Microsoft Security

Build Zero Trust Foundations

Abbas Kudrati

APAC Chief Cybersecurity Advisor

Abbas.Kudrati@Microsoft.Com

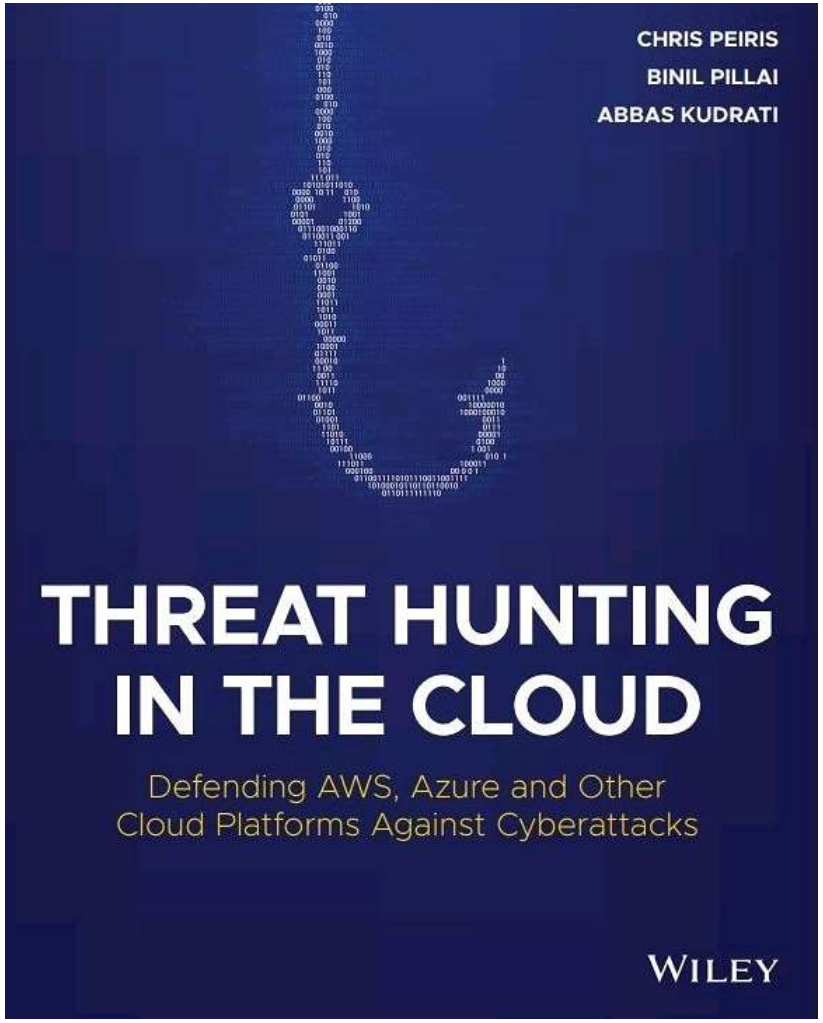
https://aka.ms/abbas

About me

"You join Microsoft, not to be cool
but to make others cool"
Satya Nadella

- **Cybersecurity practitioner and CISO with 25 years of experience in Information / Cybersecurity.**
- **Part time Cybersecurity Professor with Deakin and LaTrobe University in Melbourne, Australia.**
- **Expertise in Zero Trust, Cybersecurity Strategy, Security Operations, Risk, Compliance, Cloud Security and Architecture.**

My publications



Available now on Amazon.com

Under Editing

Zero Trust Journey across the Digital Estate

By

Abbas Kudrati & Binil Pillai

CRC Press
Taylor & Francis Group

Target release by May 2022.

Work in progress

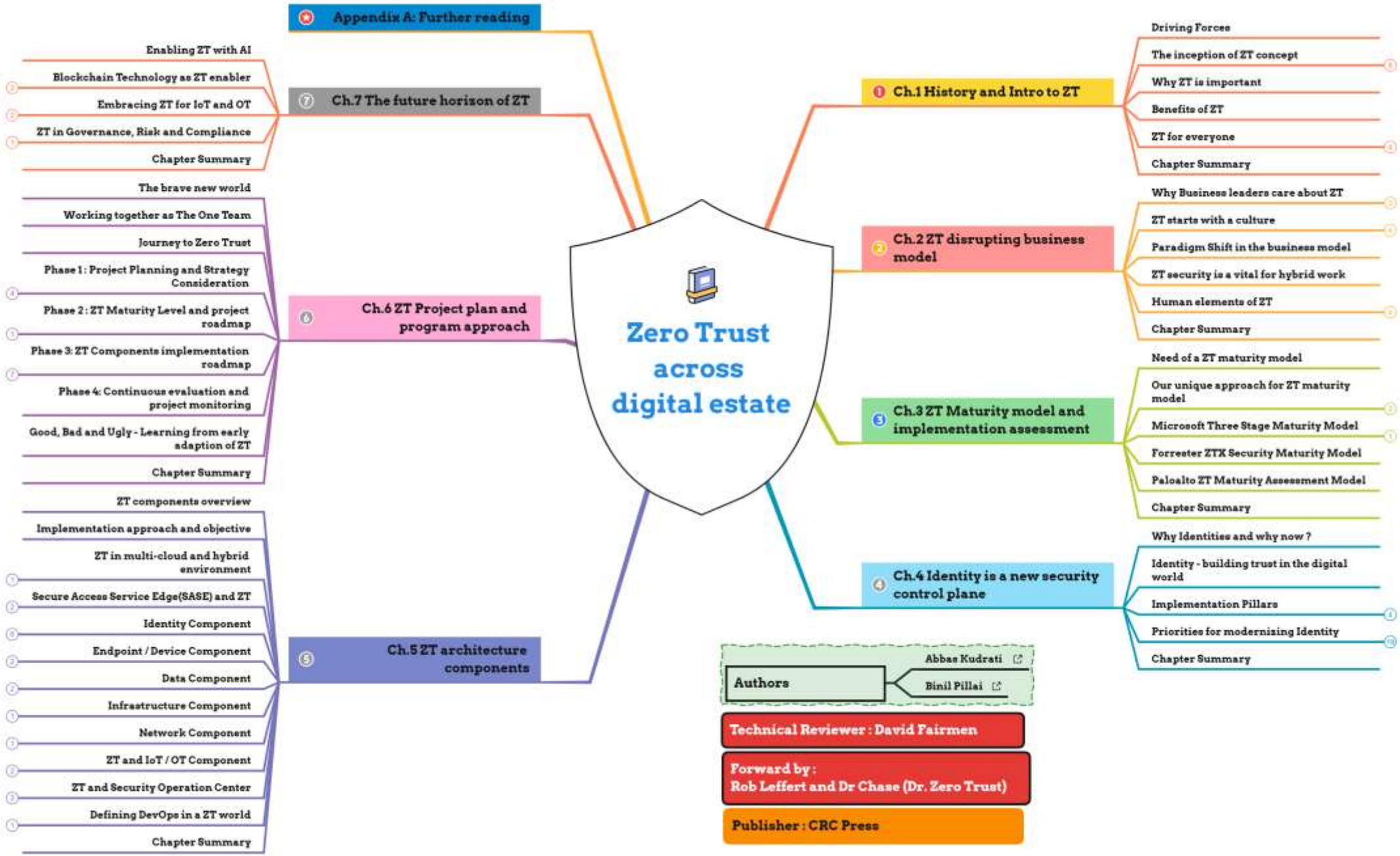
Digitization Risks in Post Pandemic World

By

Ashish Kumar, Abbas Kudrati & Shashank Kumar

Packt

Target release by April 2022.


Zero Trust across digital estate
Appendix A: Further reading
Ch.7 The future horizon of ZT
Enabling ZT with AI
Blockchain Technology as ZT enabler
Embracing ZT for IoT and OT
ZT in Governance, Risk and Compliance
Chapter Summary
Ch.6 ZT Project plan and program approach
The brave new world
Working together as The One Team
Journey to Zero Trust
Phase 1 : Project Planning and Strategy Consideration
Phase 2 : ZT Maturity Level and project roadmap
Phase 3: ZT Components implementation roadmap
Phase 4: Continuous evaluation and project monitoring
Good, Bad and Ugly - Learning from early adaption of ZT
Chapter Summary
Ch.5 ZT architecture components
ZT components overview
Implementation approach and objective
ZT in multi-cloud and hybrid environment
Secure Access Service Edge(SASE) and ZT
Identity Component
Endpoint / Device Component
Data Component
Infrastructure Component
Network Component
ZT and IoT / OT Component
ZT and Security Operation Center
Defining DevOps in a ZT world
Chapter Summary
Ch.1 History and Intro to ZT
Driving Forces
The inception of ZT concept
Why ZT is important
Benefits of ZT
ZT for everyone
Chapter Summary
Ch.2 ZT disrupting business model
Why Business leaders care about ZT
ZT starts with a culture
Paradigm Shift in the business model
ZT security is a vital for hybrid work
Human elements of ZT
Chapter Summary
Ch.3 ZT Maturity model and implementation assessment
Need of a ZT maturity model
Our unique approach for ZT maturity model
Microsoft Three Stage Maturity Model
Forrester ZTX Security Maturity Model
Paloalto ZT Maturity Assessment Model
Chapter Summary
Ch.4 Identity is a new security control plane
Why Identities and why now ?
Identity - building trust in the digital world
Implementation Pillars
Priorities for modernizing Identity
Chapter Summary
Authors
Abbas Kudrati
Binil Pillai
Technical Reviewer : David Fairmen
Forward by :
Rob Leffert and Dr Chase (Dr. Zero Trust)
Publisher : CRC Press

Today's reality | Distributed and hybrid

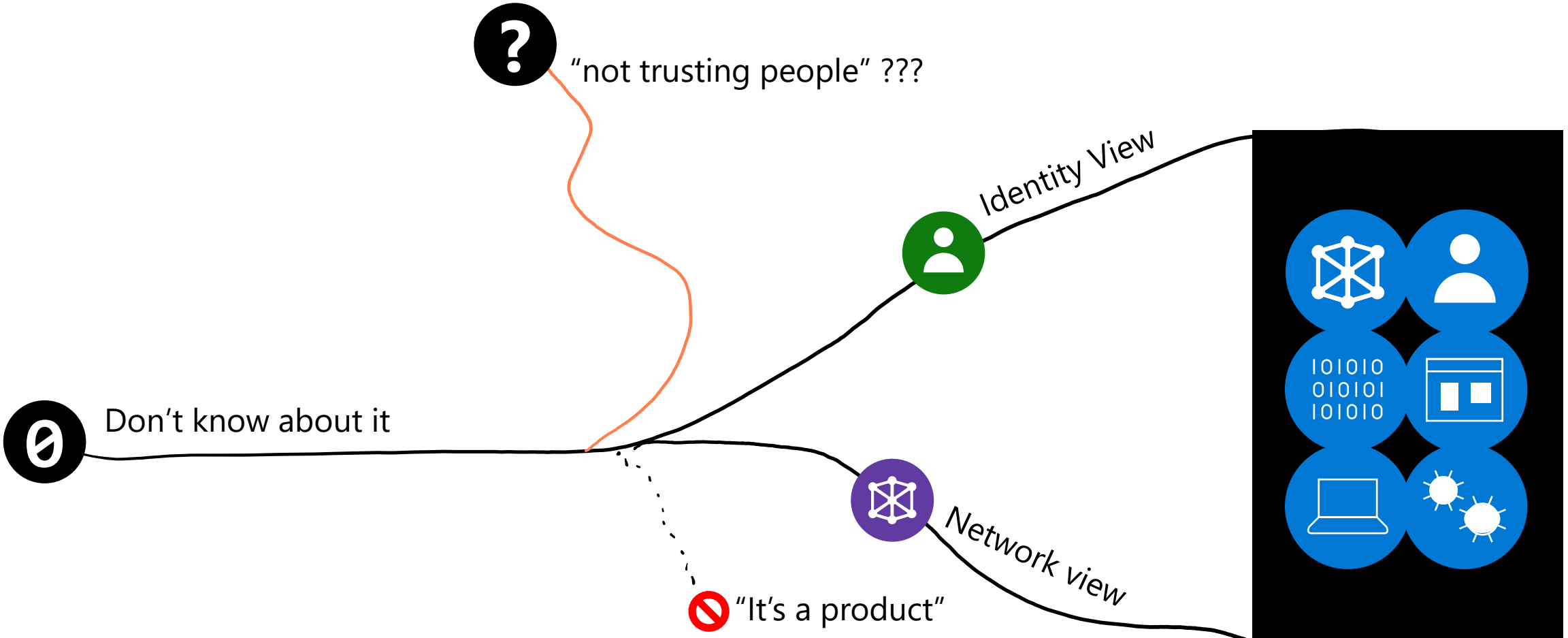
Where we work
has continued to rapidly evolve to a mix of locations.

The tools we use
are varied, from corporate to BYOD, cloud-based, or on-prem apps.

How we do our work
is an evolving mix of virtual, physical, collaborative, and data-driven styles.

Evolving risks
Increasing volume and sophistication of threats, and a wider, more distributed attack surface.

Where are customers at on zero trust journey?



Zero Trust Adaption report 2020 /21

EXHIBIT 3. HYBRID WORKPLACE INTENT

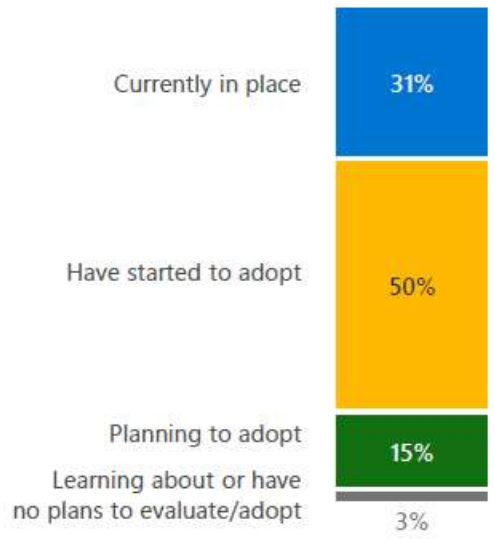


EXHIBIT 4. HYBRID WORKPLACE CONCERNS

Employees downloading unsafe apps	37%
An increase to IT workload	37%
Ransomware attacks	36%
Phishing attacks	35%
Improper use of personal devices	34%
Unauthorized access to data	31%
Inability to manage all devices	30%
Use of personal email accounts	30%
Non-compliance with data regulations	24%

EXHIBIT 1. ZERO TRUST IS CRITICAL

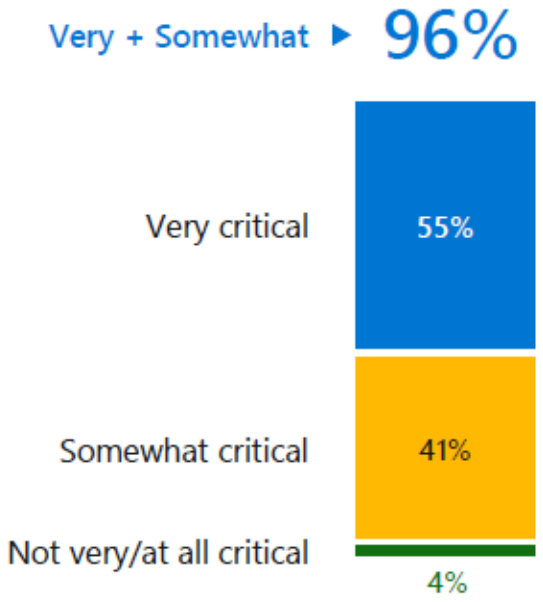


EXHIBIT 2. ZERO TRUST MOTIVATORS

Top Motivators	
Improve overall security posture	47%
Improve end user experience and productivity	44%
Transform the way security teams work together	38%
Simplify security stack	35%
Reduce security costs	35%

	US (2020)	US	DE	JP	AUS/NZ
Zero Trust implementation	70%	79%	75%	76%	71%
• Fully implemented	27%	44%	19%	32%	28%
• In progress	43%	35%	56%	44%	43%

35% Fully implemented

42% Implementation in progress

EXHIBIT 7. ZERO TRUST COMPONENT IMPLEMENTATION (TOP 3) – RANKED #1 (IMPLEMENTED FIRST)

Identities	
Strong authentication (i.e., multi-factor authentication, passwordless authentication)	32%
Automated risk detection and remediation	27%
Adaptive access policies to gate access to resources	22%

Endpoints	
Data Loss Prevention policies/controls for all unmanaged and managed devices	27%
Real-time device risk evaluation / endpoint threat detection	26%
Devices are registered with identity provider	24%

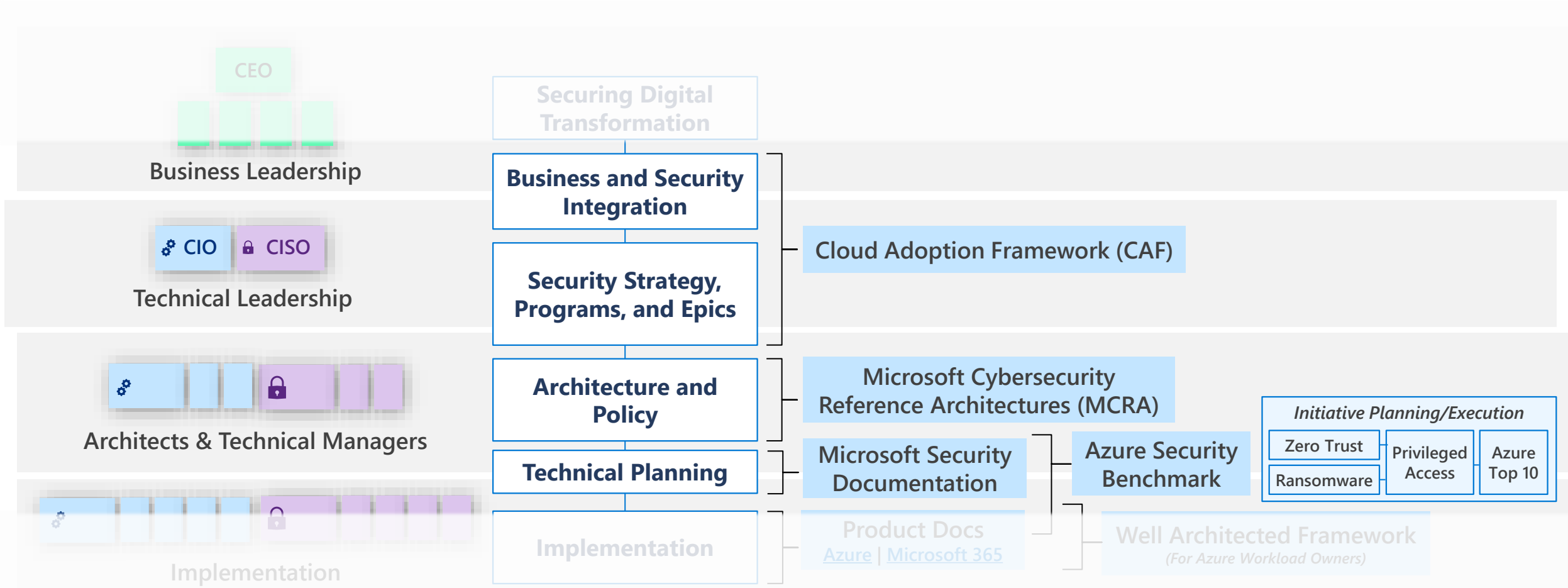
Apps	
Ongoing Shadow IT Discovery and risk assessment	23%
Granular access control to your apps (such as limited visibility or read only)	22%
Policy-based access control for apps	20%

Network	
Secure access controls to protect networks	25%
Threat protection and filtering with context-based signals	24%
All traffic is encrypted	20%

Security Guidance

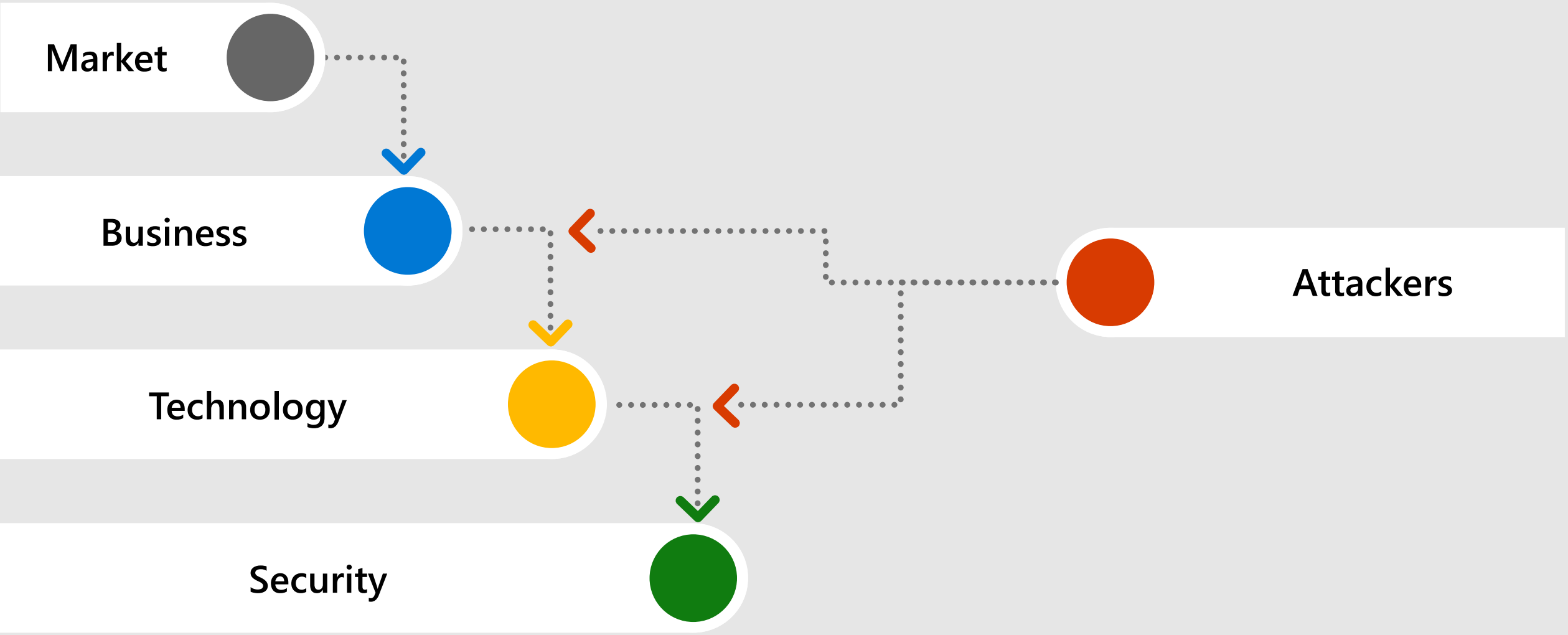
May 2021 - https://aka.ms/MCRA

Microsoft

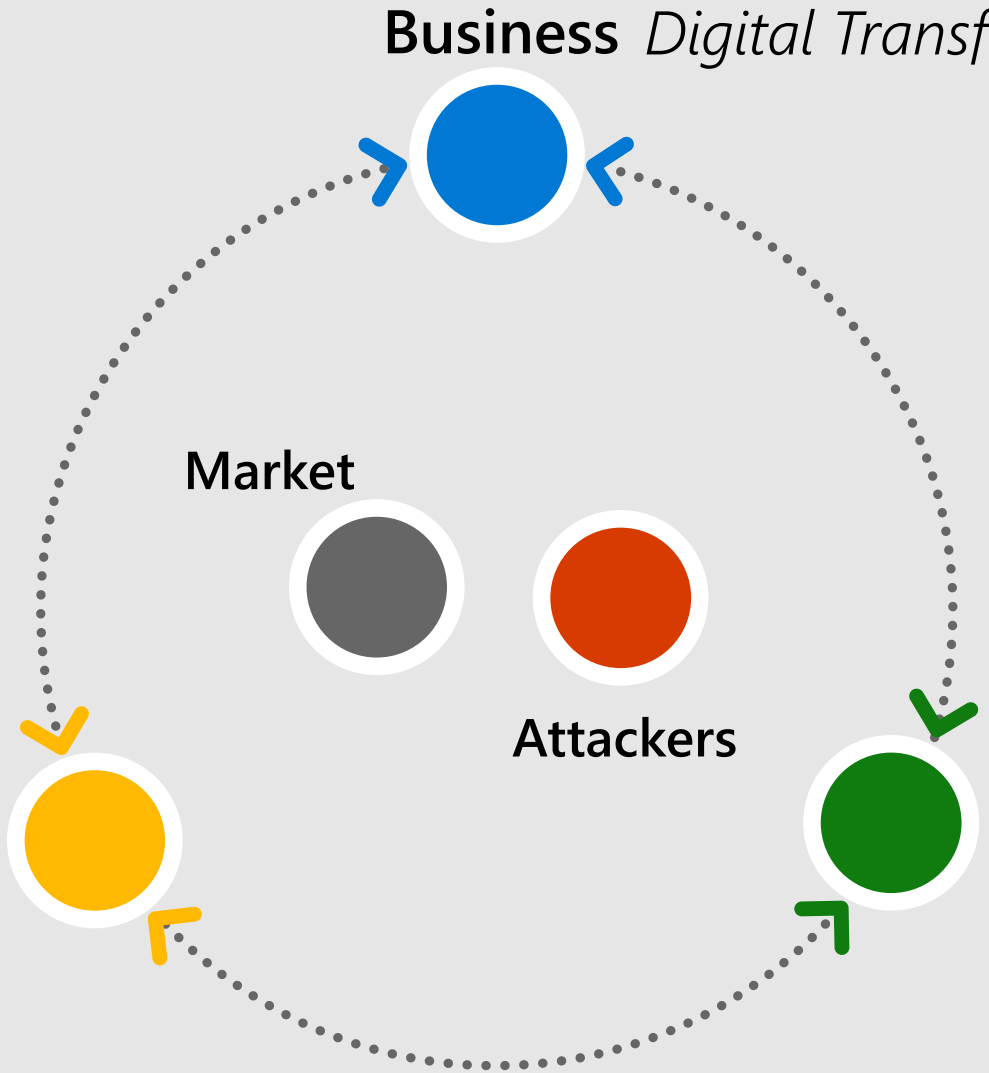


Introduction - Why Zero Trust is Important

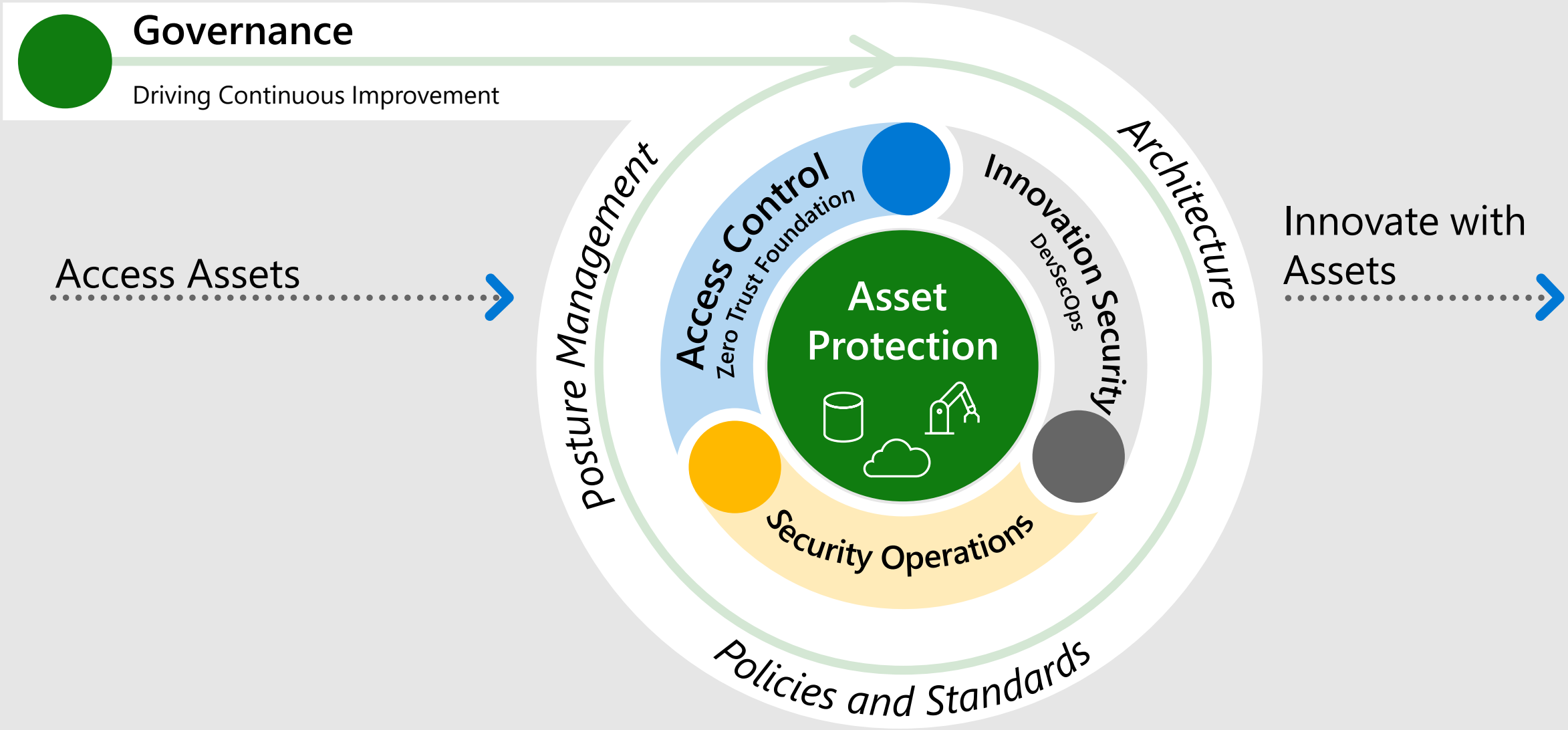
The world is transforming rapidly

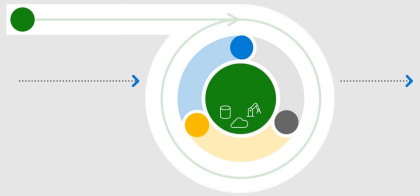


Working together



Security Shifts to Continuous Improvement





Build Modern Security

Common Modernization Initiatives

Ransomware Recovery Readiness

Ensure backups are validated, secure, and immutable to enable rapid recovery

- Zero Trust Foundations
- Modern Security Operations
- Infrastructure and Development
- OT and IoT Security
- Data, Compliance, and Governance

Examine principles and components of Zero Trust

Principles of Zero Trust

Instead of assuming everything behind the corporate firewall is safe, Zero Trust assumes *an open environment where trust must be validated*.

- **Assume breach** – Assume that attackers will succeed (partially or fully) and design accordingly
- **Verify explicitly** – Validate trust of users, devices, applications, and more using data/telemetry
- **Use least privileged access** – to limit the impact of any given compromise

Microsoft is actively working with NIST, The Open Group, CISA, and many others across industry to harmonize definitions, model, and architectures for Zero Trust

NSA Zero Trust Guidance

CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF (defense.gov)

Zero Trust is a security model, a set of system design principles, and a coordinated cybersecurity and system management strategy based on an acknowledgement that threats exist both inside and outside traditional network boundaries.

Principles align closely with Microsoft's

Embrace Zero Trust guiding principles

A Zero Trust solution requires operational capabilities that:

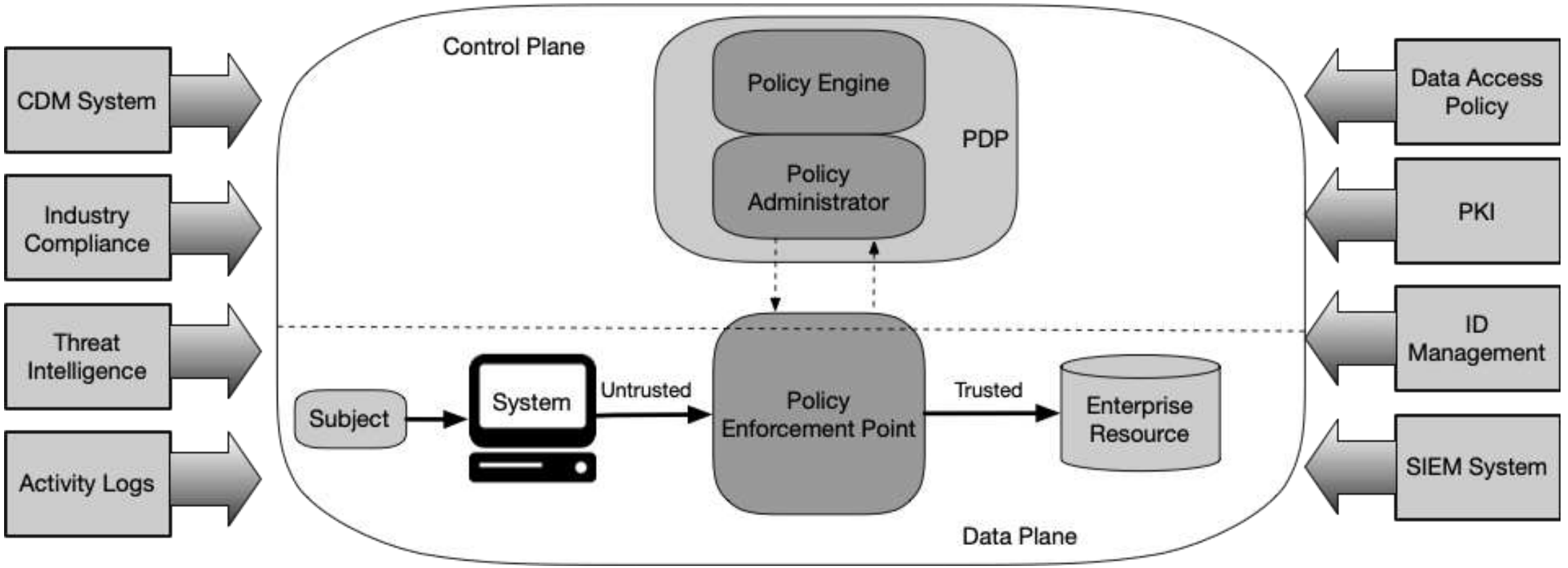
- **Never trust, always verify** – Treat every user, device, application/workload, and data flow as untrusted. Authenticate and explicitly authorize each to the least privilege required using dynamic security policies.
- **Assume breach** – Consciously operate and defend resources with the assumption that an adversary already has presence within the environment. Deny by default and heavily scrutinize all users, devices, data flows, and requests for access. Log, inspect, and continuously monitor all configuration changes, resource accesses, and network traffic for suspicious activity.
- **Verify explicitly** – Access to all resources should be conducted in a consistent and secure manner using multiple attributes (dynamic and static) to derive confidence levels for contextual access decisions to resources.

Leverage Zero Trust design concepts

When designing a Zero Trust solution:

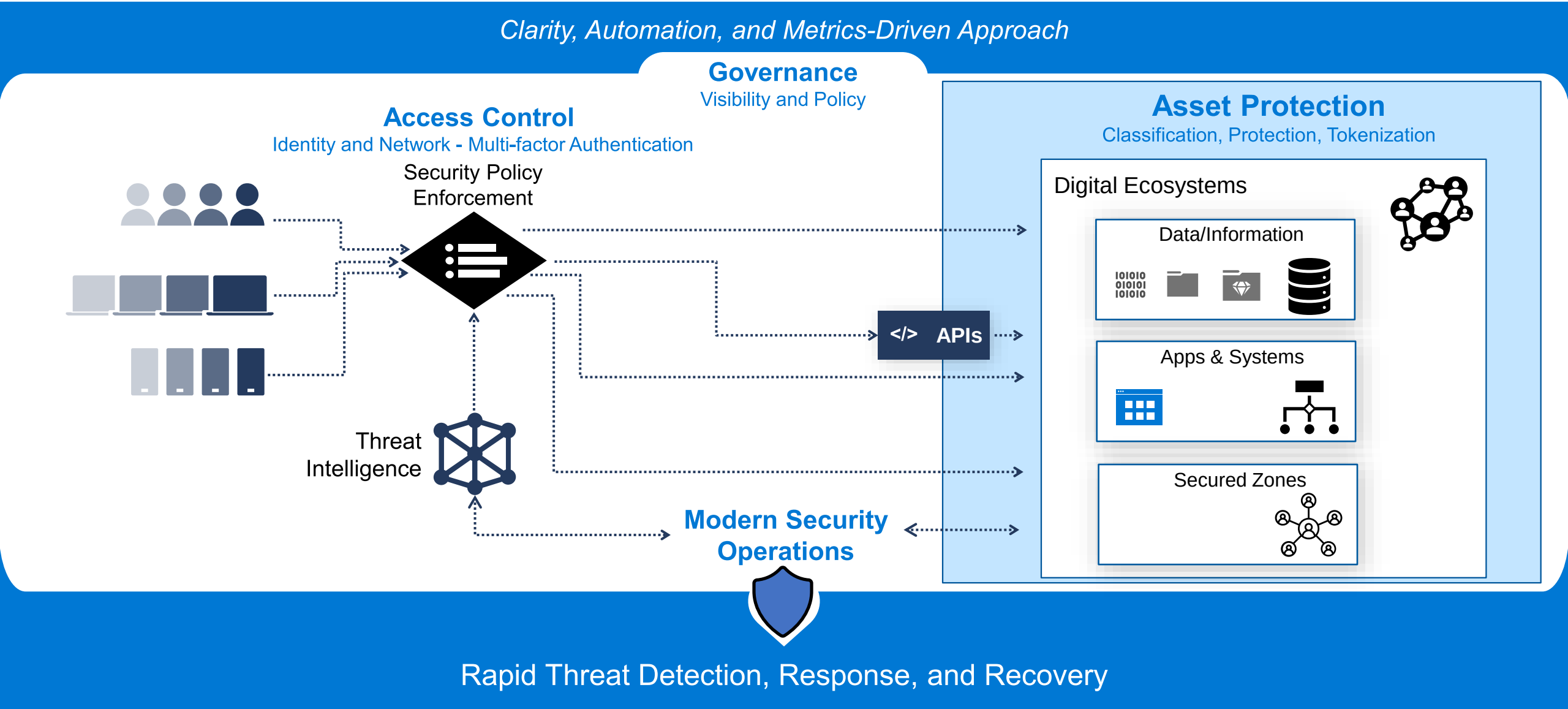
- **Define mission outcomes** – Derive the Zero Trust architecture from organization-specific mission requirements that identify the critical Data/Assets/Applications/Services (DAAS).
- **Architect from the inside out** – First, focus on protecting critical DAAS. Second, secure all paths to access them.
- **Determine who/what needs access to the DAAS to create access control policies** – Create security policies and apply them consistently across all environments (LAN, WAN, endpoint, perimeter, mobile, etc.).
- **Inspect and log all traffic before acting** – Establish full visibility of all activity across all layers from endpoints and the network to enable analytics that can detect suspicious activity.

NIST Zero Trust Architecture



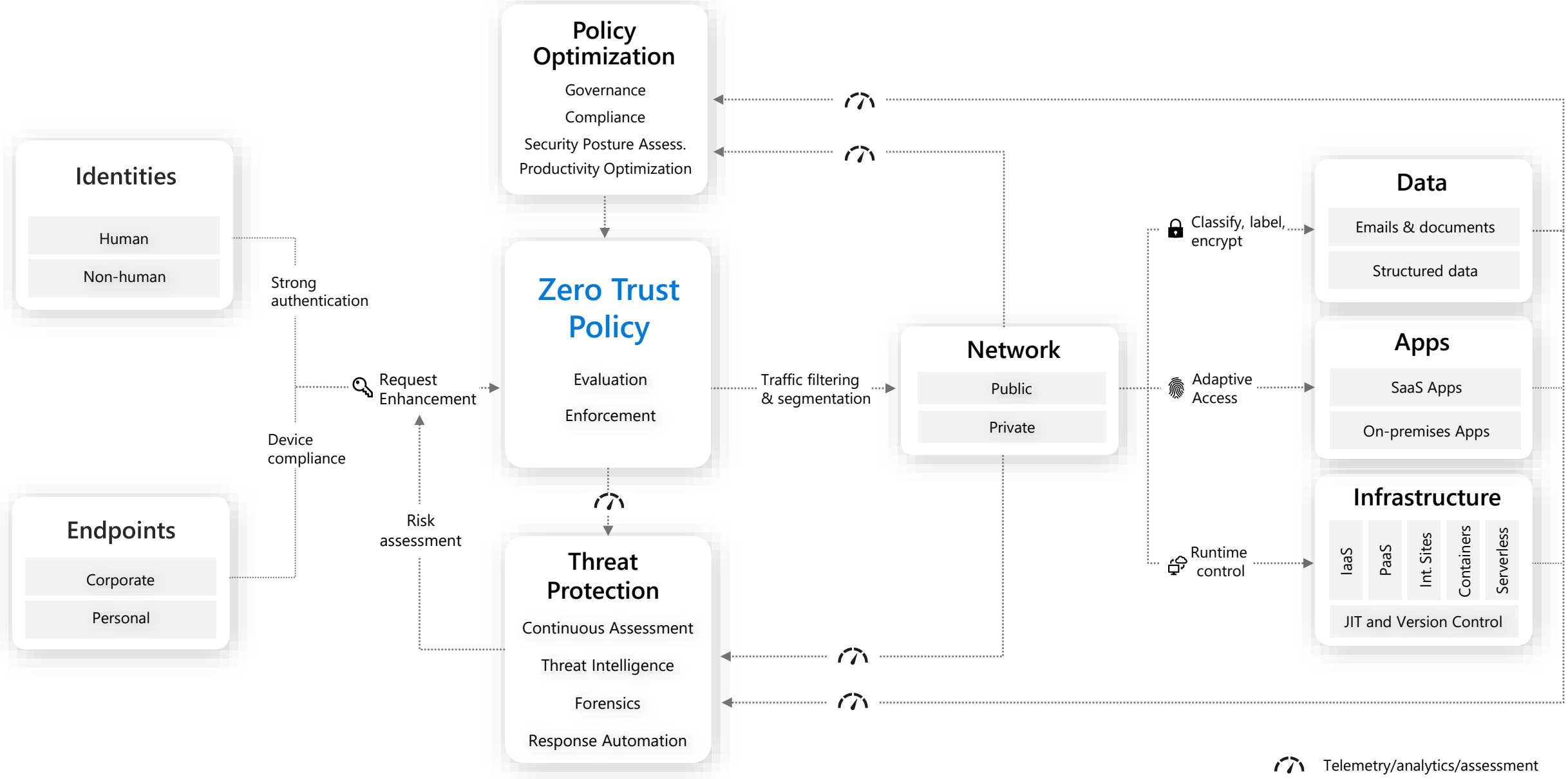
Zero Trust Components

Enable flexible business workflows for the digitized world



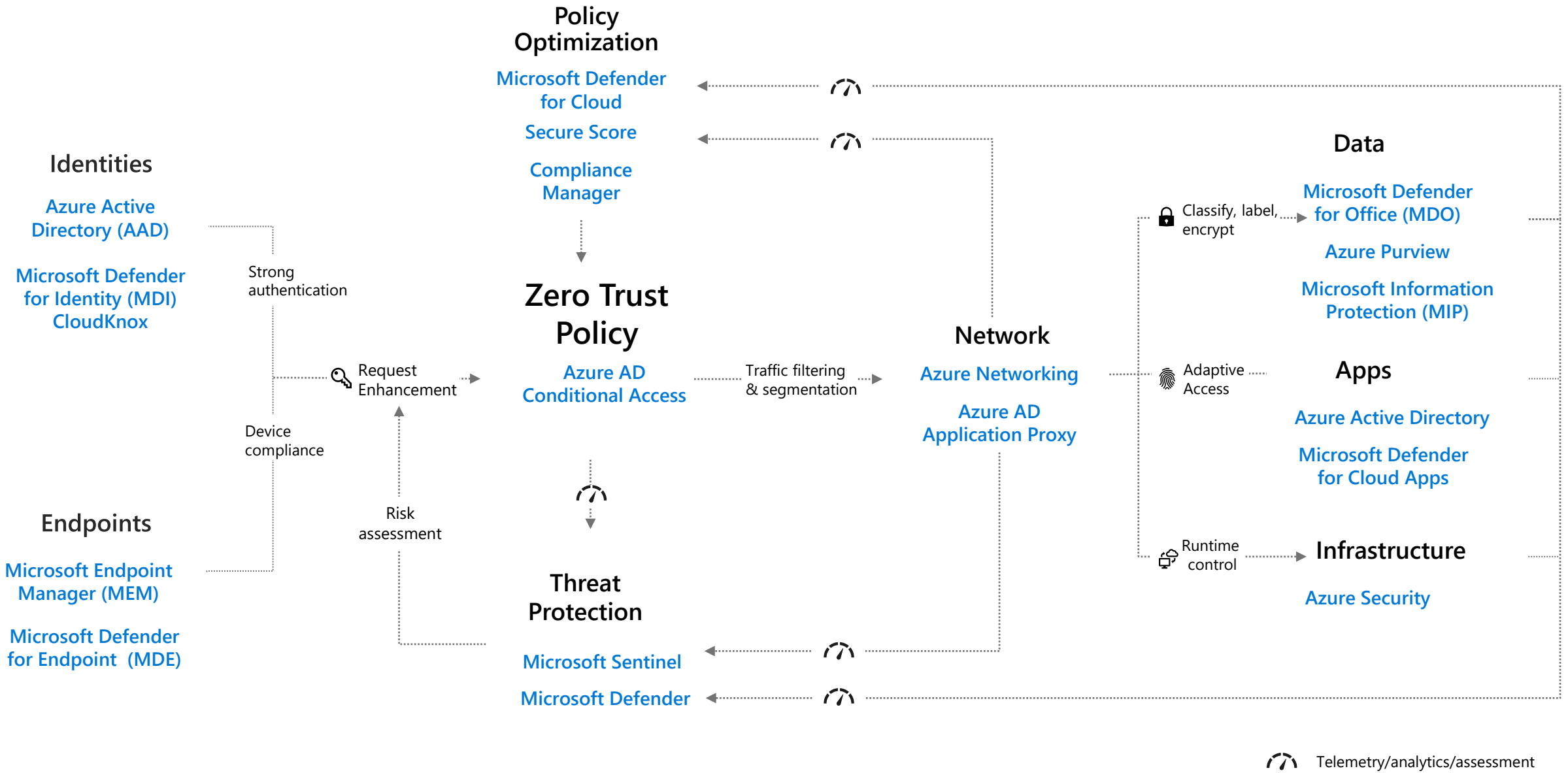
Zero Trust architecture

Microsoft Security



Microsoft Zero Trust architecture

Microsoft Security



Secure Access Service Edge (SASE)

SASE is a cloud-based architecture that converges network and security services into a cloud-delivered service model.

The SASE architecture is enabled through a set of capabilities/products while adhering to the Zero Trust principles.

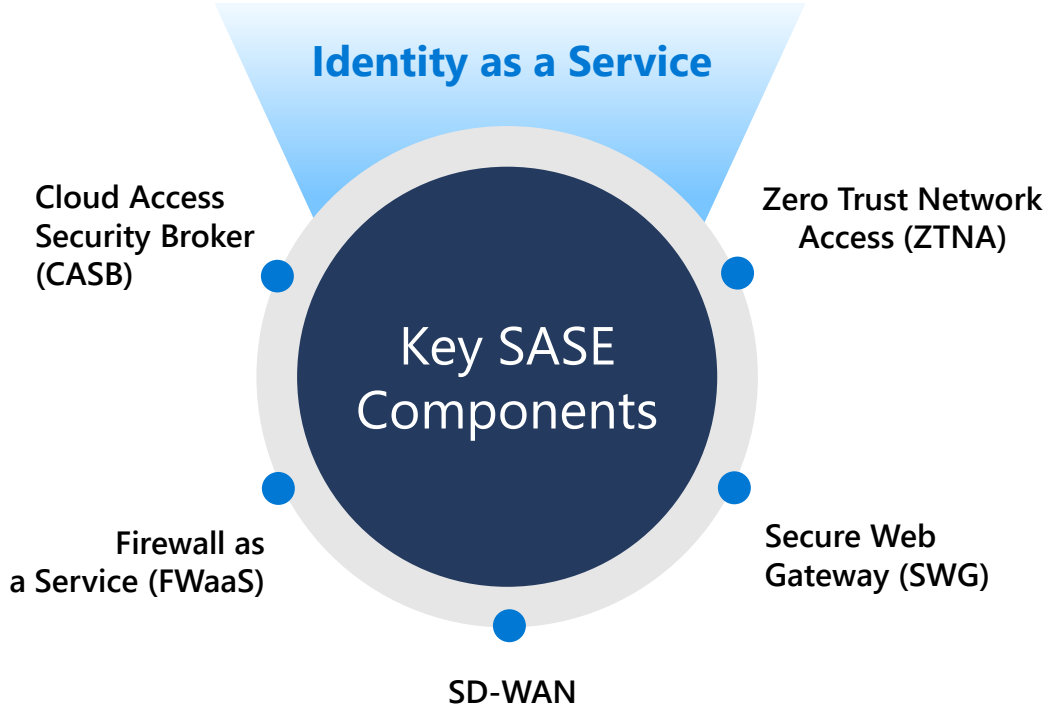
SASE capabilities are evolving in the market. Start on the SASE journey with Microsoft and partner solutions to achieve your business goals.

Secure Access Service Edge (SASE) uses Zero Trust Principles

Verify explicitly

Use least privilege access

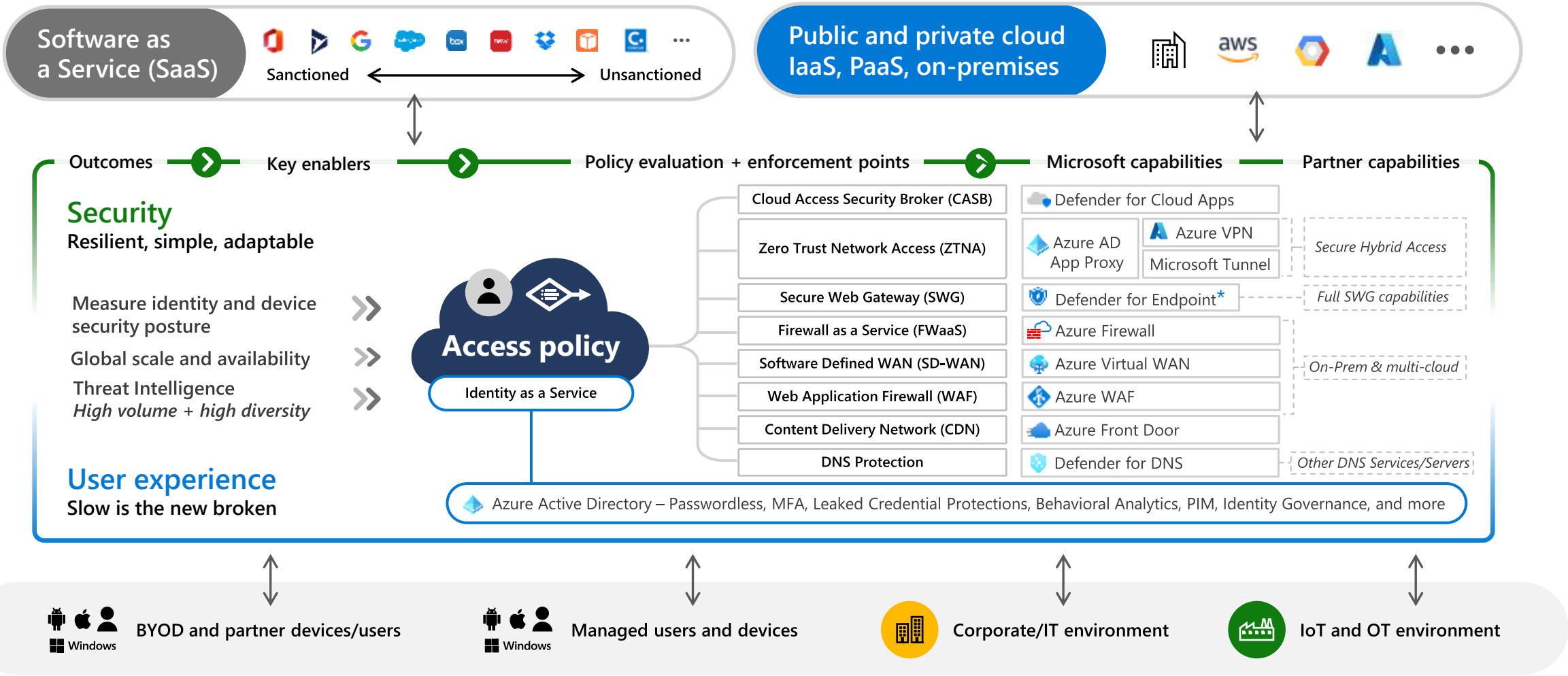
Assume breach



Secure access to resources based on identity, real-time context and security/compliance policies

Microsoft and partner solutions for SASE

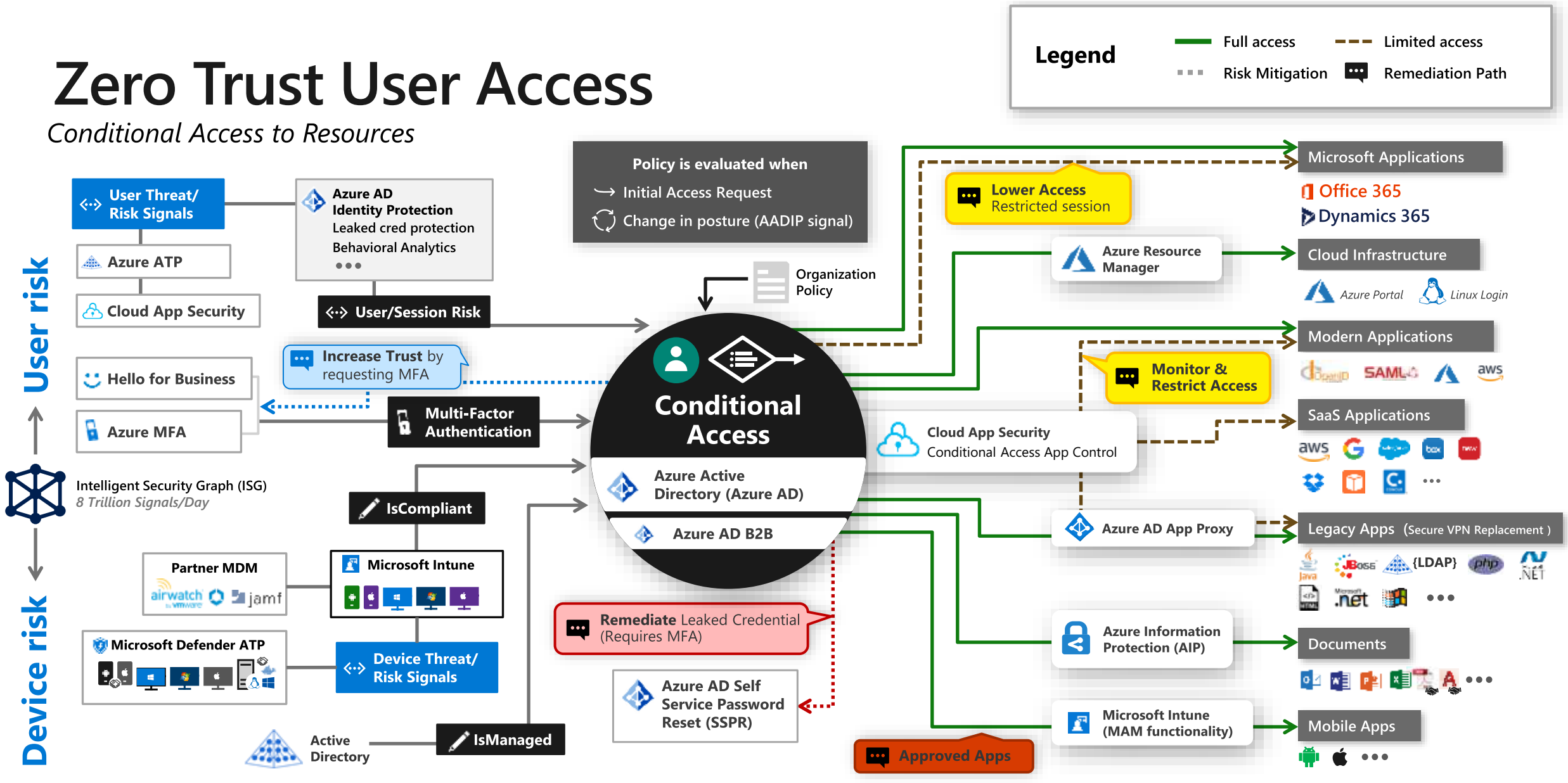
Architecture for secure, responsive, and pervasive productivity



*Microsoft Defender for Endpoint (MDE) addresses many of the use-cases of an internet gateway solution and works with MISA partners to provide full SWG capabilities

Zero Trust User Access

Conditional Access to Resources



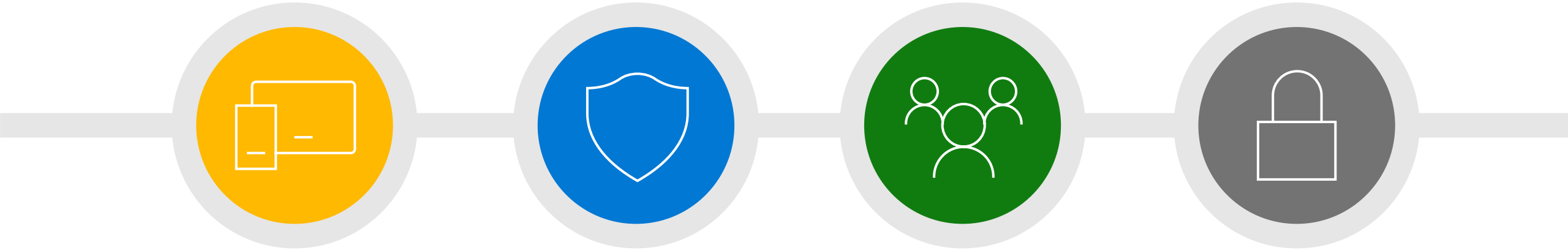
Signal
to make an informed decision

Decision
based on organizational policy

Enforcement
of policy across resources

Secure digital transformation

By building Zero Trust foundations



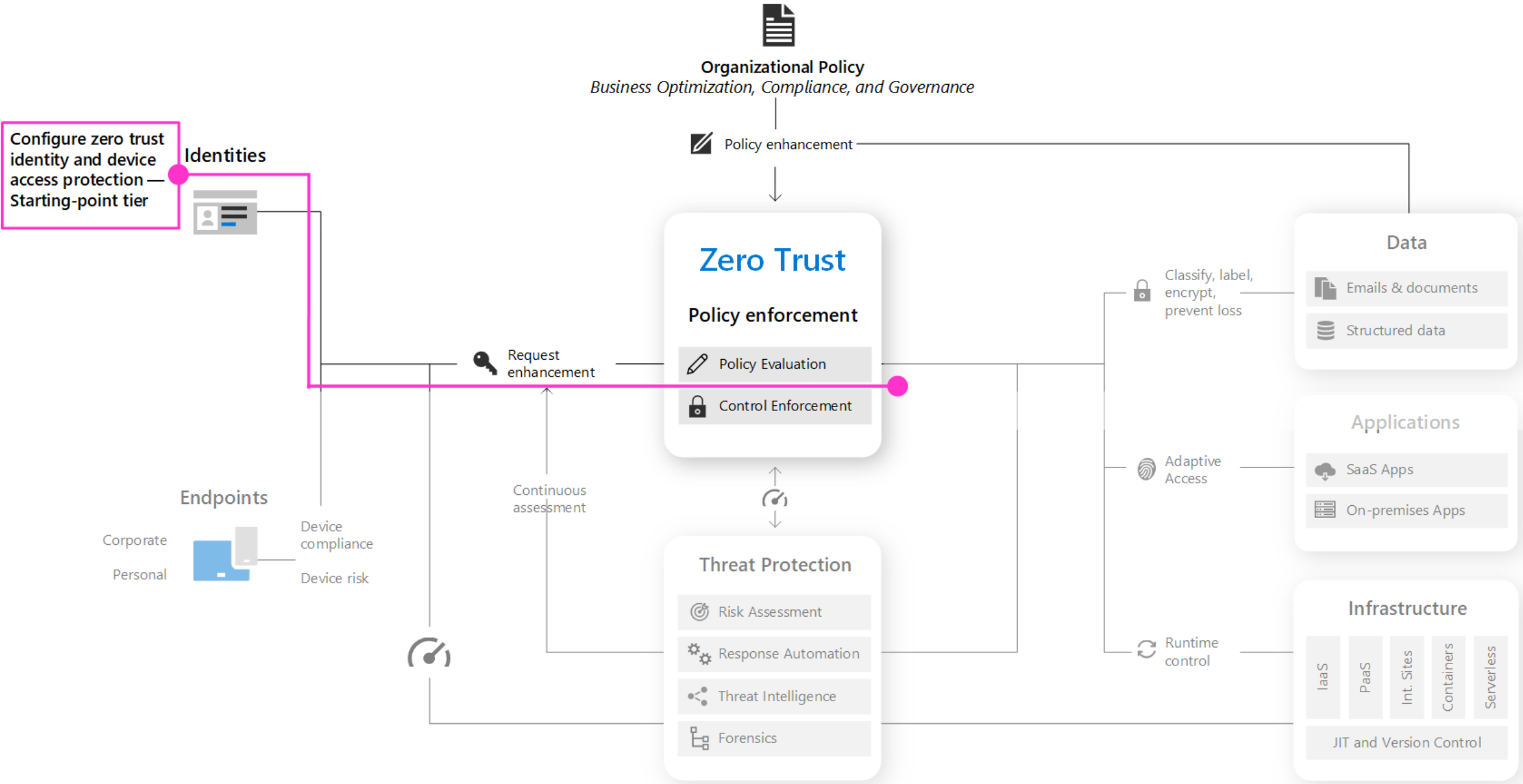
Modernize identity and endpoint management

Secure the hybrid workforce

Transform employee experiences

Customize secure access for all user types

Step 1. Configure Zero Trust identity and device access protection — starting-point policies



Zero Trust identity and device access policies

Protection level	Device type	Azure AD Conditional Access policies				Azure AD Identity Protection user risk policy	Intune device compliance policy	Intune app protection policies
Starting point	PCs	Require multi-factor authentication (MFA) when sign-in risk is *medium* or *high* ●	Require approved apps This policy enforces mobile app protection for phones & tablets.	Block clients that don't support modern authentication Clients that do not use modern authentication can bypass Conditional Access policies.		High risk users must change password This policy forces users to change their password when signing in if high risk activity is detected for their account.		Apply Level 2 App Protection Policies (APP) data protection (one for each platform)
	Phones and tablets							
Enterprise (Recommended for Zero Trust)		Require MFA when sign-in risk is *low, medium,* or *high* ●	Require approved apps		Require compliant PCs *and* mobile devices This policy enforces Intune management for PCs, phones, and tablets.		Define compliance policies (one for each platform)	Apply Level 2 App Protection Policies
Specialized security (only if needed for specific data sets or users)		Require MFA *always* This is also available for all Office 365 Enterprise plans.	Require approved apps			●		Apply Level 3 APP data protection

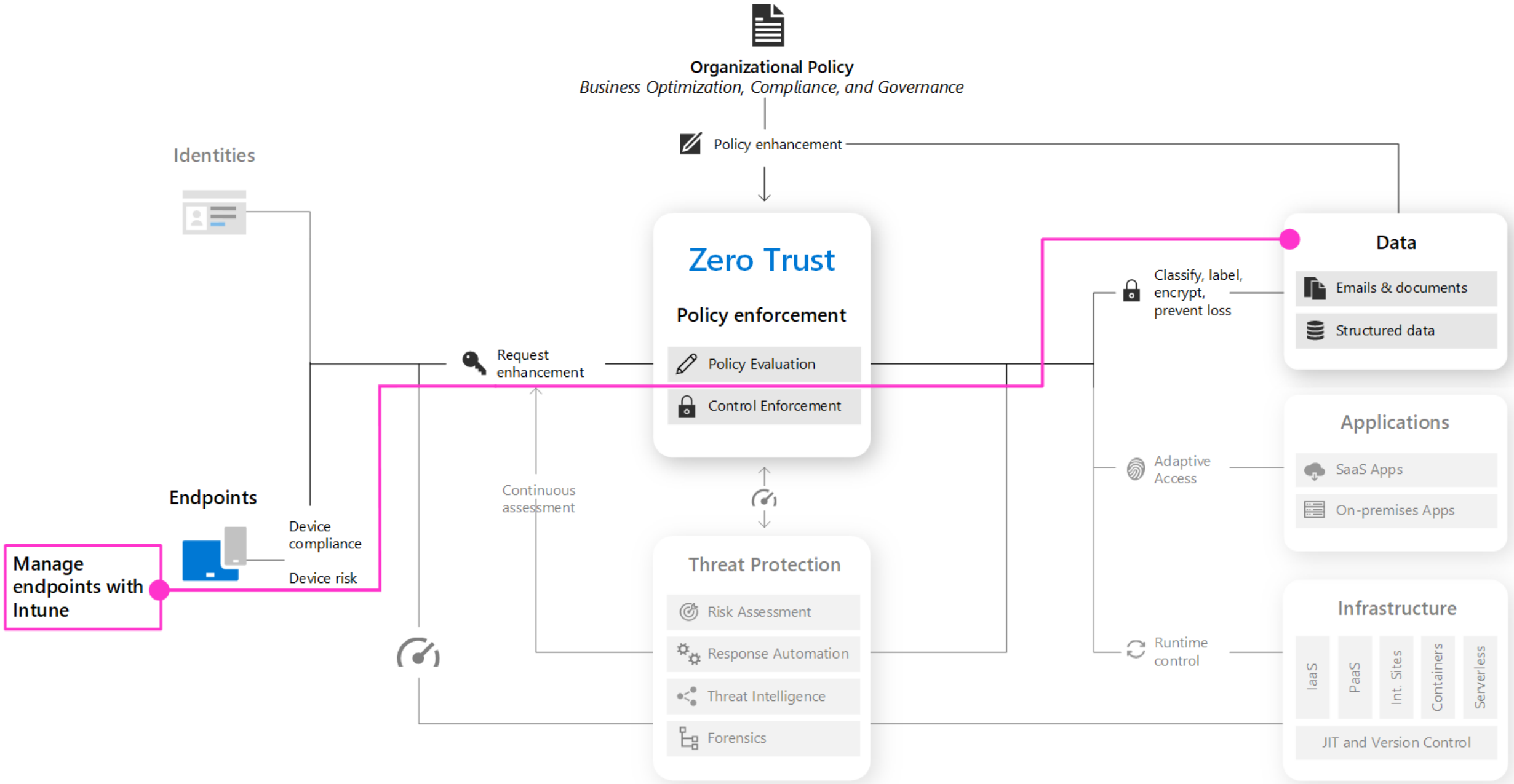
PCs include devices running the Windows or macOS platforms

Phones and tablets include devices running the iOS, iPadOS, or Android platforms

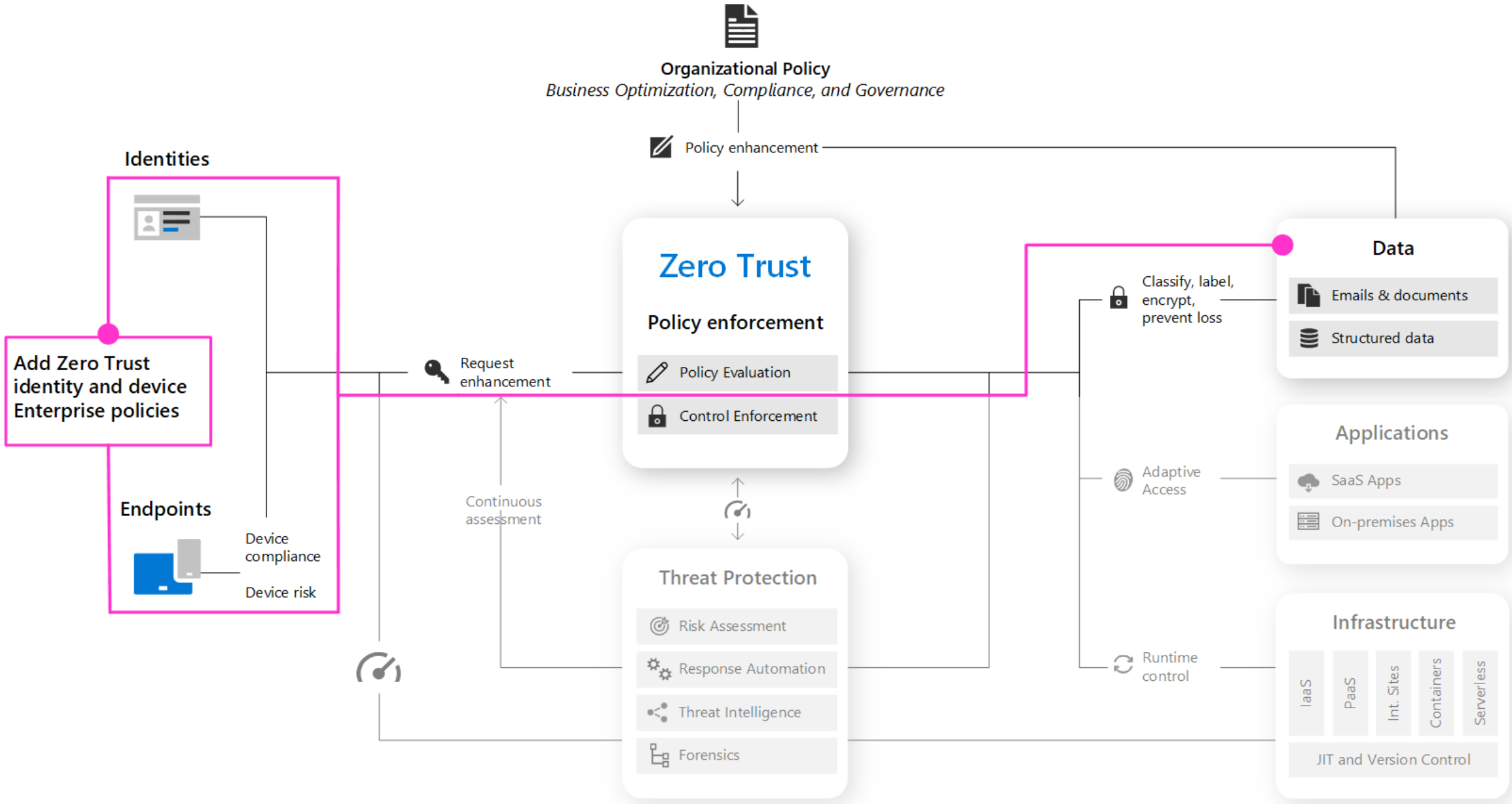
● Requires Microsoft 365 E5, Microsoft 365 E3 with the E5 Identity add-on, Office 365 with EMS E5, or individual Azure AD Premium P2 licenses

November 2021

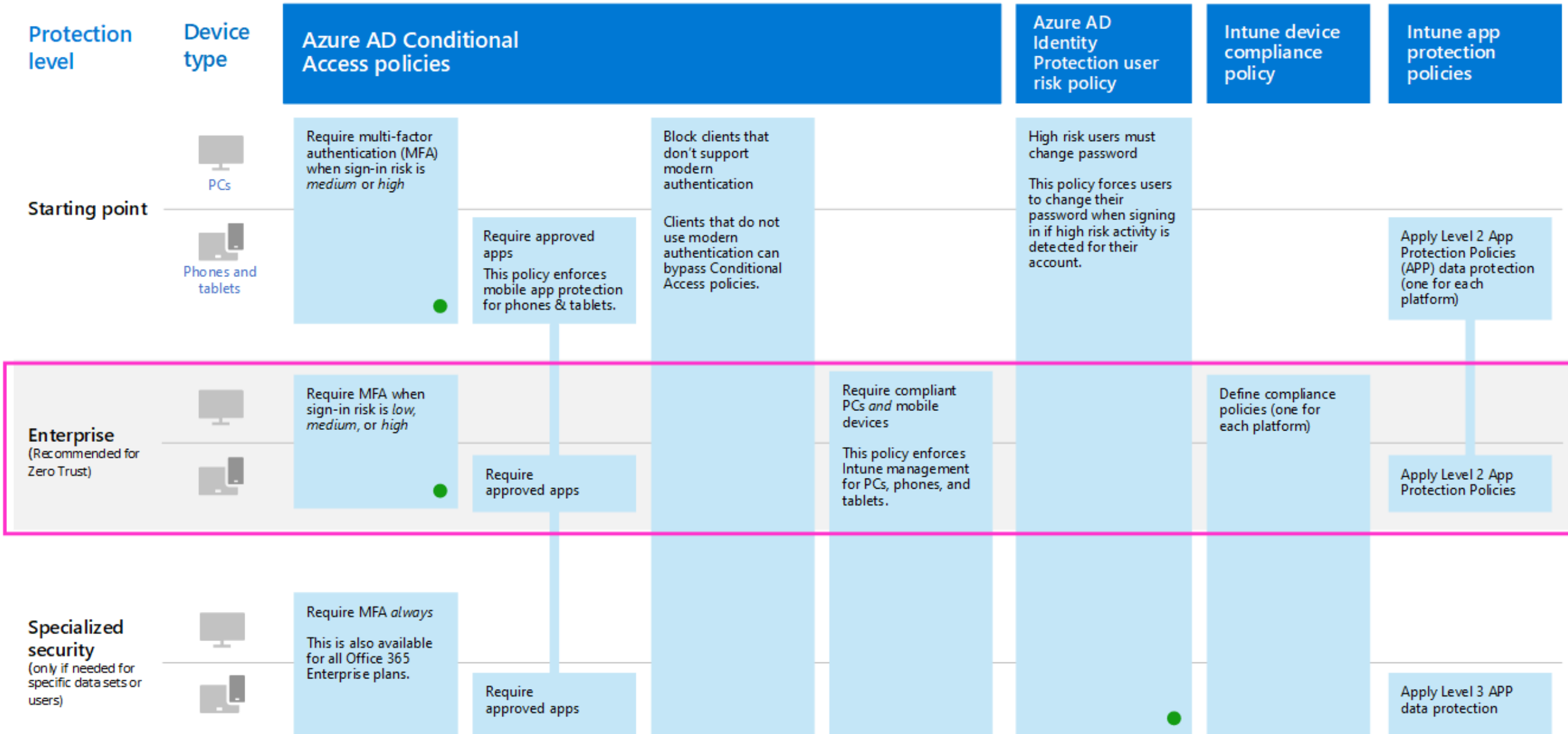
Step 2. Manage endpoints with Intune



Step 3. Add Zero Trust identity and device access protection — Enterprise policies



Zero Trust identity and device access policies



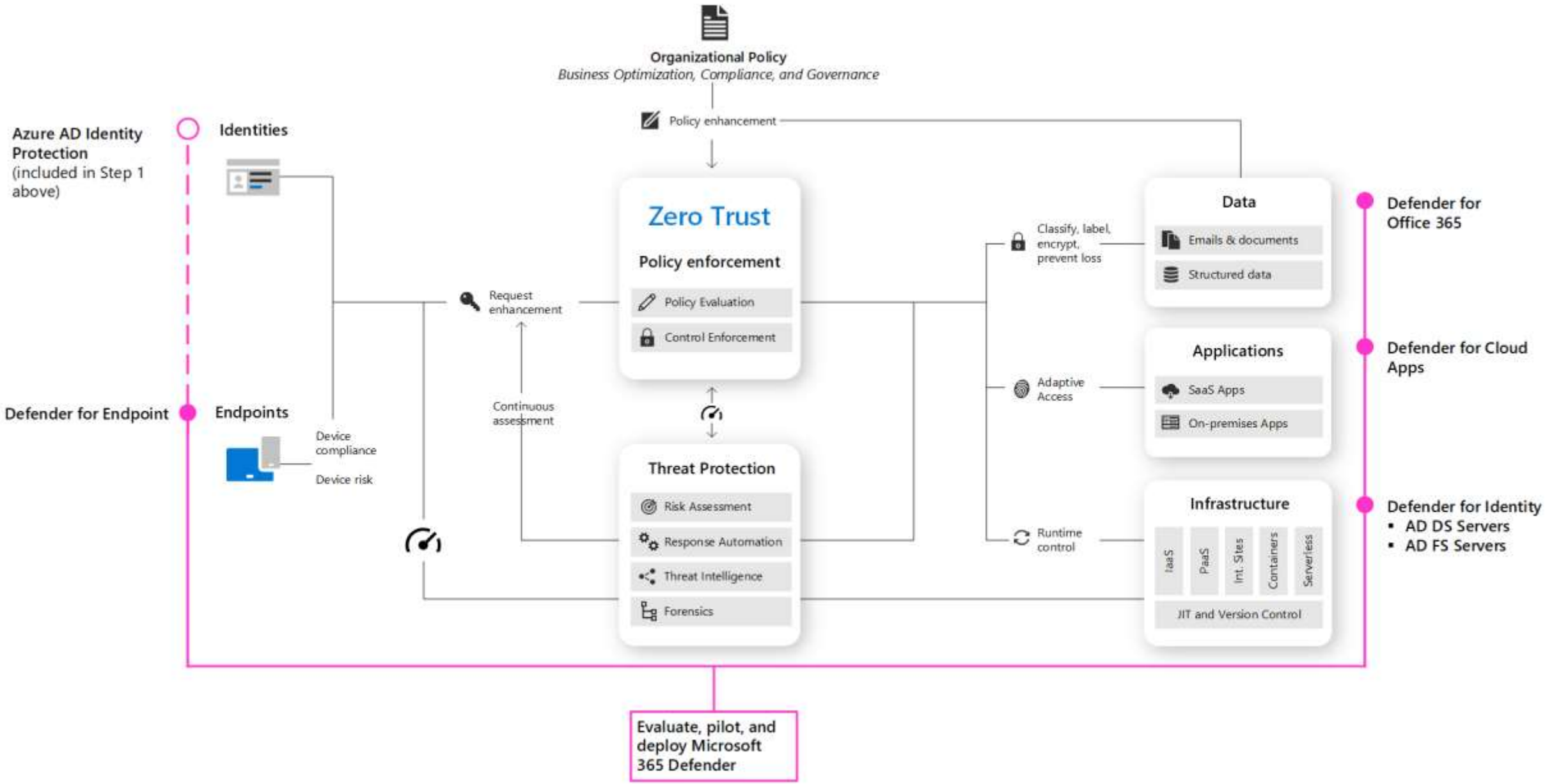
PCs include devices running the Windows or macOS platforms

Phones and tablets include devices running the iOS, iPadOS, or Android platforms

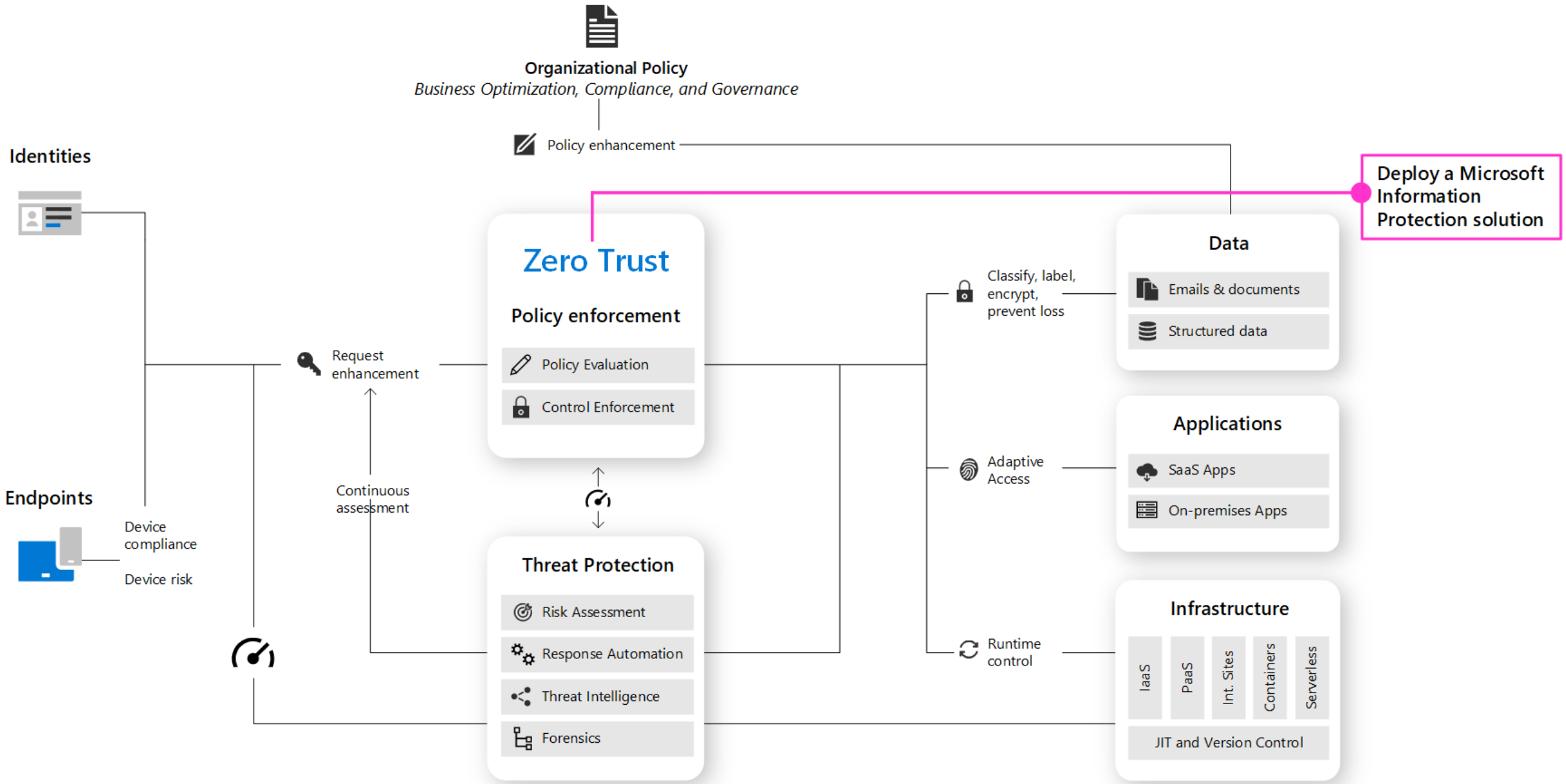
● Requires Microsoft 365 E5, Microsoft 365 E3 with the E5 Identity add-on, Office 365 with EMS E5, or individual Azure AD Premium P2 licenses

November 2021

Step 4. Evaluate, pilot, and deploy Microsoft 365 Defender



Step 5. Protect and govern sensitive data



Modernize identity and endpoint management

Secure the hybrid workforce

Transform employee experiences

Customize secure access for all user types

Why modernize your identity and endpoint management

Improve security

Prevent attacks on your on-premises infrastructure.

Increase IT efficiency

Reduce maintenance costs and operational overhead.

Accelerate digital transformation

Enable business agility and efficient allocation of resources.

Strategies for modernization

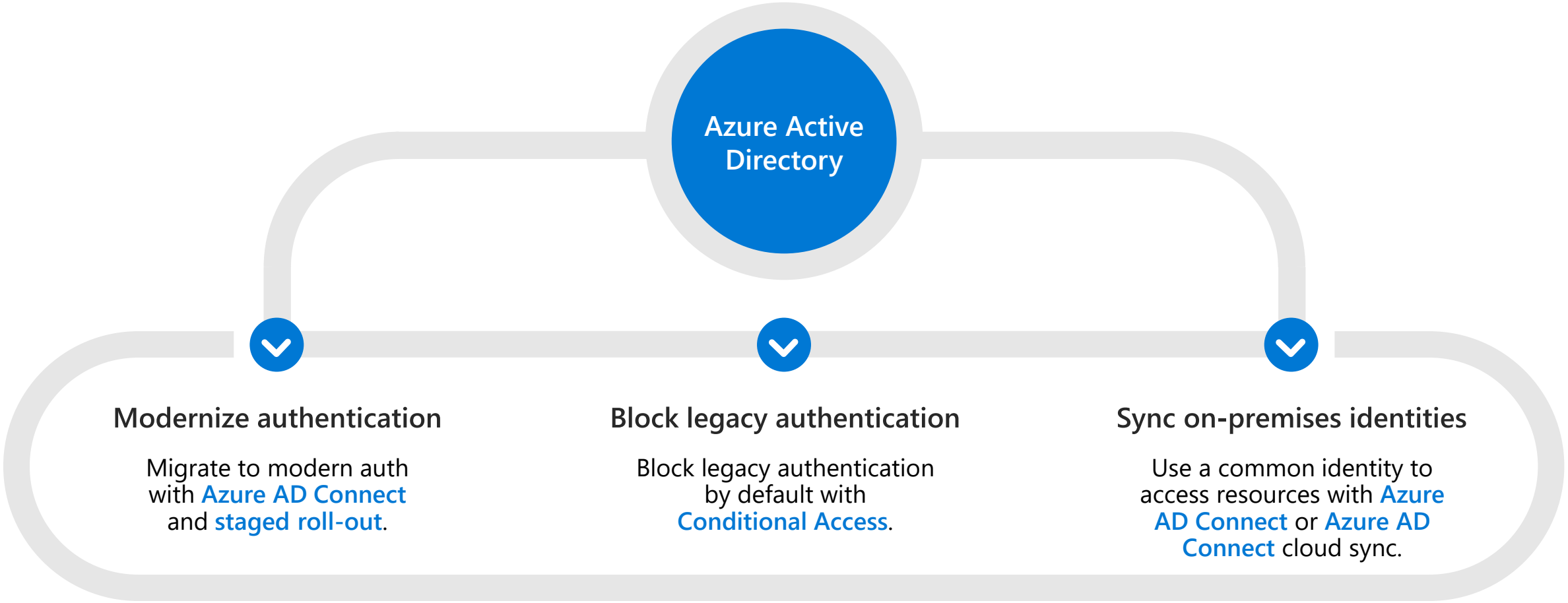
Modernize authentication and manage identities in the cloud.

Manage devices from the cloud at your own pace.

Improve visibility and control by **unifying app management**.

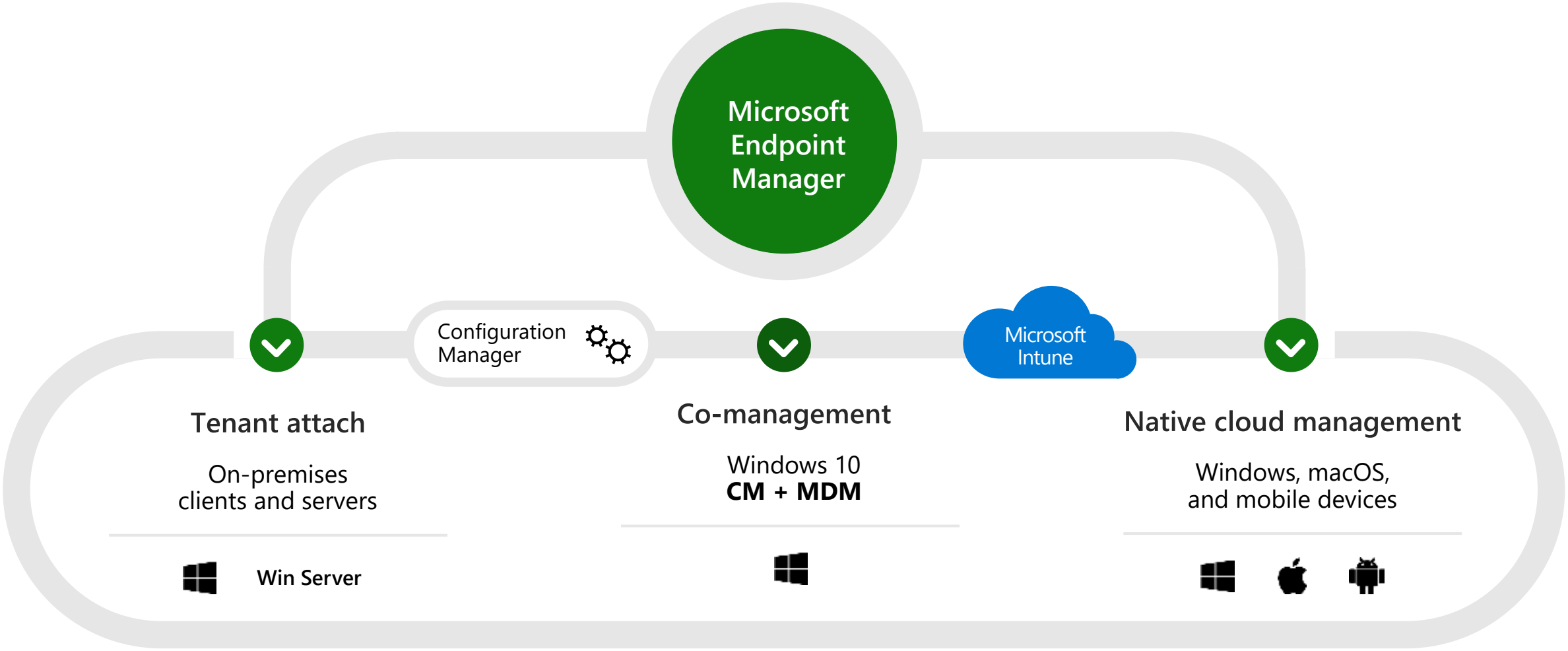
Migrate authentication and identities to the cloud

Improve security by managing all identities and access in a single cloud identity solution



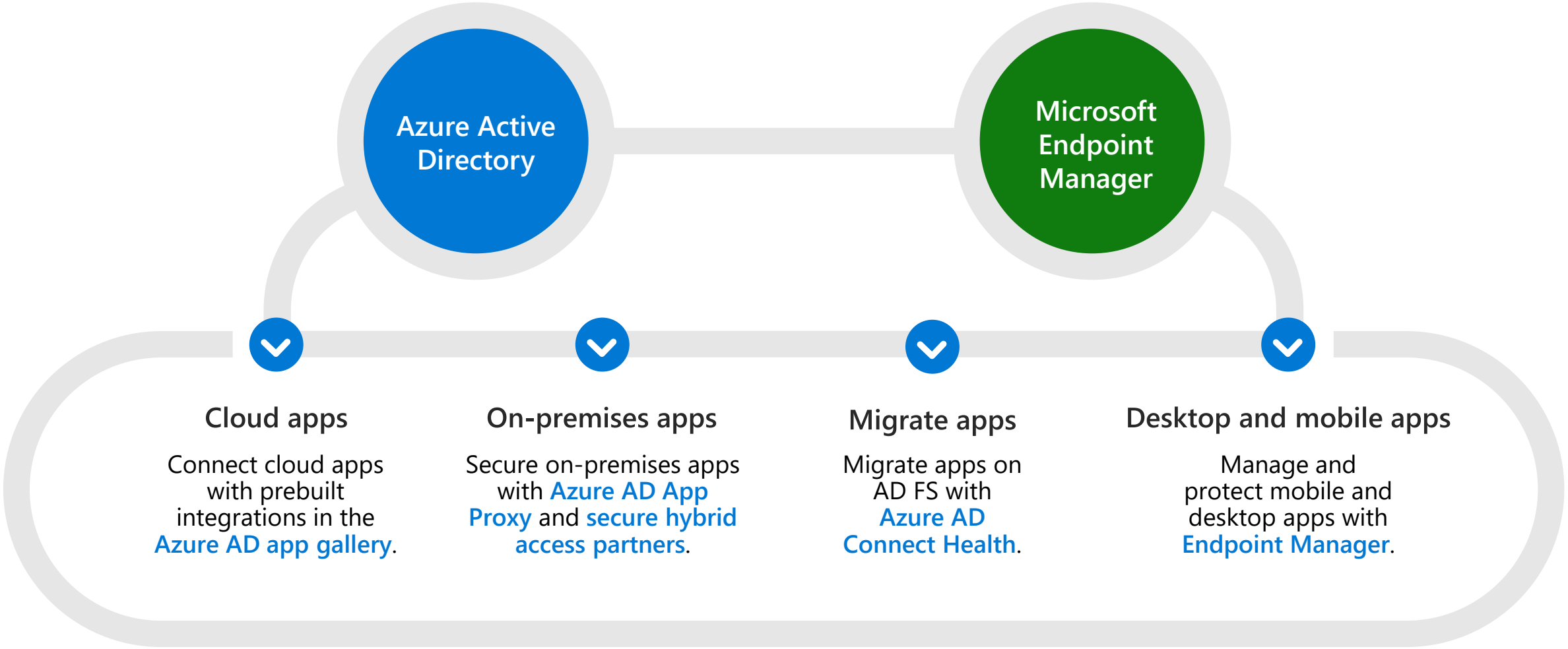
Manage endpoints in the cloud at your own pace

Endpoint security, device management, and intelligent cloud actions in a unified management platform



Unify app management

Secure access to all applications with integrated identity and endpoint management

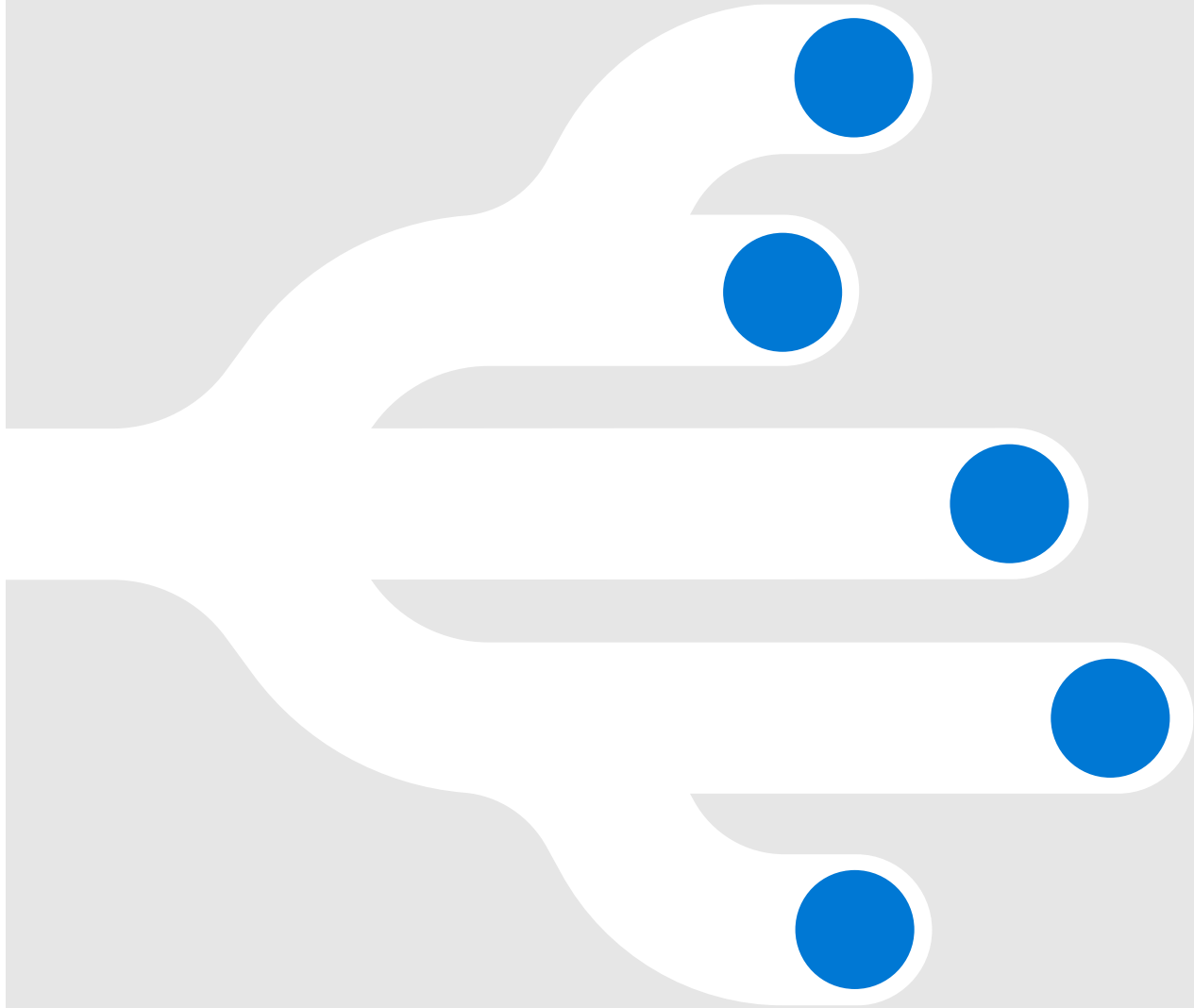


Modernize identities and endpoints

Secure the hybrid workforce

Transform employee experiences

Customize secure access for all user types



68%

of business leaders feel their cybersecurity risks are increasing.

Source: The cost of cybercrime, Accenture, 2019

Why secure the hybrid workforce

Provide remote access

Enable remote workers to securely access the apps they need from anywhere.

Secure devices and apps

Enable BYOD and unify management across devices and apps.

Protect corporate resources

Empower IT to apply controls and protect endpoints without getting in the way of productivity.

Strategies for securing the hybrid workforce

Verify user identities with **strong authentication** methods.

Allow only **compliant and trusted devices** access.

Configure **adaptive access policies** based on context and risk.

Safeguard resources with **access lifecycle management**.

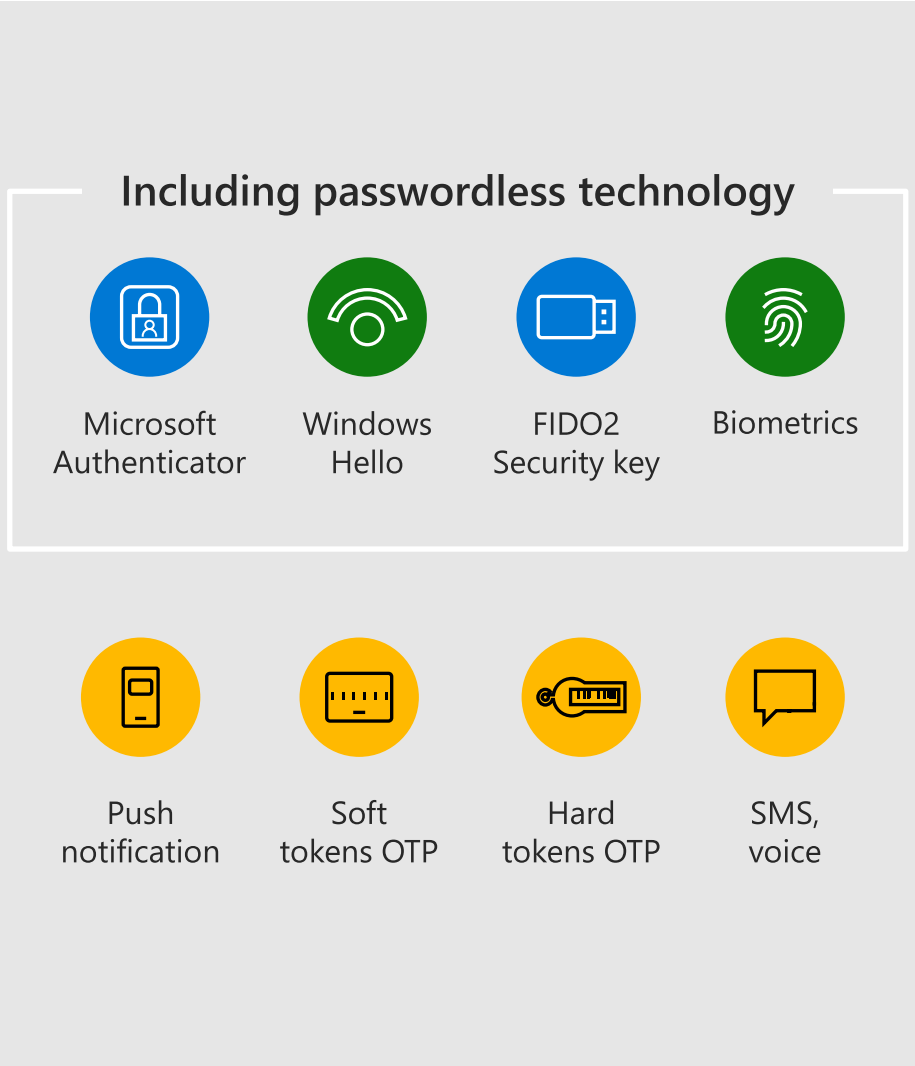
Verify user identities with strong authentication

Secure access to resources with multifactor authentication

Prevent 99.9% of identity attacks with multifactor authentication.

Choose from a broad range of multifactor authentication options.

Make sign-in even more seamless and secure with passwordless authentication.



Allow only compliant devices to access data

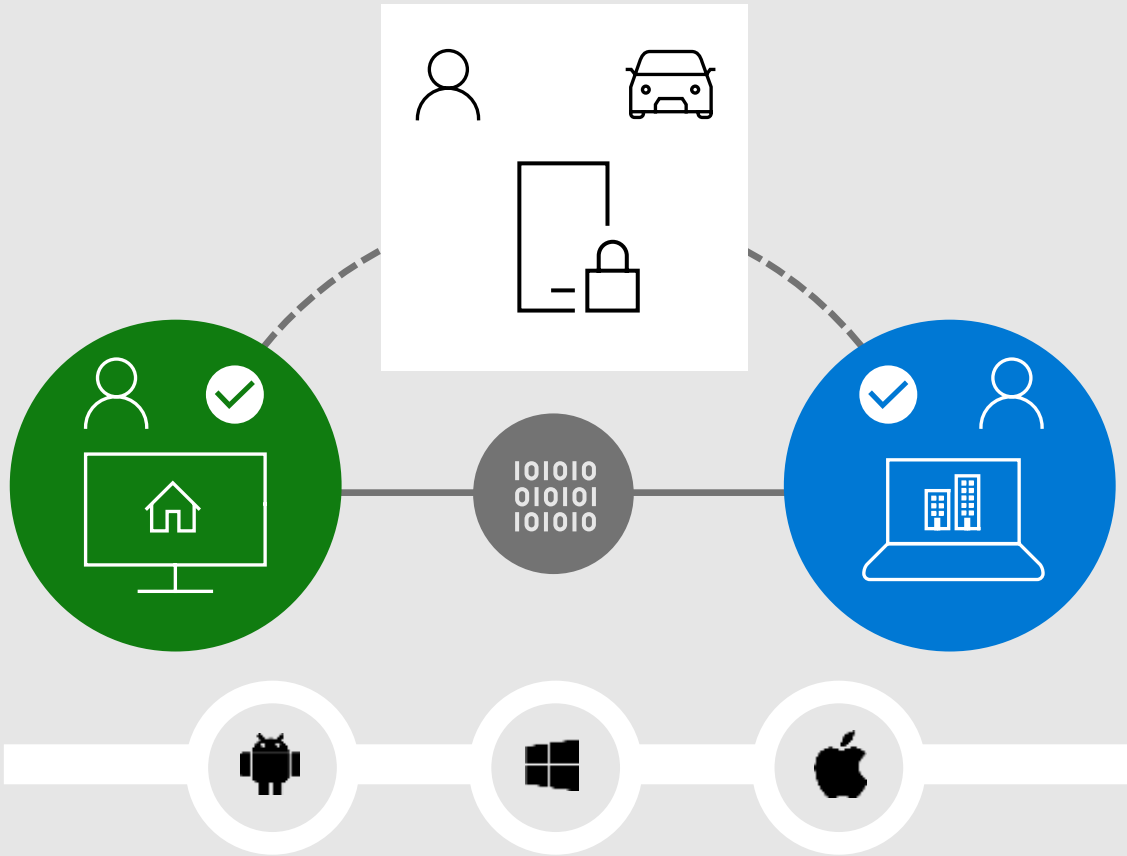
Empower IT to apply controls through endpoint cloud management

Apply data protection policies on mobile devices and applications.

Reduce risk of breaches by quickly remediating detected threats.

Manage device health with detection and response integration and insights.

Set risk-based Conditional Access for devices to protect sensitive information.



Configure adaptive access policies

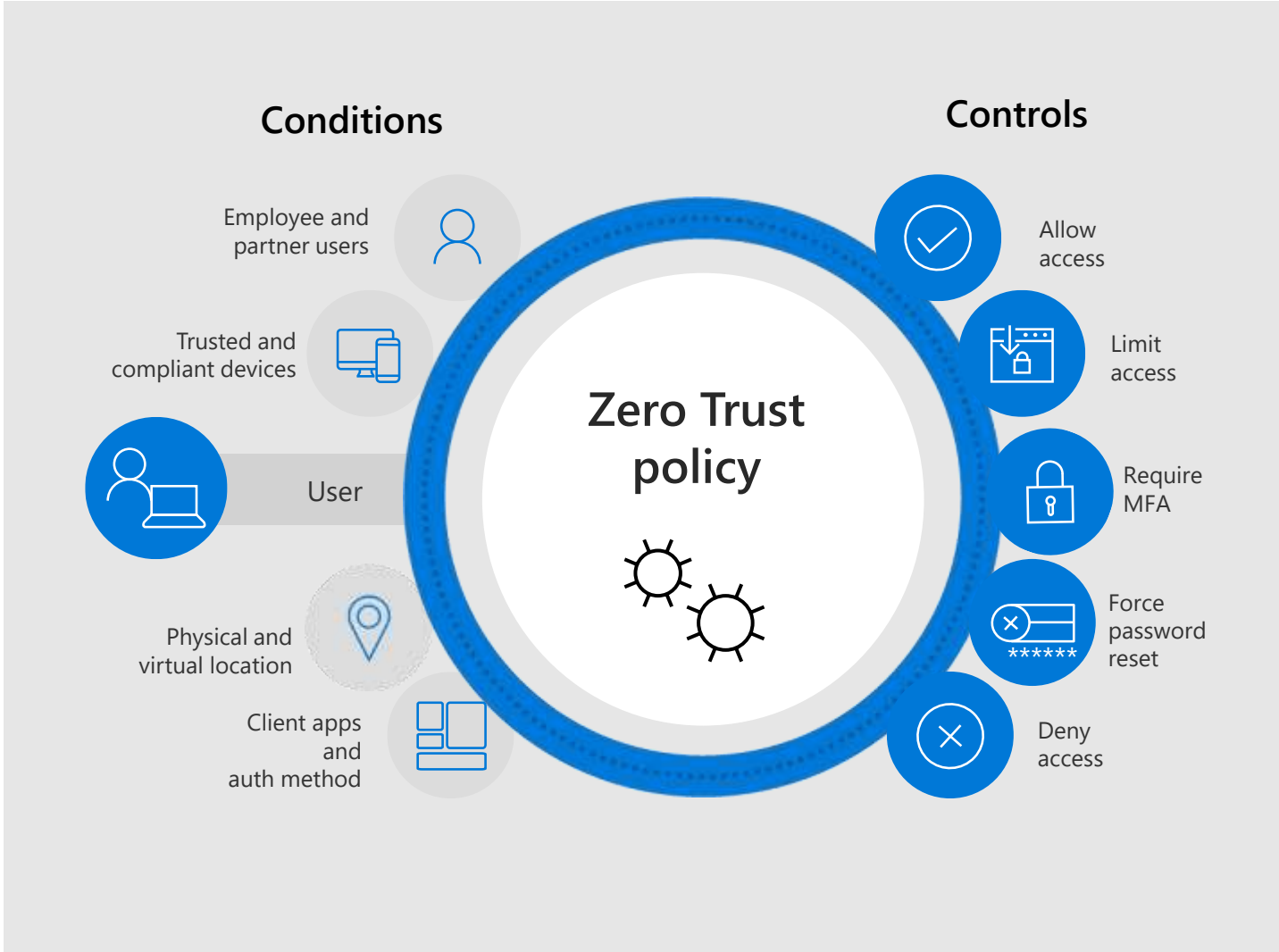
Control access with smart policies and risk assessments

Configure real-time adaptive access policies with Conditional Access.

Set flexible policies based on:

- Sign-in risk
- User risk
- Device state
- Device platform
- Location
- Applications

Extend real-time policy controls based on event changes during a user session with Continuous Access Evaluation.



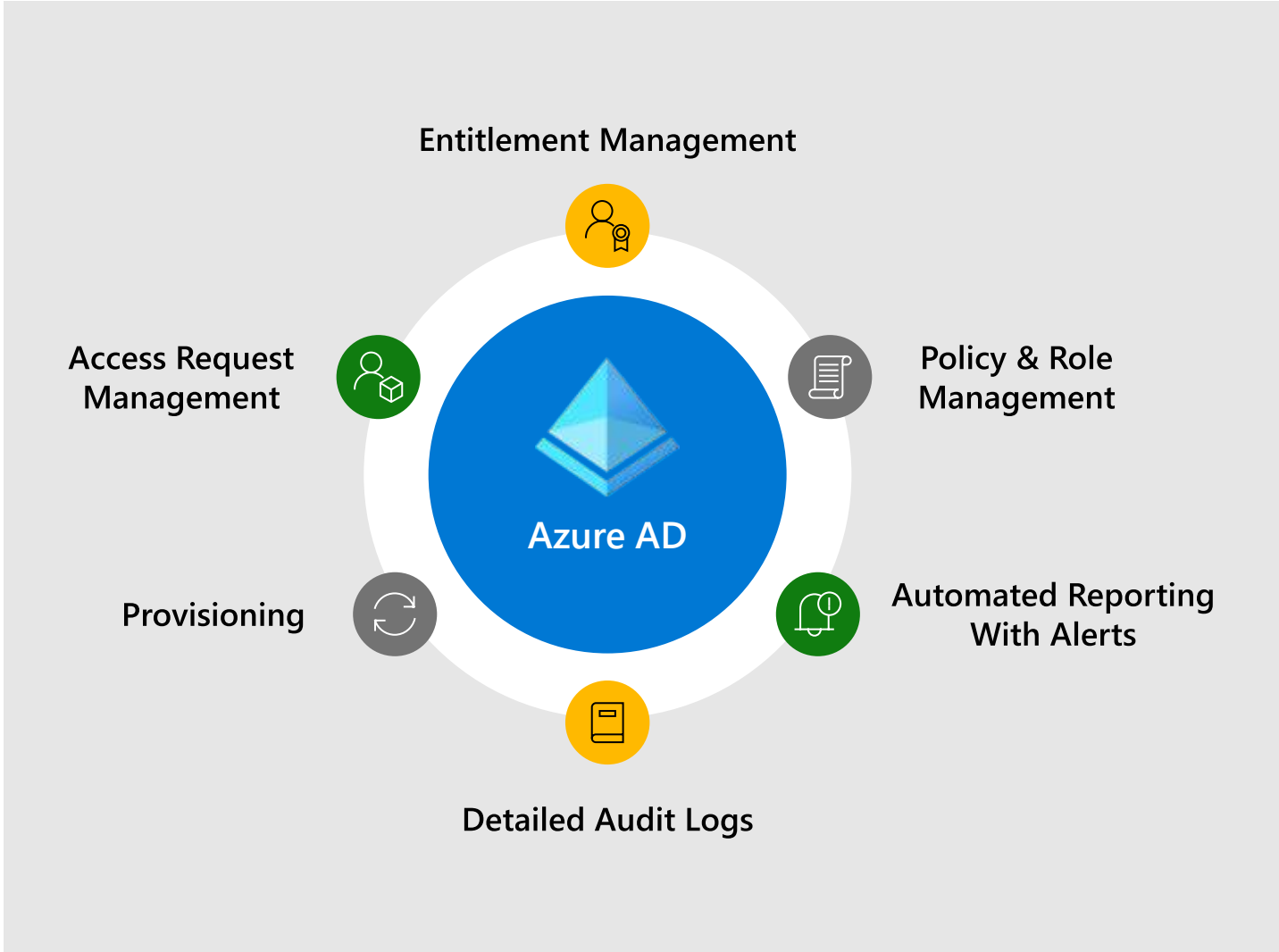
Safeguard resources with access lifecycle management

Protect, monitor, and audit access to company resources

Provide appropriate access permissions based on roles and group membership.

Reduce risk by reviewing, extending, or revoking access rights for employees and guests.

Simplify the audit process with detailed reports and logs.

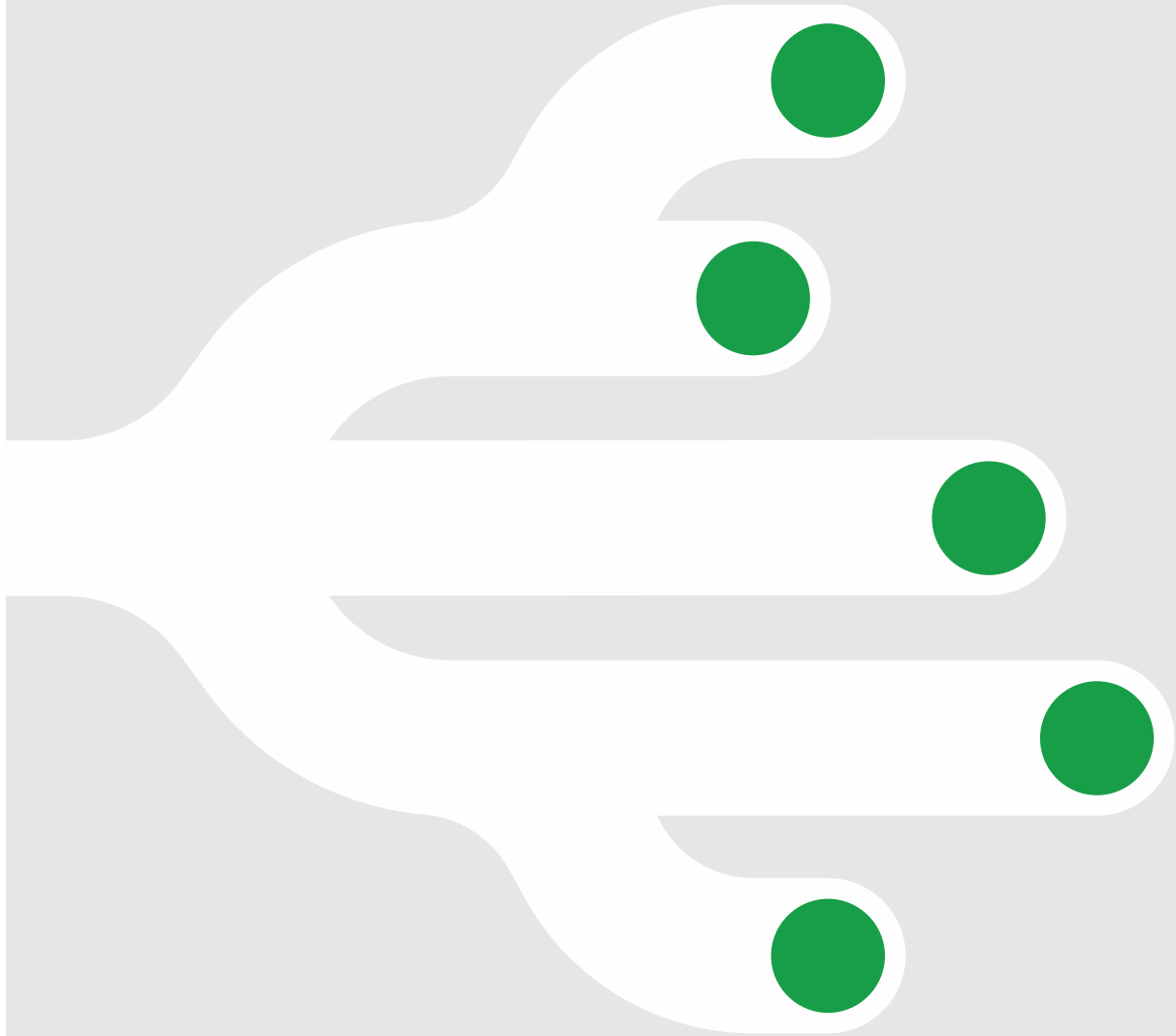


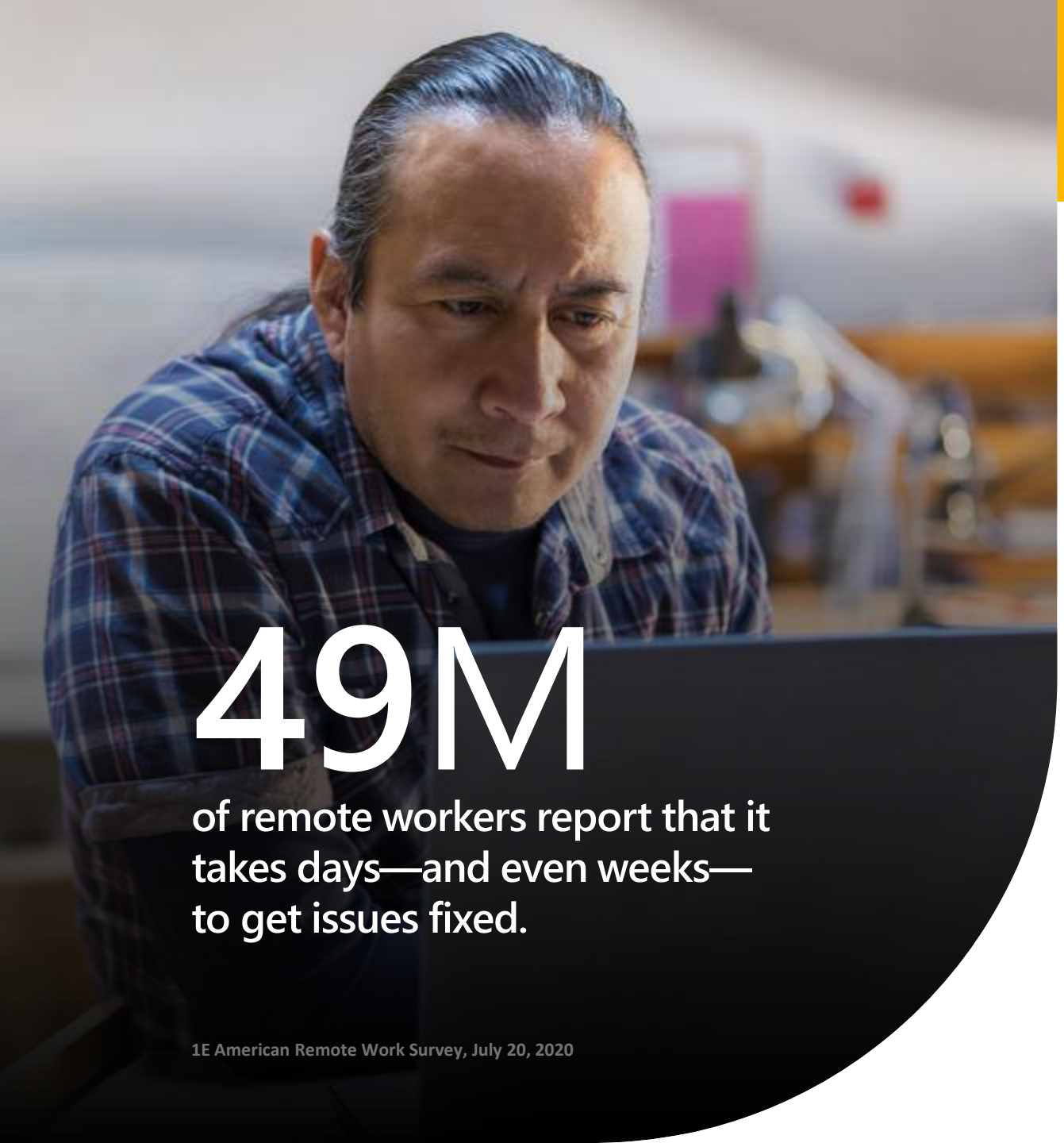
Modernize identities and endpoints

Secure the hybrid workforce

Transform employee experiences

Customize secure access for all user types





49M

of remote workers report that it takes days—and even weeks—to get issues fixed.

1E American Remote Work Survey, July 20, 2020

Why transform the employee experience

Improve productivity

Provide employees quick access and consistent sign-in experiences to all applications.

Reduce IT friction

Empower employees to be more productive by enabling them to resolve IT helpdesk issues.

Foster collaboration

Remove silos between employees and partners and improve collaboration.

Strategies for transforming employee experiences

Onboard employees quickly with **streamlined provisioning**.

Connect your workforce to all apps with **single sign-on**.

Reduce IT overhead and empower **self-service experiences**.

Facilitate seamless **collaboration across organizational boundaries**.

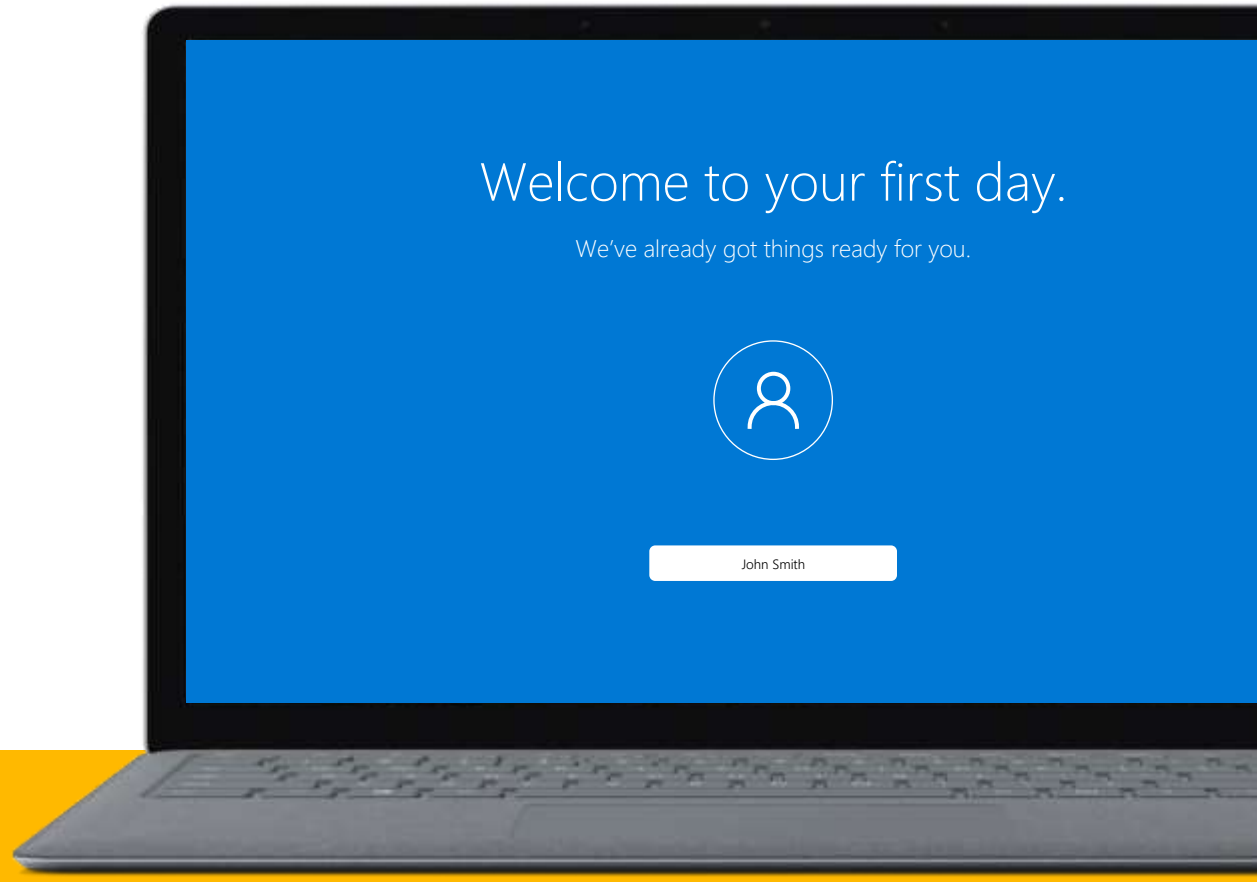
Provision access to resources efficiently

Automate onboarding and provisioning of resources for fast, secure access

Onboard users quickly with HR-driven user provisioning and enable day-one productivity.

Provision new devices and applications direct-to-employees, ready for use.

Enroll new devices automatically for easy endpoint management.



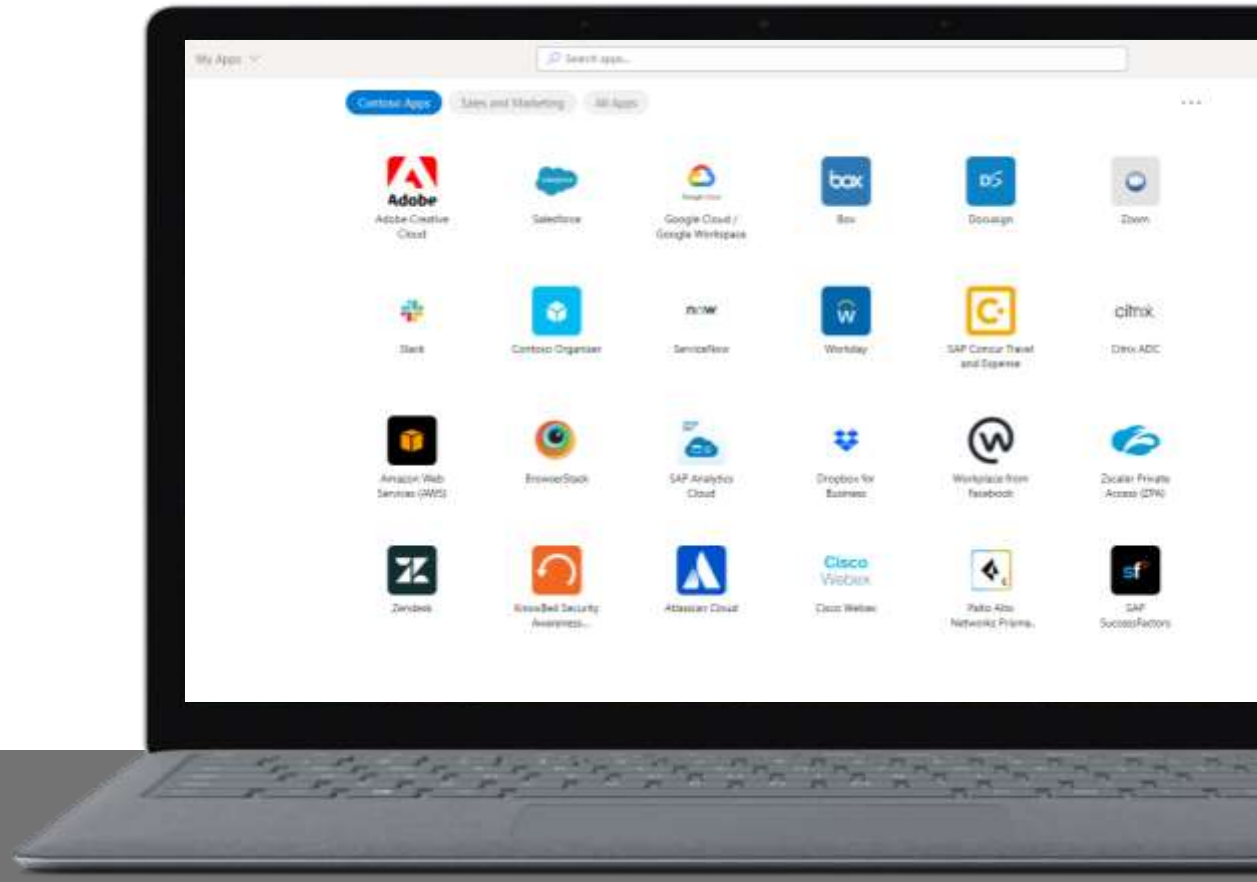
Enable seamless, secure access with single sign-on

Access popular SaaS, on-premises, and custom-built apps on any cloud

Enable SSO for cloud apps and on-premises apps with a single identity solution.

Deploy consistent experiences across apps and endpoint platforms with built-in protection.

Empower employees to discover and launch apps from a centralized app portal.



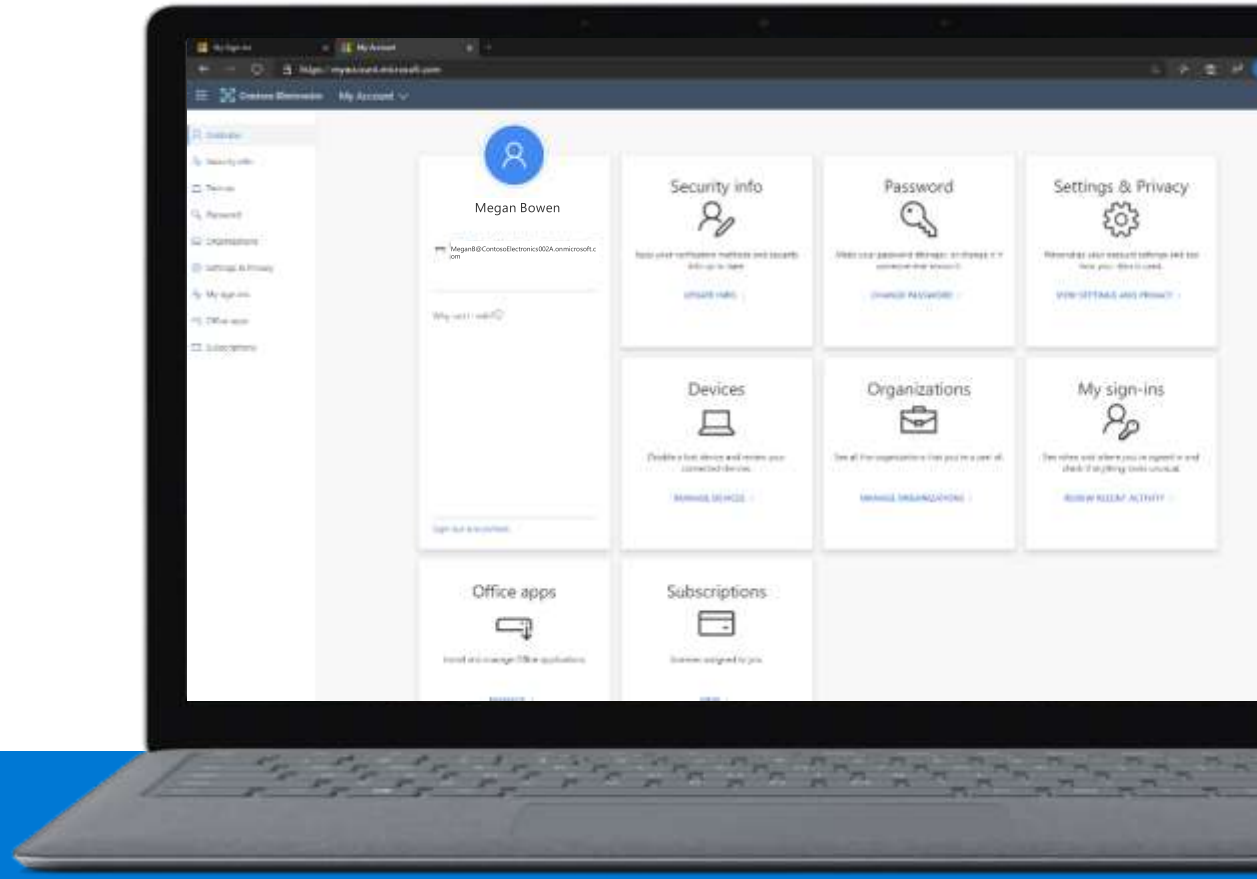
Empower employees to manage their own identity

Self-service tools to keep your users productive and minimize IT friction

Enable employees to self-service password resets.

Empower employees and guests to manage and request access packages.

Manage security contact information and detect and report risk sign-in behavior.



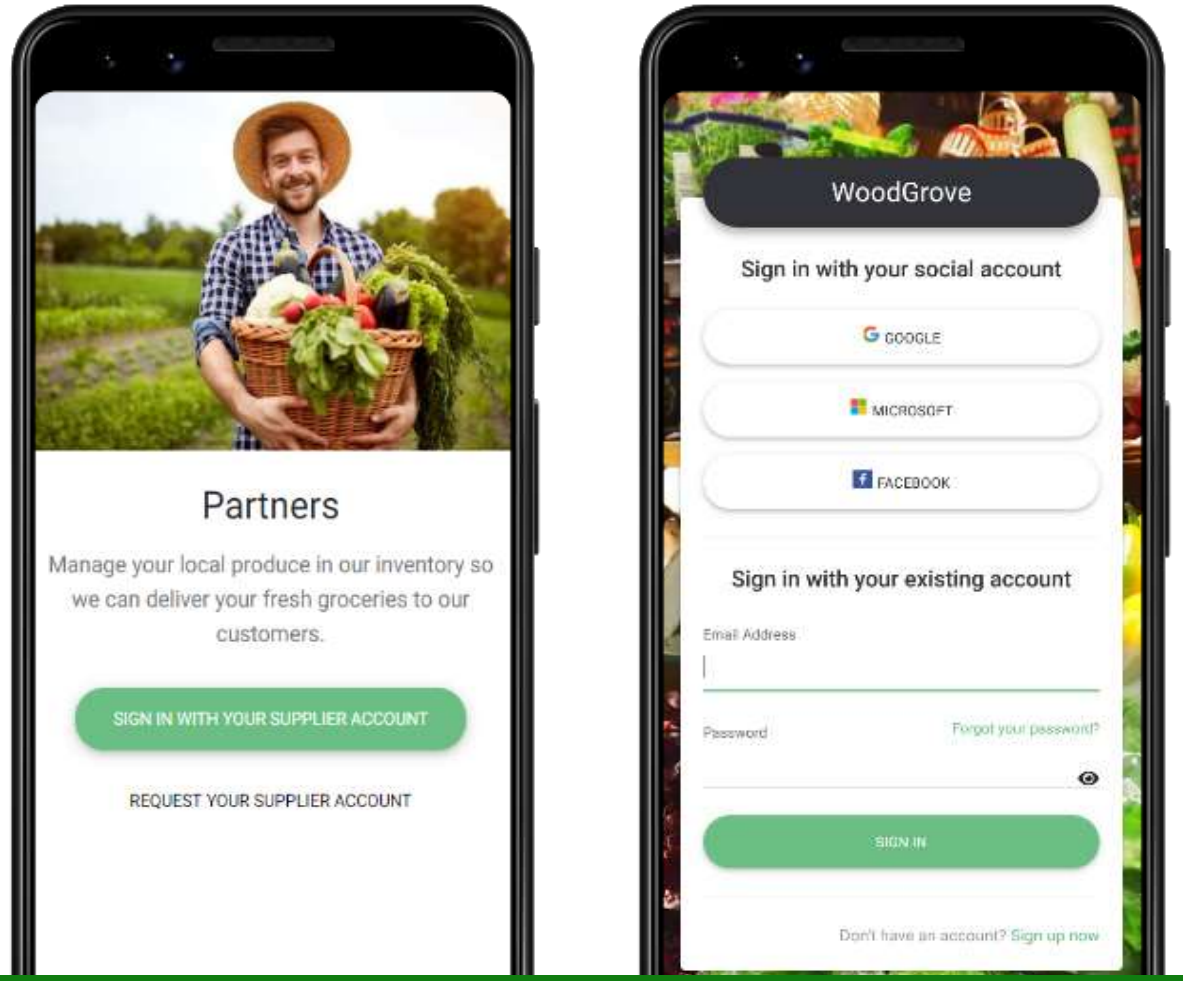
Collaborate seamlessly with partners

Grant secure access to your partners and facilitate B2B collaboration

Invite B2B partners to collaborate with your organization.

Securely share your organization's apps and resources with partners.

Empower partners to bring their own identities to self-service sign-up and sign-in to your organization's resources.

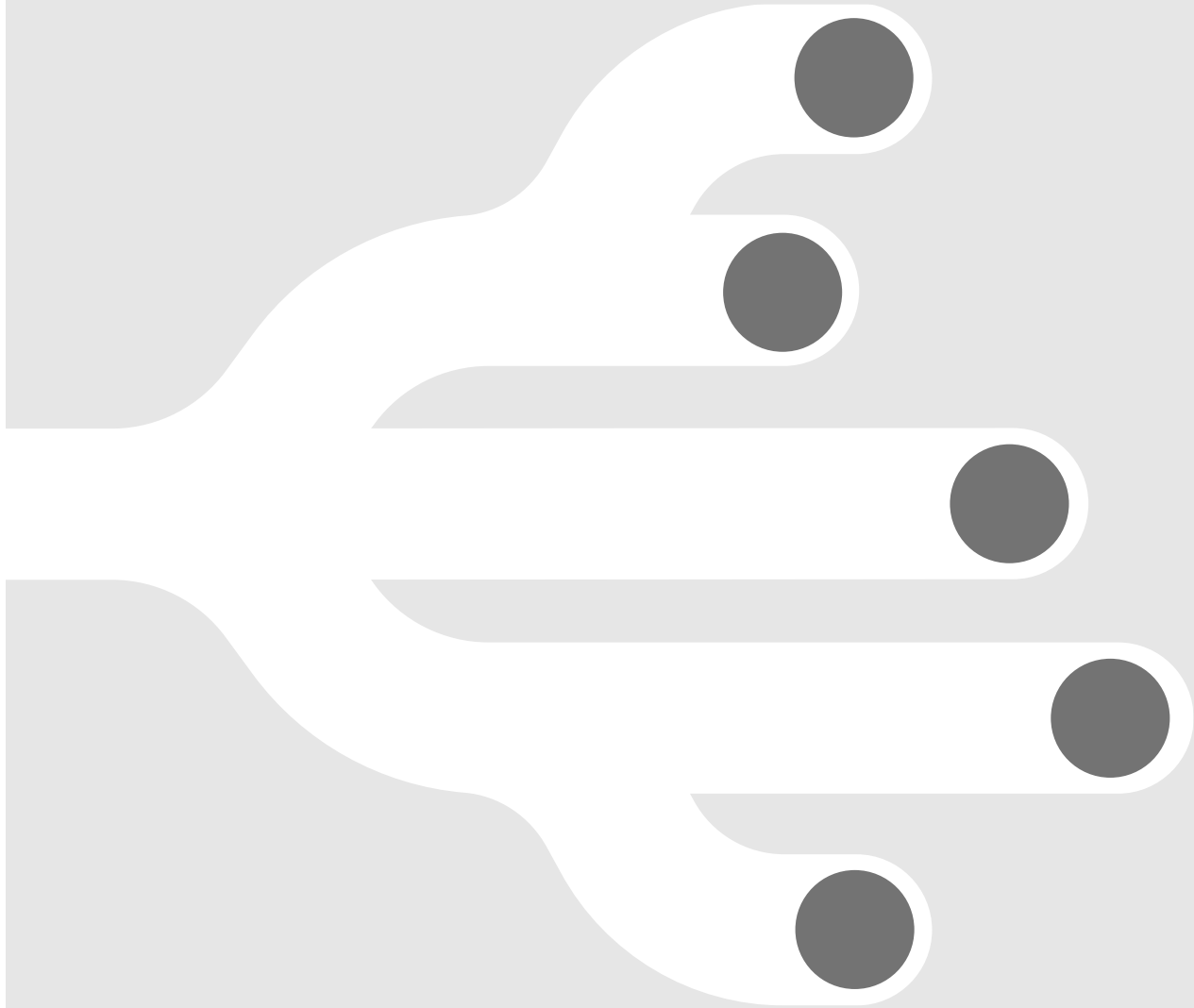


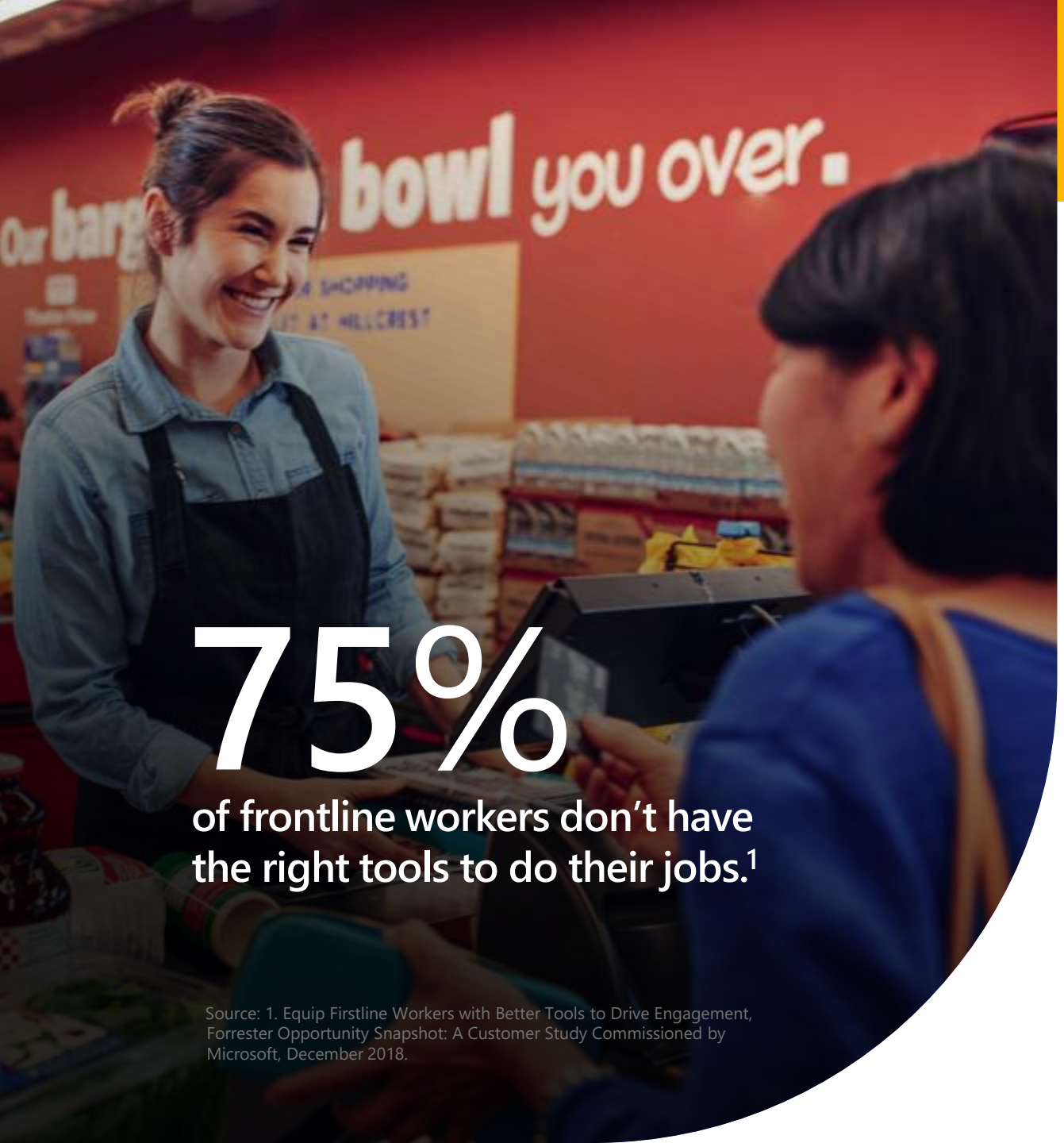
Modernize identities and endpoints

Secure the hybrid workforce

Transform employee experiences

Customize secure access for all user types





75%

of frontline workers don't have the right tools to do their jobs.[1]

Source: 1. Equip Firstline Workers with Better Tools to Drive Engagement, Forrester Opportunity Snapshot: A Customer Study Commissioned by Microsoft, December 2018.

Why customize secure access for all users

Improve collaboration

Simplify collaboration between information workers and frontline workers.

Protect your brand

Poor customer experiences put your brand and reputation at risk.

Simplify user experiences

Provide streamlined workflows that empower all user types.

Strategies for customizing secure access for all users

Empower **frontline workers** with streamlined workflows and tailored devices.

Safeguard **customer identities** and prevent fraud with identity-driven security.

Protect your revenue and customers with **fraud protection**.

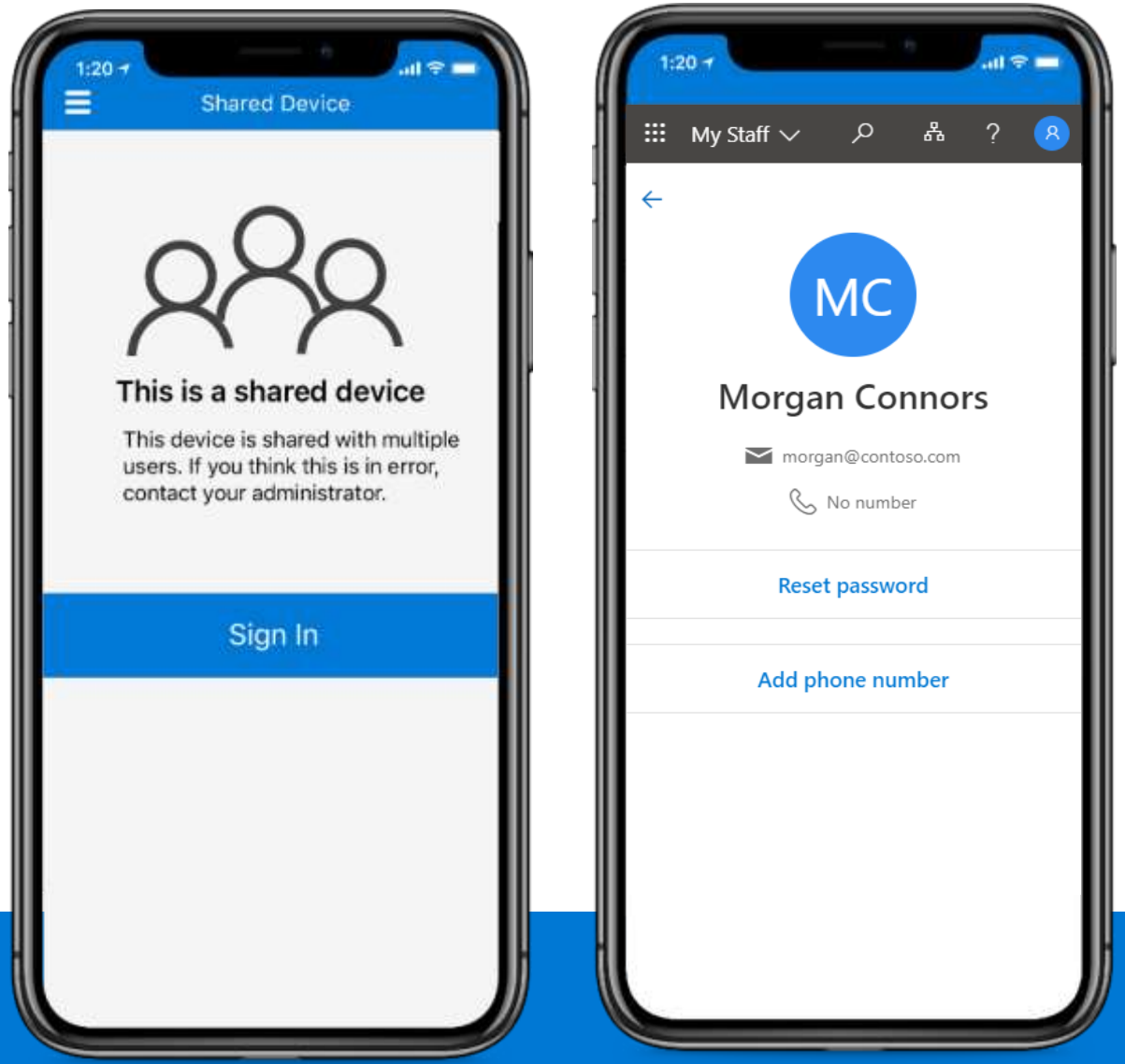
Empowering frontline workers

Deliver frontline solutions with modern identity and endpoint management

Streamline frontline worker access with SMS sign-in.

Provision devices at scale and protect devices used by multiple employees with Shared Device Mode.

Delegate user management to frontline managers with the My Staff portal.



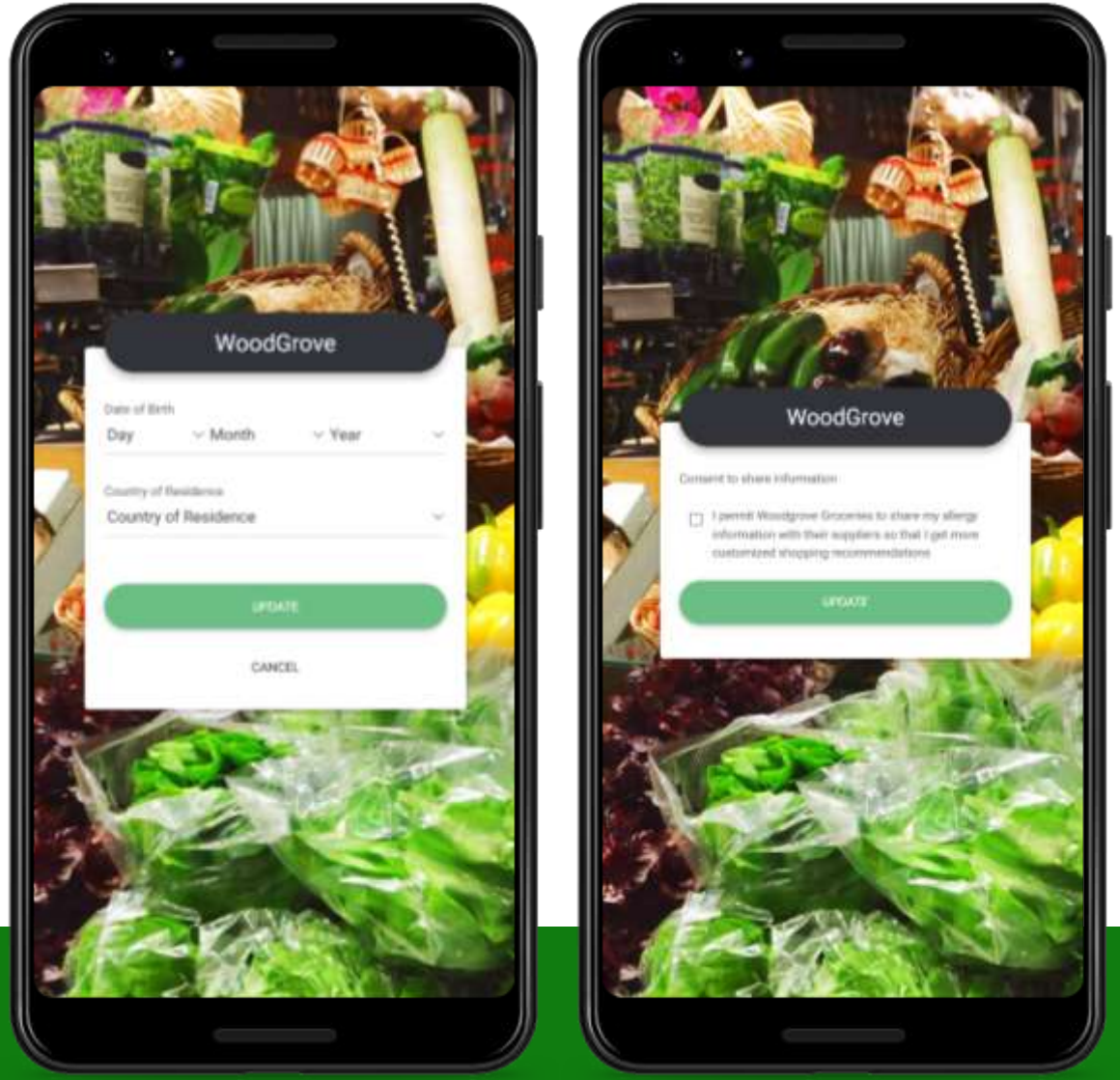
Build secure customer apps

Create secure customer experiences with Azure AD B2C

Enable seamless and secure sign-in and sign-up experiences.

Extend Identity Protection and risk-based Conditional Access to your customer accounts.

Customize the user journey to reduce friction of your sign-in and sign-up experiences.



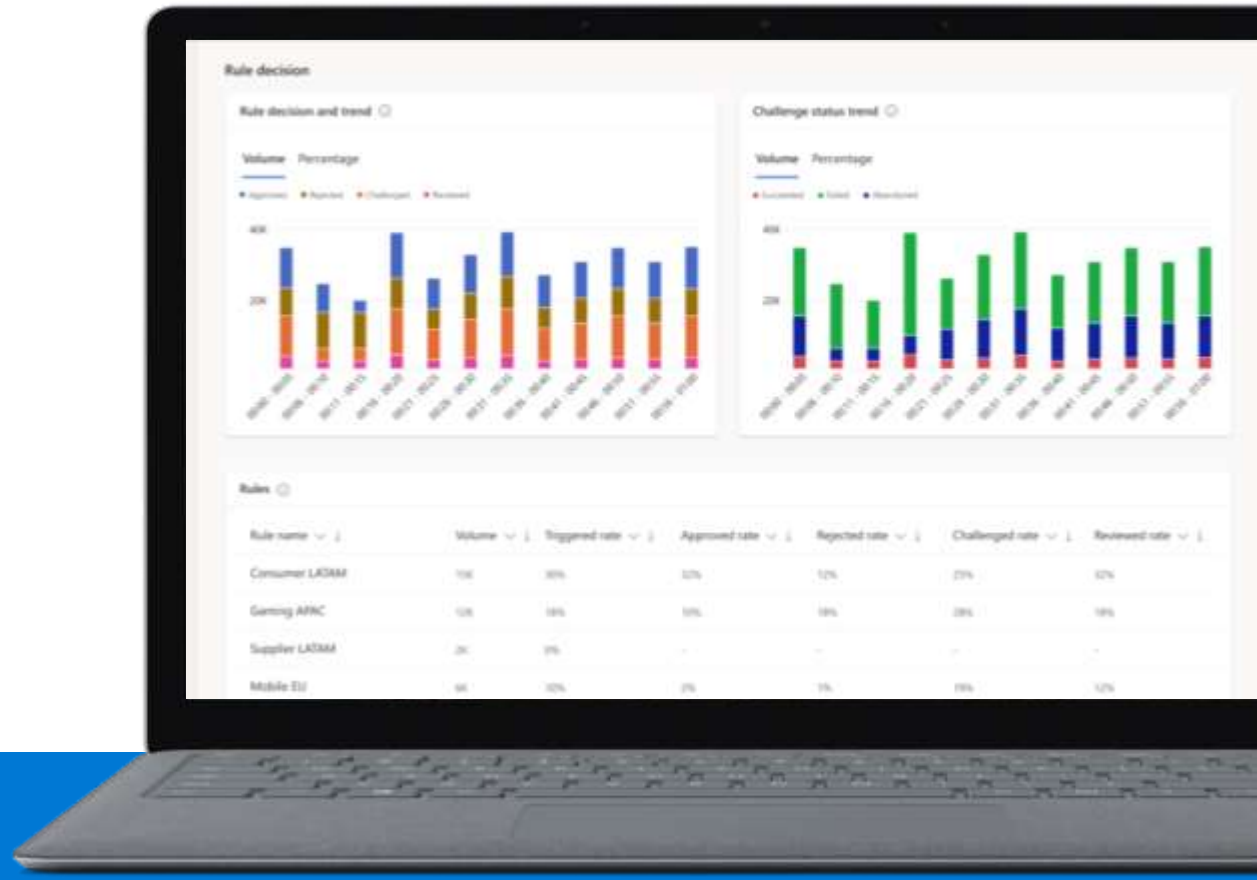
Protect your revenue and customers

Help reduce account fraud risk by pairing Azure AD B2C and Dynamics 365 Fraud Protection

Defend against bot attacks, fake account creation, account takeover, and fraudulent account access.

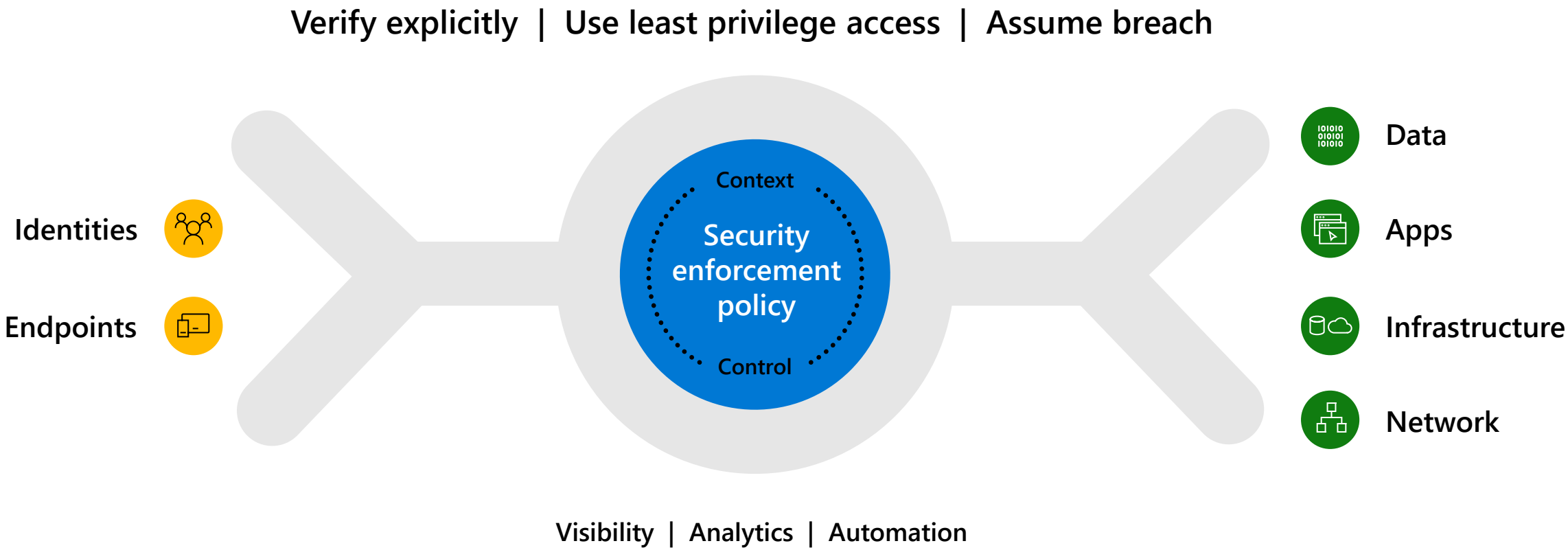
Improve transaction acceptance rates with insights that balance revenue opportunity against fraud loss and checkout friction.

Identify anomalies and potential fraud on returns and discounts and act to reduce revenue impact.



Secure your organization with Zero Trust

Increase security assurances for your critical business assets



Summary – What should be top of mind

Modernize identity and endpoint management

Reduce on-premises infrastructure.

Manage identities and endpoints in the cloud.

Secure the hybrid workforce

Ensure device compliance.

Turn on MFA.

Enforce Conditional Access policies.

Transform employee experiences

Secure all apps with an integrated Identity & Endpoint management solution.

Next steps

1

Ask your Microsoft representative for a discovery session on Zero Trust Foundations.

2

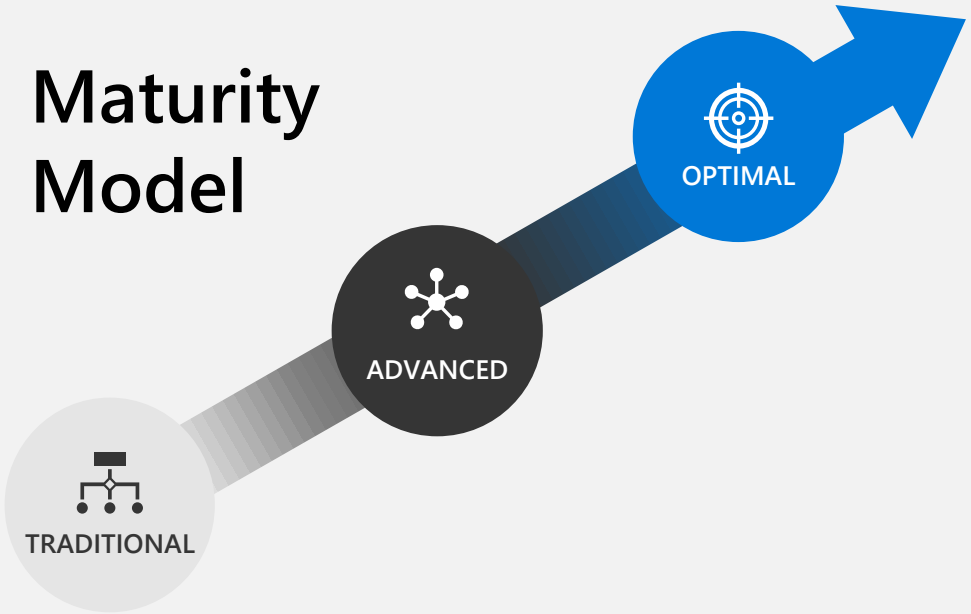
Get started modernizing identities and endpoints with FastTrack.

3

Advance your Zero Trust journey by diving deeper with us on a specific area.

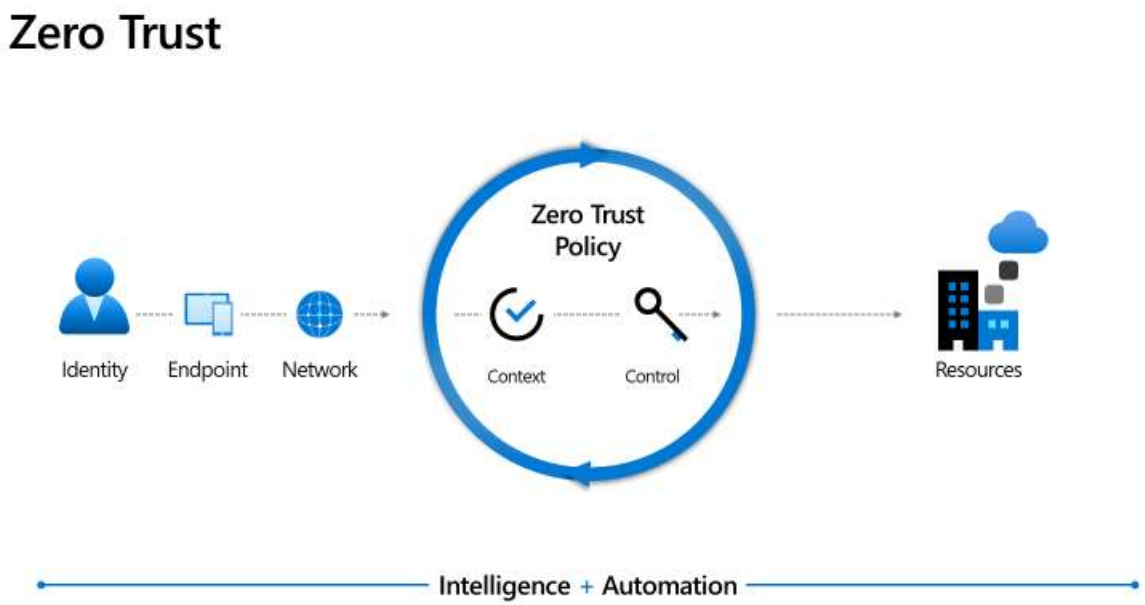
Making Zero Trust a reality

- Do you grok Zero Trust?
- Have you established a v-team with your stakeholders?
- Do you know where you want to arrive?
- Do you know where you are at today?
- Do you have buy-in from C-level to bridge that gap?



Download today at
aka.ms/ztmodel

Zero Trust networking maturity model



Traditional	Advanced	Optimal
Few network security perimeters and flat open network	cloud micro-perimeters with some micro-segmentation	ingress/egress cloud micro-perimeters and deeper micro-segmentation
Minimal threat protection and static traffic filtering	Cloud native filtering and protection for known threats	ML-based threat protection and filtering with context-based signals
Internal traffic is not encrypted	User to app internal traffic is encrypted	All traffic is encrypted
Many ingress/egress	Fully distributed	

Microsoft has rich set of cloud native services designed to help you move to zero trust model

Learn more about zero trust networking at https://www.microsoft.com/security/blog/2020/06/15/zero-trust-part-1-networking/
https://www.microsoft.com/en-us/security/zero-trust

Zero Trust Rapid Modernization Plan (RaMP)

Prioritize rapid progress on highest positive impact

Roll out to IT Admins first
- Targeted by Attackers
- High potential impact
- Provide technical feedback

Top Priorities – *critical security modernization steps*

User Access and Productivity

1. **Explicitly validate trust for all access requests (via Azure AD Conditional Access)**
   a. **User Accounts -** Require Passwordless or MFA for all users + measure risk with threat intelligence & behavior analytics
   b. **Devices -** Require device integrity for access (configuration compliance first, then XDR signals)
2. **Increase security for accessing key resources**
   a. **Apps –** Enable Azure AD for all SaaS, for VPN authentication, and publish legacy on-premises/IaaS via App Proxy
   b. **Data -** Discover and protect sensitive data (via Cloud App Security, CA App Control, Microsoft Info Protection)
3. **Governance** to continuously monitor security posture and reduce risk (via Secure Score)

Modernize Security Operations

4. **Streamline response** to common attacks with XDR for Endpoint/Email/Identity + Cloud (via M365 & Azure Defender)
5. **Unify Visibility** with modern Security Information and Event Management (SIEM via Azure Sentinel)
6. **Reduce manual effort -** using automated investigation/remediation, enforcing alert quality, & proactive threat hunting

As Needed – *typically driven by cloud adoption or OT/IoT usage*

Operational Technology (OT) and Industrial IoT

Discover – Find & classify assets with business critical, life safety, and operational/physical impact (via Azure Defender for IoT)

Protect – isolate assets from unneeded internet/production access with static and dynamic controls

Monitor – unify threat detection and response processes for OT, IT, and IoT assets (via Azure Defender for IoT)

Datacenter & DevOps Security

Security Hygiene – Rigorously monitor + remediate security configurations, security updates, MFA, and more

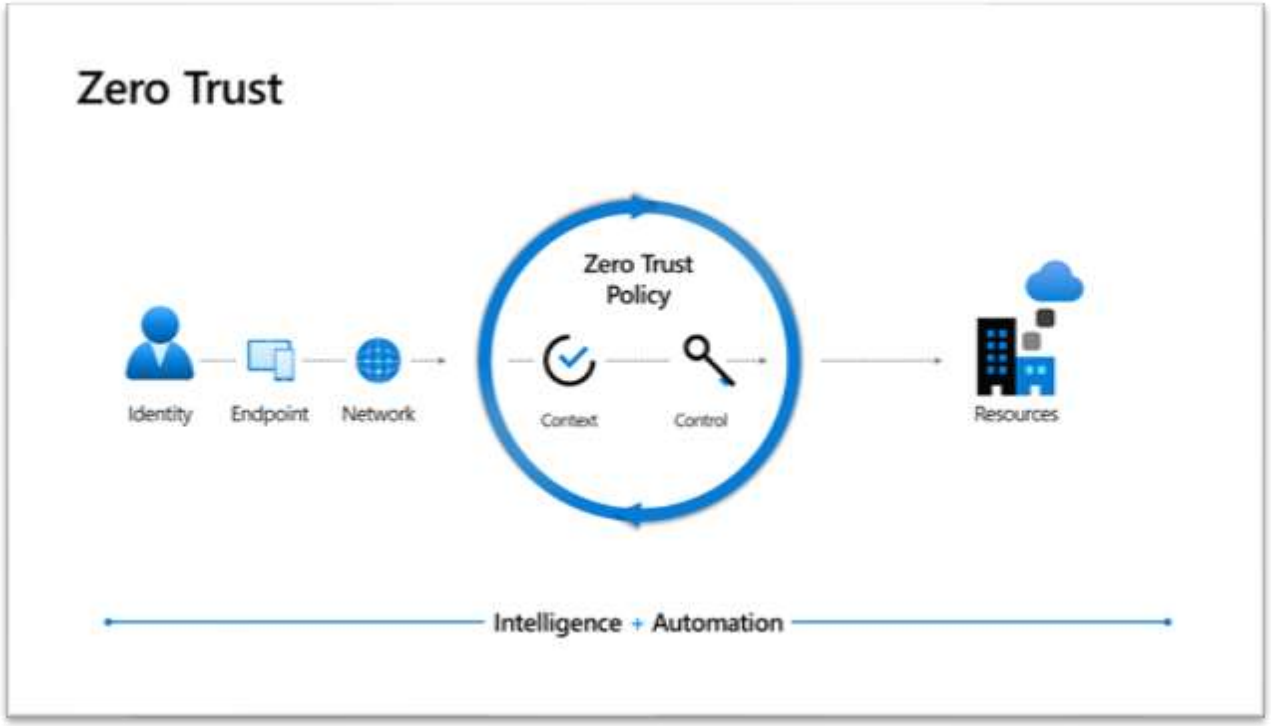
Reduce Legacy Risk – Retire or isolate legacy technology (Unsupported OS/Applications, legacy protocols)

DevOps Integration – Integrate infrastructure + development security practices into DevOps with minimal friction

Microsegmentation – Additional *identity and network* restrictions (dynamic trust-based and/or static rules)

ZT builds on classic security
Align to cloud migration schedule

Zero Trust Resources



- Zero Trust page: https://aka.ms/zerotrust
- Business Plan: aka.ms/ZTbizplan
- Zero Trust maturity model: https://aka.ms/ztmodel
- Zero Trust assessment: https://aka.ms/zttool
- Zero Trust deployment guidance: https://aka.ms/ztblogs
- Implementing a Zero Trust security model at Microsoft **LINK**
- Microsoft's approach to Zero Trust Networking and supporting Azure technologies LINK
- Microsoft helps employees work securely from home using a Zero Trust strategy LINK

- Zero Trust: Security Through a Clearer Lens session (Recording | Slides)
- CISO Workshop Slides/Videos
- Microsoft's IT Learnings from (ongoing) Zero Trust journey

Zero Trust Program Approach (Example)

Sprint 0

3-4 weeks | **2 weeks**

Discovery | Sprint planning

Day 1	6 to 9 days	2 Weeks	2 Weeks
Zero Trust Program Initiation (This workshop)	• Governance (½ - 1 day) • Identities (1 – 1½ day) • Devices (½ - 1 day) • Apps (½ - 1 day) • Infrastructure (1 day) • Network (1 day) • Data (½ - 1 day) • Security Management (1 – 1½ day)	Zero Trust Maturity Assessment Program Roadmap	Delivery Sprints planning
Key Outcomes	Briefings, Maturity Scoring	Roadmap	Milestone Plan, Backlog
Kick-Off	**Workshops & Deep Dives**	**Program Tracks**	**Sprint Planning**
• Customer Objectives Workshop • Microsoft and Zero Trust Brief • Review Pre-Engagement Questionnaire • Introduction to Agile Delivery Approach	• Topic-focused strategic and technical discovery/briefings aligned to Zero Trust/Microsoft Secure Pillars • Capabilities and Personas Selection • Technology and capability deep dives • Define and structure Objectives and Key Results (OKR's) • Clear set of outcomes defined in Azure DevOps (ADO)	• Program Roadmap by track • Report out to key stakeholders • Recommendations and priority delivery • Create a Risk Register to capture any blockers during the Zero Trust Journey	• Sprint Plan define & prioritize epics • Sprint Solution Backlog • Establish Tooling • Define Sprint Burndown

Sprint Program

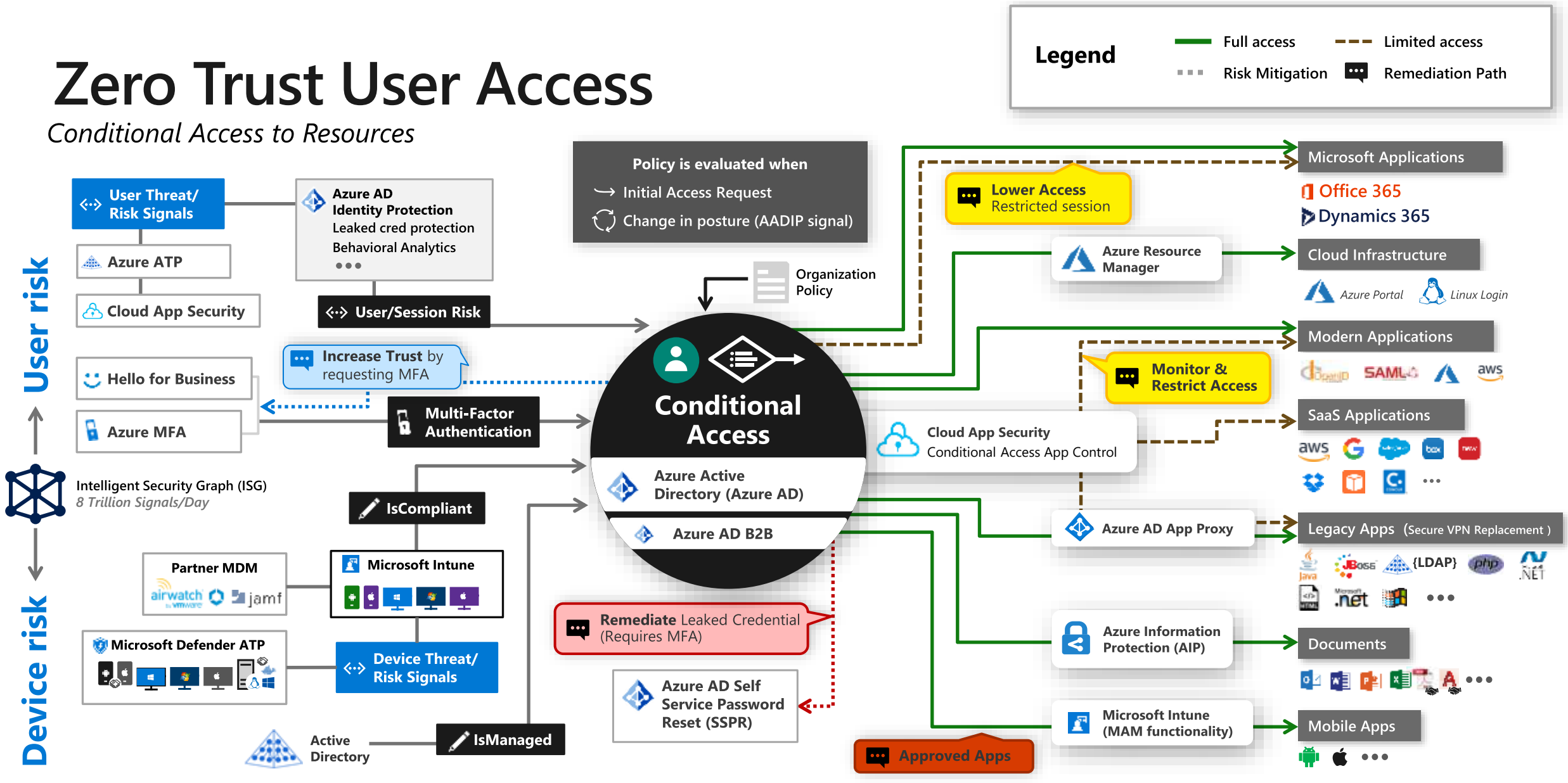
***n* weeks**

Epics

4 Weeks	4 Weeks
Delivery Sprints	
Sprint Reporting	Sprint Reporting
Sprint 1	**Sprint *n***
• Daily Standups • Demonstration • Retrospective • Sprint 1+ planning • Increment 1	• Daily Standups • Demonstration • Retrospective • Sprint 1+ planning • Increment N

Zero Trust User Access

Conditional Access to Resources



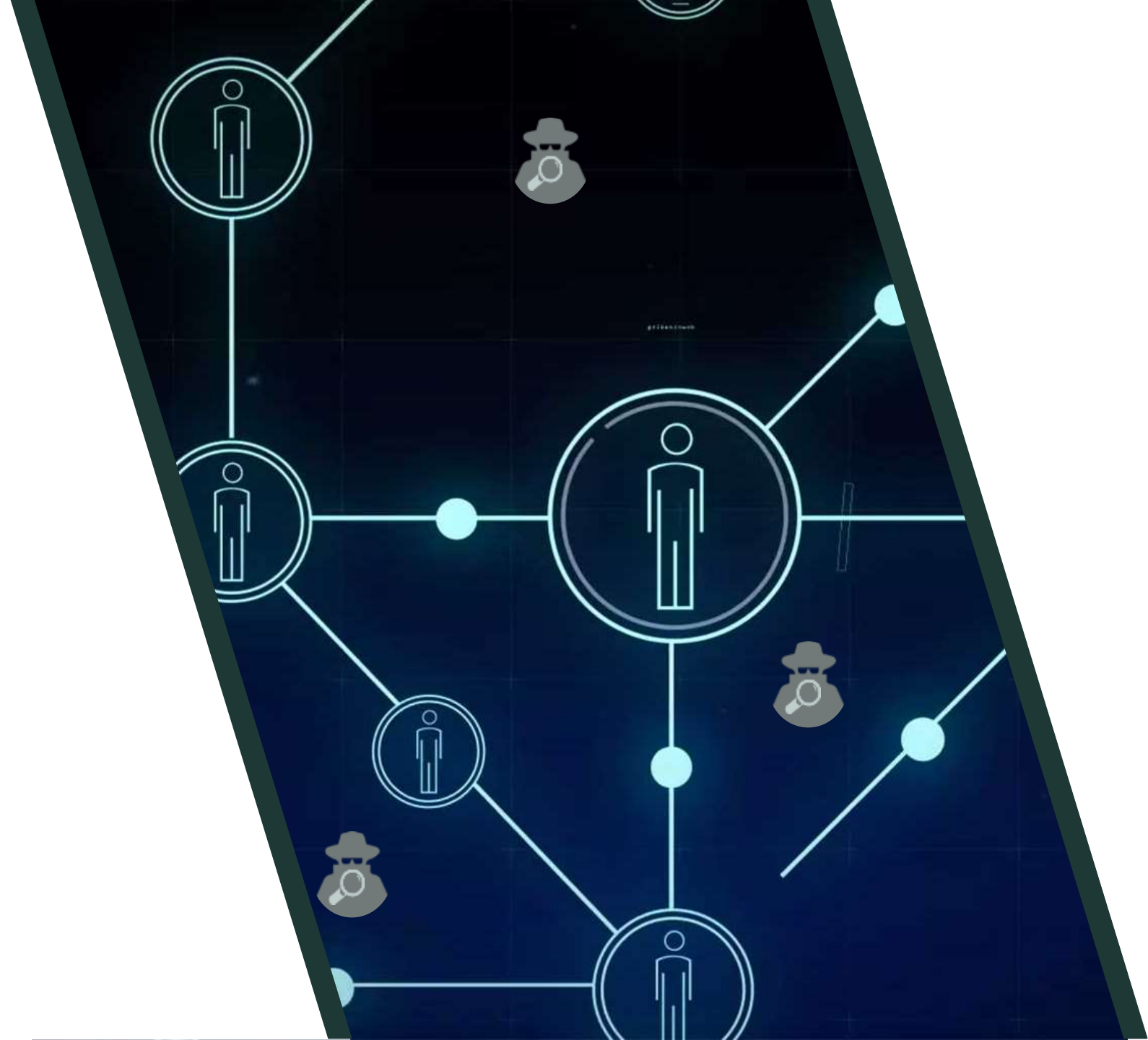
Signal
to make an informed decision

Decision
based on organizational policy

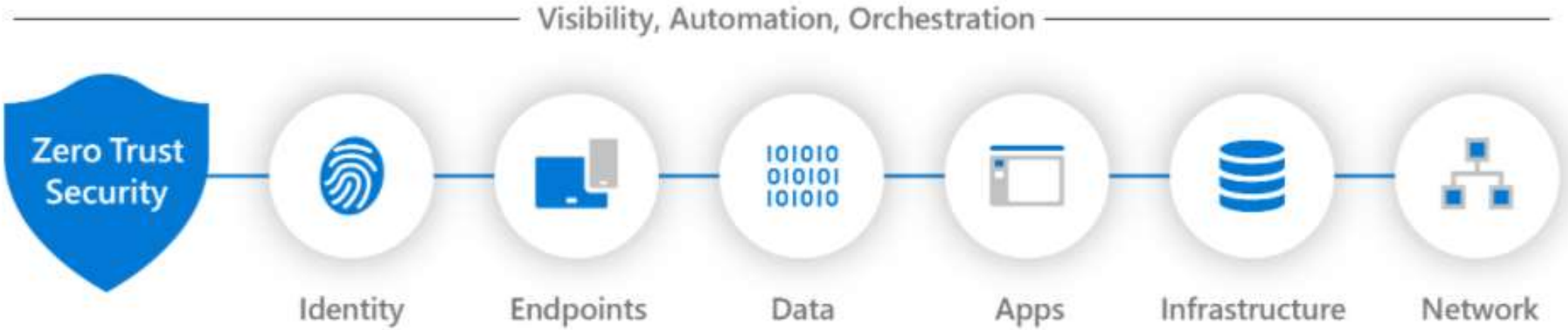
Enforcement
of policy across resources

Microsoft

Zero Trust and Microsoft Controls across M365 & Azure



Assess Zero Trust readiness and build a plan

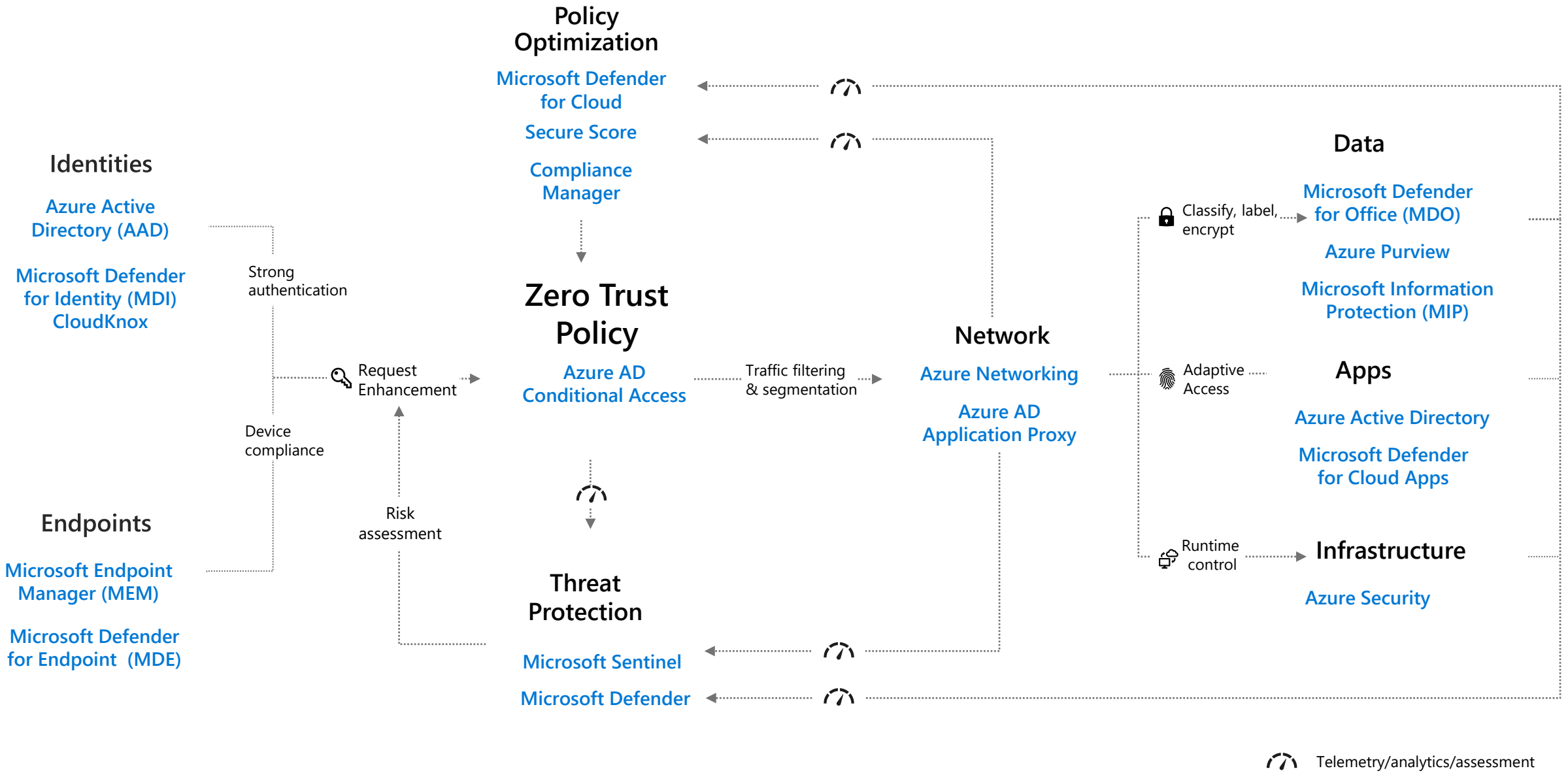


Guiding principles of Zero Trust

Verify explicitly	Use least privileged access	Assume breach
Always authenticate and authorize based on all available data points.	Limit user access with Just-In-Time and Just-Enough-Access (JIT/JEA), risk-based adaptive policies, and data protection.	Minimize blast radius and segment access. Verify end-to-end encryption and use analytics to get visibility, drive threat detection, and improve defenses.

Microsoft Zero Trust architecture

Microsoft Security



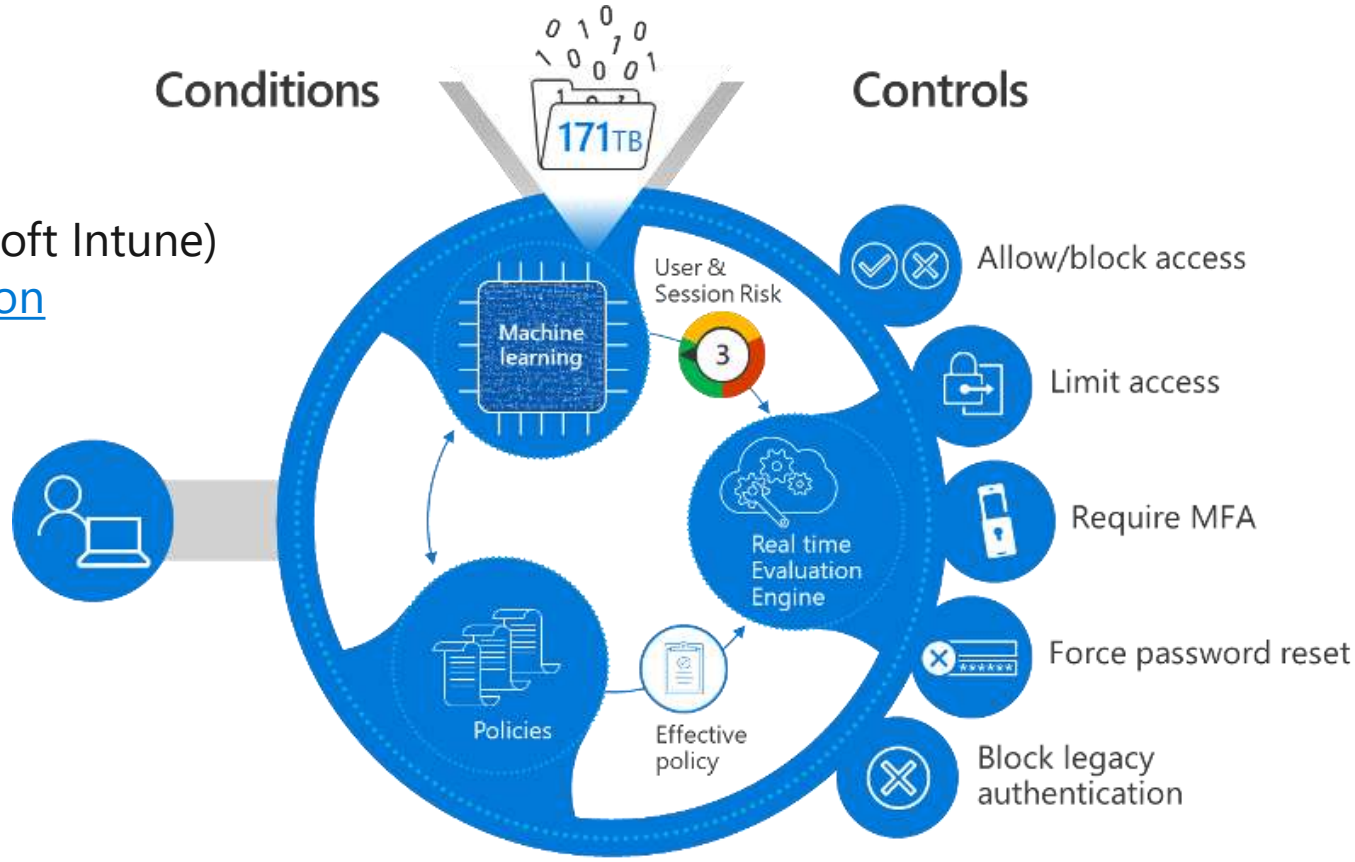
Securing identity with Zero Trust

Microsoft Azure

- Azure Active Directory
- Azure Advanced Threat Protection

Microsoft 365

- Microsoft Endpoint Manager (includes Microsoft Intune)
- Microsoft Defender Advanced Threat Protection
- SharePoint Online
- Exchange Online



https://docs.microsoft.com/en-us/security/zero-trust/identity

Secure endpoints with Zero Trust

Microsoft Azure

- Azure Active Directory

Microsoft 365

- Microsoft Endpoint Manager (includes Microsoft Intune and Configuration Manager)
- Microsoft Defender Advanced Threat Protection
- BitLocker

https://docs.microsoft.com/en-us/security/zero-trust/endpoints

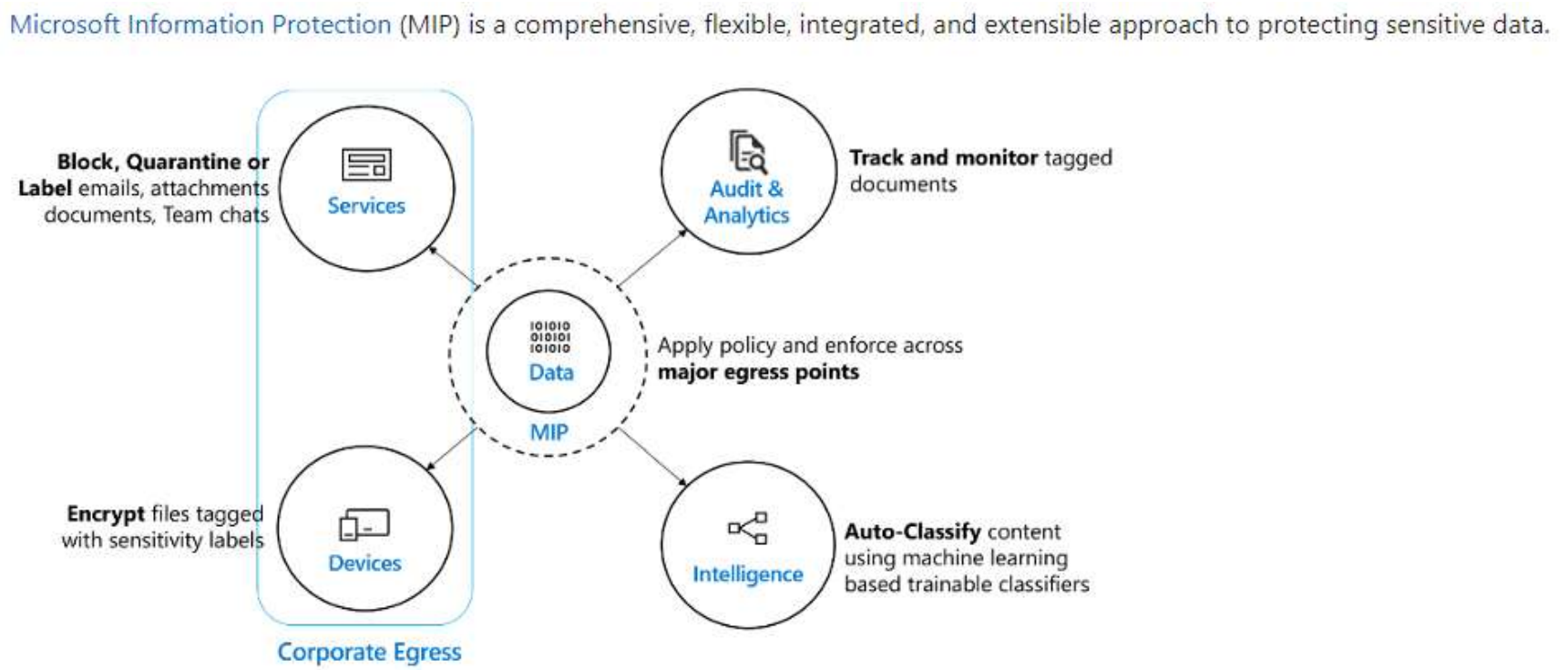
Secure data with Zero Trust

Microsoft Azure

- Azure Information Protection with Unified Labeling Client and Scanner

Microsoft 365

- Microsoft Cloud App Security



https://docs.microsoft.com/en-us/security/zero-trust/data

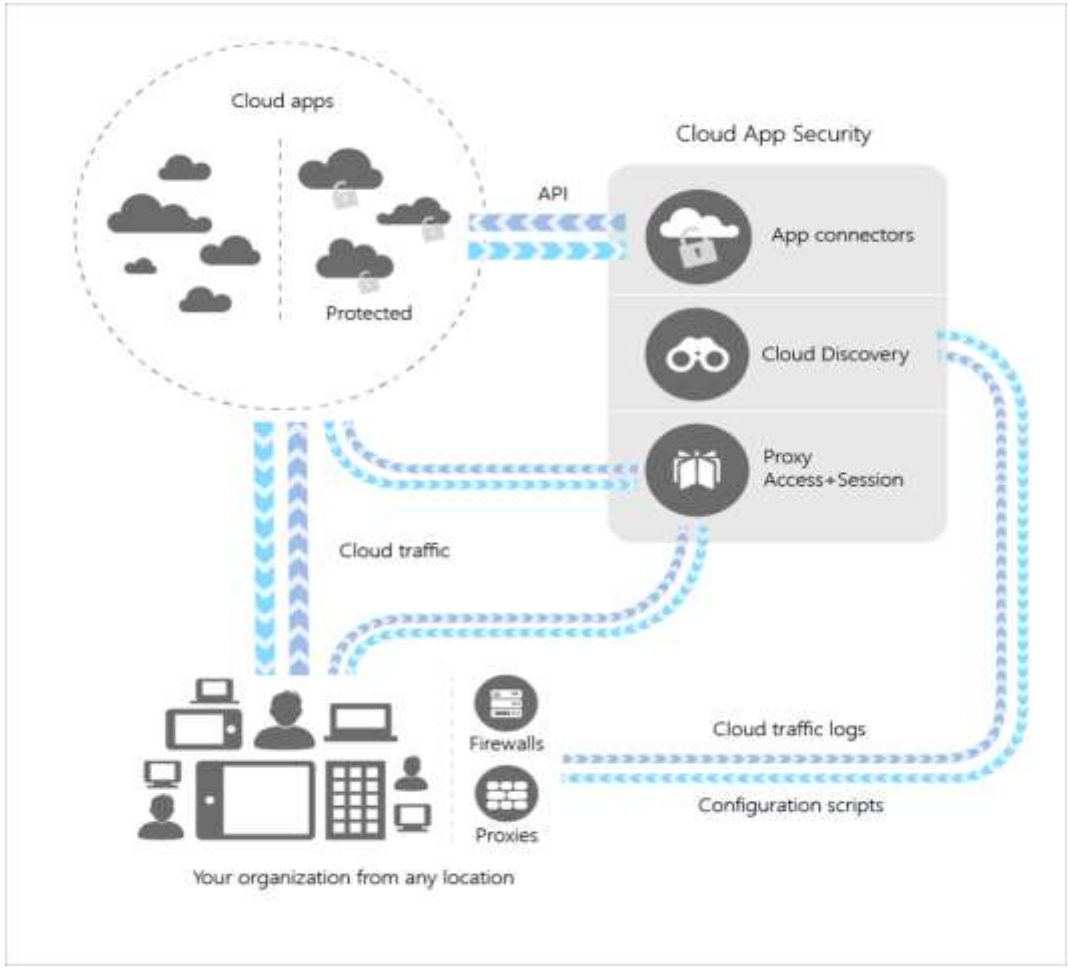
Secure applications with Zero Trust

Microsoft Azure

- Microsoft Azure Active Directory

Microsoft 365

- Microsoft Cloud App Security
- Cloud Discovery
- Microsoft Endpoint Manager (includes Microsoft Intune Configuration Manager)
- Mobile Application Management

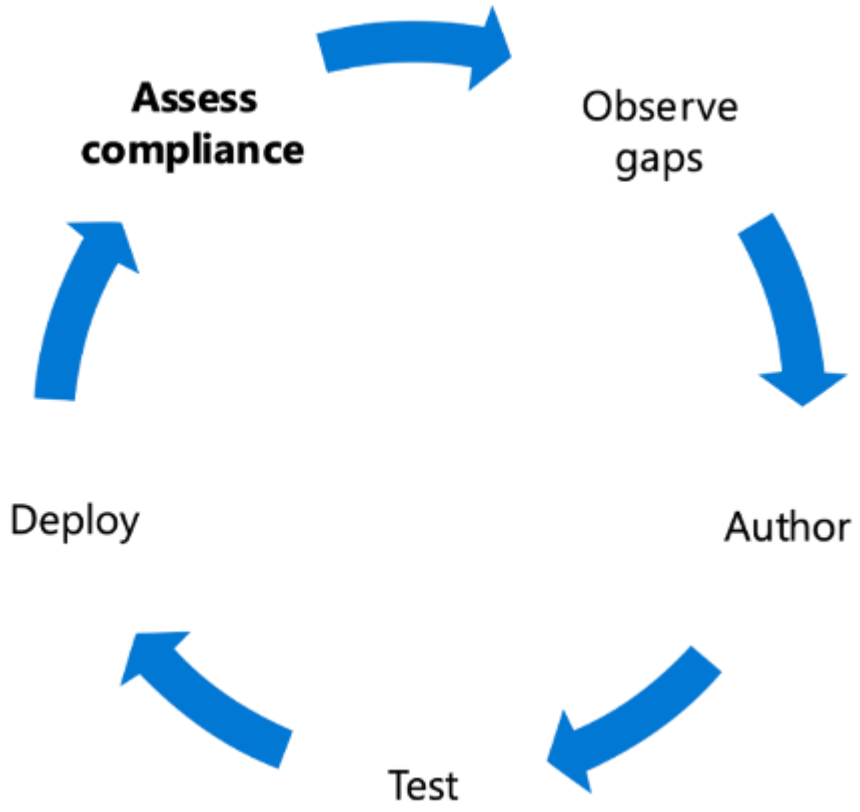


https://docs.microsoft.com/en-us/security/zero-trust/applications

Secure infrastructure with Zero Trust

Microsoft Azure

- Azure Blueprints
- Azure Policy
- Azure Arc
- Azure Security Center (ASC)
- Azure Sentinel
- Azure Resource Manager (ARM) templates

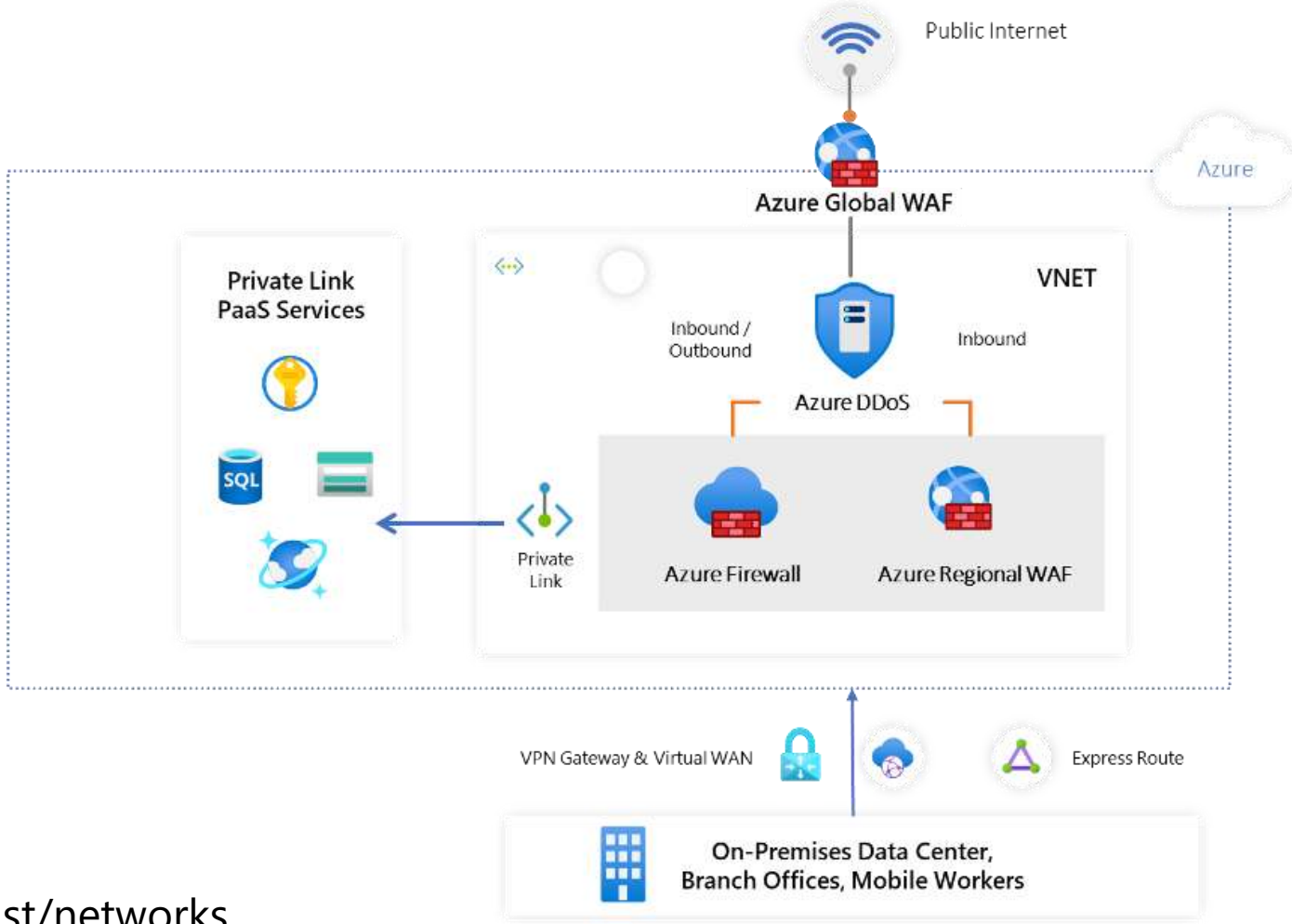


https://docs.microsoft.com/en-us/security/zero-trust/infrastructure

Secure networks with Zero Trust

Microsoft Azure

- Azure Networking
- Virtual Networks and Subnets
- Network Security Groups and
- Application Security Groups
- Azure Firewall
- Azure DDoS Protection
- Azure Web Application Firewall
- Azure VPN Gateway
- Azure ExpressRoute
- Azure Network Watcher



https://docs.microsoft.com/en-us/security/zero-trust/networks

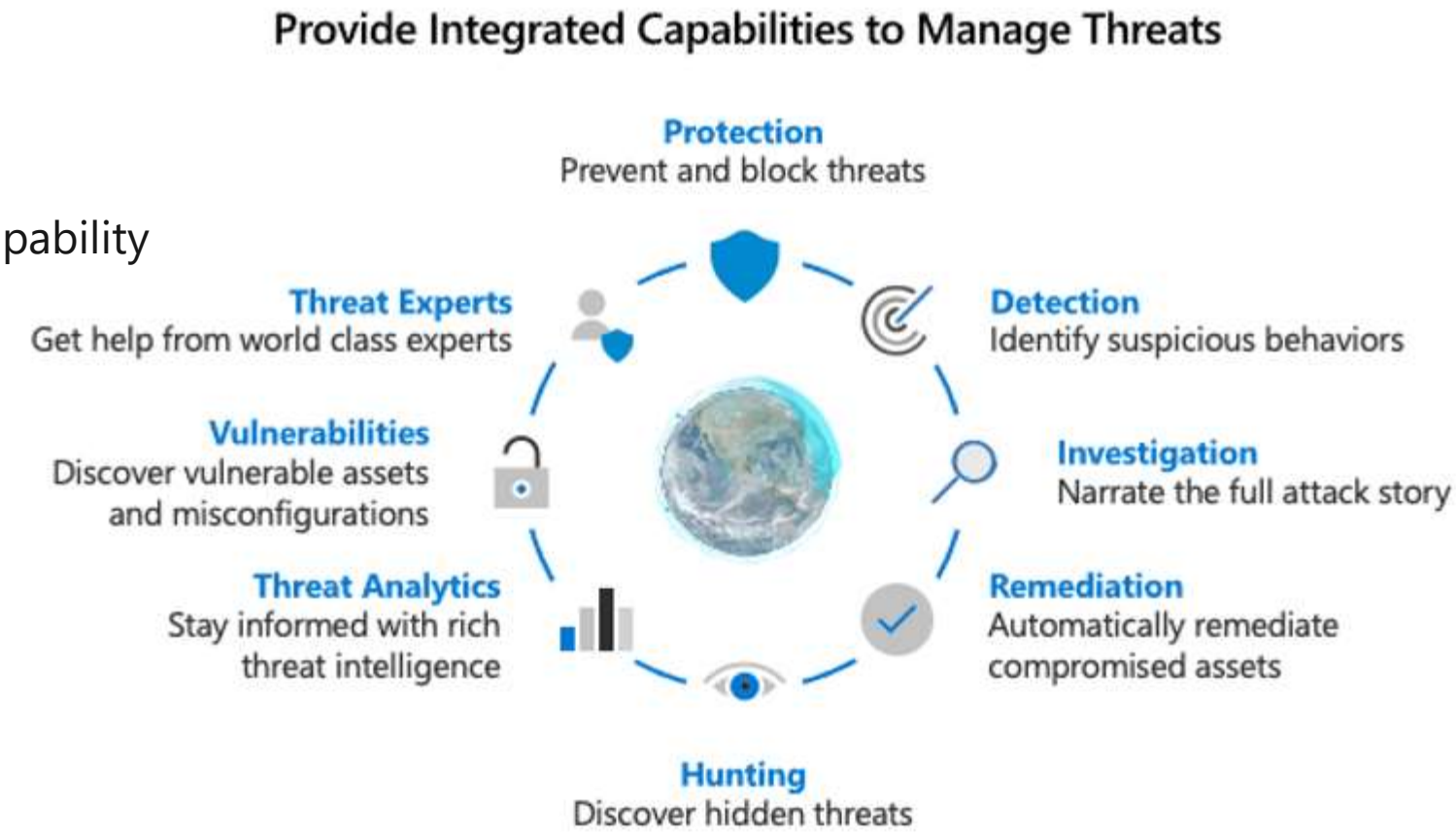
Visibility, automation, and orchestration with Zero Trust

Microsoft Azure

- Azure Advanced Threat Protection
- Azure Sentinel

Microsoft 365

- Microsoft Threat Protection - > XDR Capability



https://docs.microsoft.com/en-us/security/zero-trust/visibility-automation-orchestration

Microsoft Zero Trust Controls

Microsoft control	Build an identity perimeter	Secure the common control plane	Least privilege access to sanctioned apps	Data is protected wherever is flows	Protect resources, not networks	Healthy devices wherever they roam
Azure AD Identity Protection	✓	✓				
Conditional Access	✓	✓				
Azure ATP	✓					
Azure Password Protection	✓					
Hello for Business	✓	✓				
Azure MFA	✓	✓				
RBAC	✓	✓	✓	✓	✓	✓
Azure AD PIM	✓	✓				
Active Directory (PAW & Tier Model)	✓	✓				
Credential Guard	✓					✓
MCAS	✓		✓	✓		
Cloud Infrastructure (Subscription, Resource Group, vNet, NSG, ASG, ExpressRoute, VPN Gateway, Azure Firewall, Azure Automation, Azure Blueprints, Azure DevOps, Azure Disk Encryption, ExpressRoute, Storage ATP)		✓	✓	✓	✓	
Resource Group			✓	✓		
Office 365 ATP	✓			✓		✓
Data Loss Prevention				✓		
Microsoft Information Protection				✓		
Defender Firewall					✓	✓
Microsoft Defender ATP						✓
Intune	✓		✓			✓
Exploit Guard	✓		✓	✓	✓	✓
Bitlocker				✓		✓
Advanced Audit	✓		✓	✓		
Azure Security Centre	✓	✓	✓	✓	✓	✓
Azure Log Analytics	✓	✓	✓	✓	✓	✓
Azure Sentinel	✓	✓	✓	✓	✓	✓
Azure ARC	✓	✓	✓	✓	✓	✓
Azure Lighthouse	✓	✓	✓	✓	✓	✓
Intelligent Security Graph	✓	✓	✓	✓	✓	✓

Thank you

Understanding SASE

Organizations are learning about SASE architecture and how it complements and leverages the Zero Trust approach

(Pronounced “Sassy”)

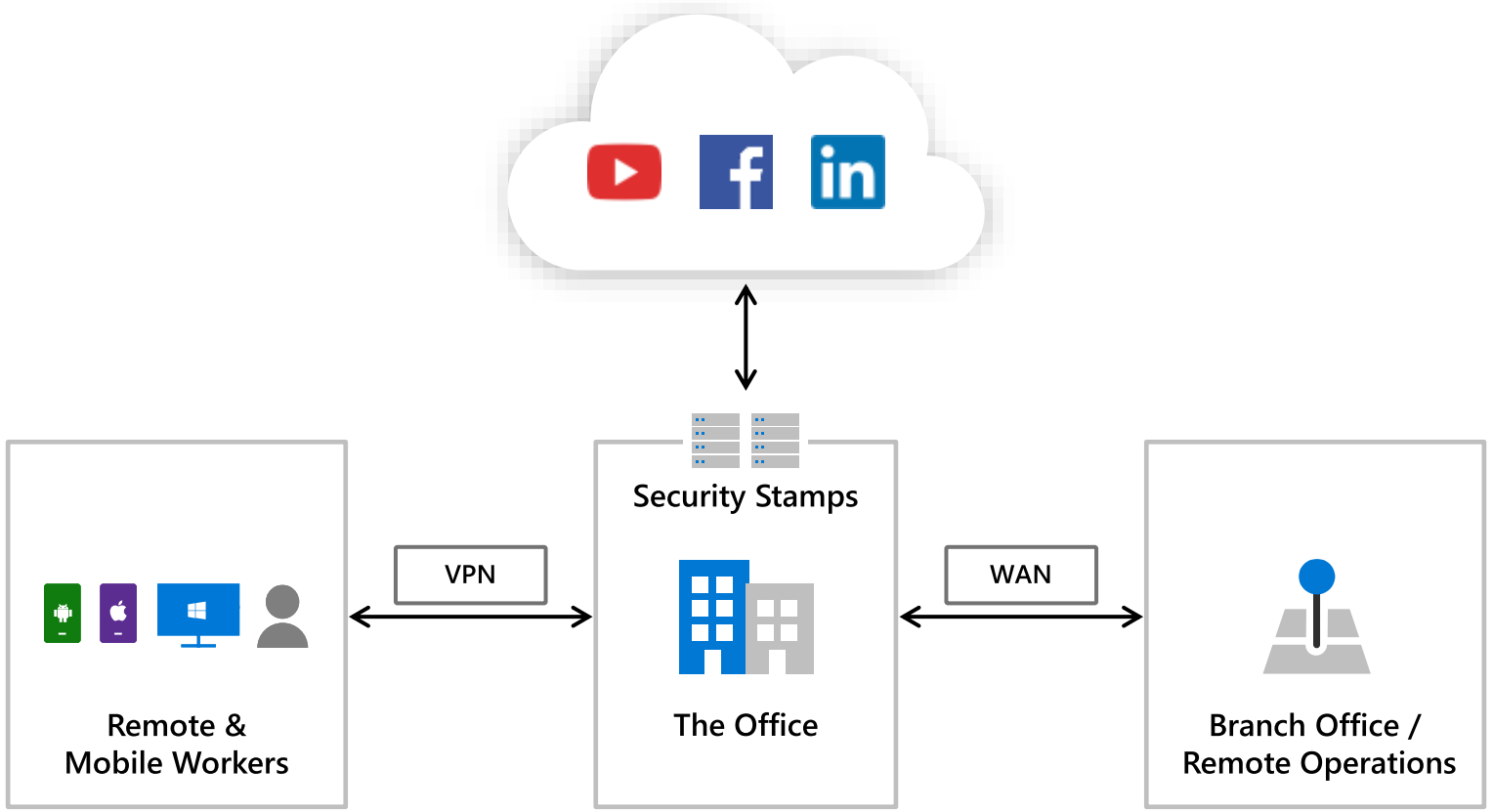
Start with a Zero Trust Approach

Increase security assurances for your critical business assets

Zero Trust

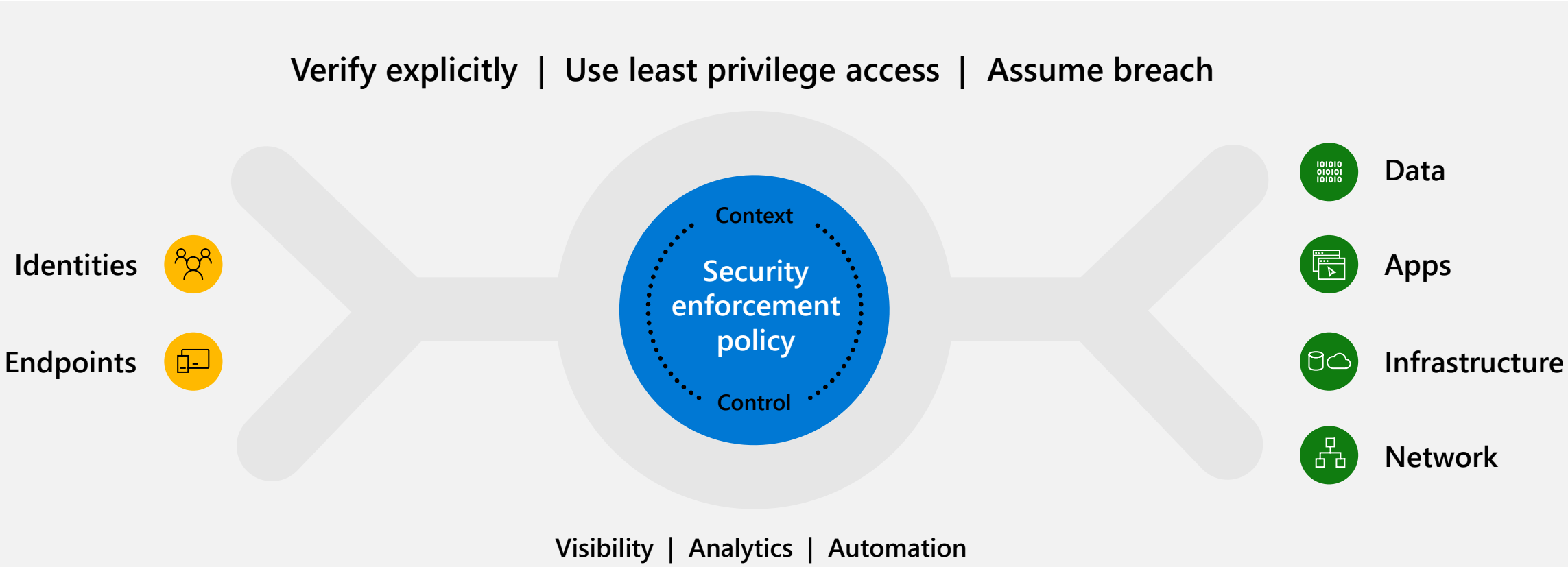
A proactive approach to security that uses adaptive controls and continuous verification to prevent and respond to threats more quickly and efficiently

Traditional networking model



Start with a Zero Trust Approach

Increase security assurances for your critical business assets



Secure Access Service Edge (SASE)

SASE is a cloud-based architecture that converges network and security services into a cloud-delivered service model.

The SASE architecture is enabled through a set of capabilities/products while adhering to the Zero Trust principles.

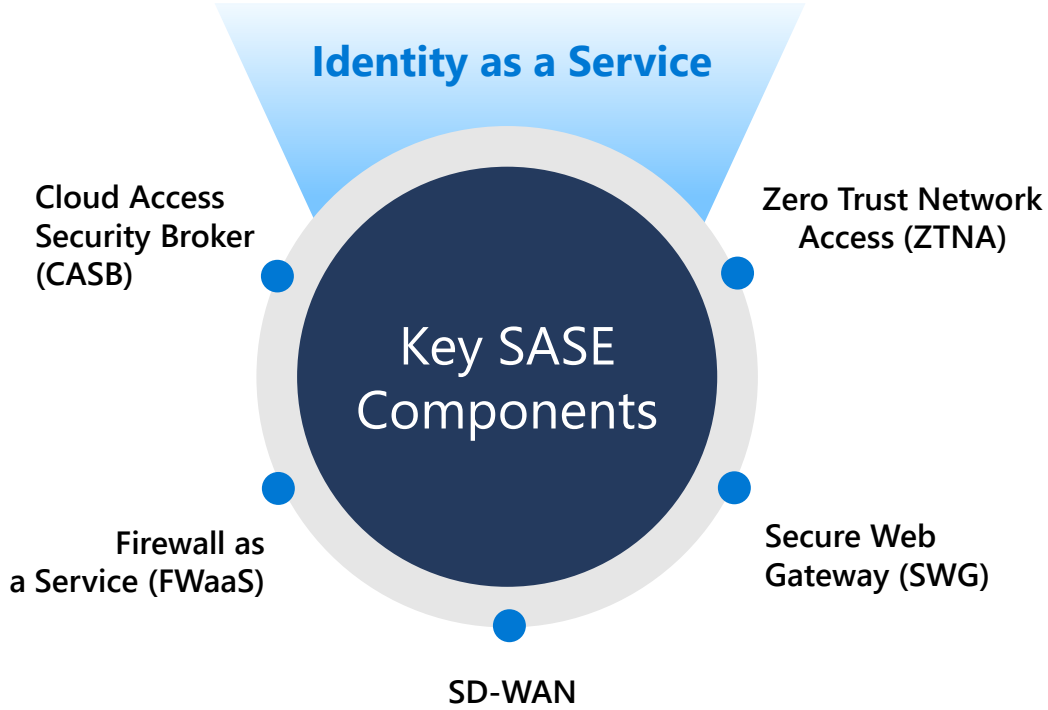
SASE capabilities are evolving in the market. Start on the SASE journey with Microsoft and partner solutions to achieve your business goals.

Secure Access Service Edge (SASE) uses Zero Trust Principles

Verify explicitly

Use least privilege access

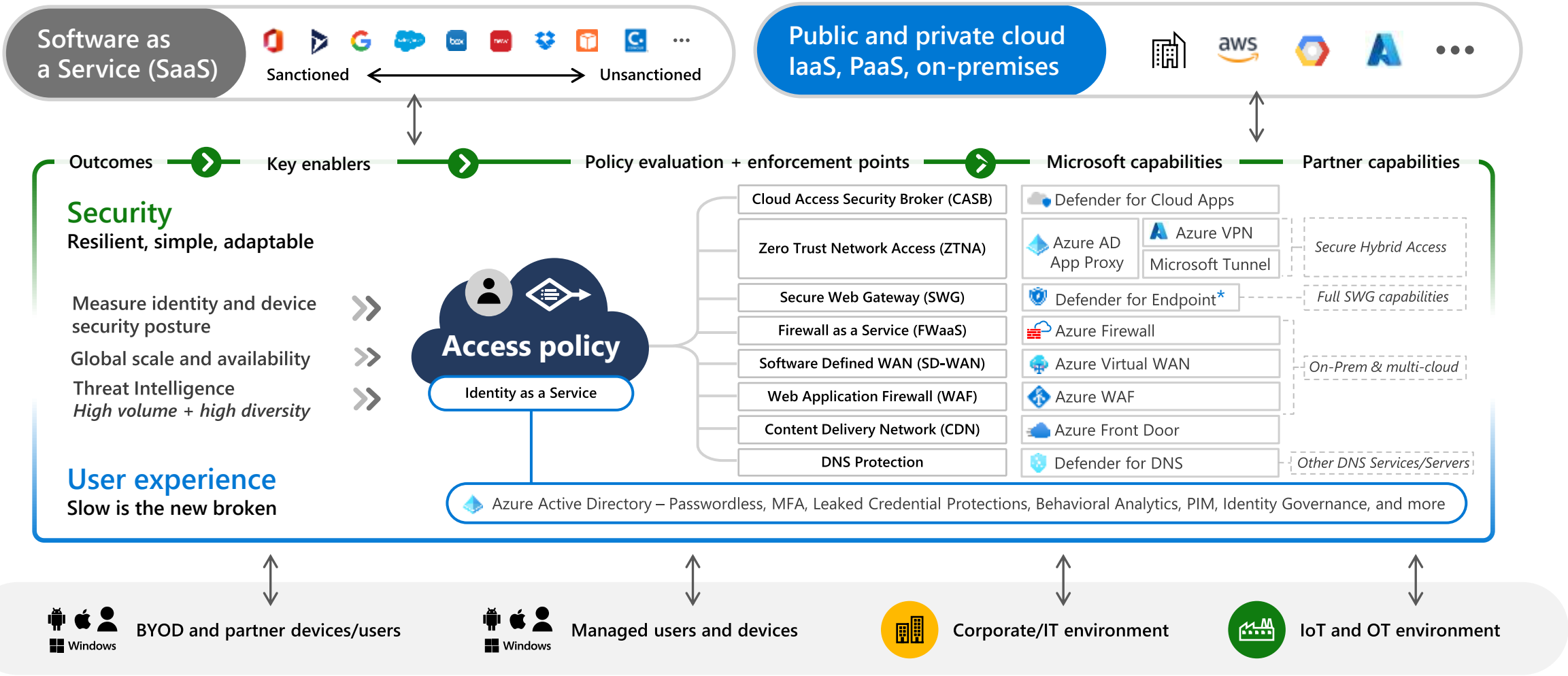
Assume breach



Secure access to resources based on identity, real-time context and security/compliance policies

Microsoft and partner solutions for SASE

Architecture for secure, responsive, and pervasive productivity

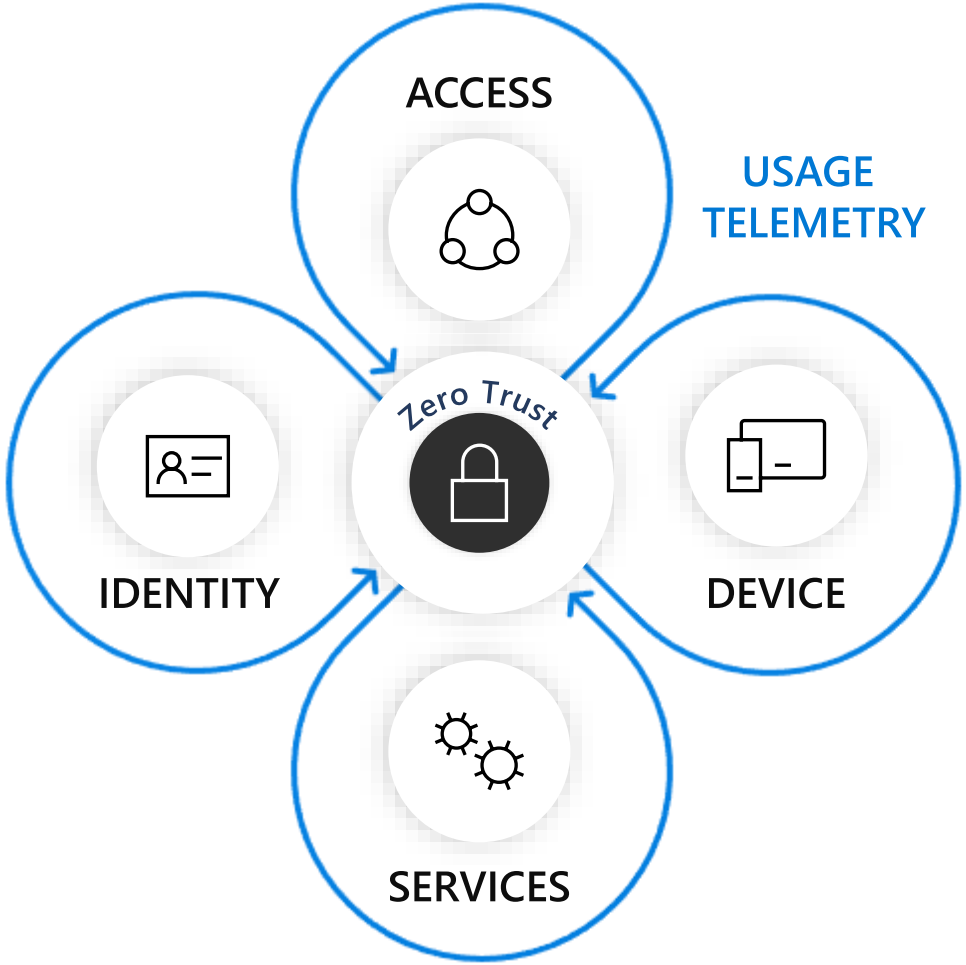


*Microsoft Defender for Endpoint (MDE) addresses many of the use-cases of an internet gateway solution and works with MISA partners to provide full SWG capabilities

How Microsoft achieved “Zero Trust”?

“Strong identity + device health + least privilege user access & verified with telemetry”

- ✓ Assets are moved from the internal network to the internet… except for the most critical assets
- ✓ Enhanced user experience with Internet First
- ✓ Reduced attack surface of the environment
- ✓ Comprehensive telemetry, artificial intelligence for anomaly detection, service health verification



Major phases of zero trust networking

Pre-Zero Trust

- ✗ Device management isn't required
- ✗ Single factor authentication to resources
- ✓ Capability to enforce strong identity exists
- ✓ Data classification and information protection exists

Verify identity

- ✓ Strong identity is verified and enforced
- ✓ Passwords are eliminated in favor of biometrics
- ✓ Access to applications and data is limited to minimum required to perform job function

Verify device

- ✓ Client device health is enforced
- ✓ Unmanaged devices have secure alternative access methods
- ✓ Users don't have administrative permissions on client devices

Verify access

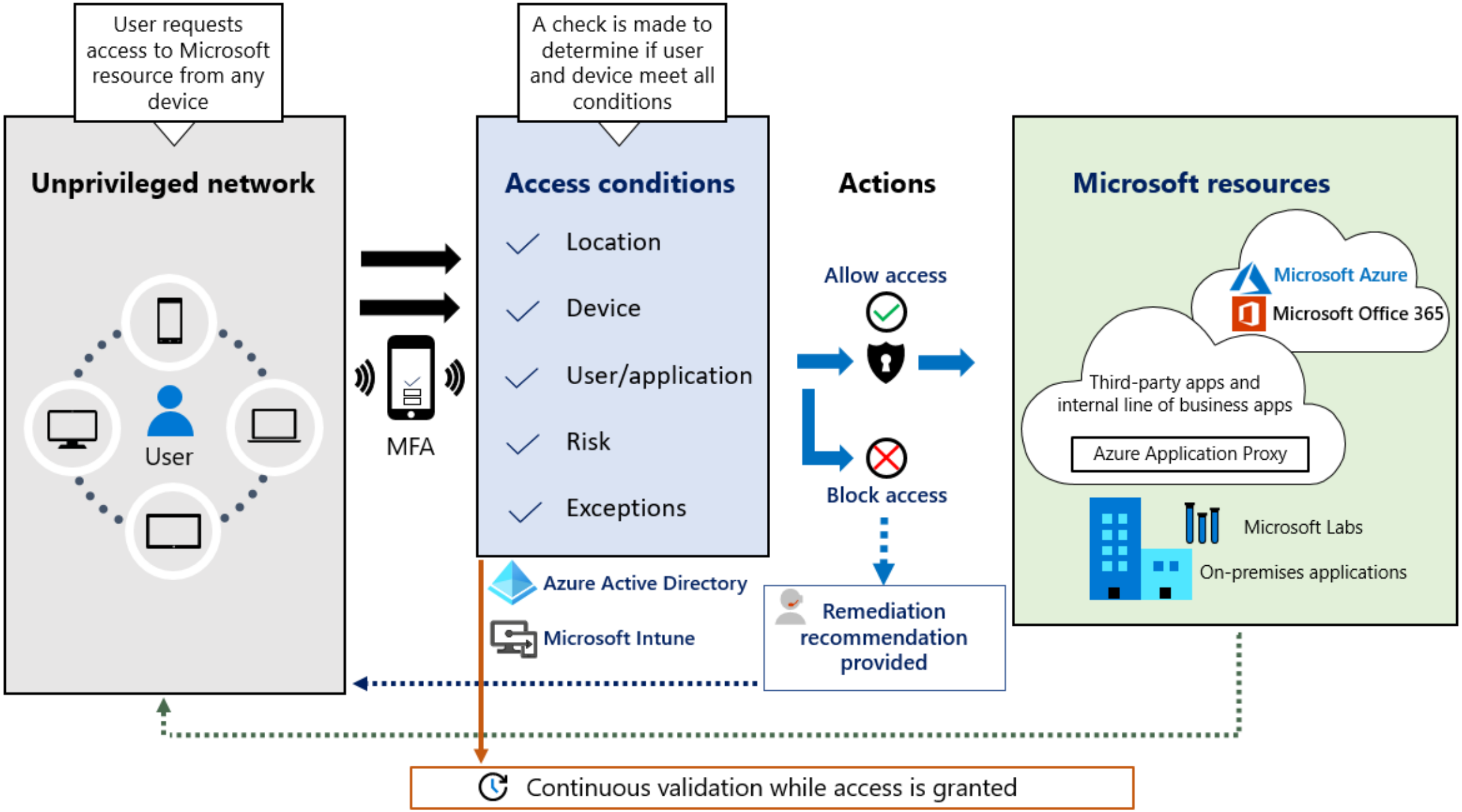
- ✓ Internet is the default network in all Microsoft office locations
- ✓ Network segmentations are built based on role and function

Verify services

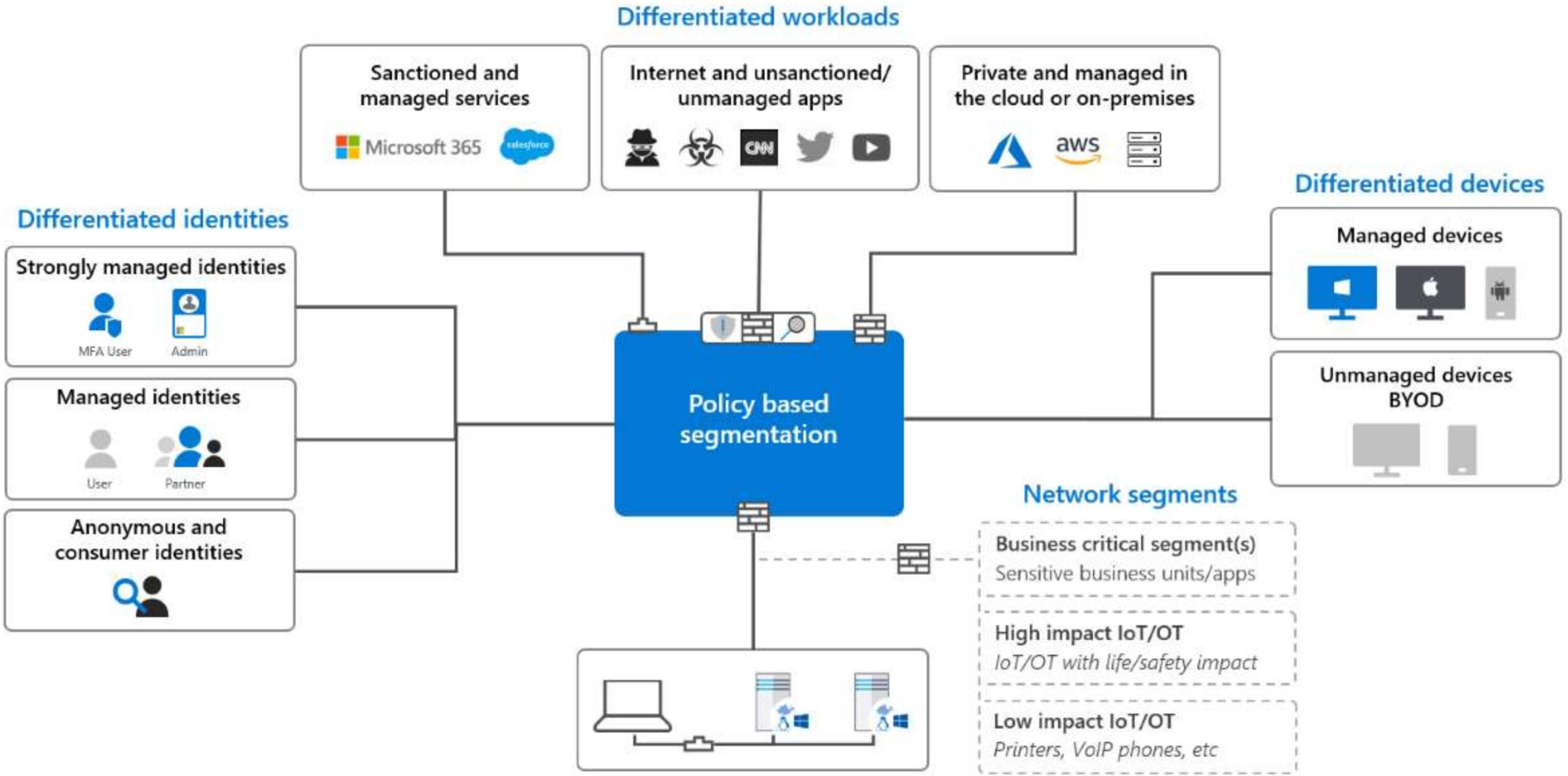
- ✓ Applications and conditions are enforced using conditional access
- ✓ Applications and services are accessible directly from the internet

Pervasive telemetry

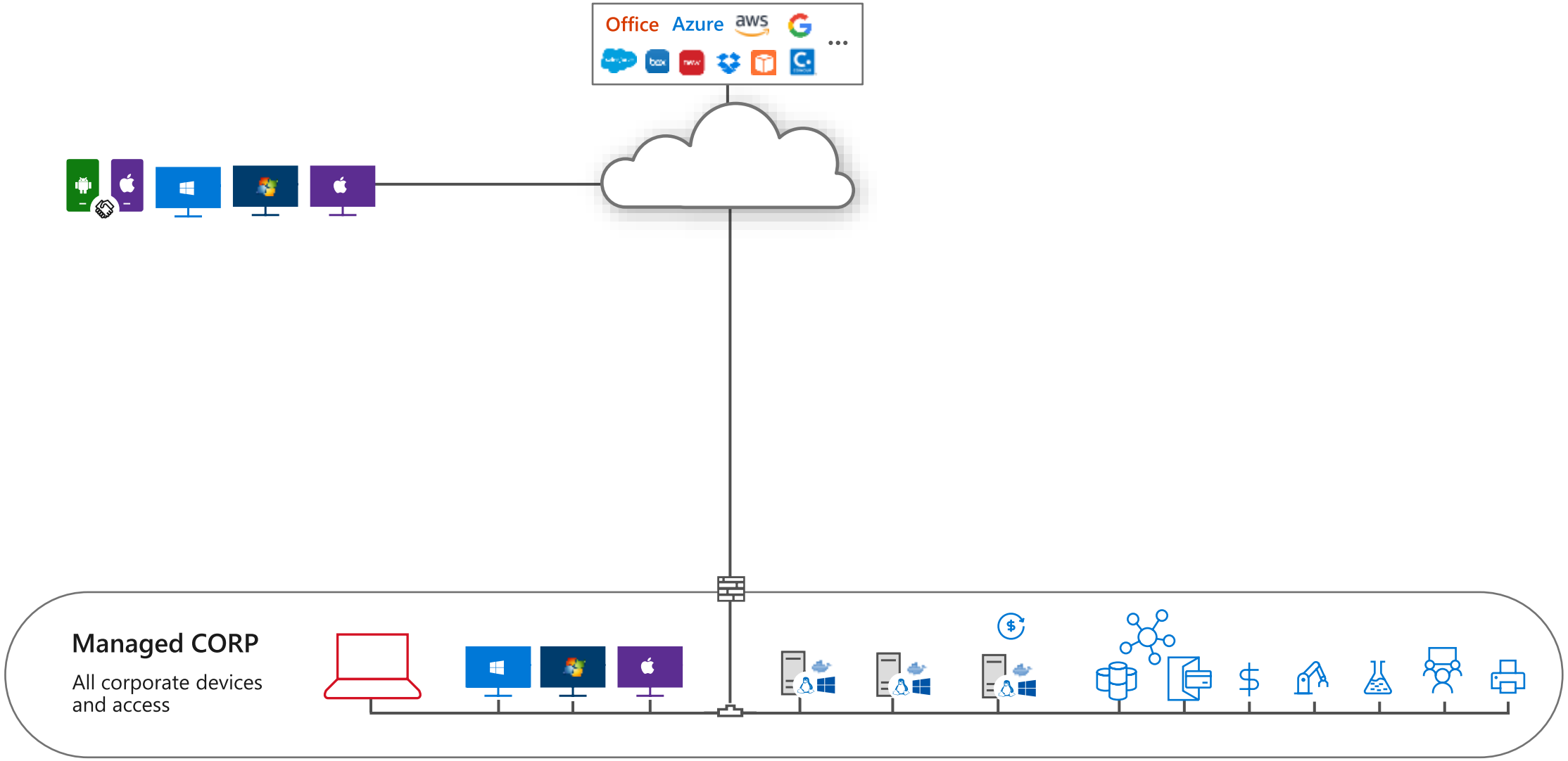
Microsoft's Zero Trust Architecure



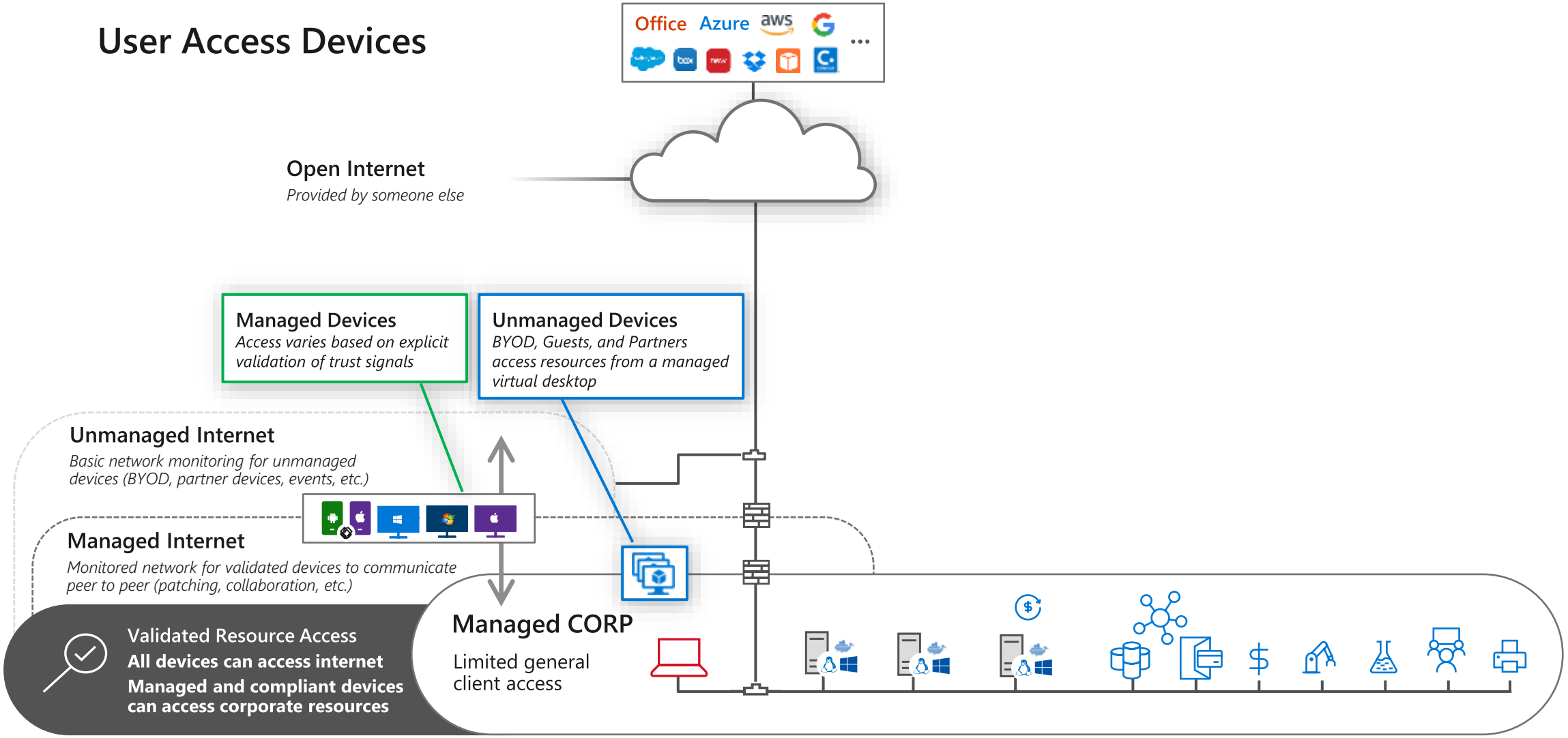
Zero Trust- Network segmentation transformation



Typical ‘Flat’ Network

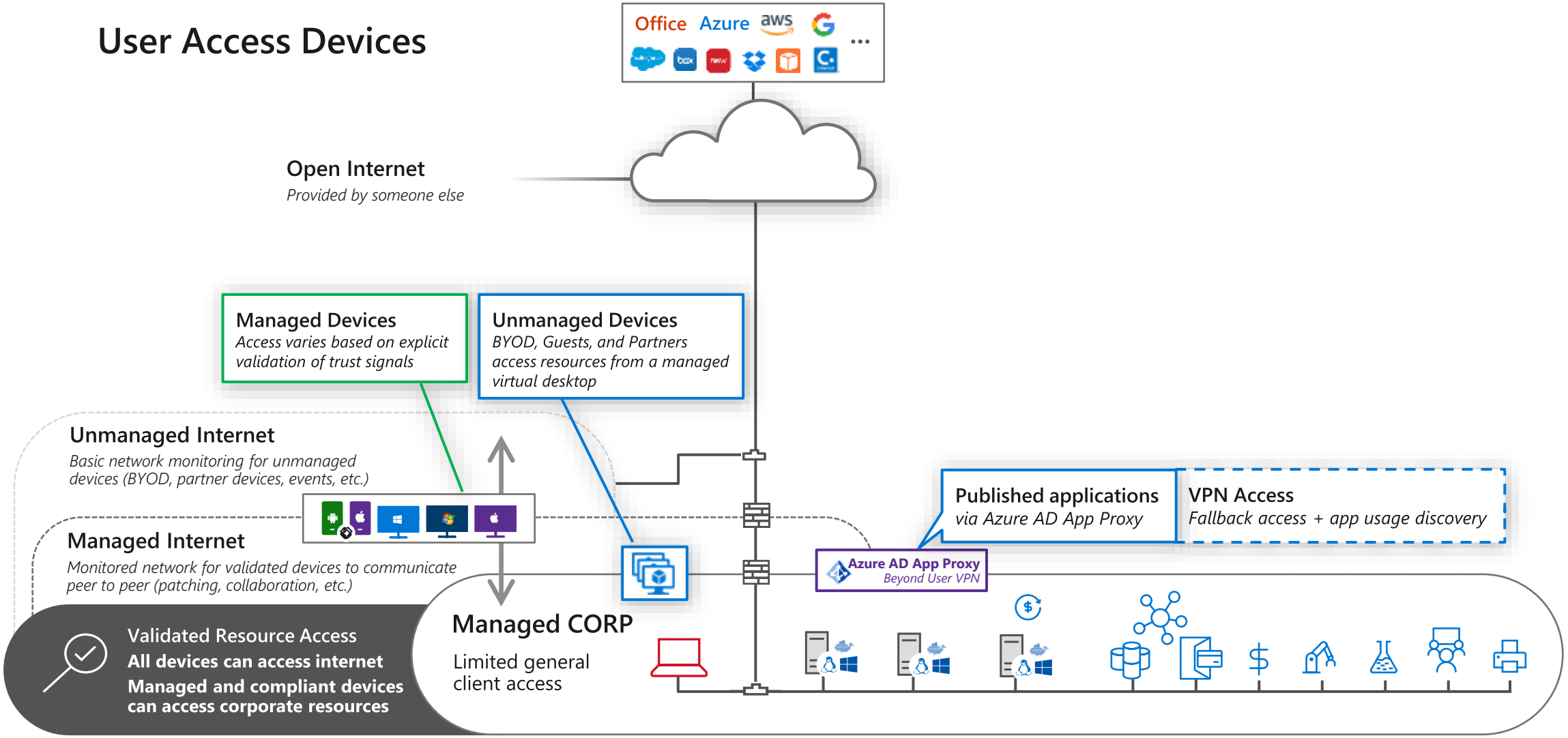


Zero Trust – Client Security Transformation



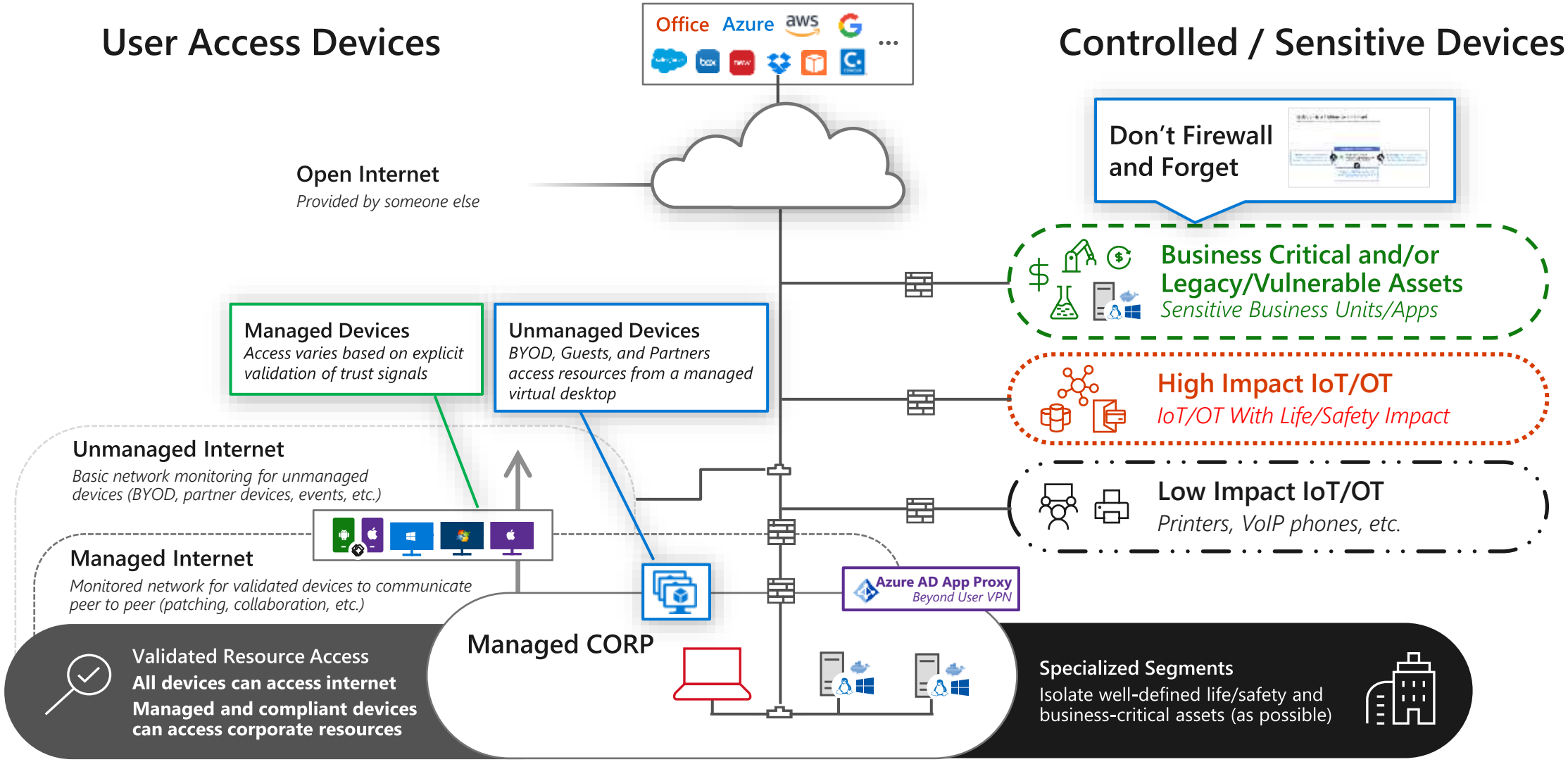
Spans on-premises & Azure environments

Zero Trust – App Access for Clients



Spans on-premises & Azure environments

Zero Trust – Network Segment Transformation

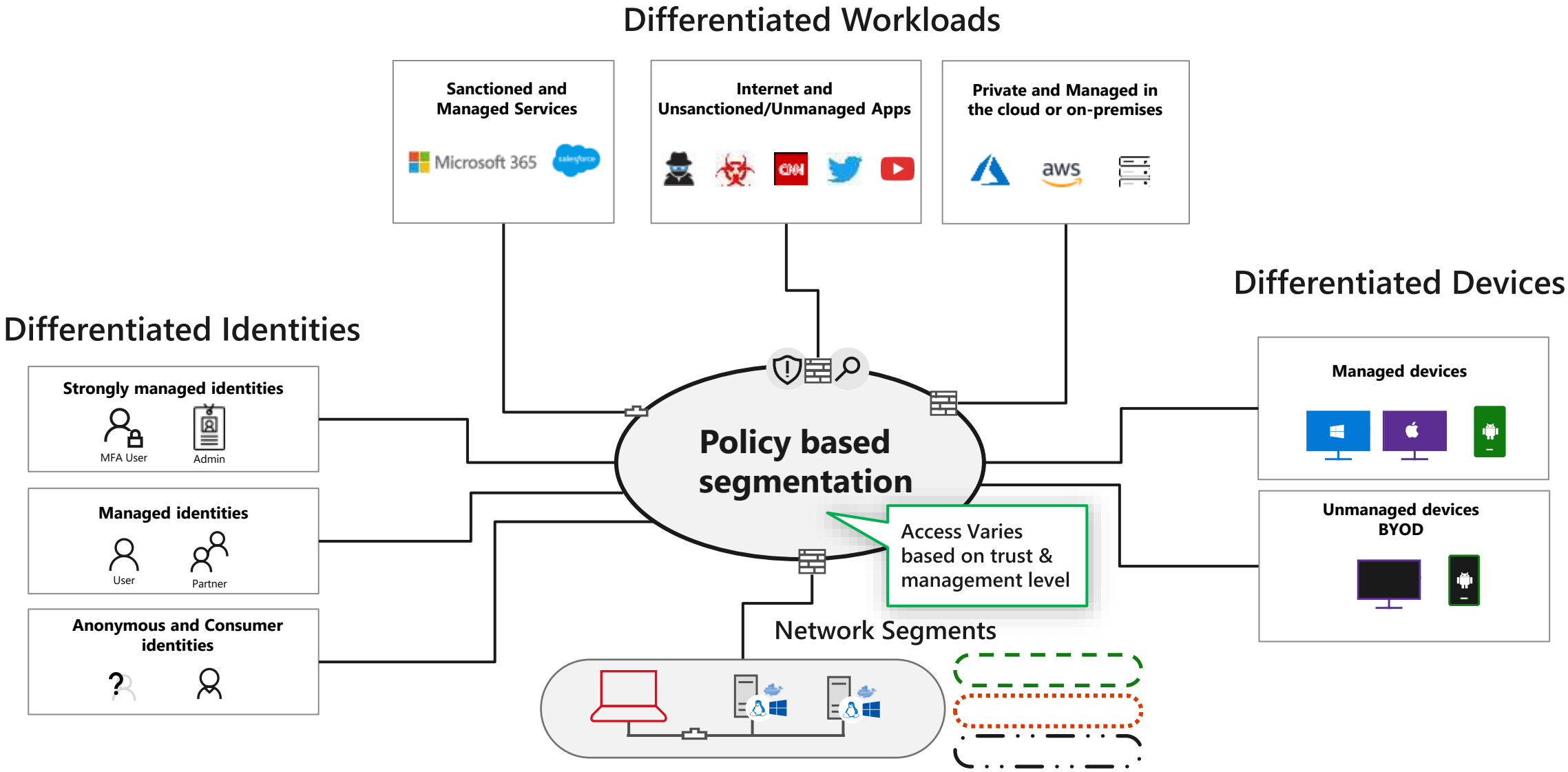


Spans on-premises & Azure environments

Full Zero Trust End State

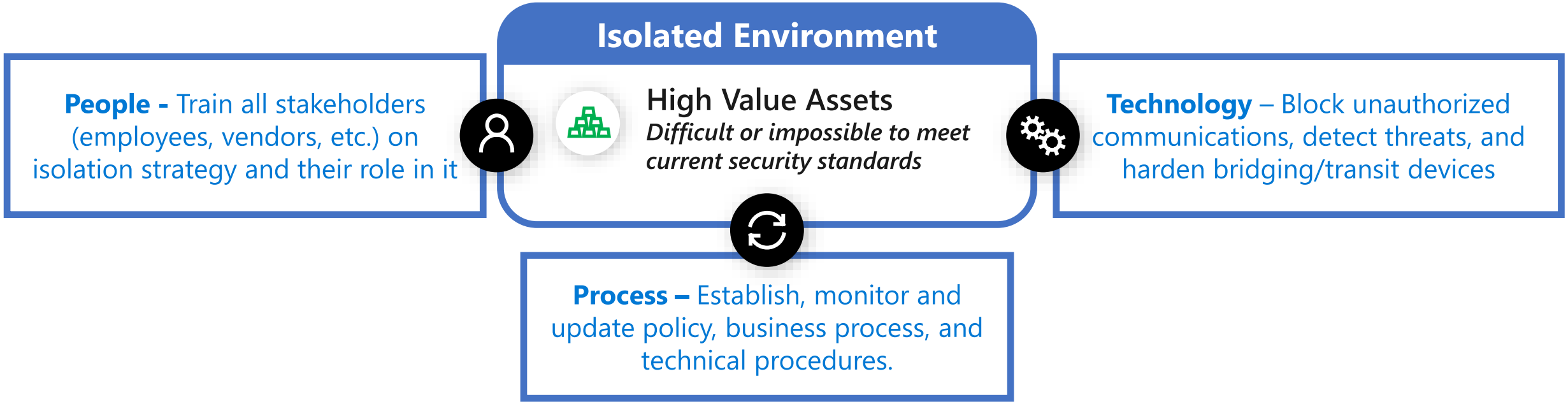
Bringing the best of both worlds

Similar in concept to Secure Access Service Edge (SASE)

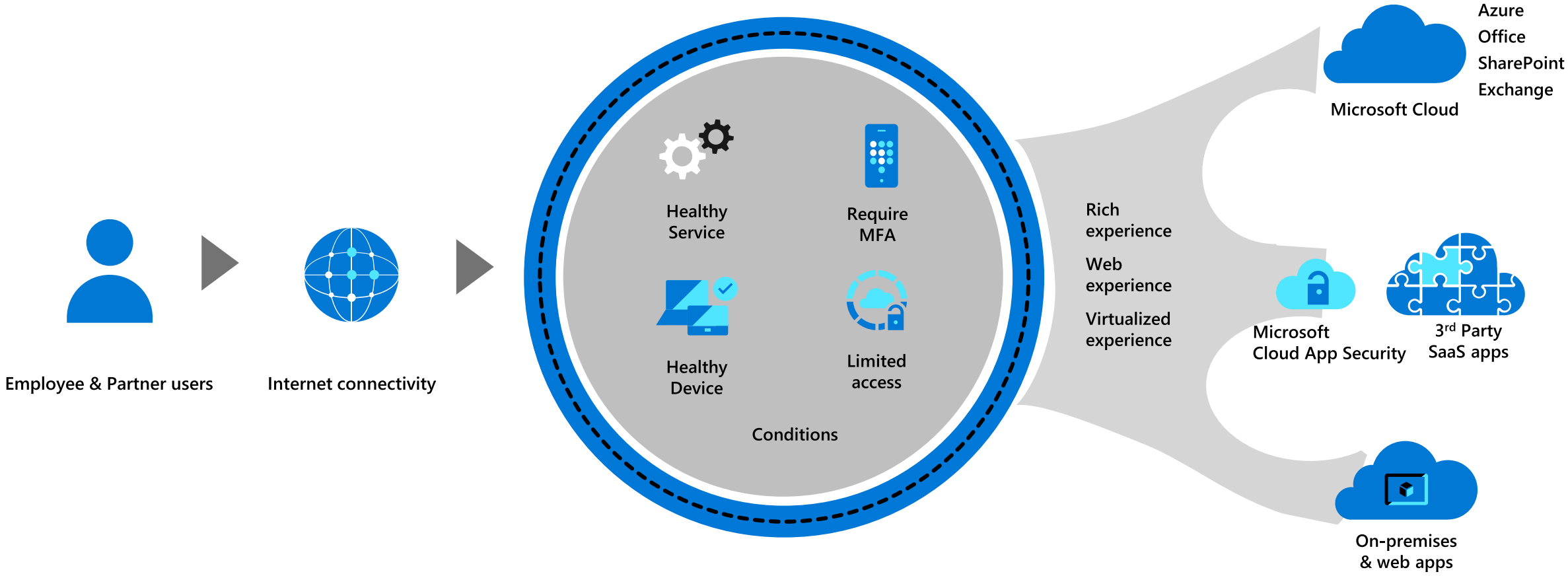


Isolation is a lifetime commitment

Avoid “firewall and forget” approach that creates false sense of security



Zero Trust Access Model



Productivity Benefits:
50% update time reduction
75% reduction in device issues
2x battery life
Faster device boot times – 75% improvement

Security Benefits:
Elimination of "shadow" VPN & Wireless APs
4x security auths – no user interaction
Reduction of surface area – 42% reduction
No more passwords – Helpdesk call reduction

Zero Trust Maturity

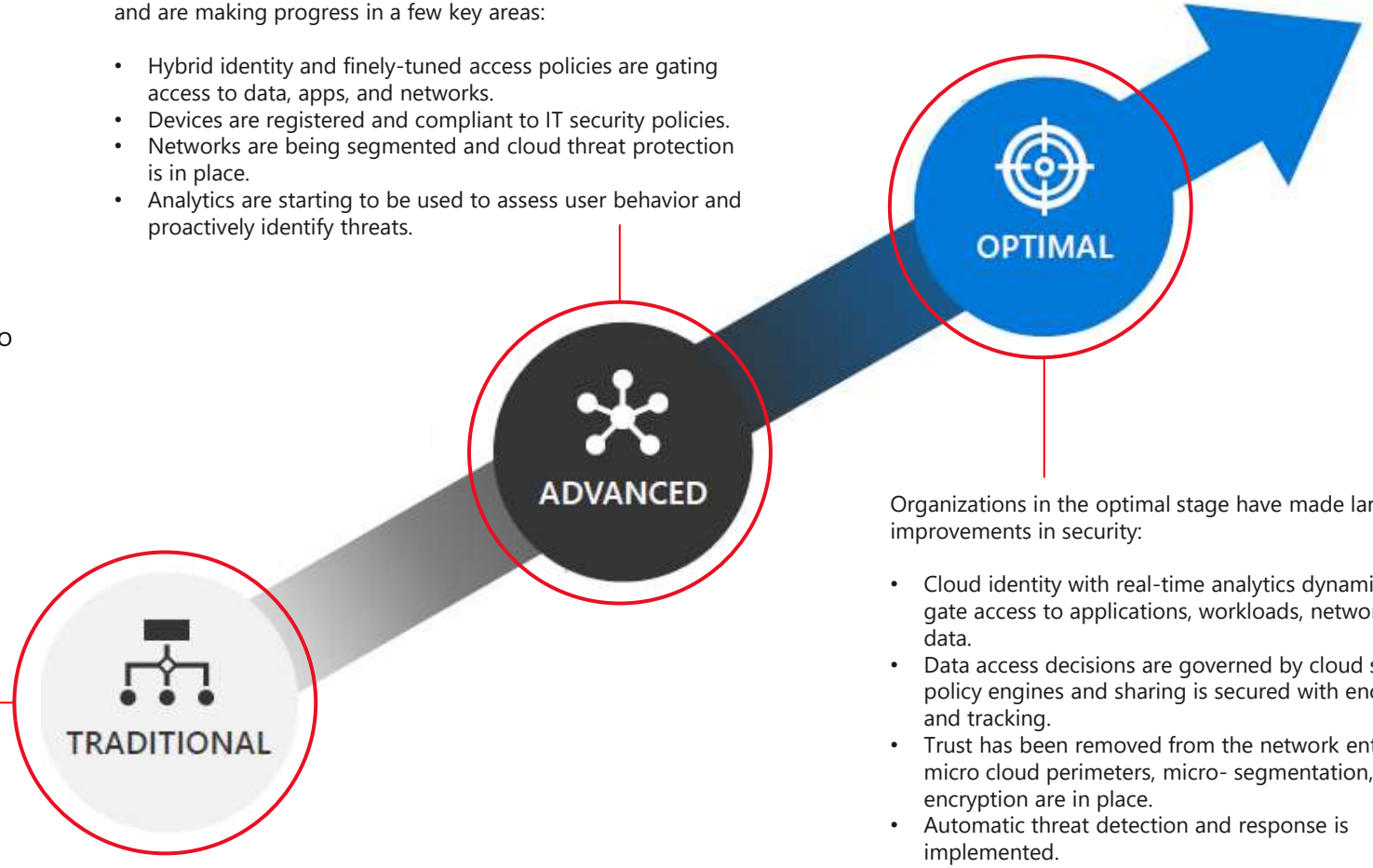
Zero Trust Maturity Model Explained

- **A three-stage maturity model developed by Microsoft**

- Different organizational requirements, existing technology implementations, and security stages all affect how a Zero Trust security model implementation is planned.
- Using our experience in helping customers to secure their organizations as well as implementing our own Zero Trust model, we've developed the following maturity model to help organizations assess their Zero Trust readiness and build a plan to get to Zero Trust. We recommend this maturity plan to be the source anchor for measuring the progress of the Zero Trust journey.

In this stage, organizations have begun their Zero Trust journey and are making progress in a few key areas:

- Hybrid identity and finely-tuned access policies are gating access to data, apps, and networks.
- Devices are registered and compliant to IT security policies.
- Networks are being segmented and cloud threat protection is in place.
- Analytics are starting to be used to assess user behavior and proactively identify threats.



This is where most organizations generally sit today if they haven't started their Zero Trust journey:

- On-premises identity with static rules and some SSO.
- Limited visibility is available into device compliance, cloud environments, and logins.
- Flat network infrastructure results in broad risk exposure.

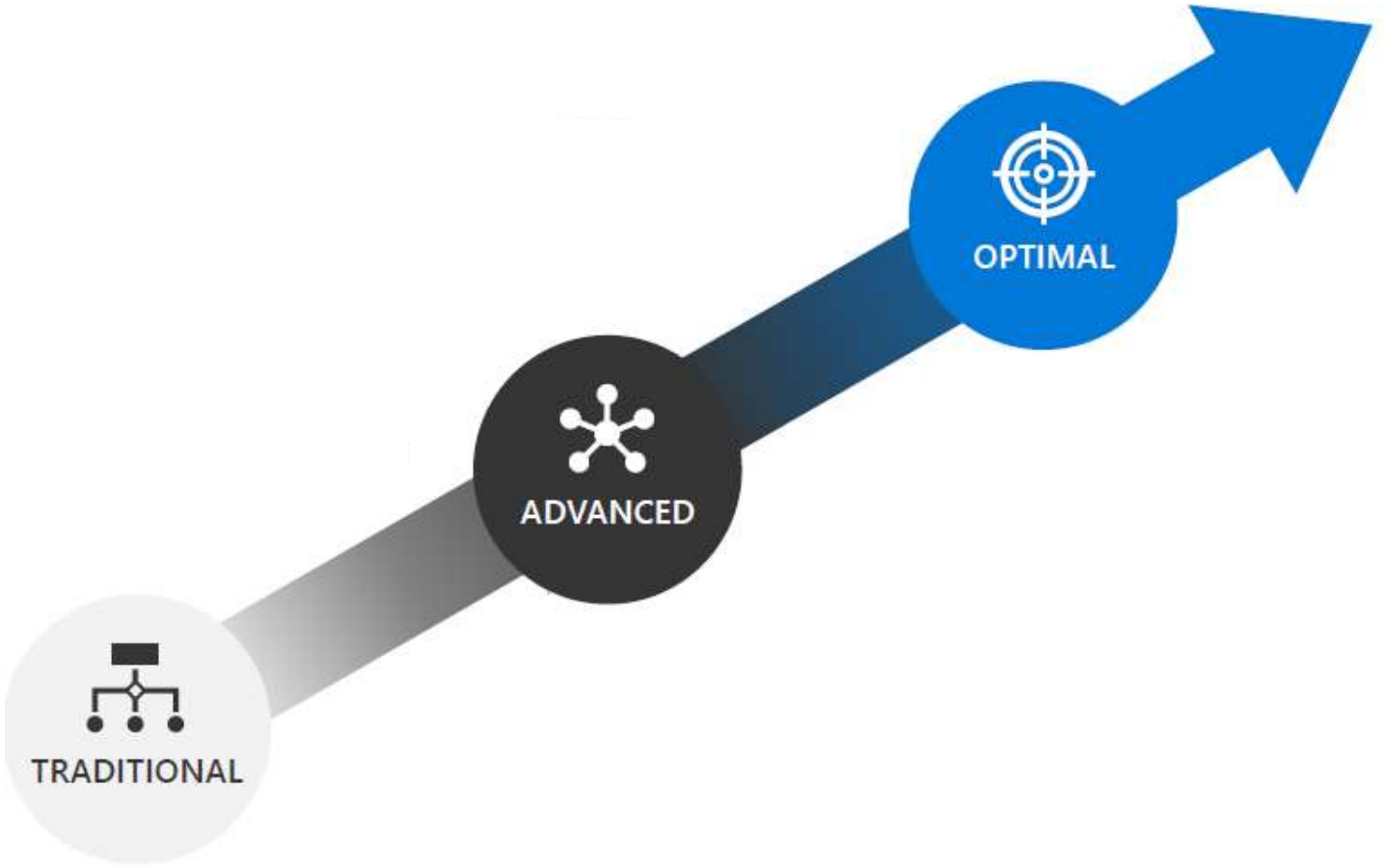
Organizations in the optimal stage have made large improvements in security:

- Cloud identity with real-time analytics dynamically gate access to applications, workloads, networks, and data.
- Data access decisions are governed by cloud security policy engines and sharing is secured with encryption and tracking.
- Trust has been removed from the network entirely - micro cloud perimeters, micro- segmentation, and encryption are in place.
- Automatic threat detection and response is implemented.

Zero Trust Maturity

The Three-Stage Model

- Different organizational requirements, existing technology implementations, and security stages all affect how a Zero Trust security model implementation is planned.
- Using our experience in helping customers to secure their organizations as well as implementing our own Zero Trust model, we've developed the following maturity model to help organizations assess their Zero Trust readiness and build a plan to get to Zero Trust.

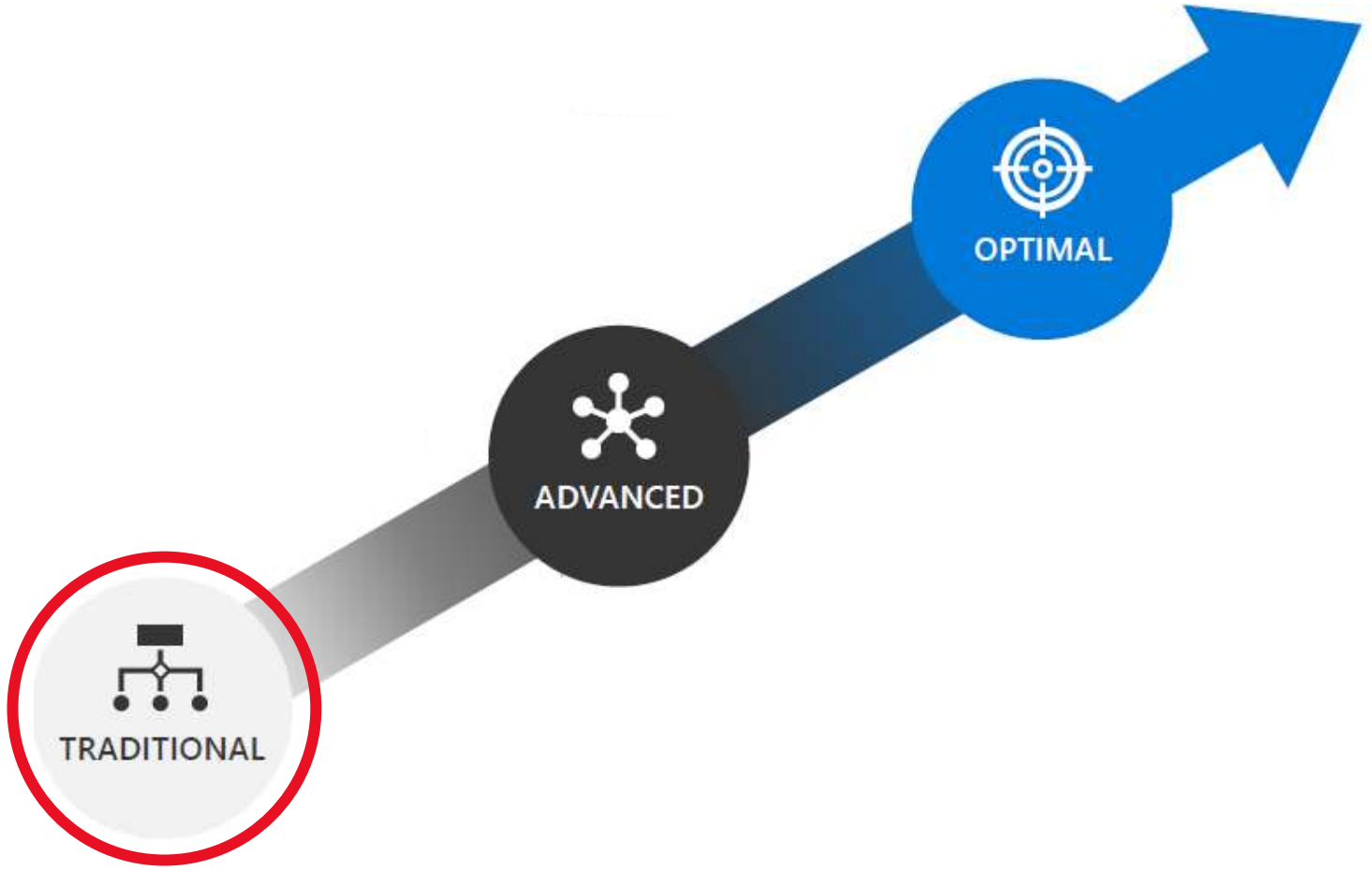


Zero Trust Maturity

The Three-Stage Model – Traditional

This is where most organizations generally sit today if they haven't started their Zero Trust journey:

- On-premises identity with static rules and some SSO.
- Limited visibility is available into device compliance, cloud environments, and logins.
- Flat network infrastructure results in broad risk exposure.

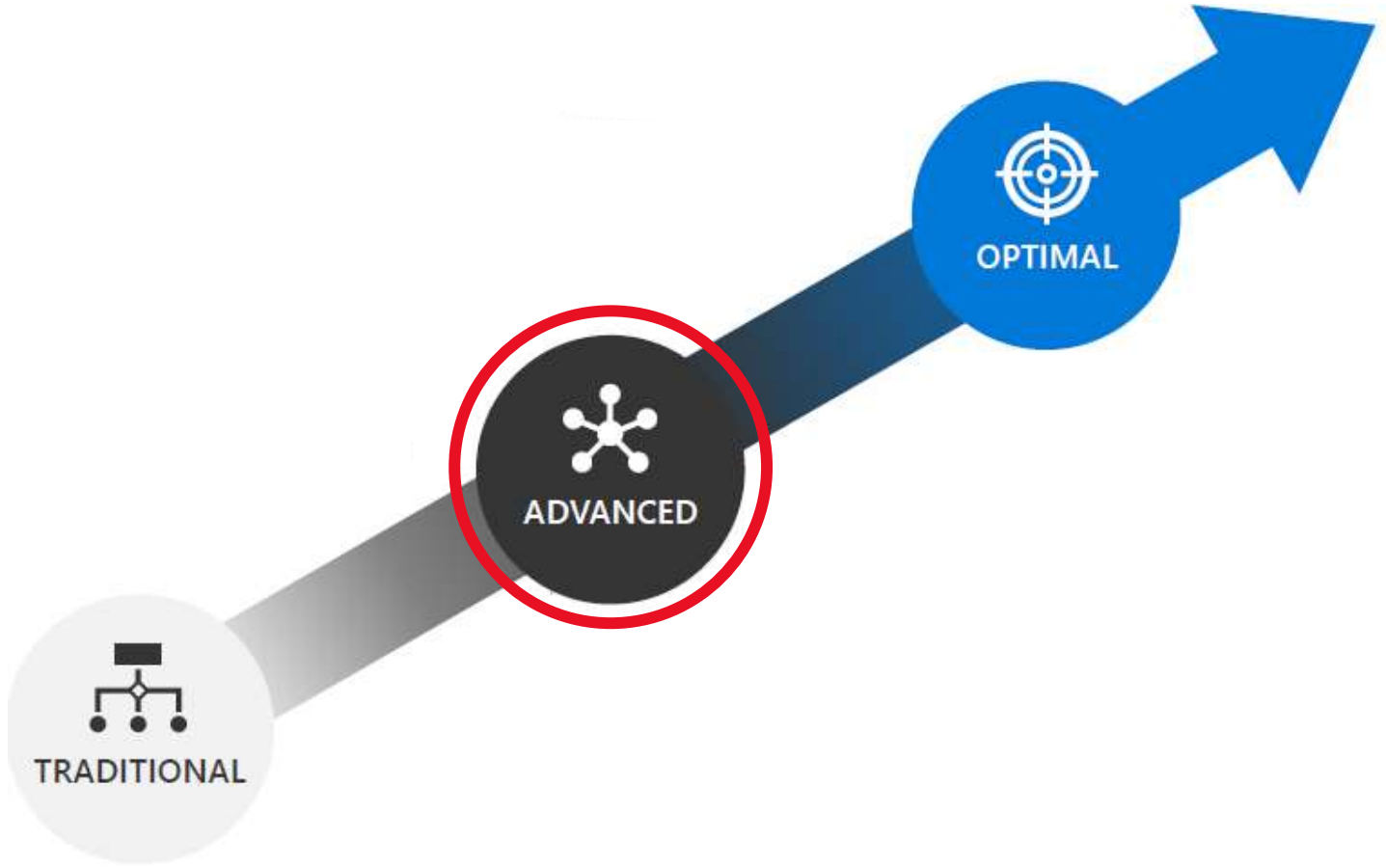


Zero Trust Maturity

The Three-Stage Model – Advanced

In this stage, organizations have begun their Zero Trust journey and are making progress in a few key areas:

- Hybrid identity and finely-tuned access policies are gating access to data, apps, and networks.
- Devices are registered and compliant to IT security policies.
- Networks are being segmented and cloud threat protection is in place.
- Analytics are starting to be used to assess user behavior and proactively identify threats.

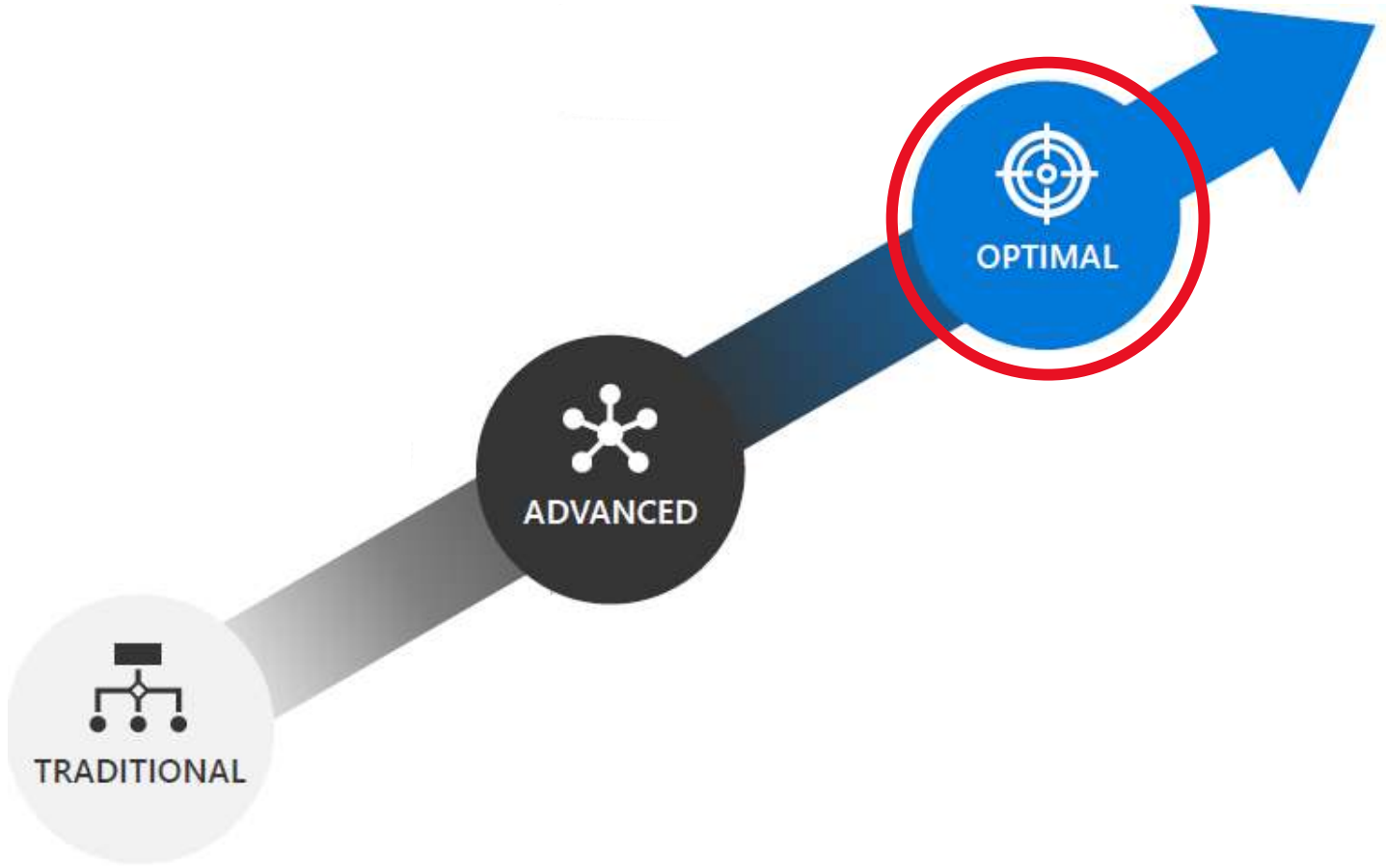


Zero Trust Maturity

The Three-Stage Model – Optimal

Organizations in the optimal stage have made large improvements in security:

- Cloud identity with real-time analytics dynamically gate access to applications, workloads, networks, and data.
- Data access decisions are governed by cloud security policy engines and sharing is secured with encryption and tracking.
- Trust has been removed from the network entirely - micro cloud perimeters, micro-segmentation, and encryption are in place.
- Automatic threat detection and response is implemented.



Zero Trust Maturity

Readiness across the six Foundational Elements – Identity

Identities

Traditional	Advanced	Optimal
On-premises identity provider is in use	Cloud identity federates with on-premises system	Passwordless authentication is enabled
No SSO is present between cloud and on-premises apps	Conditional access policies gate access and provide remediation actions	User, device, location, and behavior is analyzed in real time to determine risk and deliver ongoing protection
Visibility into identity risk is very limited	Analytics improve visibility	

Zero Trust Maturity

Readiness across the six Foundational Elements – Data

Data

Traditional	Advanced	Optimal
Access is governed by perimeter control, not data sensitivity	Data is classified and labeled via regex/keyword methods	Classification is augmented by smart machine learning models
Sensitivity labels are applied manually, with inconsistent data classification	Access decisions are governed by encryption	Access decisions are governed by a cloud security policy engine
		DLP policies secure sharing with encryption and tracking

Zero Trust Maturity

Readiness across the six Foundational Elements – Devices

Devices

Traditional	Advanced	Optimal
Devices are domain joined and managed with solutions like Group Policy Object or Config Manager	**Devices are registered with cloud identity provider**	Endpoint threat detection is used to monitor device risk
Devices are required to be on network to access data	**Access only granted to cloud managed & compliant devices**	Access control is gated on device risk for both corporate and BYO devices
	DLP policies are enforced for BYO and corporate devices	

Zero Trust Maturity

Readiness across the six Foundational Elements – Apps

Apps

Traditional	Advanced	Optimal
On-premises apps are accessed through physical networks or VPN	**On-premises apps are internet-facing and cloud apps are configured with SSO**	All apps are available using least privilege access with continuous verification
Some critical cloud apps are accessible to users	**Cloud Shadow IT risk is assessed; critical apps are monitored and controlled**	Dynamic control is in place for all apps with in-session monitoring and response

Zero Trust Maturity

Readiness across the six Foundational Elements – Infrastructure

	Traditional	Advanced	Optimal
 **Infrastructure**	Permissions are managed manually across environments Configuration management of VMs and servers on which workloads are running	**Workloads are monitored and alerted for abnormal behavior** **Every workload is assigned app identity** **Human access to resources requires Just-In-Time**	Unauthorized deployments are blocked and alert is triggered Granular visibility and access control are available across all workloads User and resource access is segmented for each workload

Zero Trust Maturity

Readiness across the six Foundational Elements – Identity

Network

Traditional	Advanced	Optimal
Few network security perimeters and flat open network	Many ingress/egress cloud micro-perimeters with some micro-segmentation	Fully distributed ingress/egress cloud micro-perimeters and deeper micro-segmentation
Minimal threat protection and static traffic filtering	Cloud native filtering and protection for known threats	ML-based threat protection and filtering with context-based signals
Internal traffic is not encrypted	User to app internal traffic is encrypted	All traffic is encrypted

Zero Trust Maturity

Key Investments for Zero Trust

As organizations begin to assess their Zero Trust readiness and begin to plan on the changes to improve protection across identities, devices, applications, data, infrastructure, and networks, these key investments should be considered to help drive their Zero Trust implementation more effectively.

Through our own experience, we've found each of the following to be critical to closing important capability and resources gaps.

1. **Strong authentication**. Ensure strong multi factor authentication and session risk detection as the backbone of your access strategy to minimize the risk of identity compromise.
2. **Policy based adaptive access**. Define acceptable access policies for your resources and enforce them with a consistent security policy engine that provides both governance and insight into variances.
3. **Micro segmentation**. Move beyond simple centralized network-based perimeter to comprehensive and distributed segmentation using software defined micro perimeters.
4. **Automation**. Invest in automated alerting and remediation to reduce your mean time to respond (MTTR) to attacks.
5. **Intelligence and AI**. Utilize cloud intelligence and all available signals to detect and respond to access anomalies in real time.
6. **Data classification and protection**. Discover, classify, protect, and monitor sensitive data to minimize exposure from malicious or accidental exfiltration.

Zero Trust Maturity Model Key Capabilities

	Traditional	Advanced	Optimal
 **Identities**	• On-premises identity provider is in use • No SSO is present between cloud and on-premises apps • Visibility into identity risk is very limited	• Cloud identity federates with on-premises system • Conditional access policies gate access and provide remediation actions • Analytics improve visibility	• Passwordless authentication is enabled • User, device, location, and behavior is analyzed in real time to determine risk and deliver ongoing protection
 **Devices**	• Devices are domain joined and managed with solutions like Group Policy Object or Config Manager • Devices are required to be on network to access data	• Devices are registered with cloud identity provider • Access only granted to cloud managed & compliant devices • DLP policies are enforced for BYO and corporate devices	• Endpoint threat detection is used to monitor device risk • Access control is gated on device risk for both corporate and BYO devices
 **Apps**	• On-premises apps are accessed through physical networks or VPN • Some critical cloud apps are accessible to users	• On-premises apps are internet-facing and cloud apps are configured with SSO • Cloud Shadow IT risk is assessed; critical apps are monitored and controlled	• 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
 **Infrastructure**	• Permissions are managed manually across environments • Configuration management of VMs and servers on which workloads are running	• Workloads are monitored and alerted for abnormal behavior • Every workload is assigned app identity • Human access to resources requires Just-In-Time	• Unauthorized deployments are blocked and alert is triggered • Granular visibility and access control are available across all workloads • User and resource access is segmented for each workload
 **Network**	• Few network security perimeters and flat open network • Minimal threat protection and static traffic filtering • Internal traffic is not encrypted	• Many ingress/egress cloud micro-perimeters with some micro-segmentation • Cloud native filtering and protection for known threats • User to app internal traffic is Encrypted	• Fully distributed ingress/egress cloud micro-perimeters and deeper micro-segmentation • ML-based threat protection and filtering with context-based signals • All traffic is encrypted
 **Data**	• Access is governed by perimeter control, not data sensitivity • Sensitivity labels are applied manually, with inconsistent data Classification	• Data is classified and labeled via regex/keyword methods • Access decisions are governed by encryption	• Classification is augmented by smart machine learning models • Access decisions are governed by a cloud security policy engine • DLP policies secure sharing with encryption and tracking

The Journey to Advanced *(Detailed)*

Traditional → Advanced → Optimal

	Identities	Devices	Apps	Infrastructure	Network	Data
Advanced	• Cloud identity federates with on-premises system • Conditional Access policies gate access and provide remediation actions • Analytics improve visibility • Identity segmentation • Raise attacker cost	• Devices are registered with cloud identity provider • Access only granted to cloud managed and compliant devices • DLP policies are enforced for BYO and corporate devices	• On-premises apps are internet-facing and cloud apps are configured with SSO • Cloud Shadow IT risk is assessed; critical apps are monitored and controlled	• Workloads are monitored and alerted for abnormal behavior • Every workload assigned app identity • Human access to resources requires Just-In-Time	• Many ingress/egress cloud micro-perimeters with some micro-segmentation • Cloud native filtering and protection for known threats • User to app internal traffic is encrypted	• Data is classified and labelled via regular expressions/keyword • Access decisions governed by encryption • Raise attacker cost
Controls	• MFA for privileged access • Azure security defaults • Azure ATP for global • Tier 0 PAWs • AD DS tier 0 • Leaked credential detection (PHS) • Azure AD password protection • Azure Key Vault • Azure AD Conditional Access • BitLocker protected DCs	• Accelerate MMD roll-out • MDATP owned and talking to the SOC for high value assets (e.g. PAWs) • Intune for BYOD • Defender SmartScreen for all • Credential Guard for all clients • Defender Exploit Guard	• Standardize on modern apps • Azure AD for modern and Ping Identity for legacy apps • MCAS Conditional Access and session control policies for high-value assets and data • MCAS discover and sanction apps • Office 365 advanced audit	• High value assets enrolled into Azure Security Center (ASC) • JIT for high value workloads • Azure AD PIM • Secure Windows Server 2019 build	• Cloud adoption framework followed • Tier 0 assets segmented • Critical legacy protocol triage	• Communication compliance and DLP for teams • Enable Office 365 ATP safe links and safe attachments • Configure 3-tier protection for Teams • Deploy MIP unified labelling and classification • Discover, classify and label cloud data with MCAS • Enable AIP unified scanner for on-prem

The Journey to Optimal *(Detailed)*

Traditional → Advanced → Optimal

	Identities	Devices	Apps	Infrastructure	Network	Data
Optimal	• Password-less authentication is enabled • User, device, location, and behavior is analyzed in real time to determine risk and deliver ongoing protection • Complete identity segmentation	• Endpoint threat detection is used to monitor device risk • Access control is gated on device risk for both corporate and BYO Devices	• 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	• Unauthorized deployments are blocked, and alert is triggered • Granular visibility and access control are available across all workloads • User and resource access is segmented for each workload	• Fully distributed ingress/egress cloud micro-perimeters and deeper micro-segmentation • ML-based threat protection and filtering with context-based signals • All traffic is encrypted	• Classification is augmented by smart machine learning models • Access decisions are governed by a cloud security policy engine • DLP policies secure sharing with encryption and tracking
Controls	• MFA for all employees and B2B access • WH4B for all • Azure ATP for markets • AADIDP integrated with Conditional Access and session control • Azure AD IDP risky sign-in • MCAS, MDATP, Azure ATP, Azure AD IPP integrated for signaling and investigation • All Microsoft feeds into Sentinel • AD DS tier 1 and 2 implemented with PAWs	• Complete MMD roll-out • MDATP for all devices, reporting to Sentinel and the SOC • Risk-based access control • Intune for all • Credential guard for member servers • Defender web content filtering • Defender firewall	• Azure AD and MCAS Conditional Access & session control for all apps and data • MCAS blocking for unsanctioned apps • Automate app tagging with app discovery policies and risk levels	• Inventory all assets in ASC • Azure ARC managing multi-cloud & on-prem • Azure Lighthouse managing both tenants • High value assets threat-modelled • Exposed keys discovered with CredScan	• Azure Security Center (ASC) policies • Identify and remove legacy protocols	• Automated labelling and protection • Encrypted email • Update labels to apply protection • Enforce DLP and compliance policies

Microsoft Zero Trust Controls

Microsoft control	Build an identity perimeter	Secure the common control plane	Least privilege access to sanctioned apps	Data is protected wherever is flows	Protect resources, not networks	Healthy devices wherever they roam
Azure AD Identity Protection	✓	✓				
Conditional Access	✓	✓				
Azure ATP	✓					
Azure Password Protection	✓					
Hello for Business	✓	✓				
Azure MFA	✓	✓				
RBAC	✓	✓	✓	✓	✓	✓
Azure AD PIM	✓	✓				
Active Directory (PAW & Tier Model)	✓	✓				
Credential Guard	✓					✓
MCAS	✓		✓	✓		
Cloud Infrastructure (Subscription, Resource Group, vNet, NSG, ASG, ExpressRoute, VPN Gateway, Azure Firewall, Azure Automation, Azure Blueprints, Azure DevOps, Azure Disk Encryption, ExpressRoute, Storage ATP)		✓	✓	✓	✓	
Resource Group			✓	✓		
Office 365 ATP	✓			✓		✓
Data Loss Prevention				✓		
Microsoft Information Protection				✓		
Defender Firewall					✓	✓
Microsoft Defender ATP						✓
Intune	✓		✓			✓
Exploit Guard	✓		✓	✓	✓	✓
Bitlocker				✓		✓
Advanced Audit	✓		✓	✓		
Azure Security Centre	✓	✓	✓	✓	✓	✓
Azure Log Analytics	✓	✓	✓	✓	✓	✓
Azure Sentinel	✓	✓	✓	✓	✓	✓
Azure ARC	✓	✓	✓	✓	✓	✓
Azure Lighthouse	✓	✓	✓	✓	✓	✓
Intelligent Security Graph	✓	✓	✓	✓	✓	✓