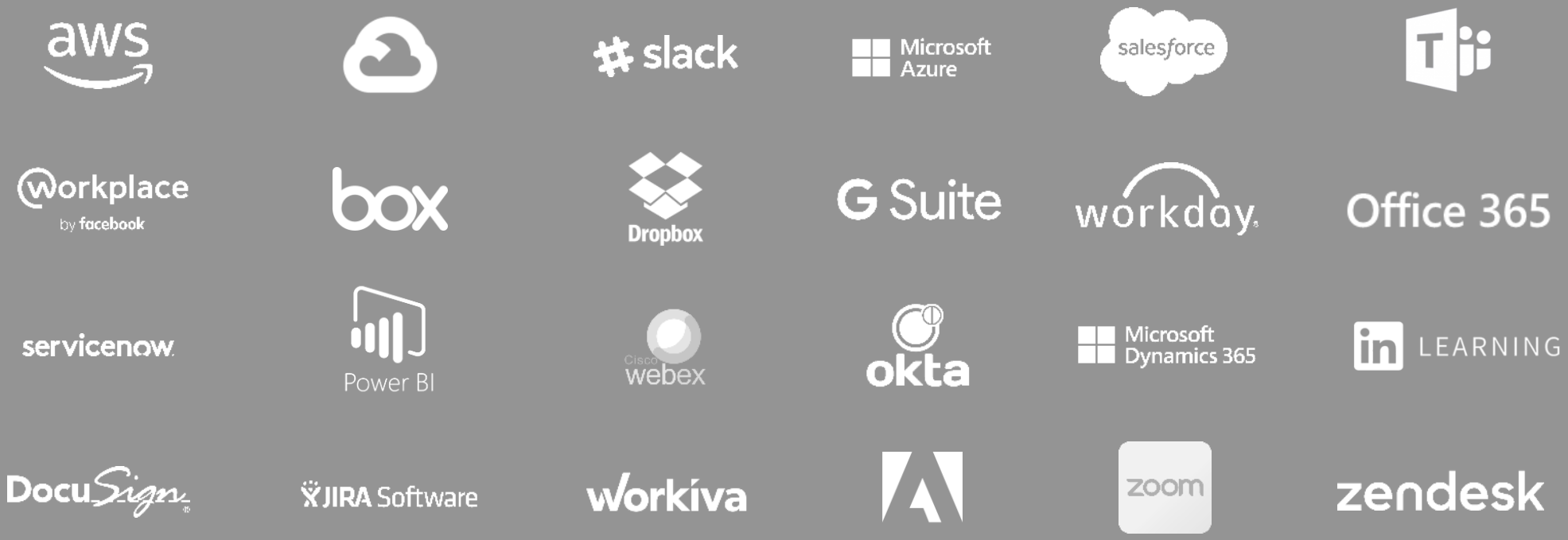
Classify, label and protect data across cloud apps

- 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

Protect apps from risks and threats across the clouds



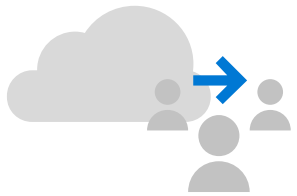
Threat delivery and persistence

Indicators of a compromised session

Malicious use of an end-user account

Malicious use of a privileged user

Harden defenses and detect and respond to threats in real time



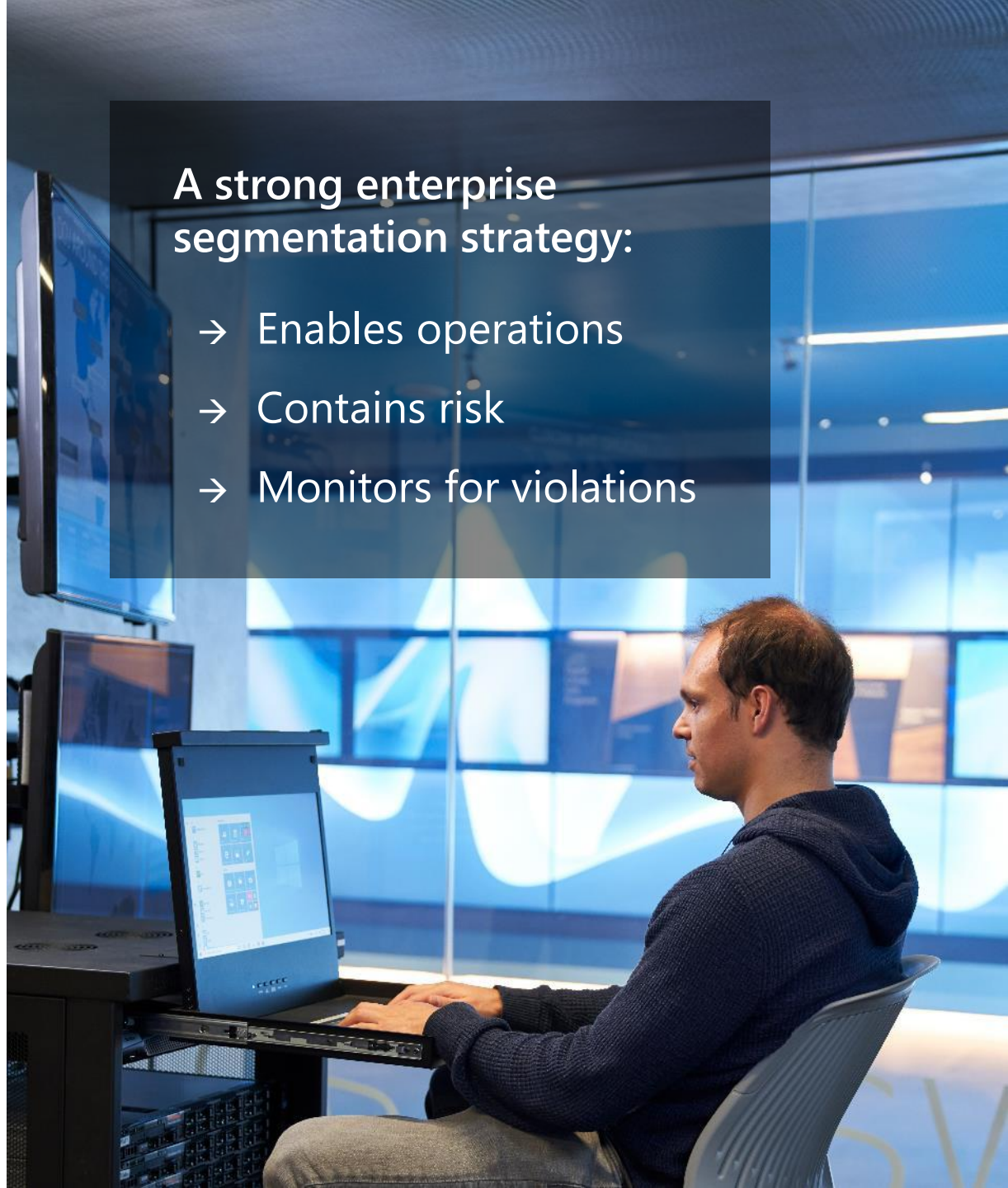
Align segmentation strategy and role-based access control

Rapidly find and fix configuration (and other) vulnerabilities

Use real-time threat monitoring to detect attacks and anomalies

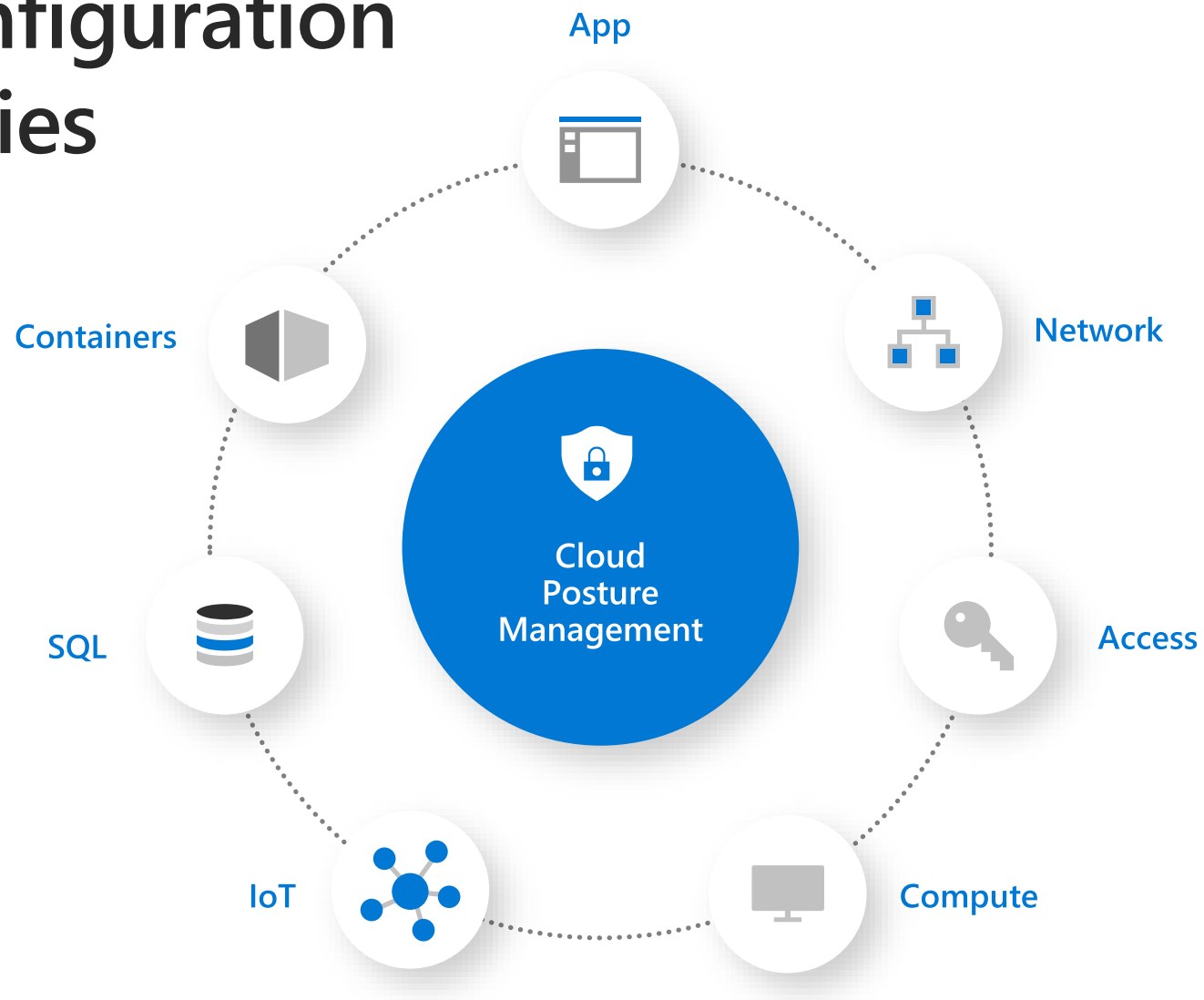
Align segmentation strategy and role-based access control

- Ensure alignment of technical teams to a single enterprise segmentation strategy
- Broadening containment by establishing a modern perimeter based on zero trust principles
- Bolster network controls for legacy applications by exploring micro segmentation strategies



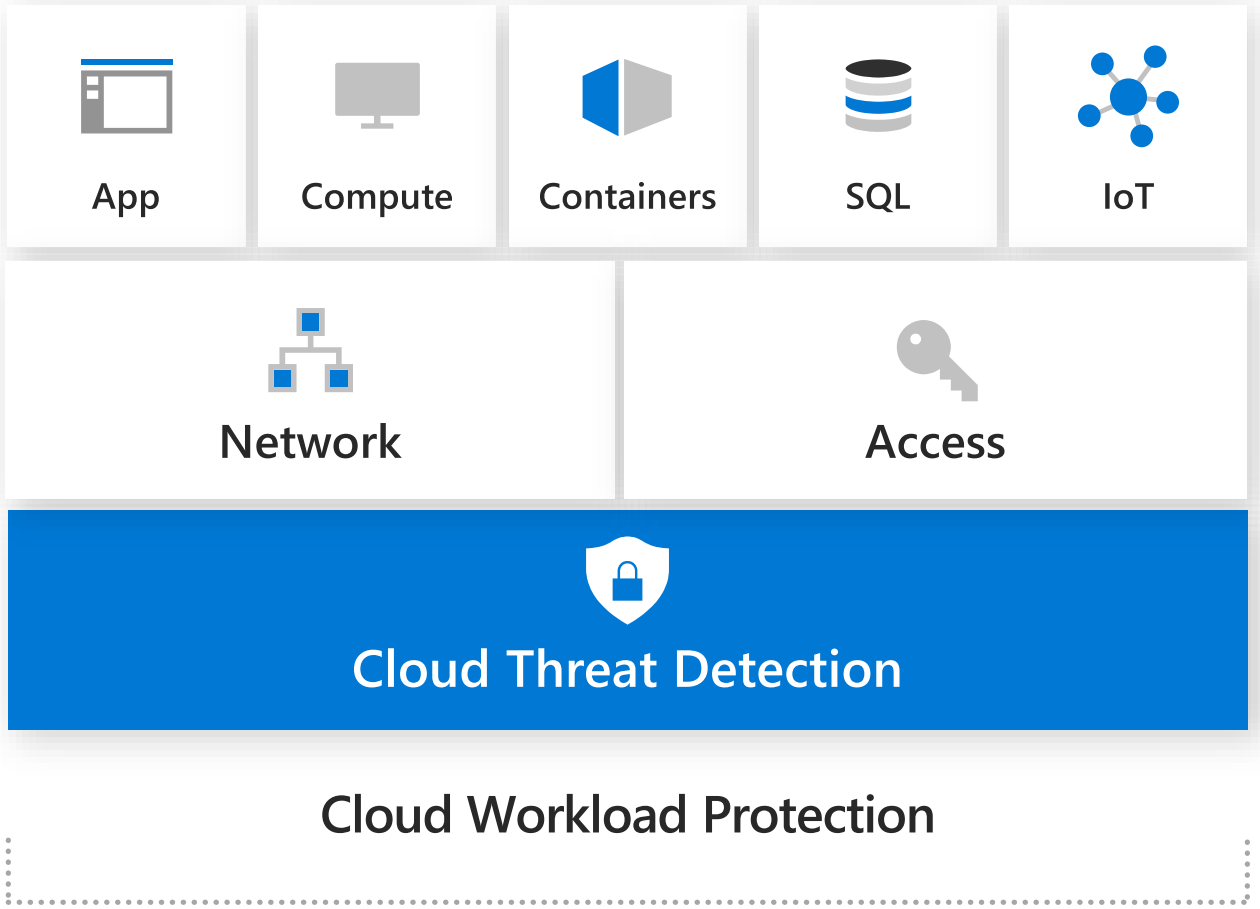
Rapidly find and fix configuration (and other) vulnerabilities

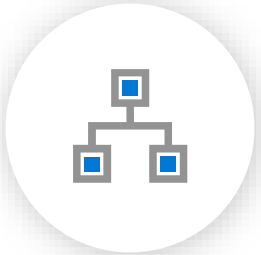
- Get a bird's-eye security posture view
- Continuously monitor and protect all your cross-cloud resources
- Follow best practice recommendations
- Get visibility into the compliance state of your cloud environment



Use real-time threat monitoring to detect attacks and anomalies

- Detect and block advanced malware and threats on any cloud
- Protect cloud-native services from threats
- Protect data services against malicious attacks
- Protect your IoT solution with near real-time monitoring





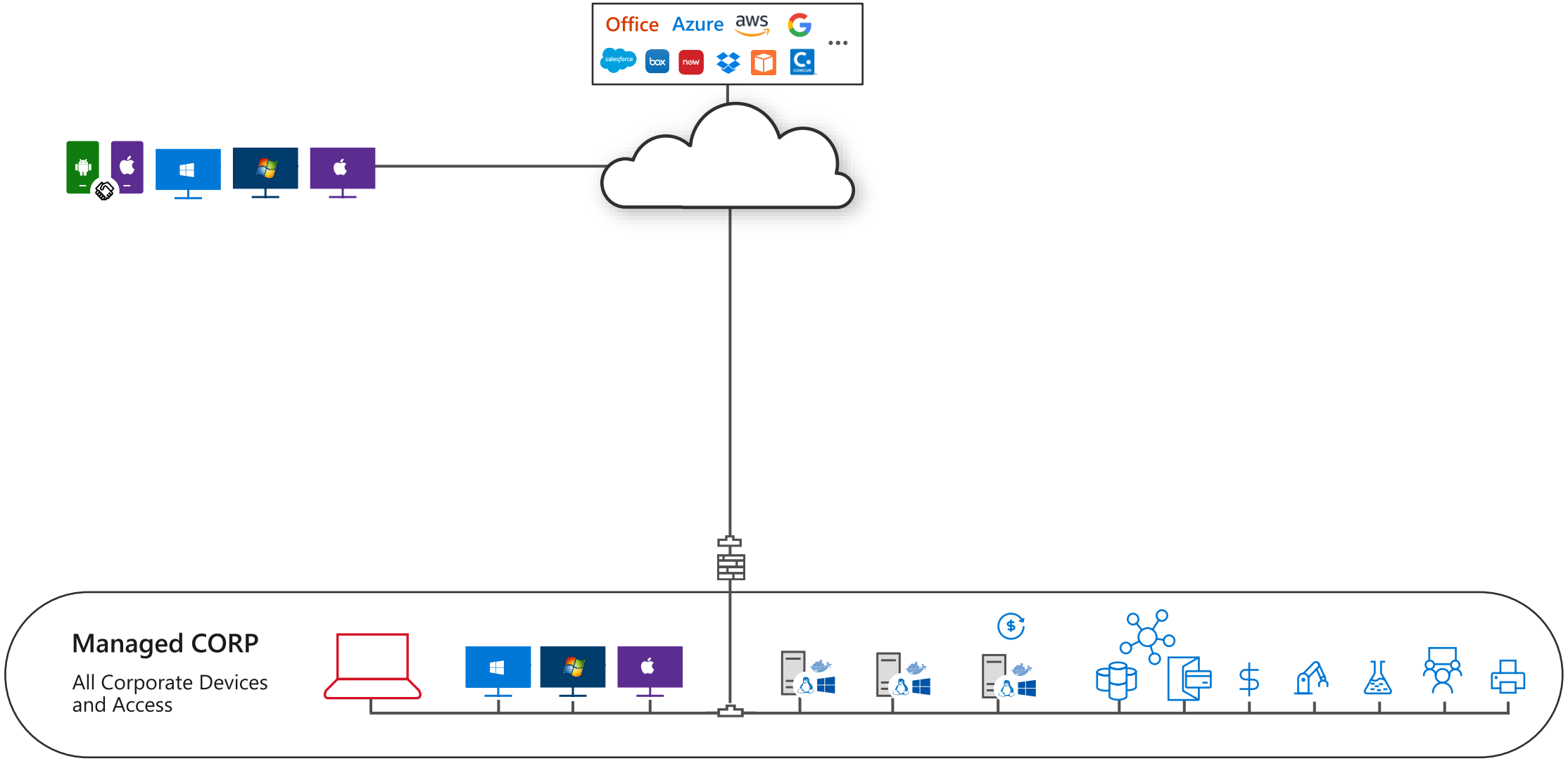
Move beyond traditional network security approaches

Segment networks and implement context-driven access controls

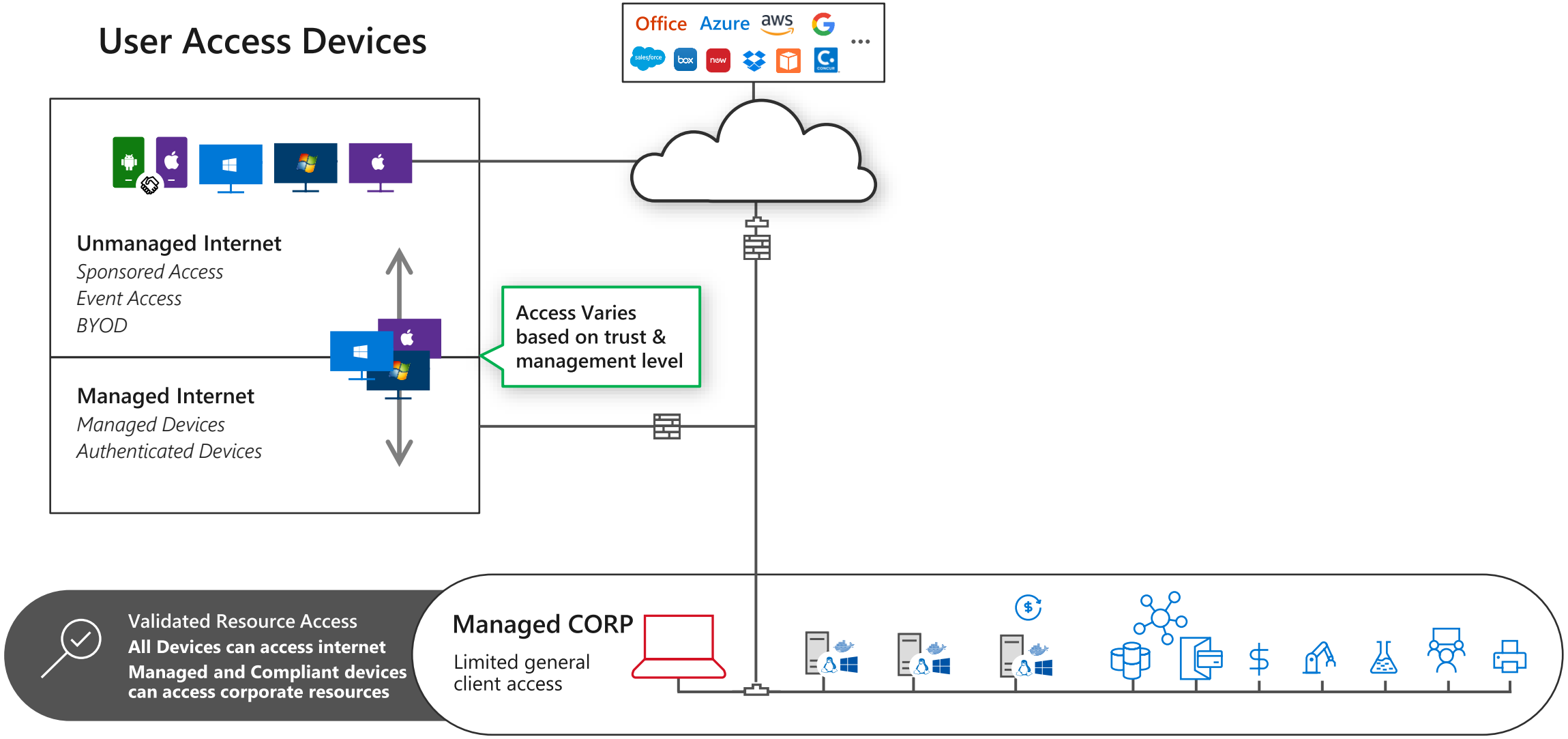
Use real-time threat protection to detect and respond to threats

Protect data with end-to-end encryption

Typical ‘Flat’ Network

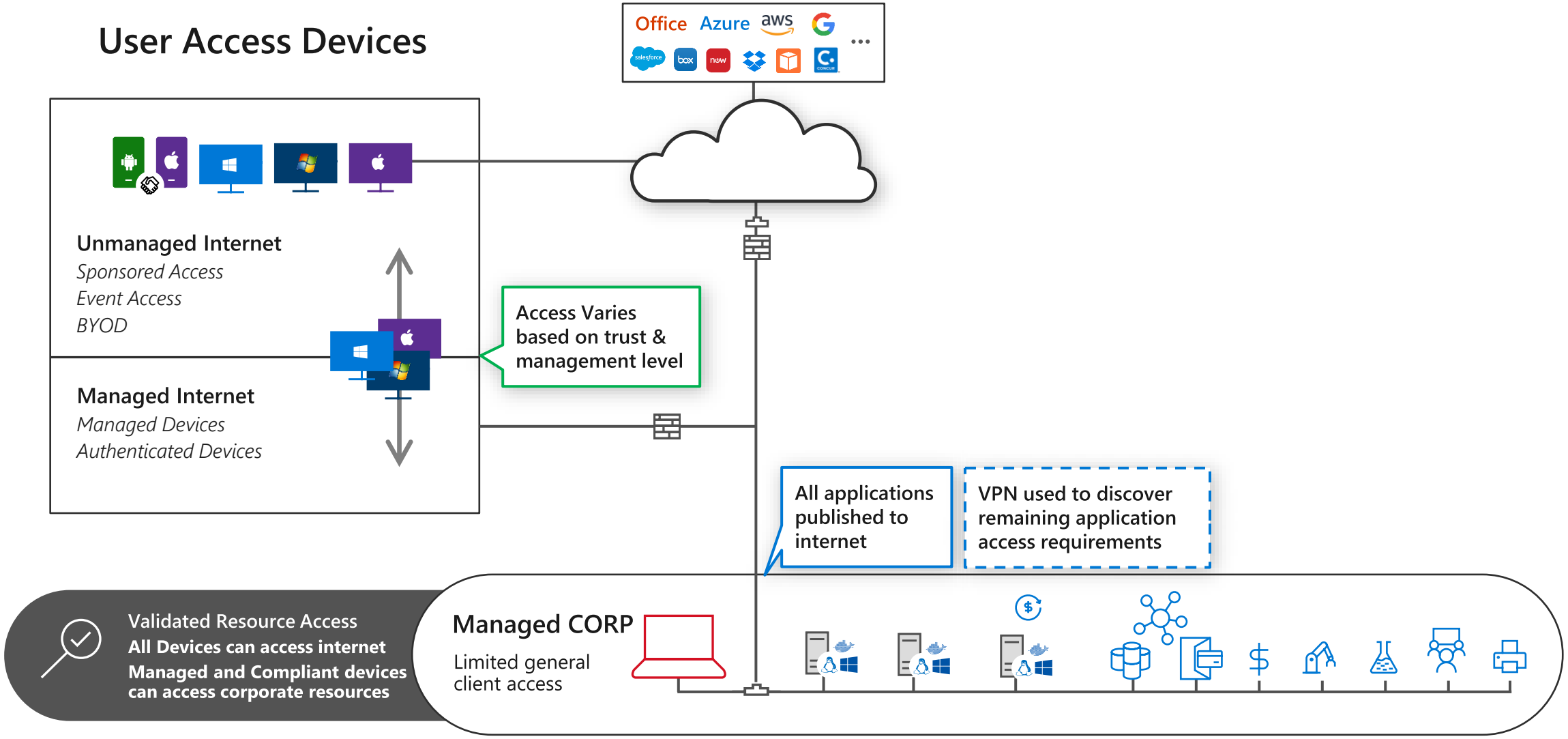


Zero Trust – Client Security Transformation



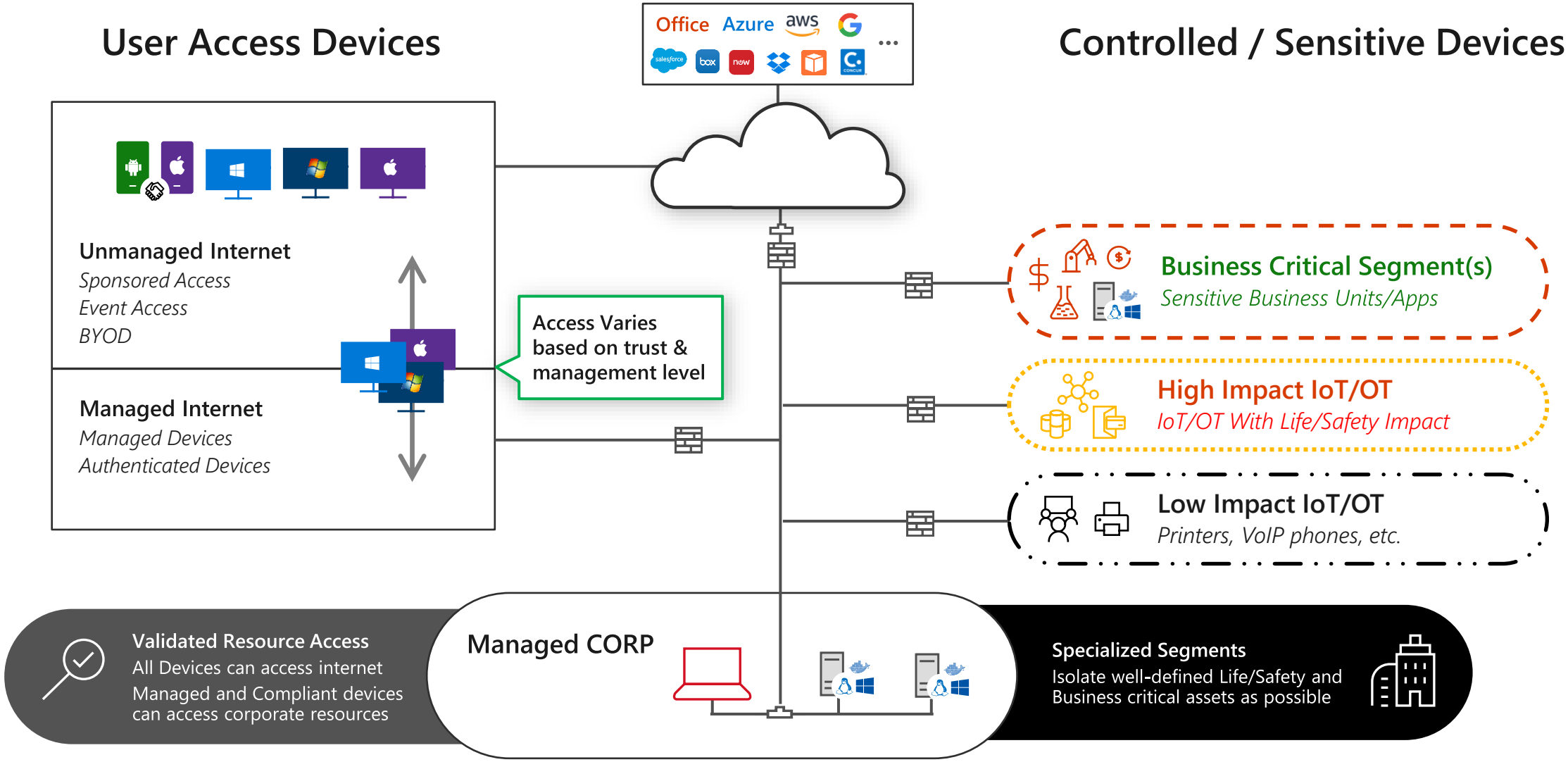
Spans on-premises & PaaS/IaaS environments

Zero Trust – Client Security Transformation



Spans on-premises & PaaS/IaaS environments

Zero Trust – Network Segment Transformation

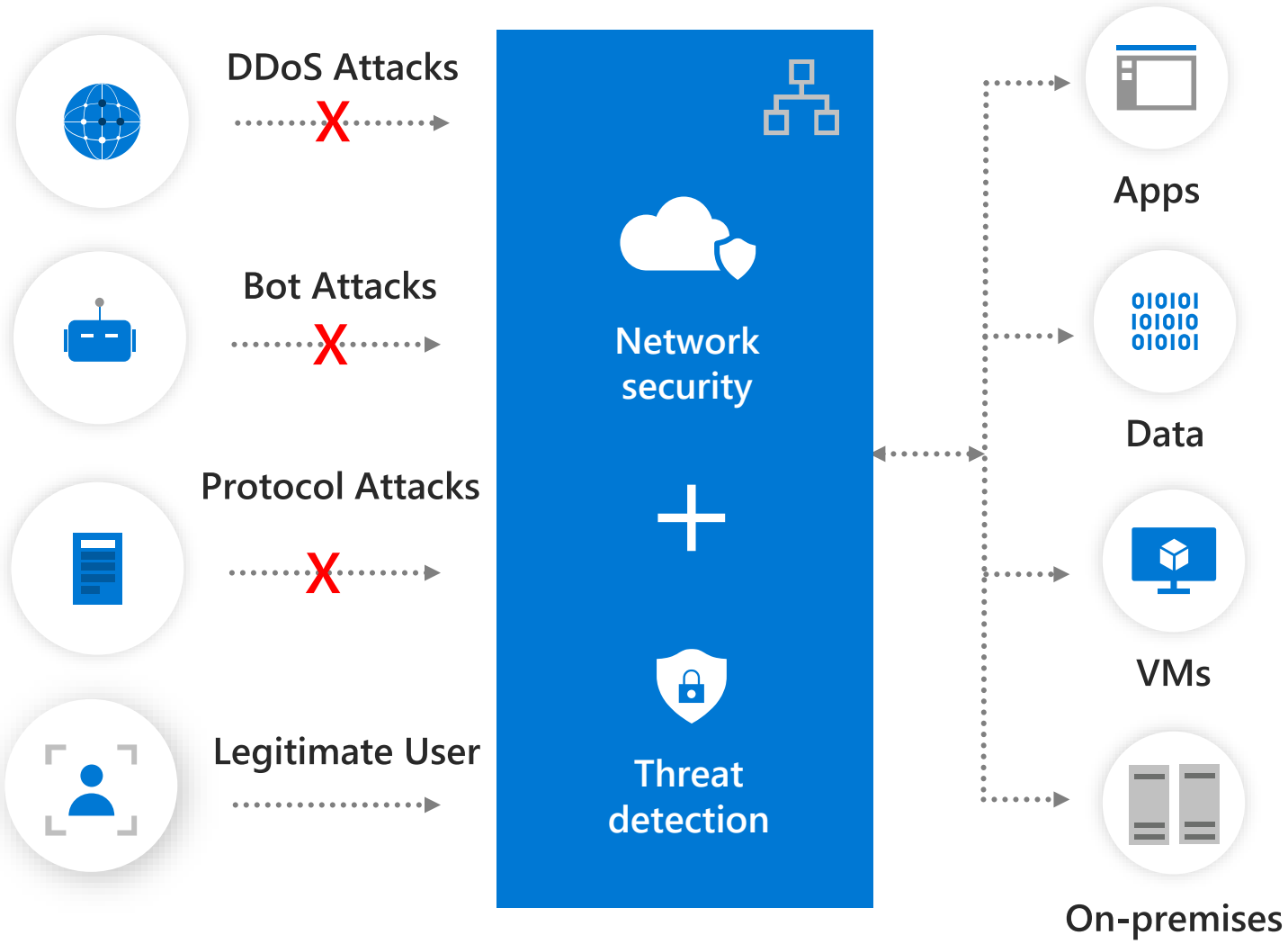


Spans on-premises & PaaS/IaaS environments

Threat protection at the network layer

Detect and respond to cyber threats in real-time

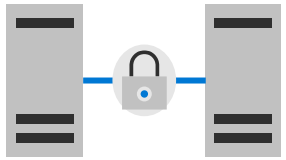
- Real-time network protection powered by threat intelligence
- Safeguard resources from inbound threats and lateral movements
- Select controls that work together and share signal and intelligence across platforms



Encryption built into infrastructure and applications

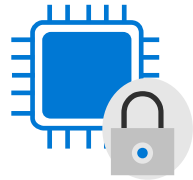
At rest

Encrypt VM disks, storage, and data



In transit

Encrypt data on the wire

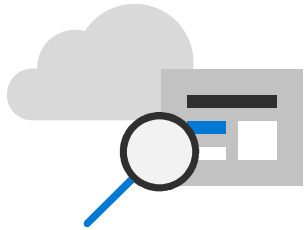


In use

Utilize hardware-based secure enclaves

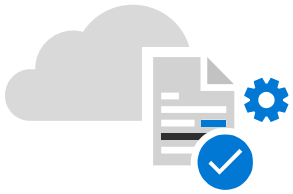
Management of keys, secrets, and certificates backed by hardware security modules

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

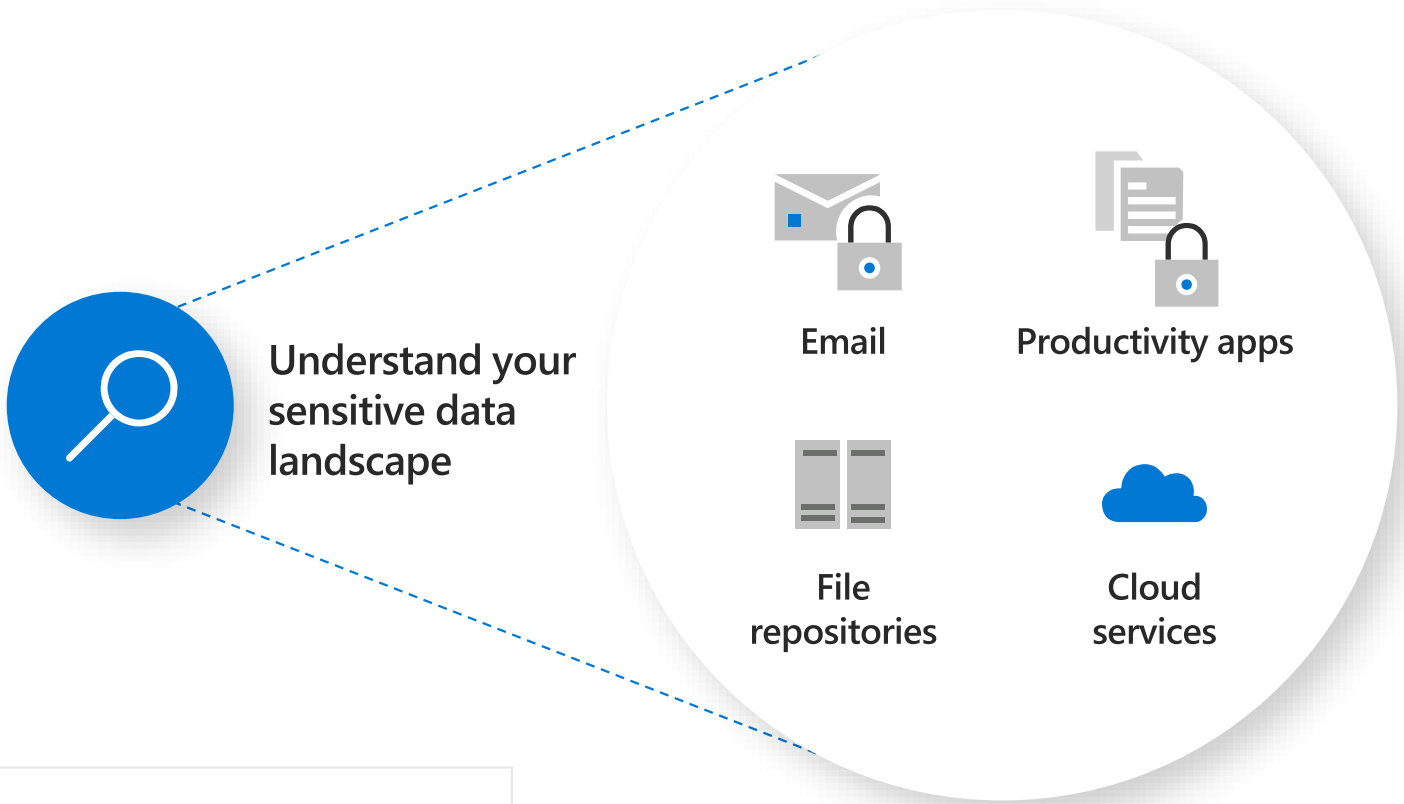


Gain visibility into sensitive data activity, policy violations, and risky sharing

Discover and classify your data

Understand your sensitive data exposure and define your protection policies

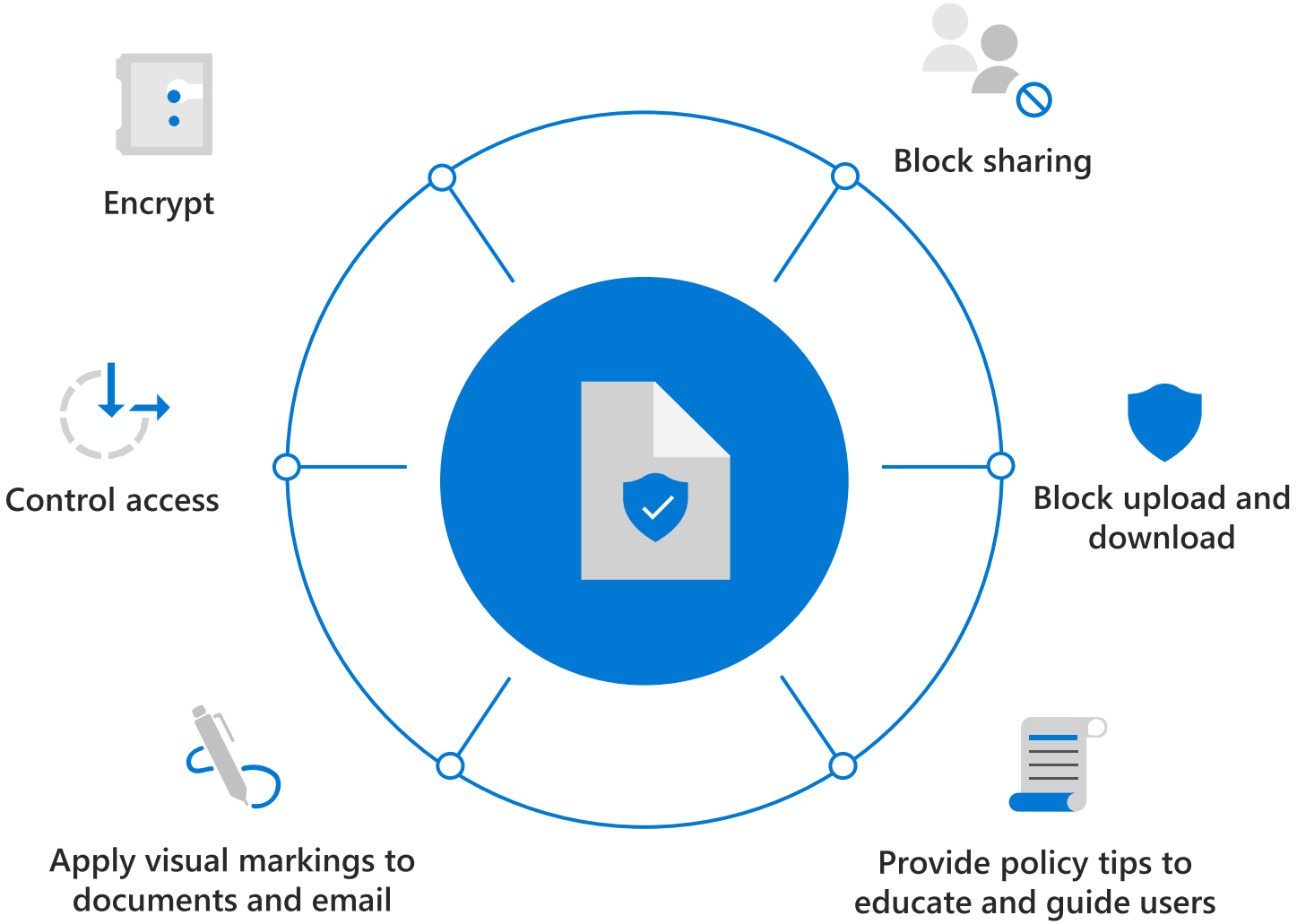
- Define your policies for security and compliance requirements
- Automatically inspect documents and emails across locations
- Detect common data types such as financial, healthcare, PII—or customize your own



163 zettabytes of data per year will be created by 2025

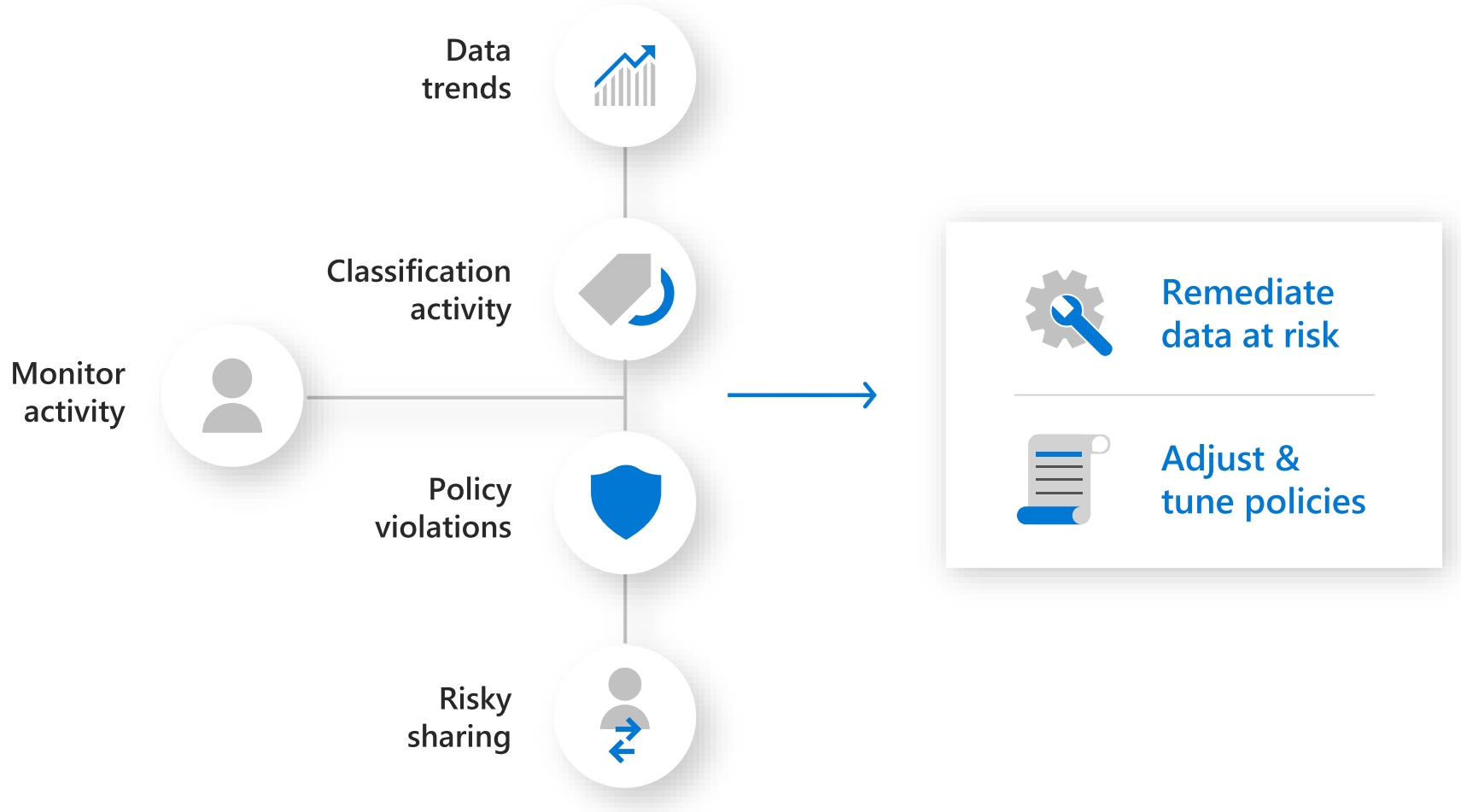
Apply comprehensive protection to data and files

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



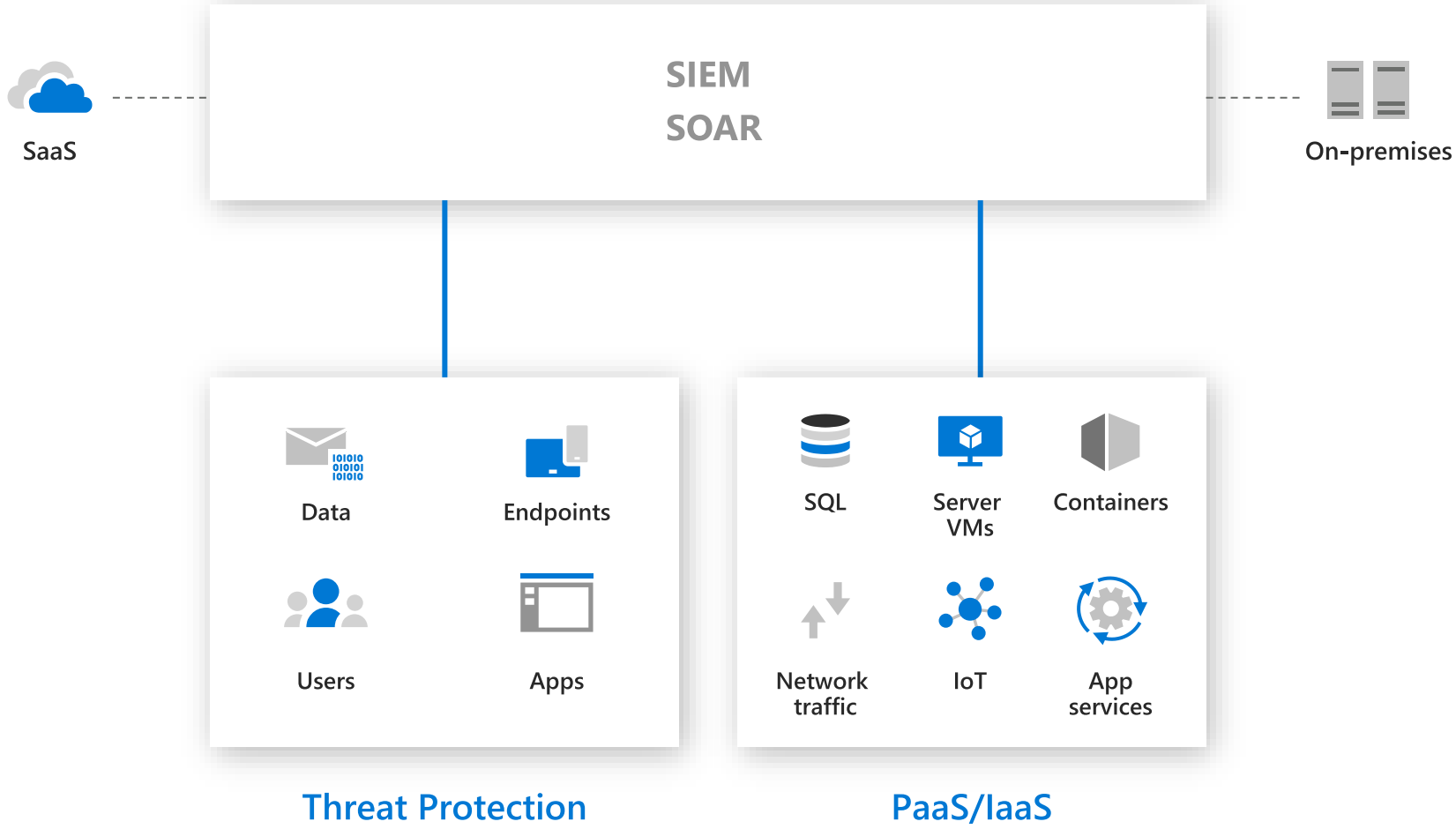
Monitor and remediate

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

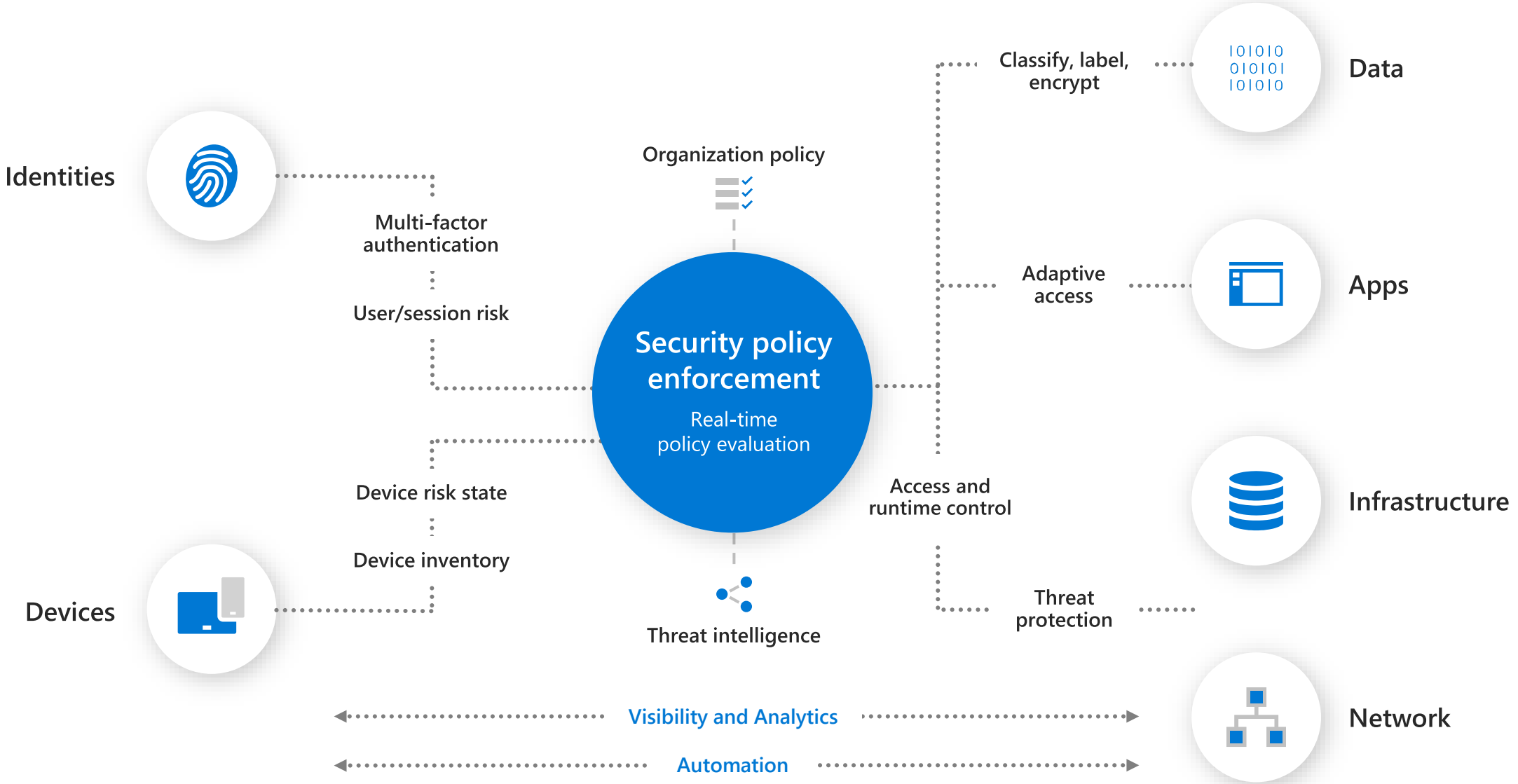


Gain insights across your enterprise

Integrated, end-to-end security



Zero Trust Architecture



Available resources

aka.ms/Zero-Trust

Microsoft

Thank you