

Build Zero Trust Foundations

Abbas Kudrati

APAC Lead 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"

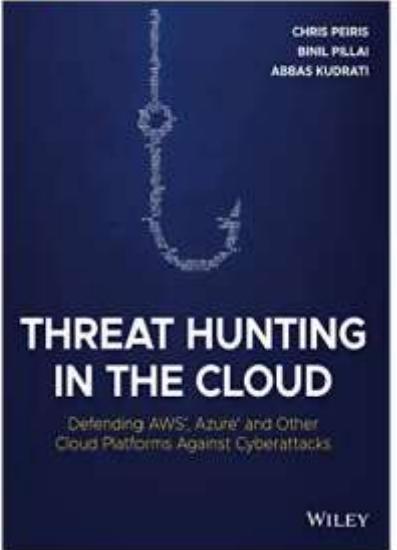
Satya Nadella

- **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

Best Seller

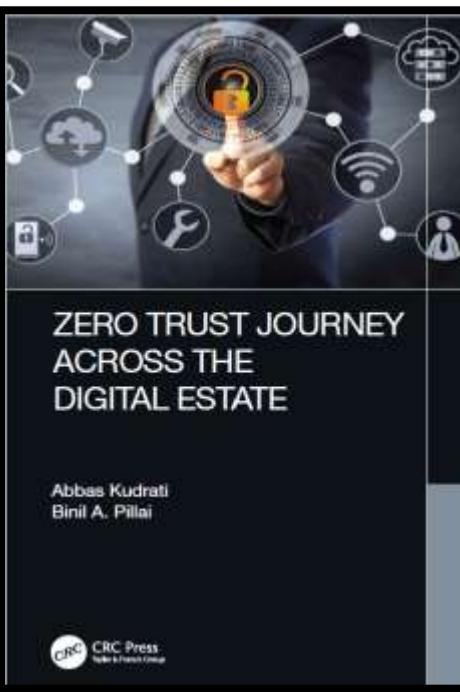


THREAT HUNTING IN THE CLOUD

Defending AWS, Azure, and Other
Cloud Platforms Against Cyberattacks

WILEY

[Get it on Amazon](#)
Or send me a request for a free
copy



[Order on Amazon](#)

Work in progress

DIGITIZATION RISKS IN POST- PANDEMIC WORLD

Abbas Kudrati
Ashish Kumar
Shashank Kumar

Packt

Releasing soon by Oct
2022

Work in progress

BEGINNING WITH CYBERSECURITY MESH ARCHITECTURE

Abbas Kudrati
Sweta Katke
Anirudh Majumdar



Releasing soon by Dec
2022

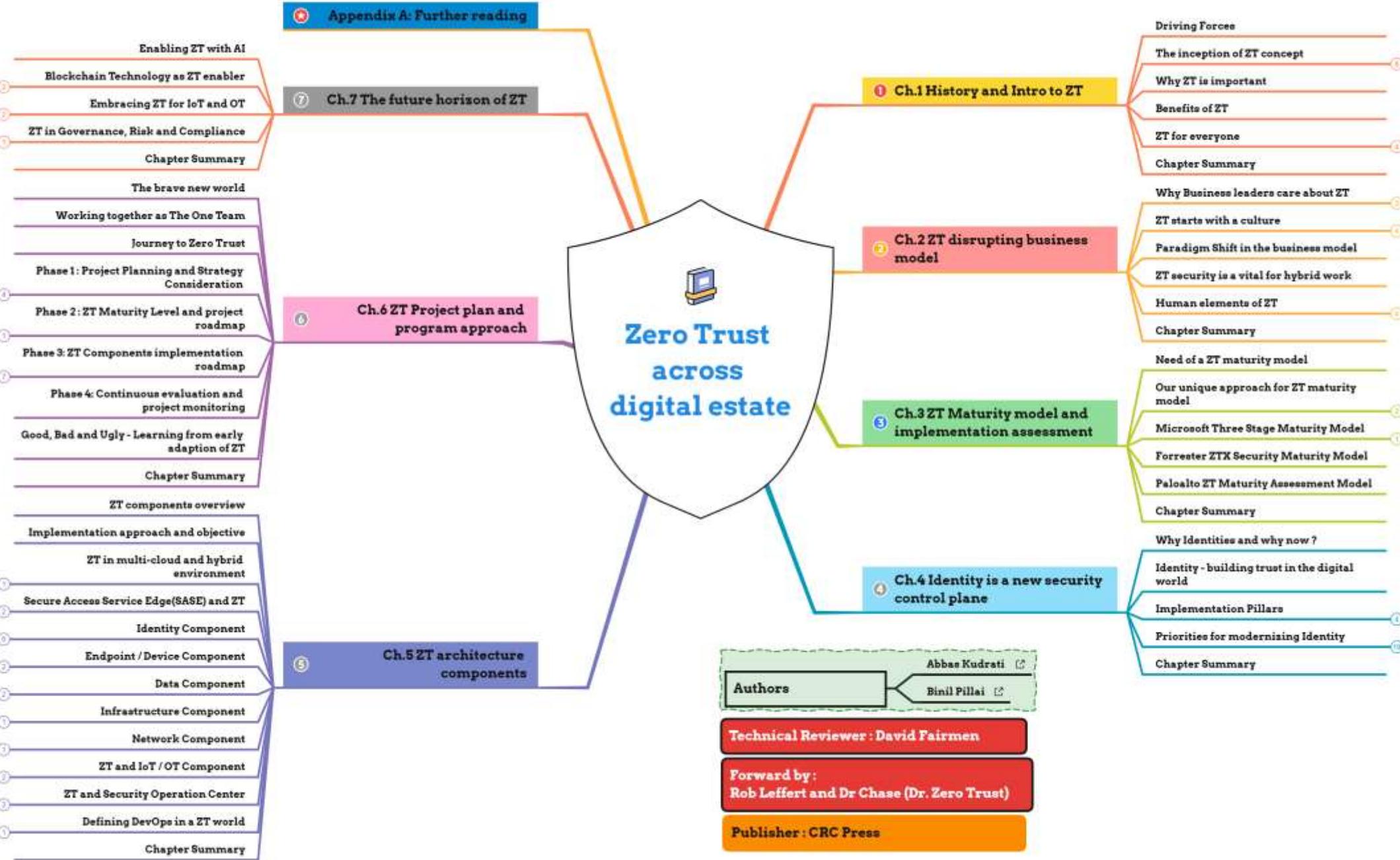
Work in progress

CYBER RÉSILIENCY DURING THE TIME OF ADVERSORY

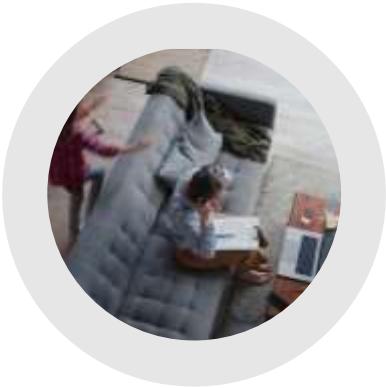
Sarah Armstrong
Abbas Kudrati



Releasing soon by
March 2023



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?

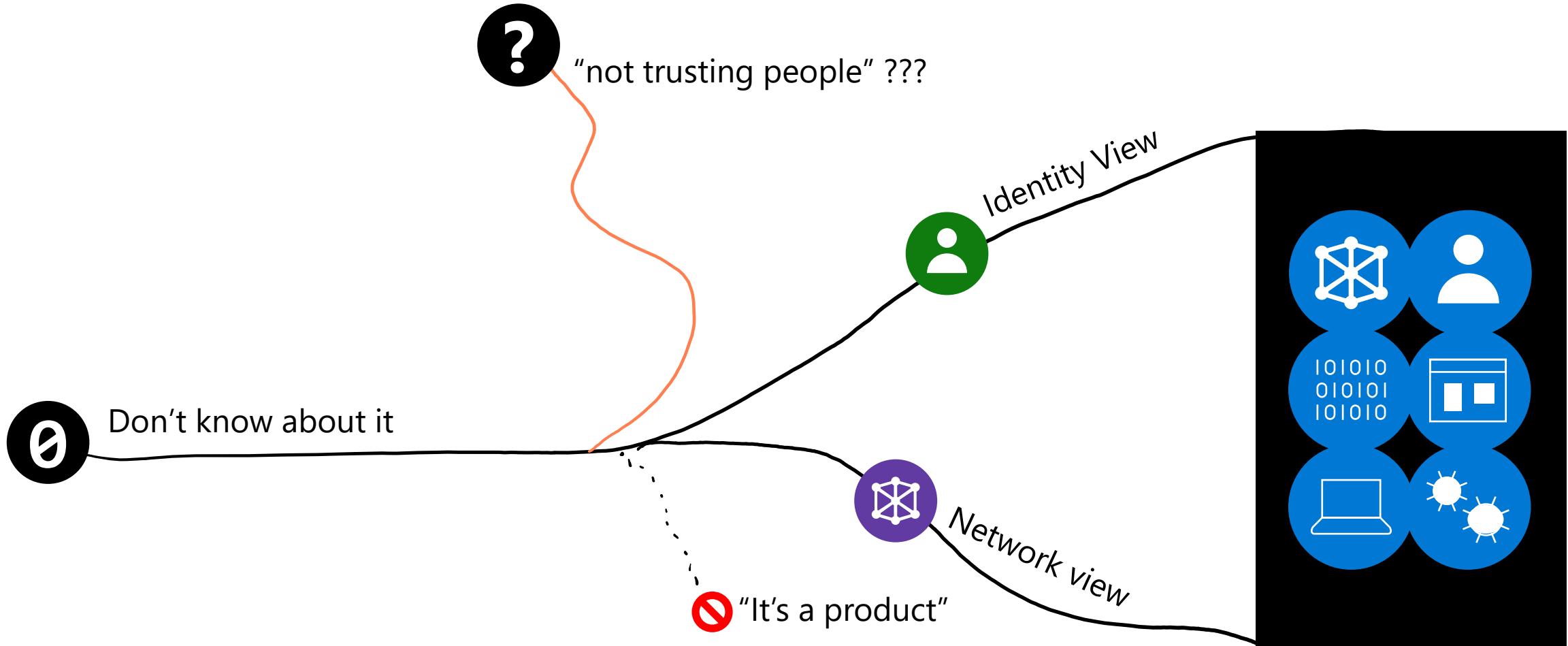


EXHIBIT 3. HYBRID WORKPLACE INTENT



EXHIBIT 4. HYBRID WORKPLACE CONCERN

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%

Zero Trust Adaption report 2020 /21

EXHIBIT 1. ZERO TRUST IS CRITICAL

Very + Somewhat ▶ 96%

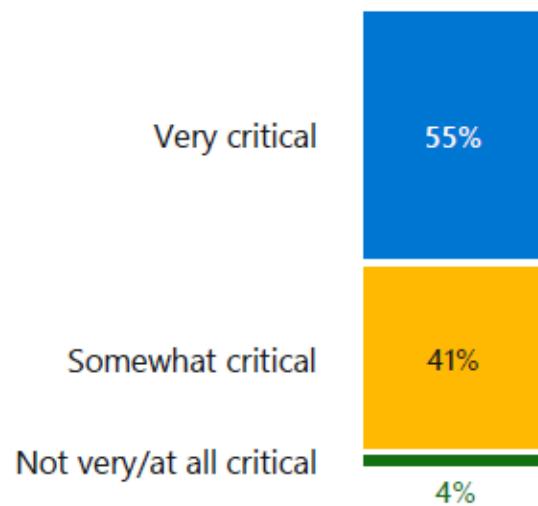


EXHIBIT 2. ZERO TRUST MOTIVATORS

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

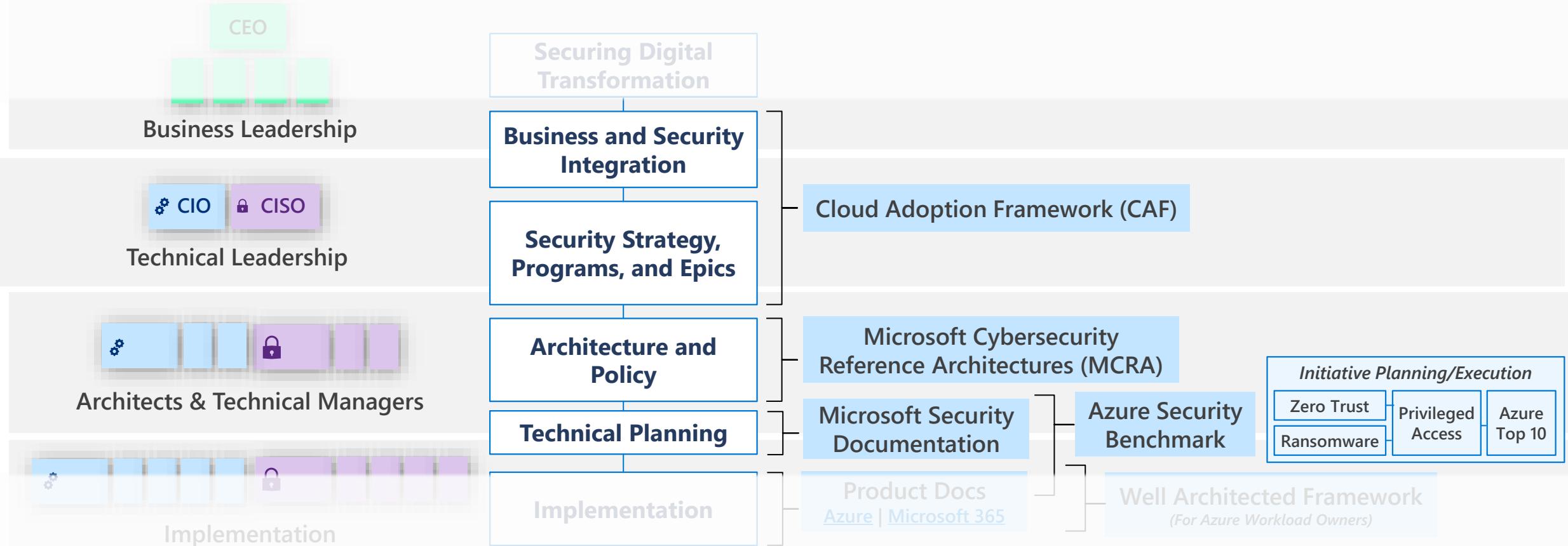


EXHIBIT 7. ZERO TRUST COMPONENT IMPLEMENTATION (TOP 3) – RANKED #1 (IMPLEMENTED FIRST)

Identities		Endpoints	
Strong authentication (i.e., multi-factor authentication, passwordless authentication)	32%	Data Loss Prevention policies/controls for all unmanaged and managed devices	27%
Automated risk detection and remediation	27%	Real-time device risk evaluation / endpoint threat detection	26%
Adaptive access policies to gate access to resources	22%	Devices are registered with identity provider	24%
Apps		Network	
Ongoing Shadow IT Discovery and risk assessment	23%	Secure access controls to protect networks	25%
Granular access control to your apps (such as limited visibility or read only)	22%	Threat protection and filtering with context-based signals	24%
Policy-based access control for apps	20%	All traffic is encrypted	20%

Security Guidance

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



Introduction - Why Zero Trust is Important

The world is transforming rapidly

Market



Business



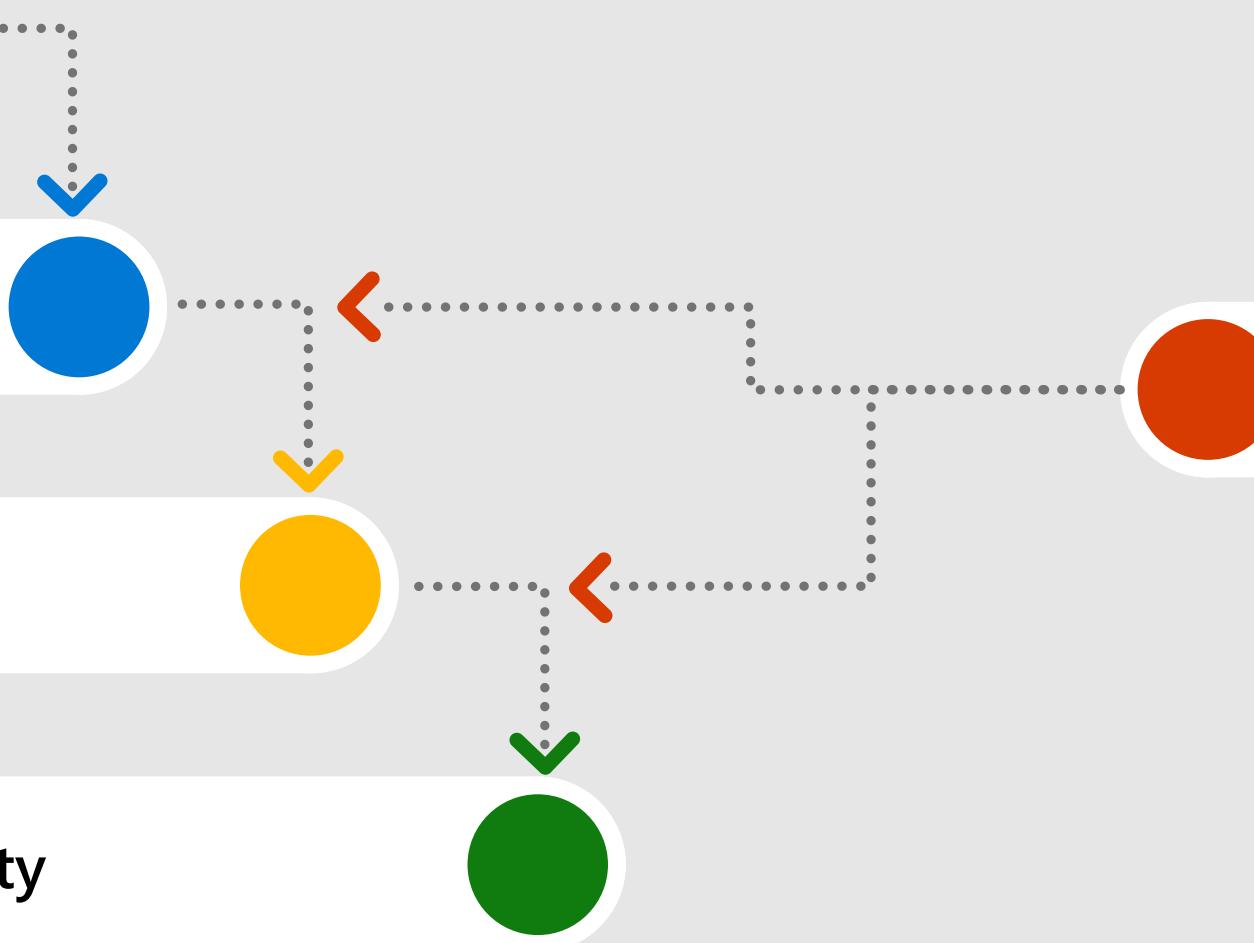
Technology



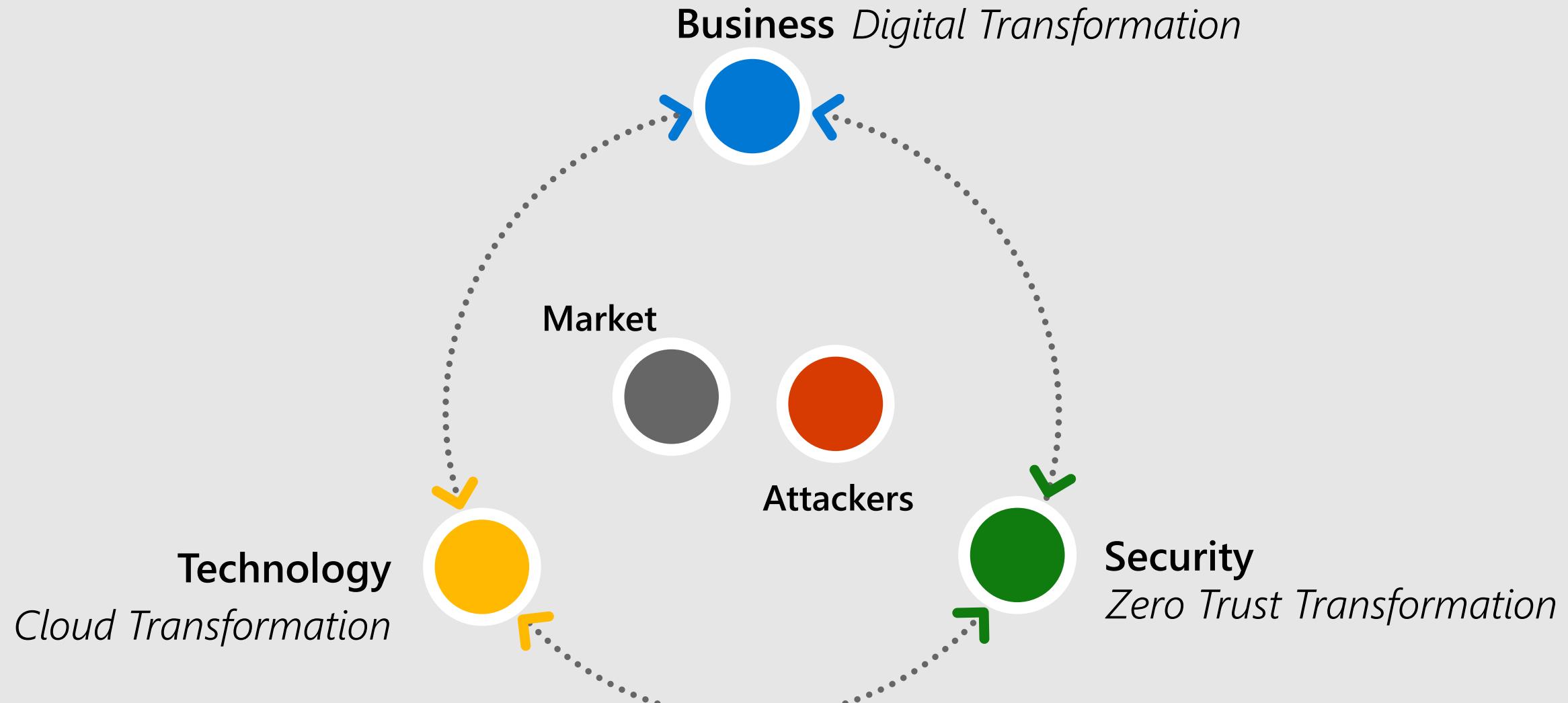
Security



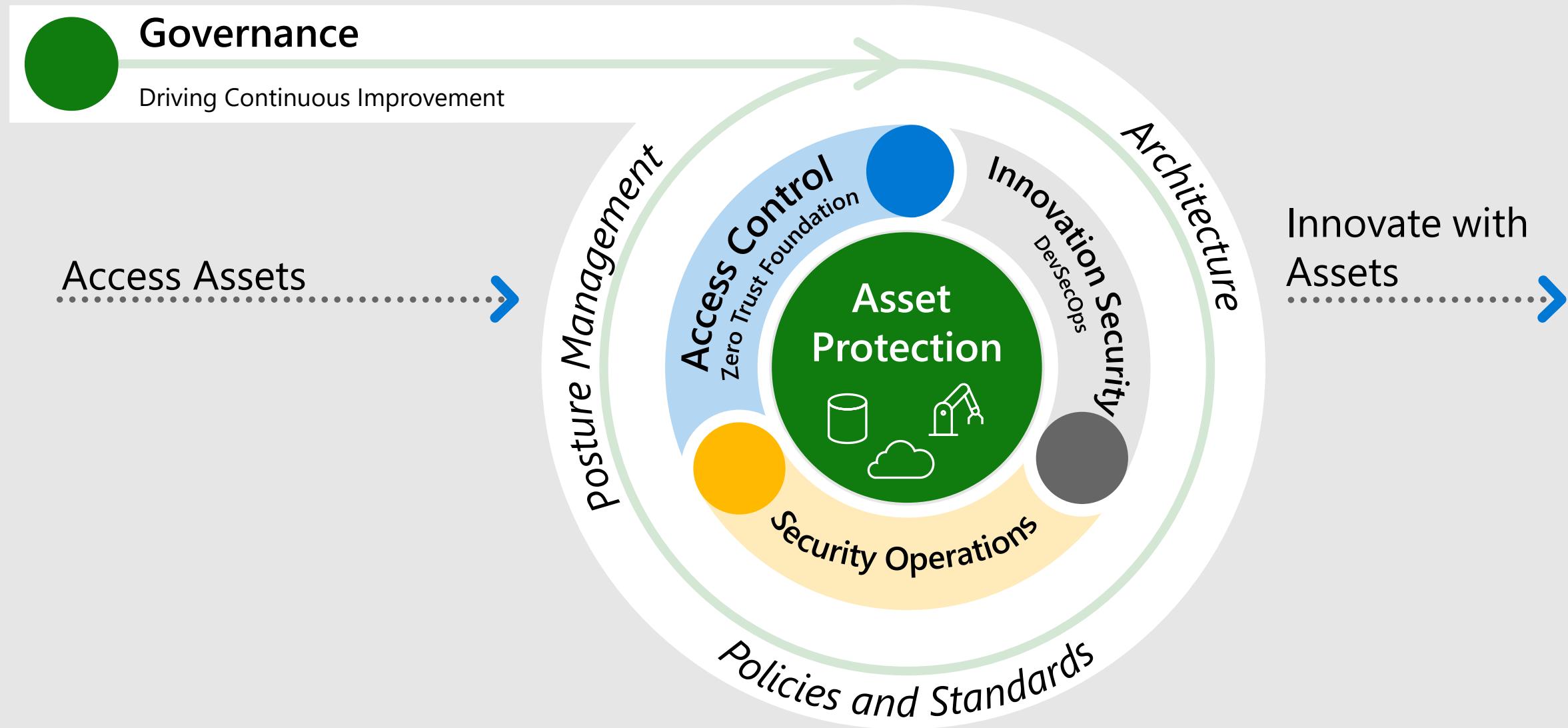
Attackers



Working together



Security Shifts to Continuous Improvement



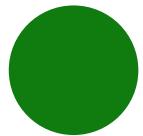


Build Modern Security

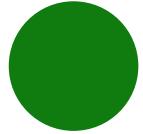
Common Modernization Initiatives



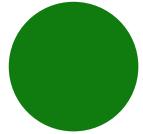
Ransomware Recovery Readiness
Ensure backups are validated, secure, and immutable to enable rapid recovery



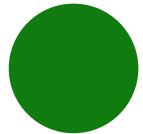
Zero Trust Foundations



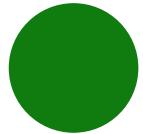
Modern Security Operations



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:

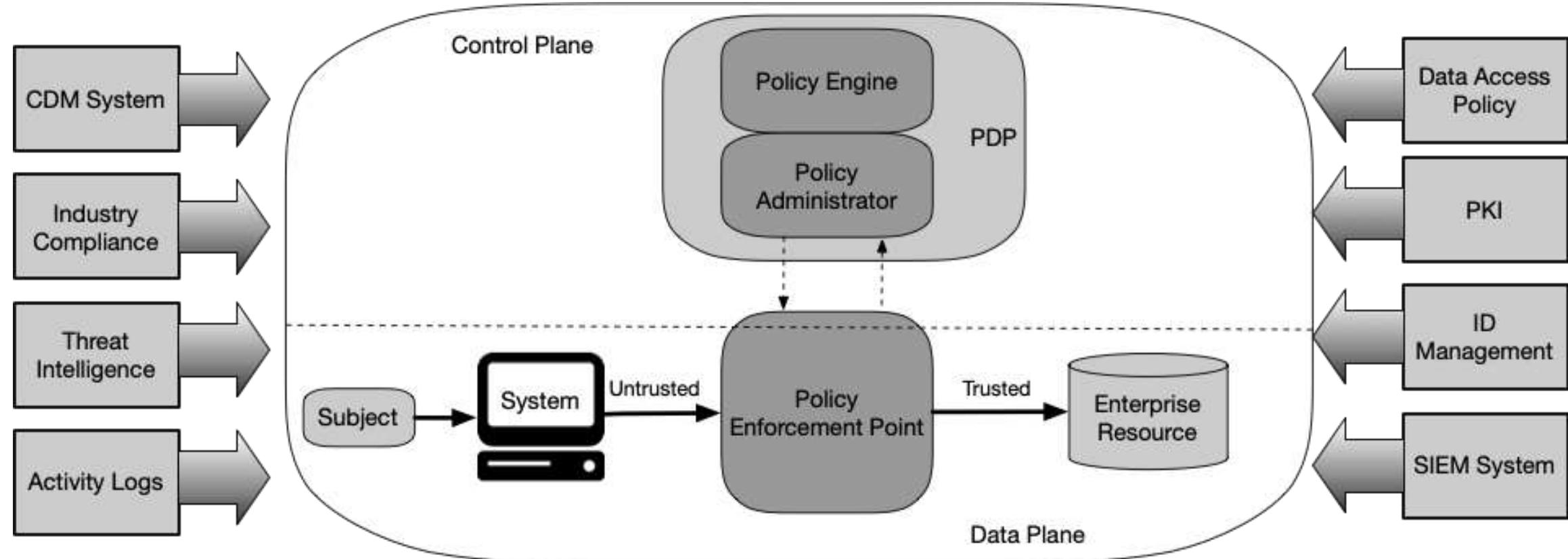
- **Never trust, always verify** – Treat every user, device, application/workload, and data flow as untrusted. Authenticate and explicitly authorize each to the least privilege required using dynamic security policies.
- **Assume breach** – Consciously operate and defend resources with the assumption 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.

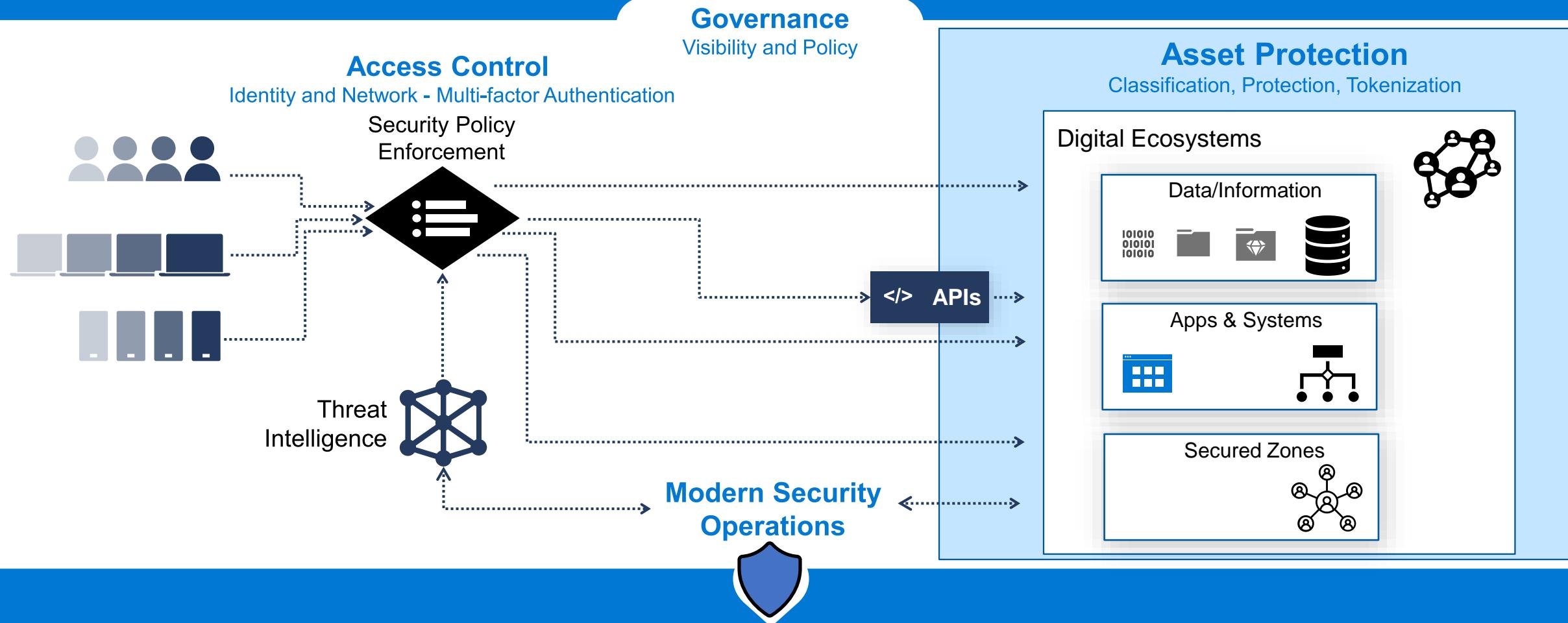
NIST Zero Trust Architecture



Zero Trust Components

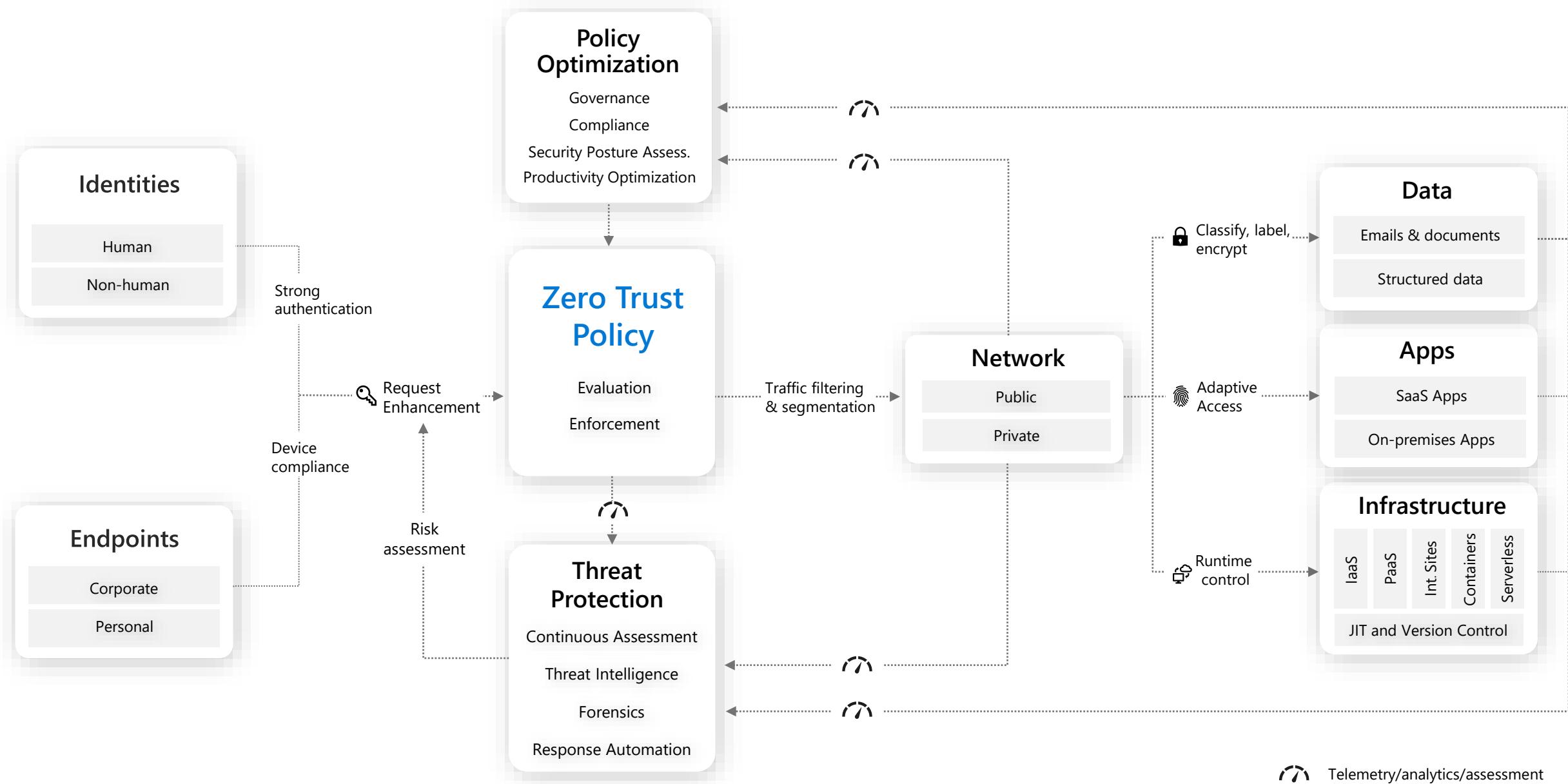
Enable flexible business workflows for the digitized world

Clarity, Automation, and Metrics-Driven Approach

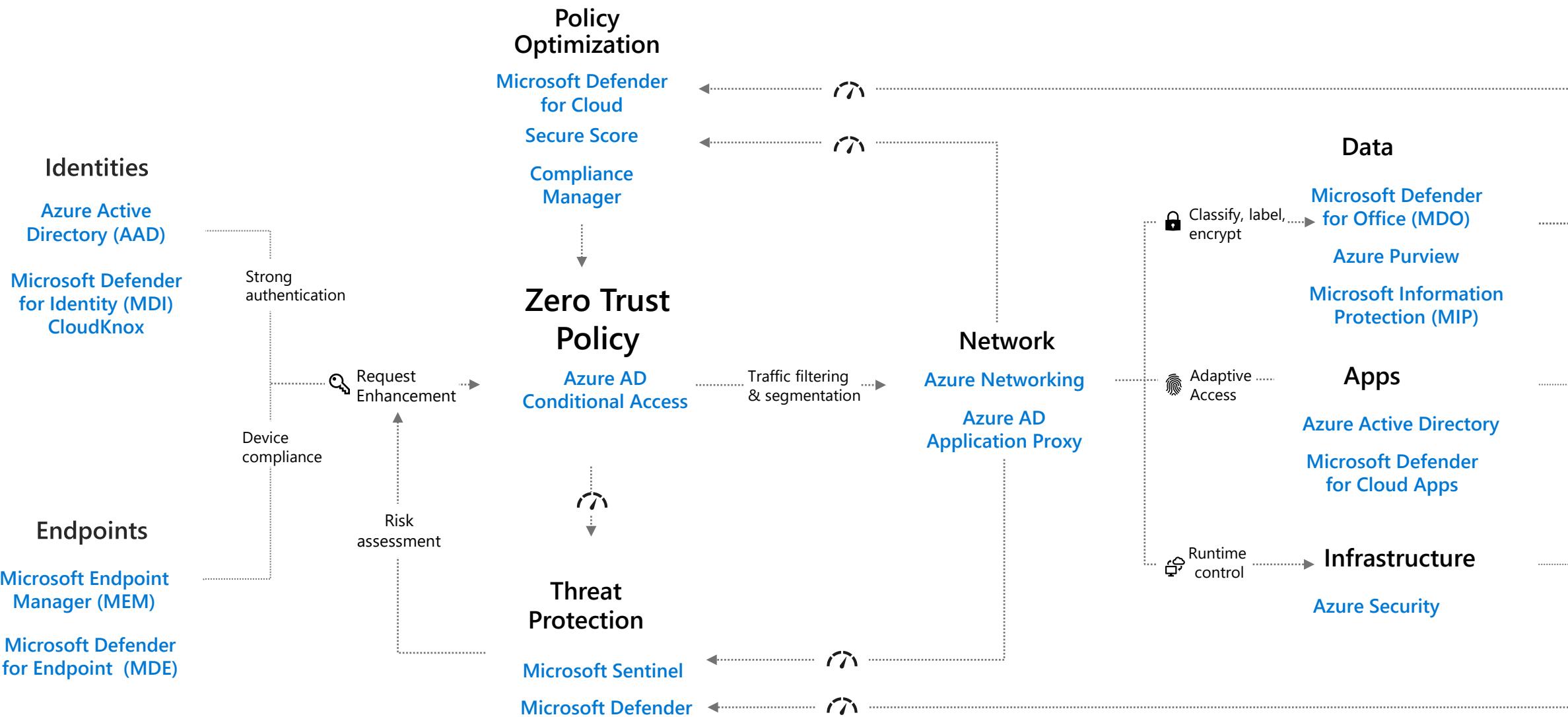


Rapid Threat Detection, Response, and Recovery

Zero Trust architecture



Microsoft Zero Trust architecture



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



Modernize identity and endpoint management



Secure the hybrid workforce

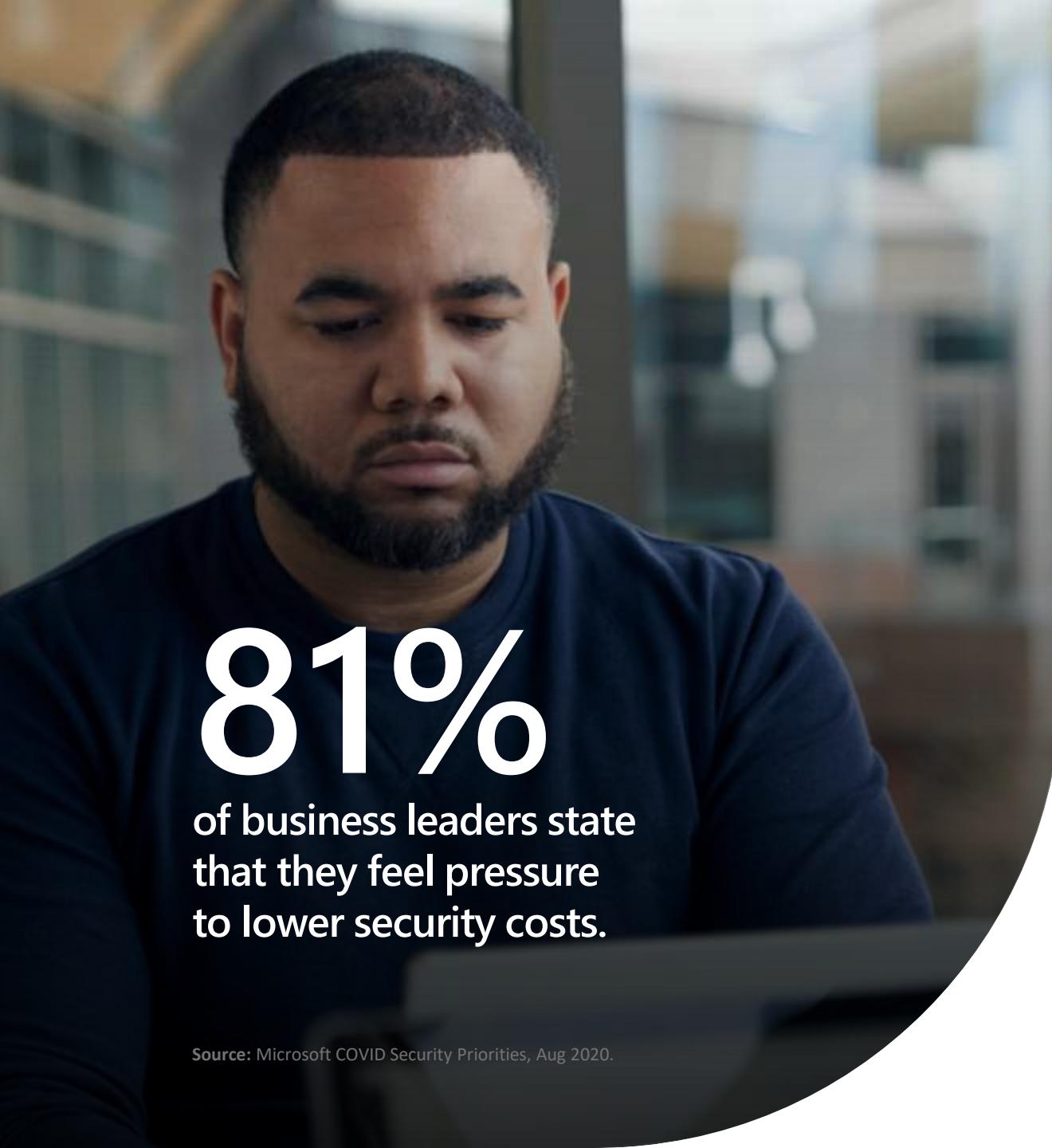


Transform employee experiences



Customize secure access for all user types





81%

of business leaders state
that they feel pressure
to lower security costs.

Source: Microsoft COVID Security Priorities, Aug 2020.

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



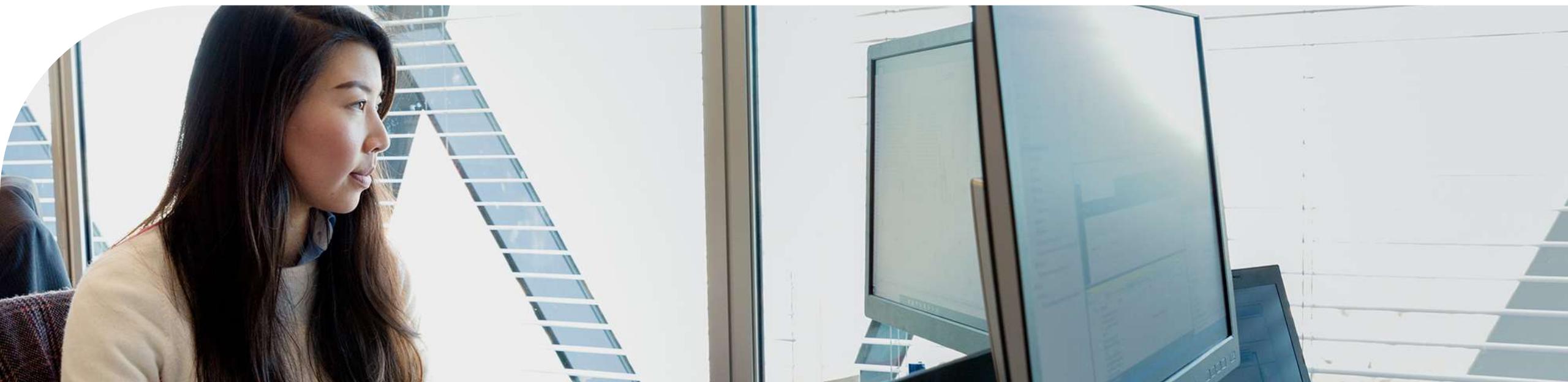
Modernize authentication and manage identities in the cloud.



Manage devices from the cloud at your own pace.

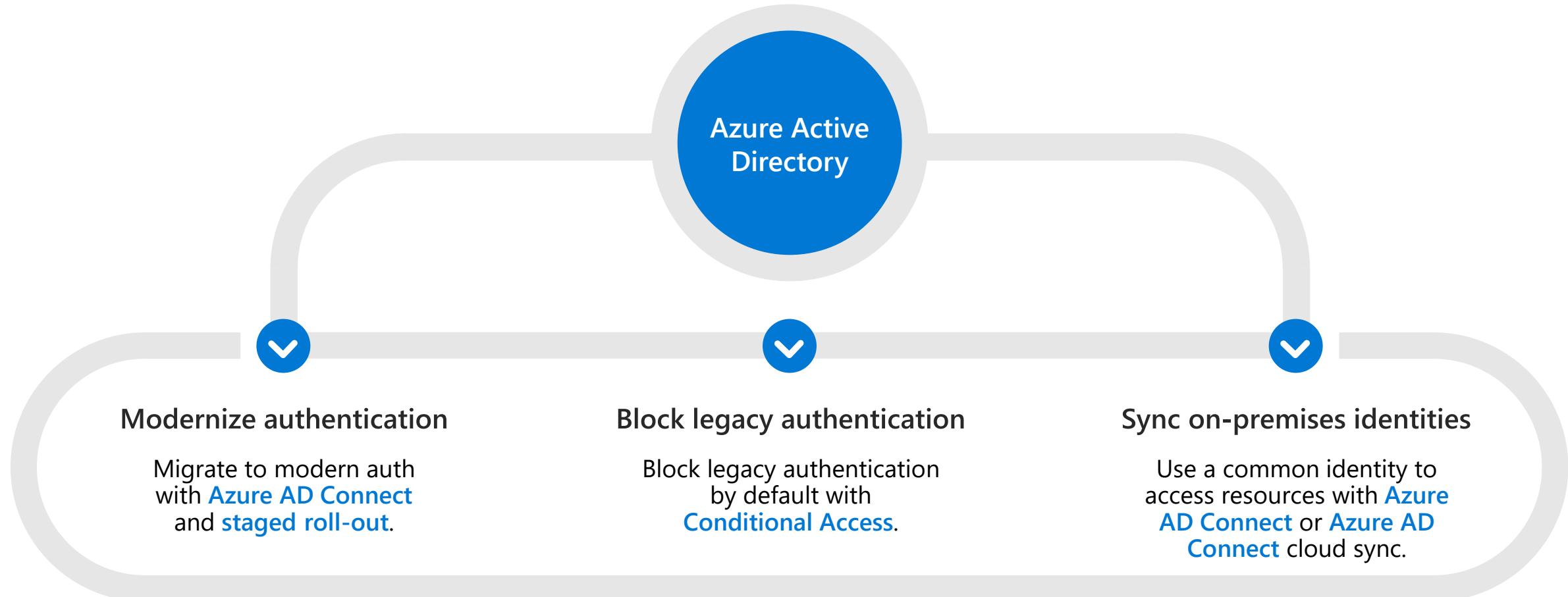


Improve visibility and control by **unifying app management**.



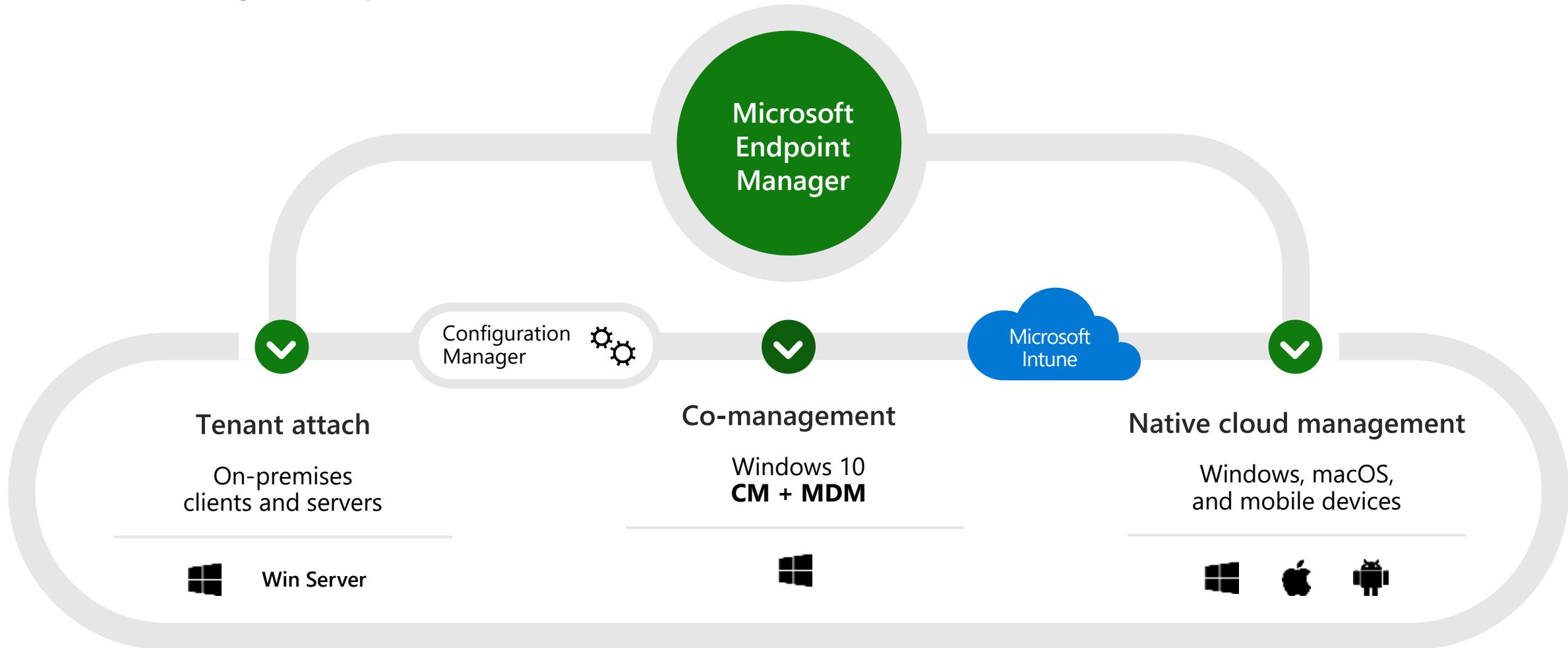
Migrate authentication and identities to the cloud

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



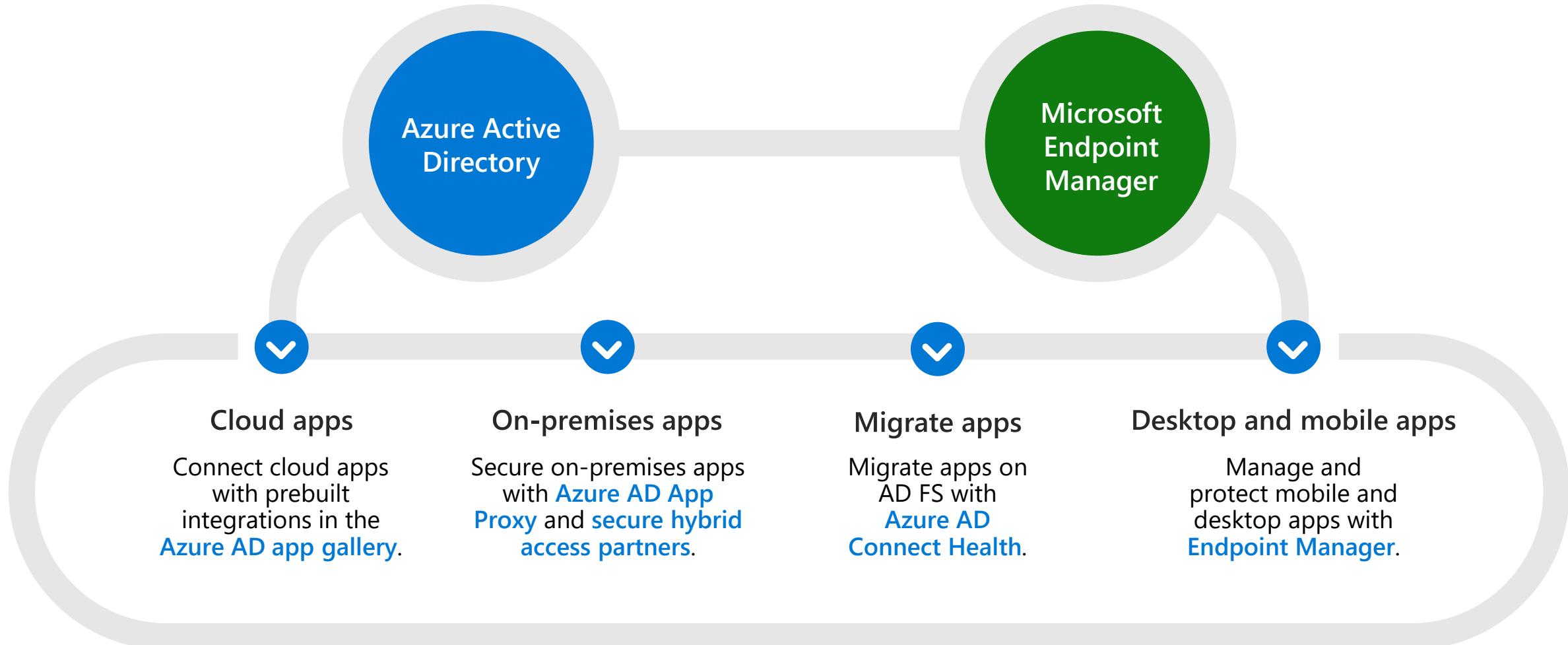
Manage endpoints in the cloud at your own pace

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



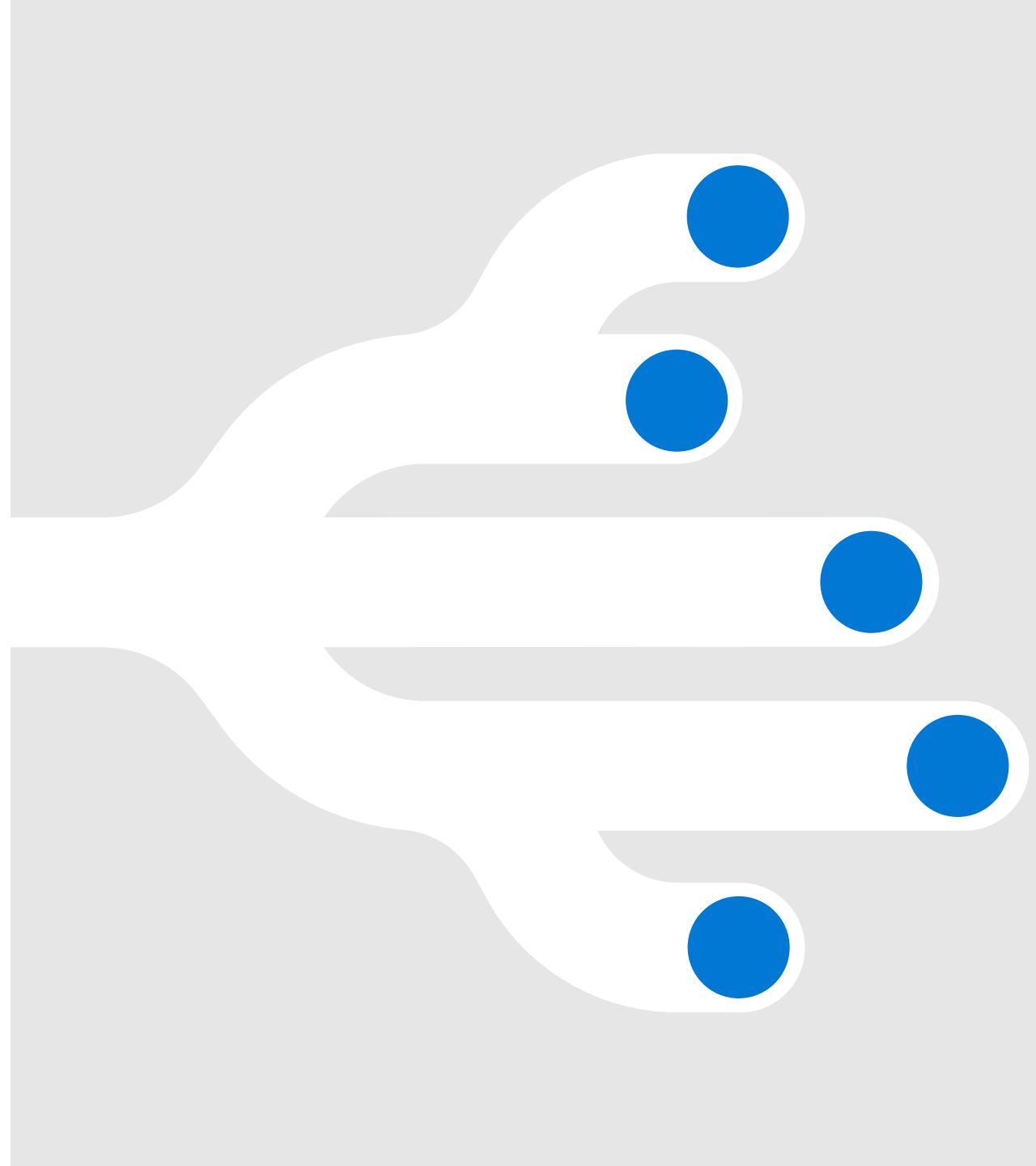
Secure the hybrid workforce



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.

Including passwordless technology



Microsoft
Authenticator



Windows
Hello



FIDO2
Security key



Biometrics



Push
notification



Soft
tokens OTP



Hard
tokens OTP



SMS,
voice

Allow only compliant devices to access data

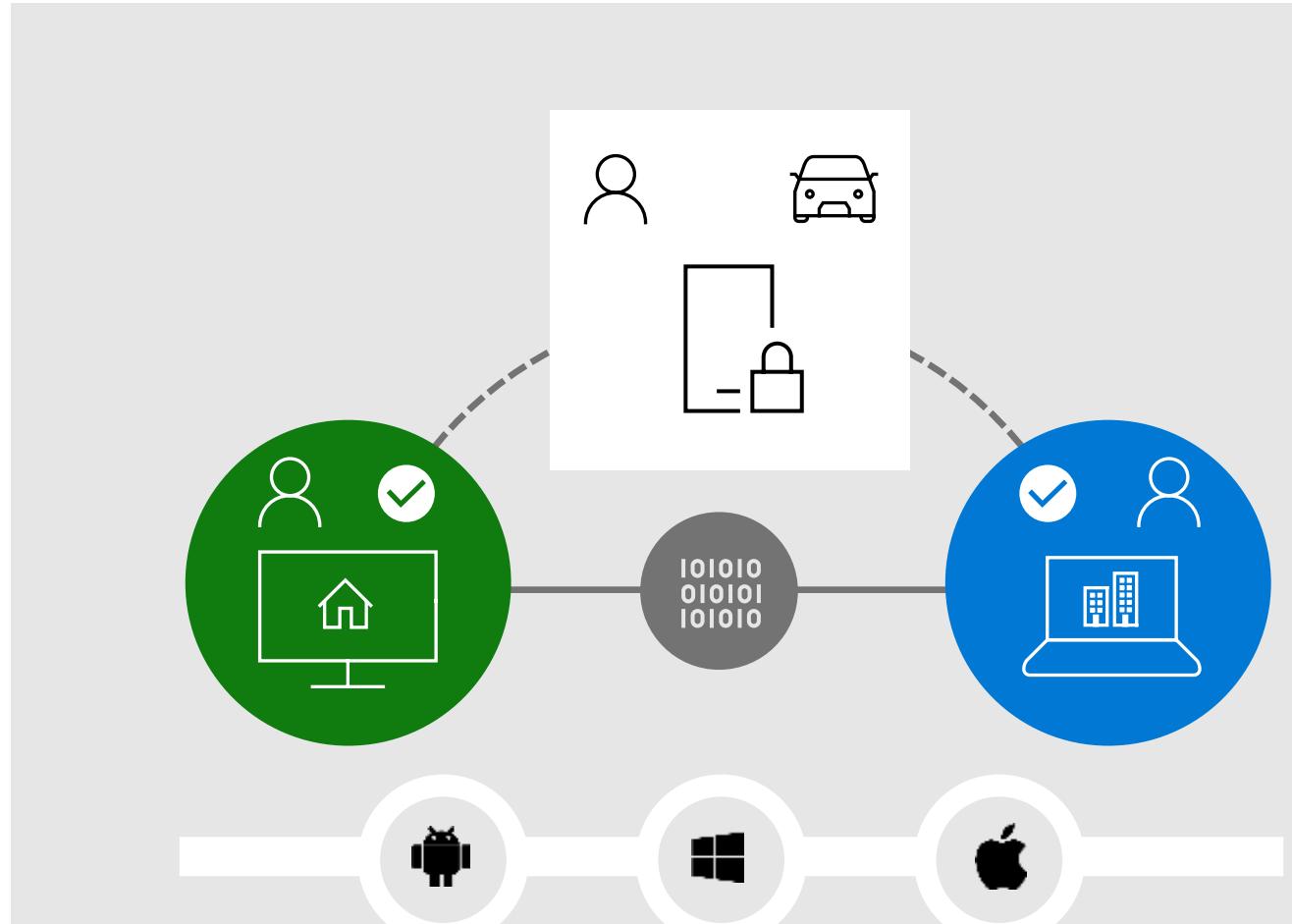
Empower IT to apply controls through endpoint cloud management

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

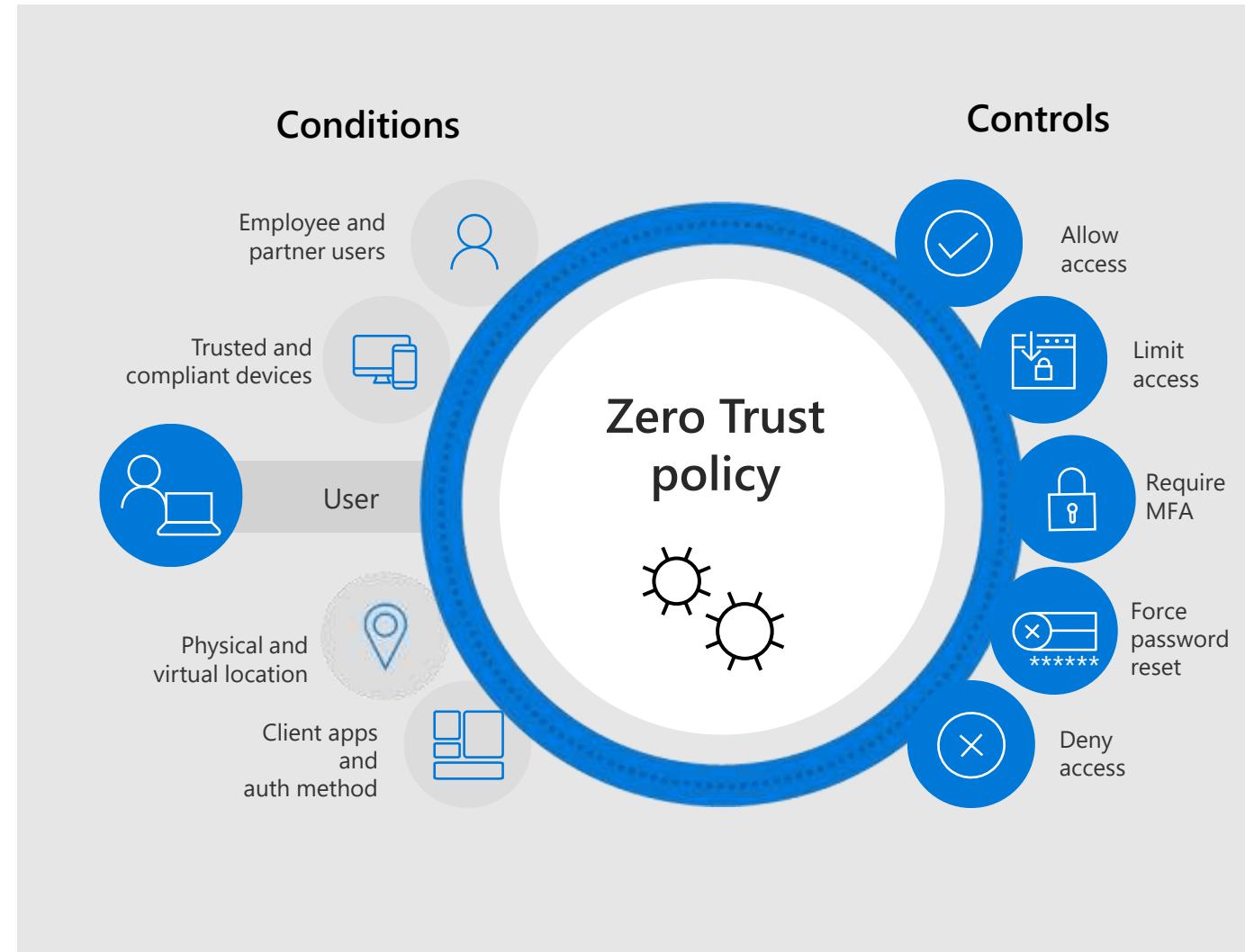
Control access with smart policies and risk assessments

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.



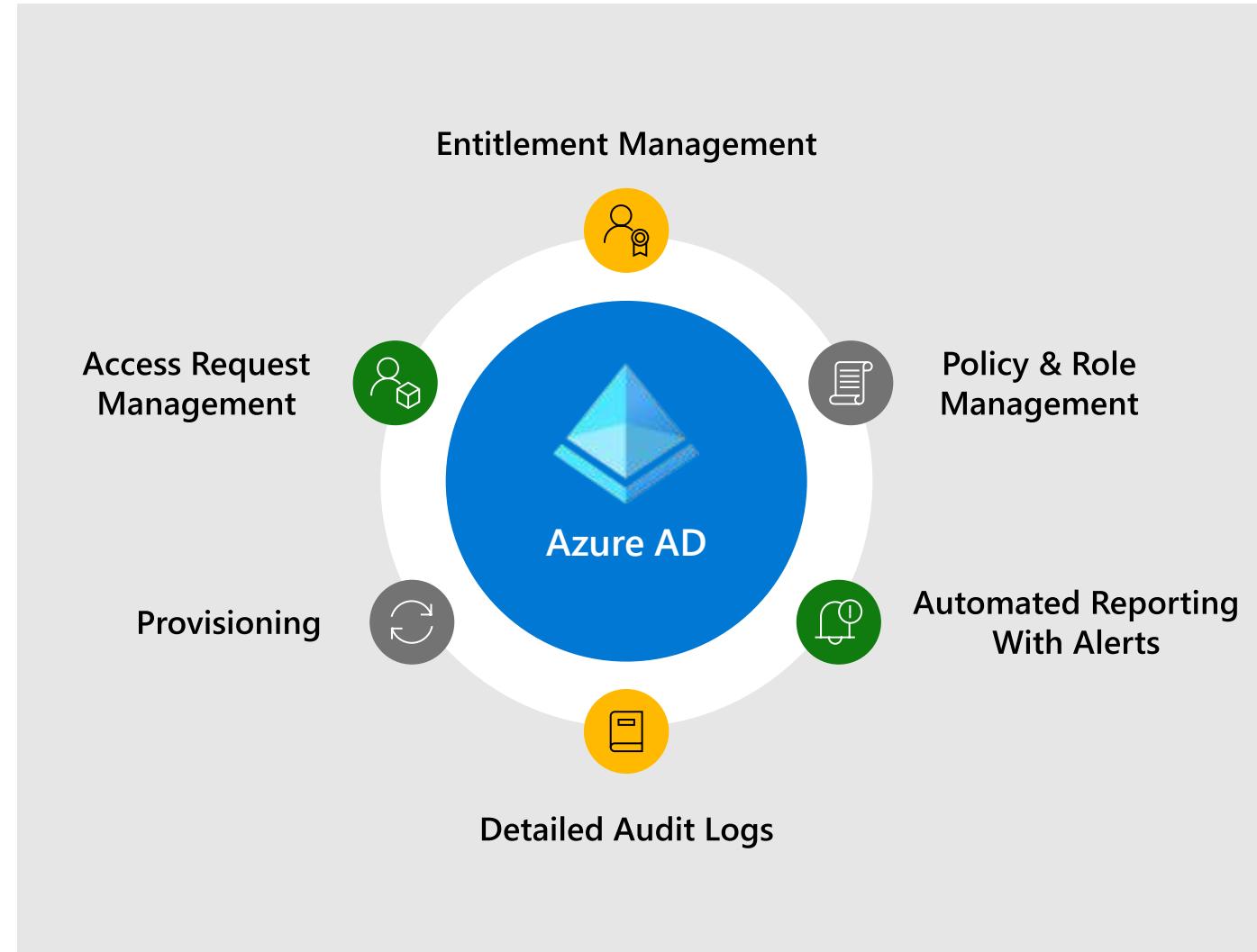
Safeguard resources with access lifecycle management

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



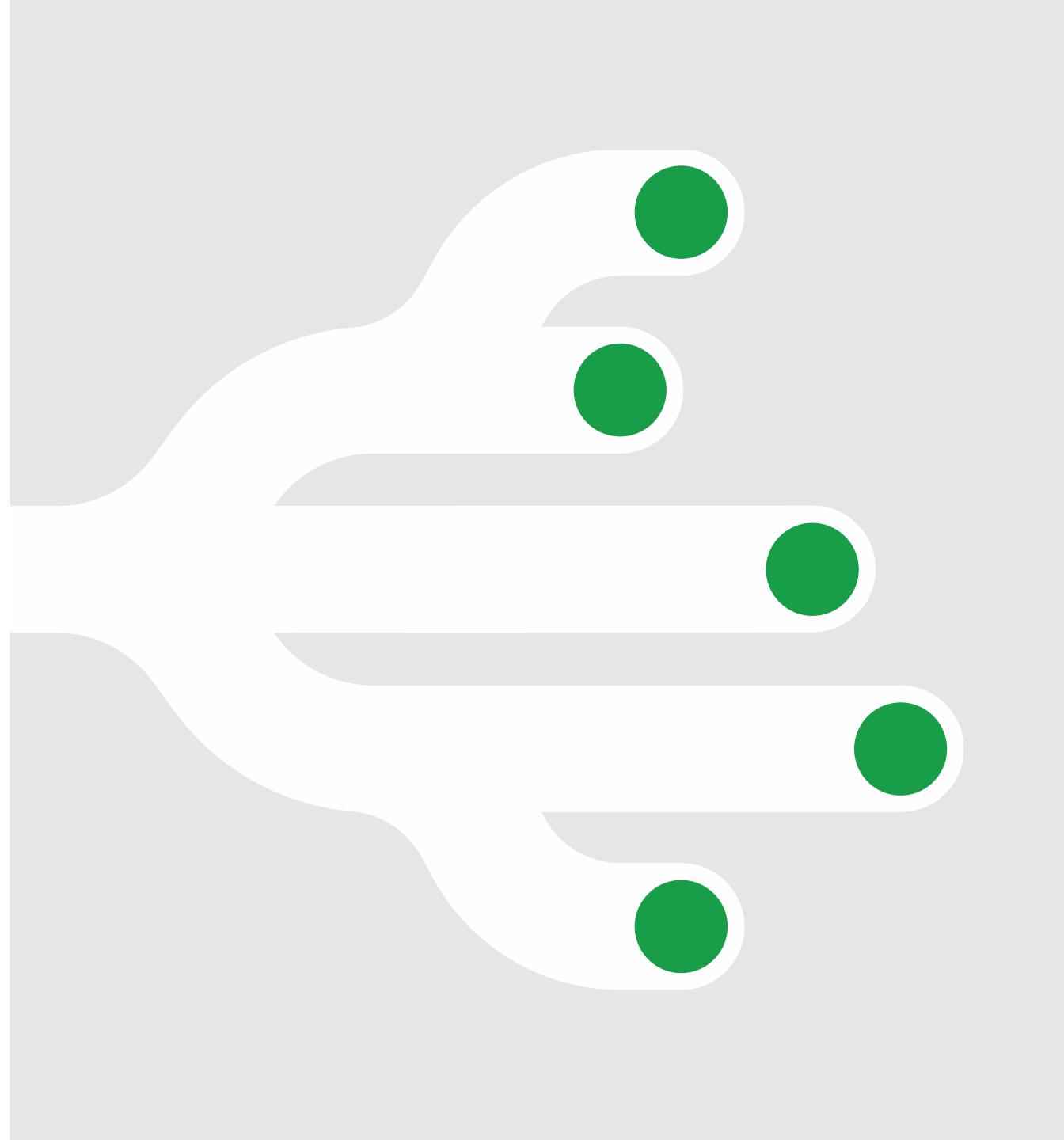
Secure the hybrid workforce



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**.



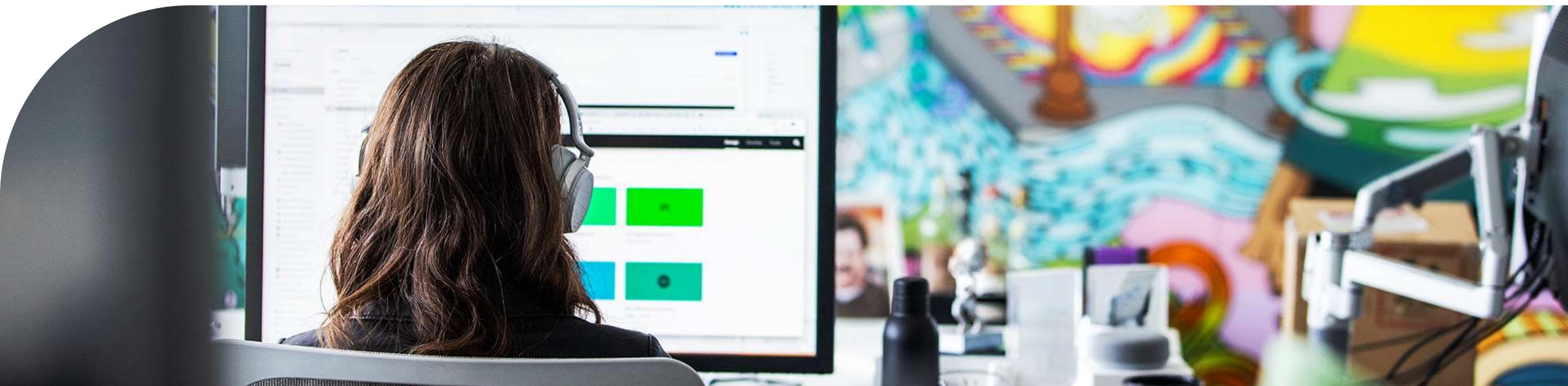
Connect your workforce to all apps with **single sign-on**.



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



Facilitate seamless **collaboration across organizational boundaries**.



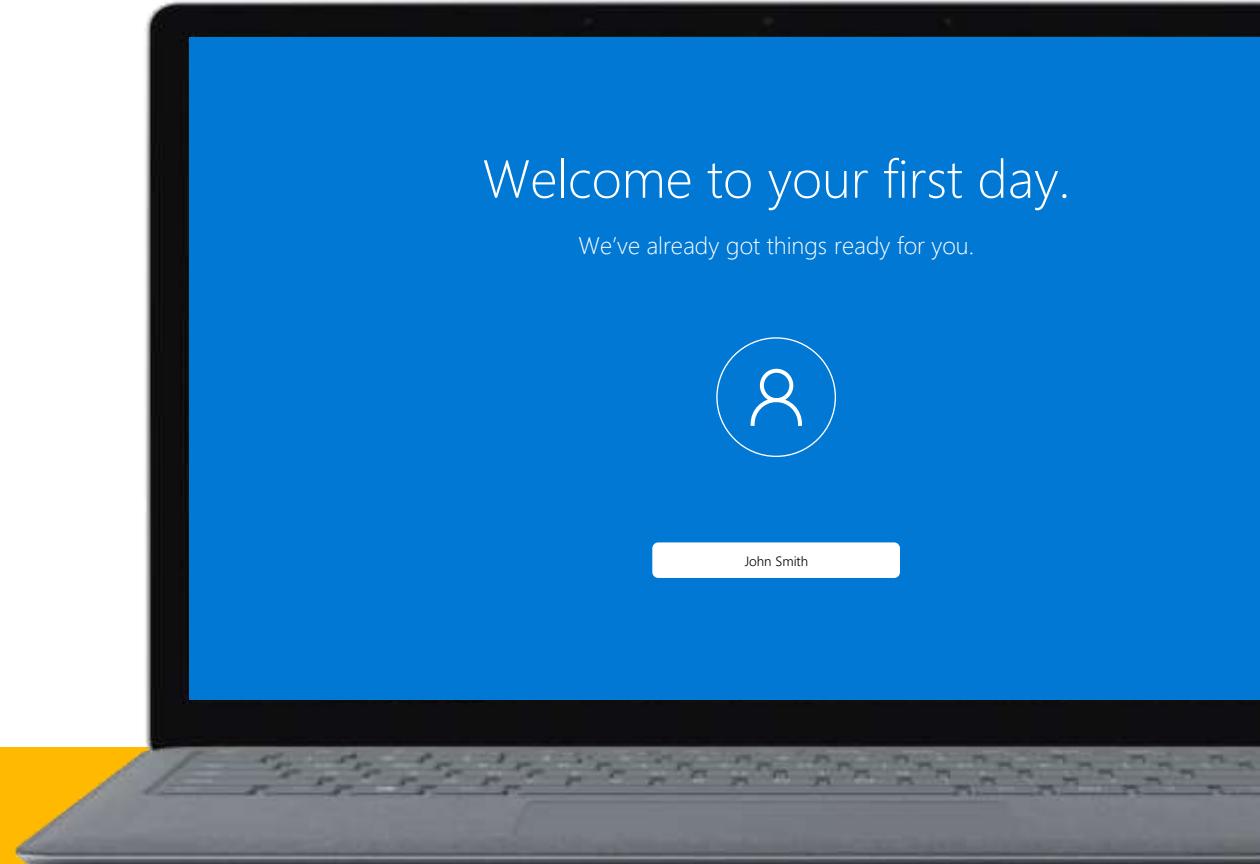
Provision access to resources efficiently

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.



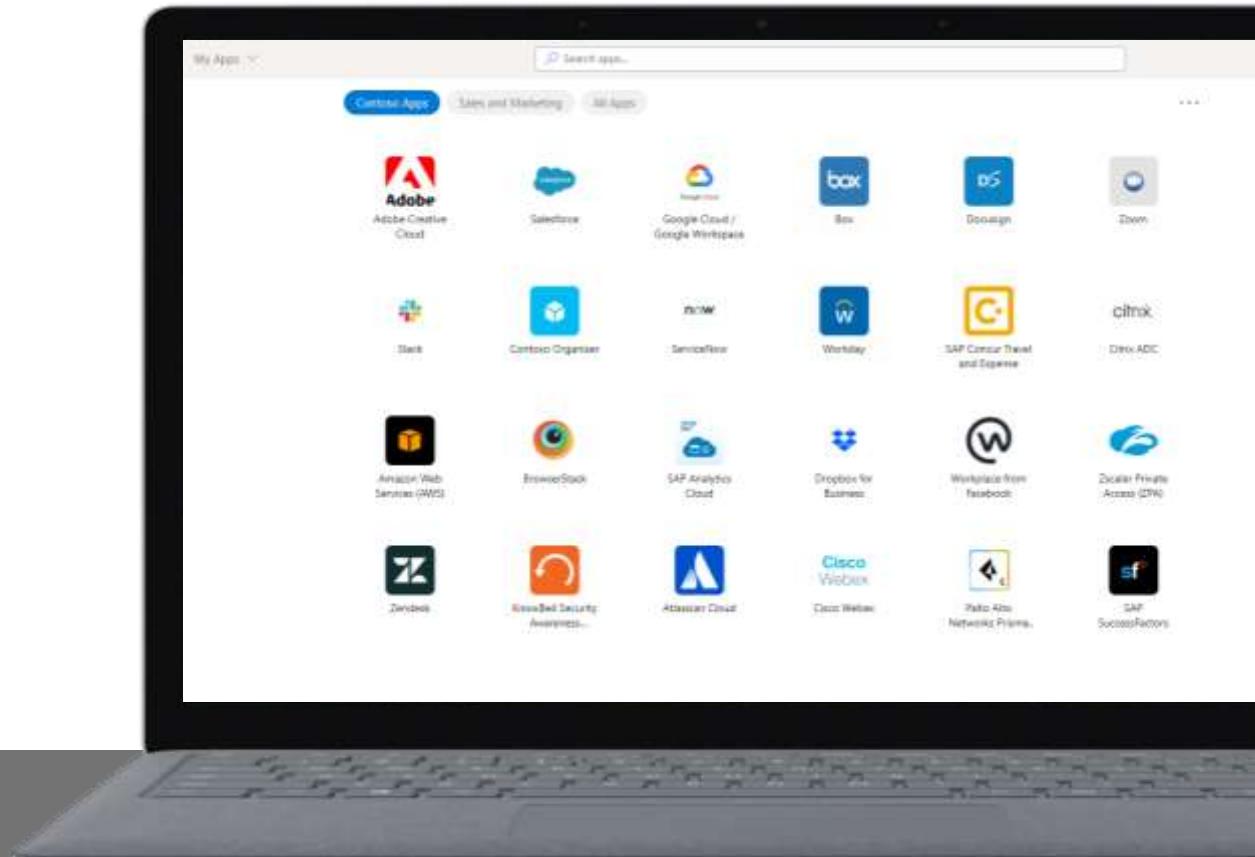
Enable seamless, secure access with single sign-on

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.



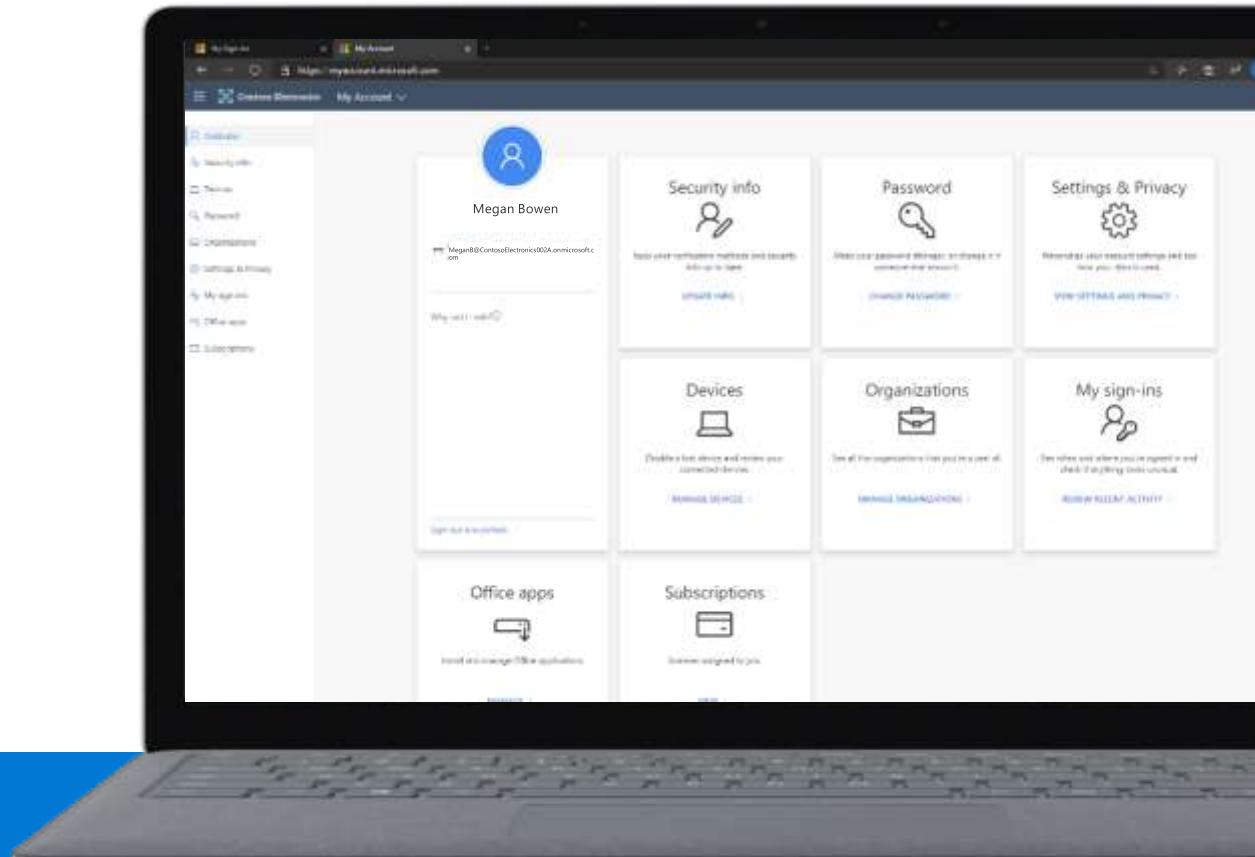
Empower employees to manage their own identity

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.



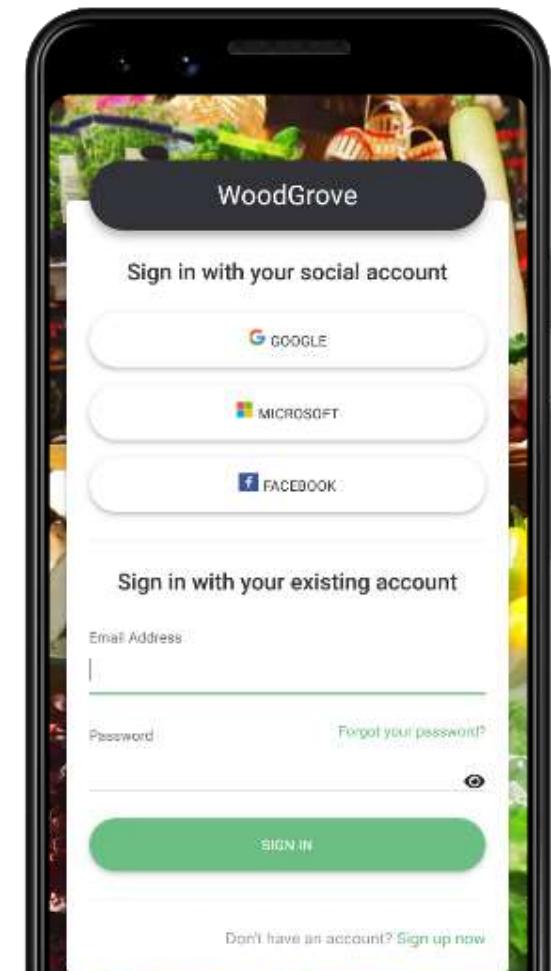
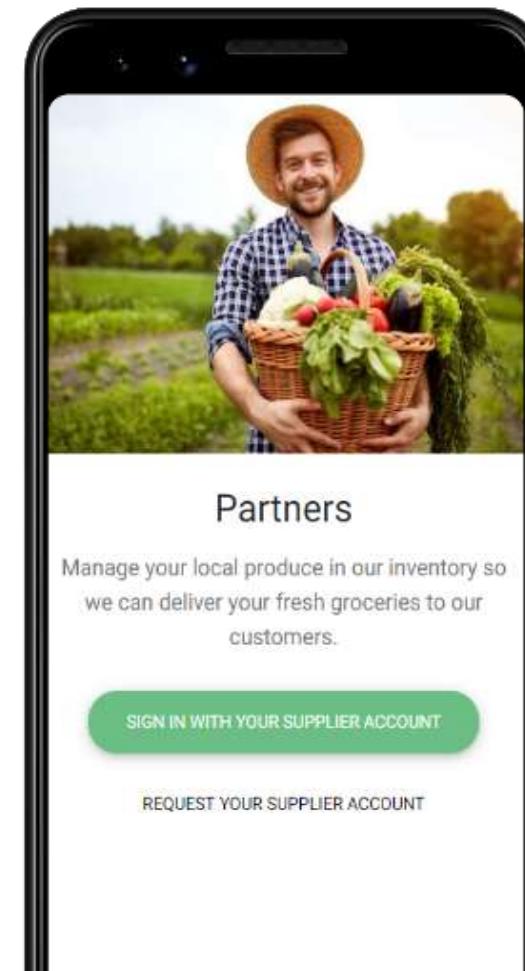
Collaborate seamlessly with partners

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



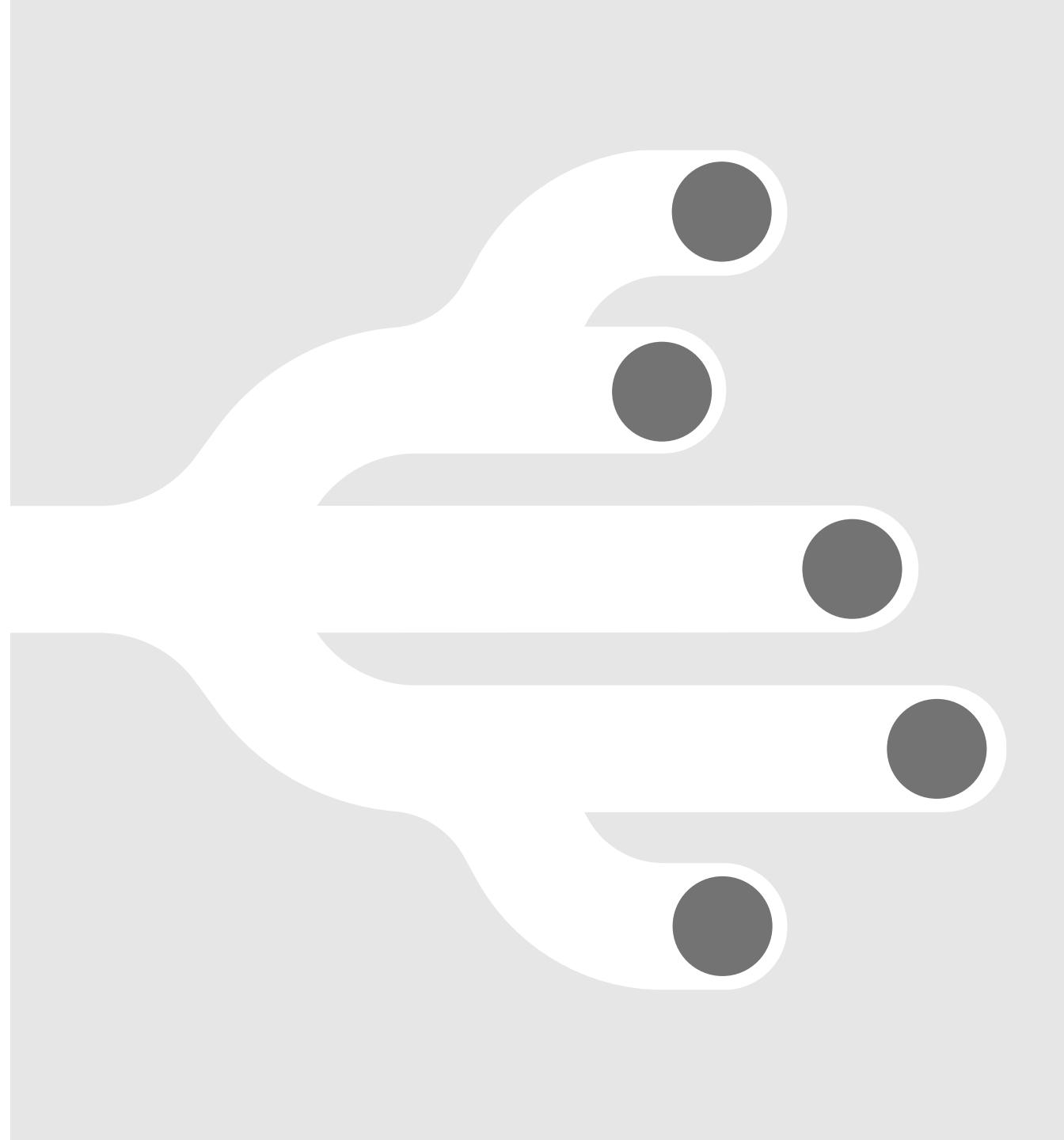
Secure the hybrid workforce



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**.



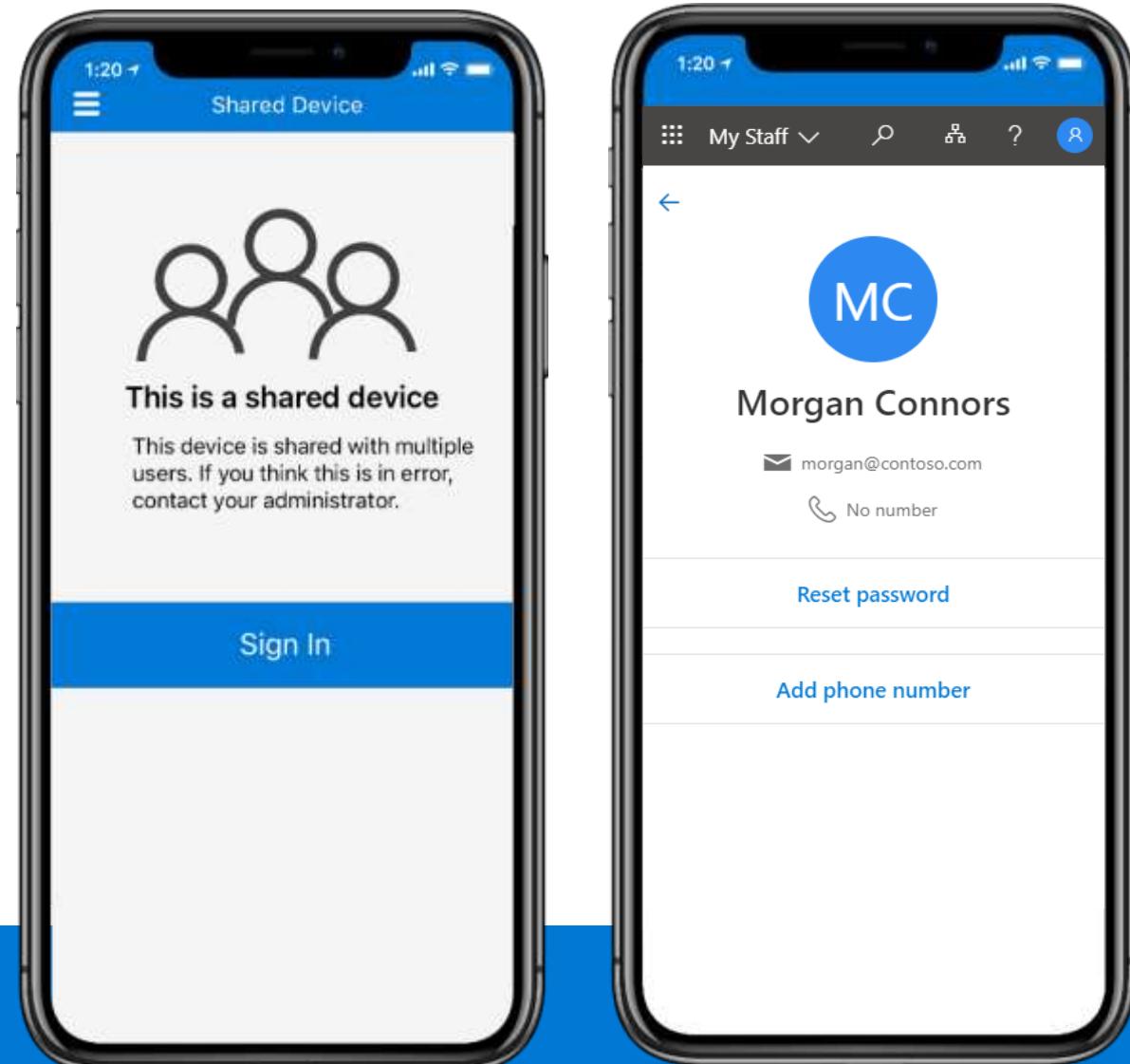
Empowering frontline workers

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.



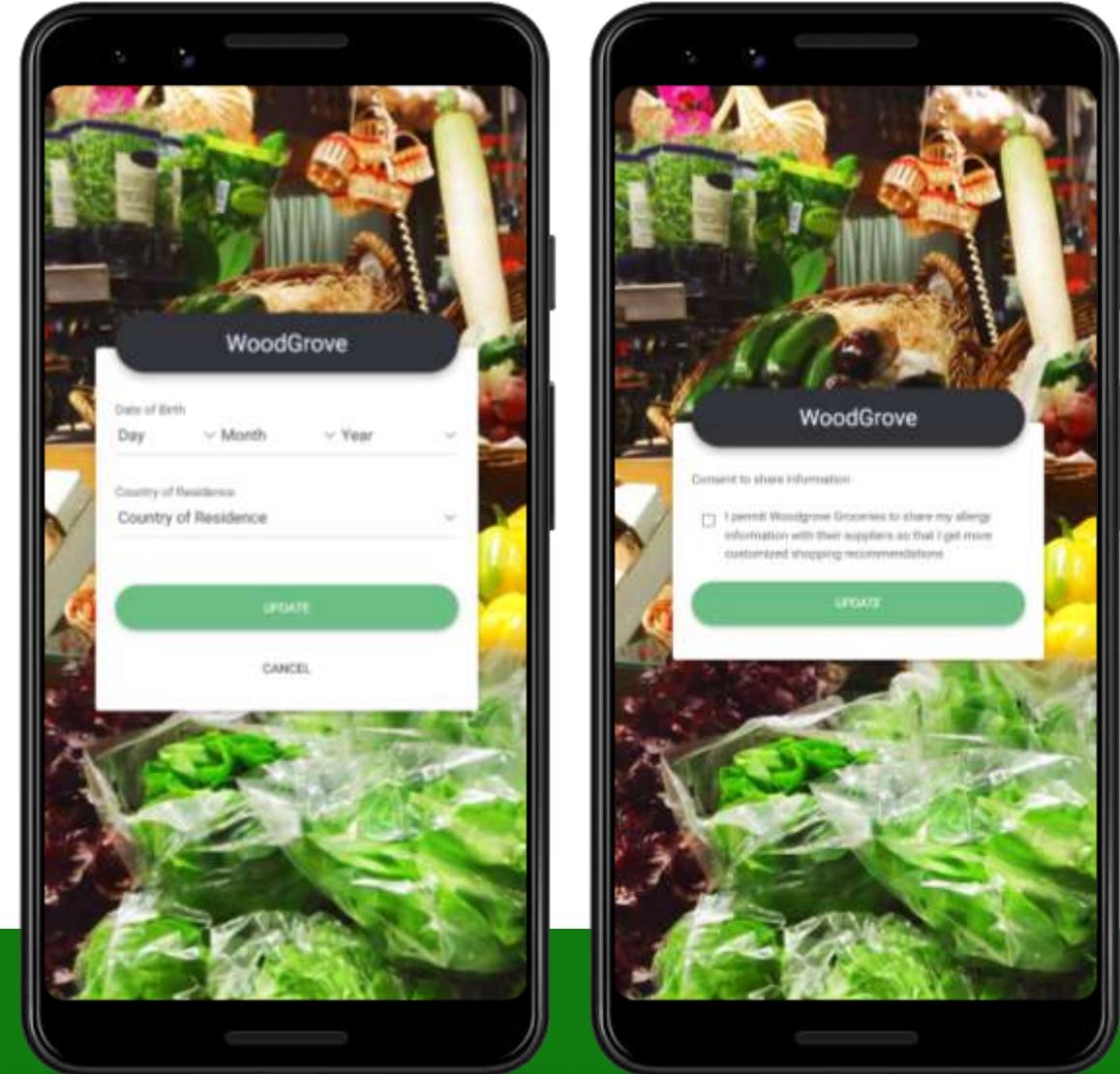
Build secure customer apps

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.



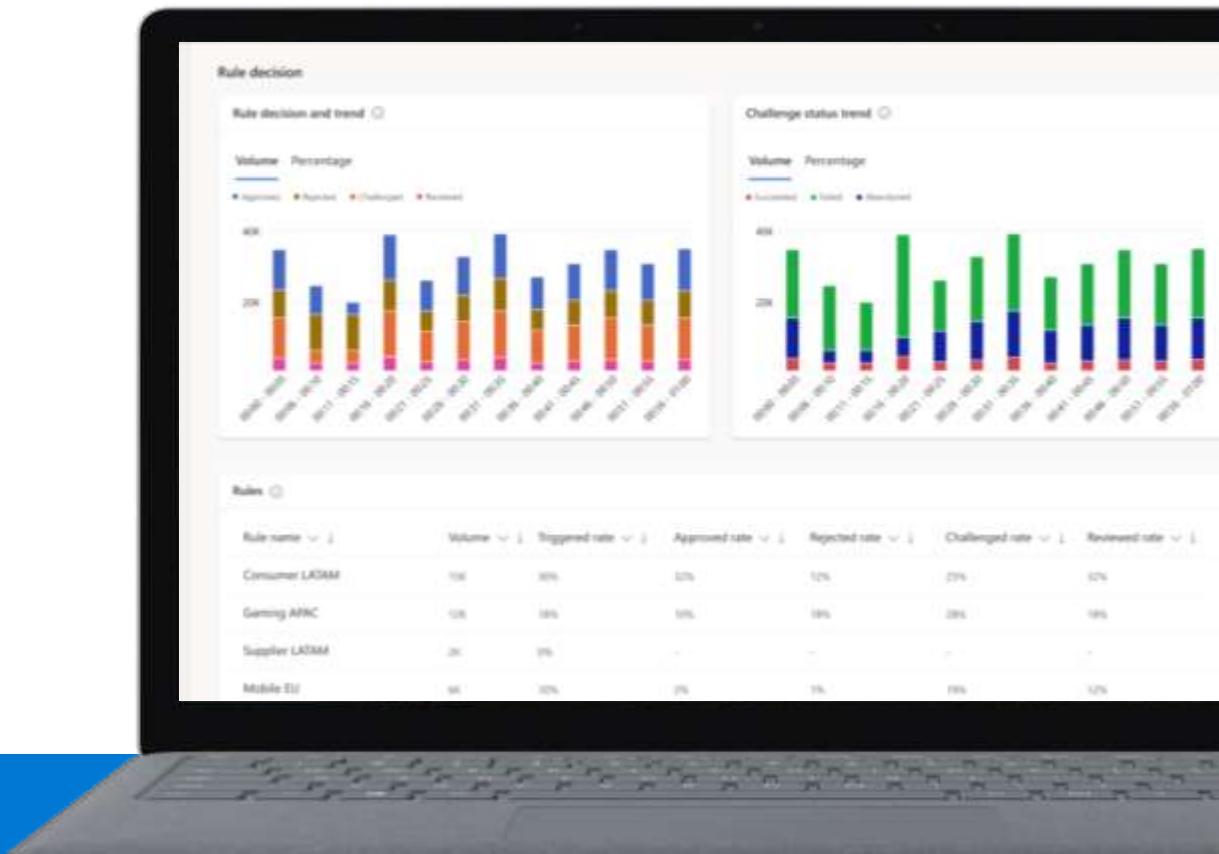
Protect your revenue and customers

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.



Microsoft security and compliance

Safeguard your people, data, and infrastructure



Protect everything

Safeguard your entire organization with integrated security, compliance, and identity solutions built to work across platforms and cloud environment



Simplify the complex

Prioritize the right risks with unified management tools created to maximize the human expertise inside your company



Catch what others miss

Leading AI, automation, and expertise help you detect threats quickly, respond effectively, and fortify your security posture



Grow your future

With the peace of mind that comes with a comprehensive security solution, you're free to grow, create, and innovate your business

Enable Zero Trust with Microsoft security solutions



Protect identities and manage access

Safeguard access to resources with a complete identity solution that securely connects all your users, apps, and devices



Stop threats with integrated, automated protection

Secure your business with security information and event management (SIEM) and extended detection and response (XDR)



Secure your apps and resources across clouds

Safeguard your entire cloud estate with complete visibility and comprehensive protection across workloads



Protect and govern sensitive data

Safeguard data across clouds, apps, and endpoints by configuring protection and retention labels



Identify and remediate risks

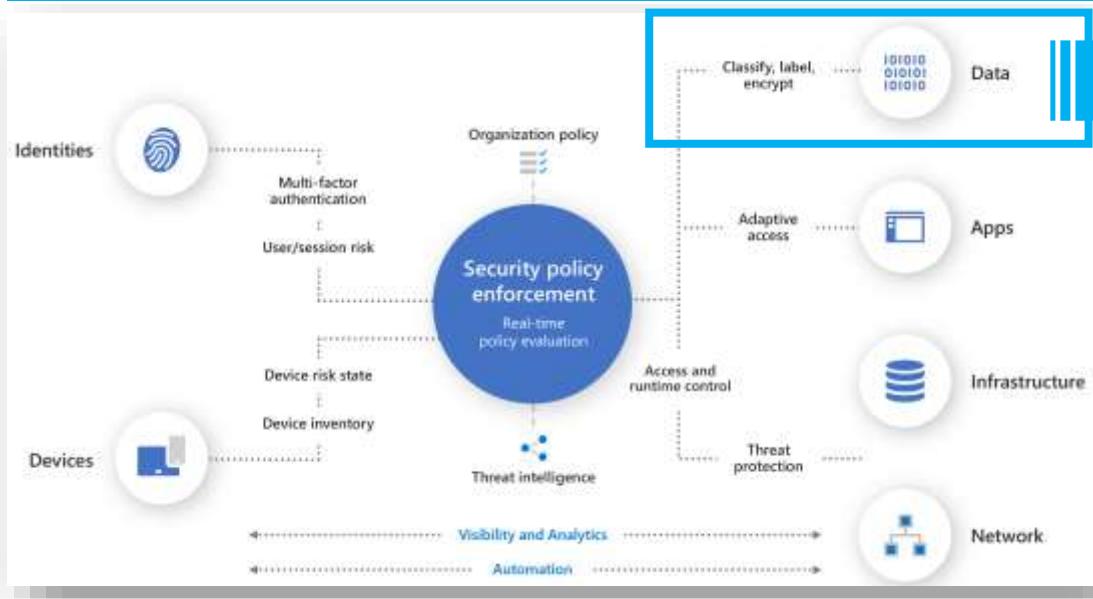
Prevent, investigate, and remediate both malicious and inadvertent activities within your organization



Simplify compliance & privacy management

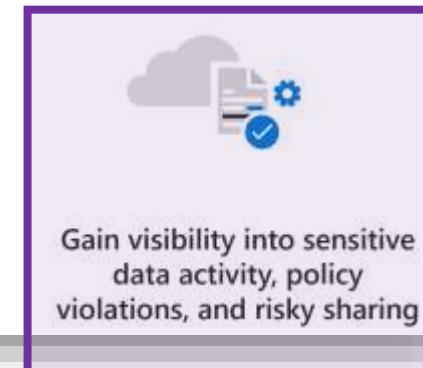
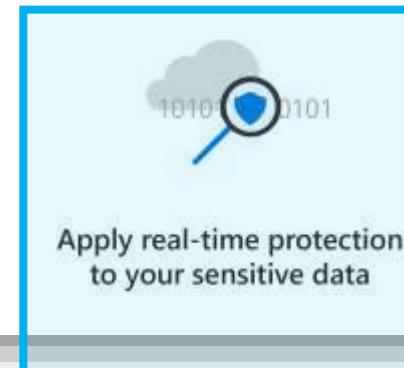
Assess, improve, and monitor compliance to address legal and regulatory compliance requirements

Zero Trust architecture



Compliance & Data Protection

Protect your sensitive data—
wherever it lives or travels



1

- Identify your legal and regulatory requirements
- Build your classification and labelling framework (e.g. public, confidential, highly confidential)

2

- Implement a multilayered information protection strategy:
- Automatically apply a sensitivity label to documents
 - Automatically enforce protection policies (e.g.: encryption)
 - Automatically limit access to the right people

3

- Monitor your sensitive data landscape
- Respond to data leak scenarios
- Respond to legal investigations and data access requests

M365
Information Protection and Governance

Microsoft Information Protection (MIP)

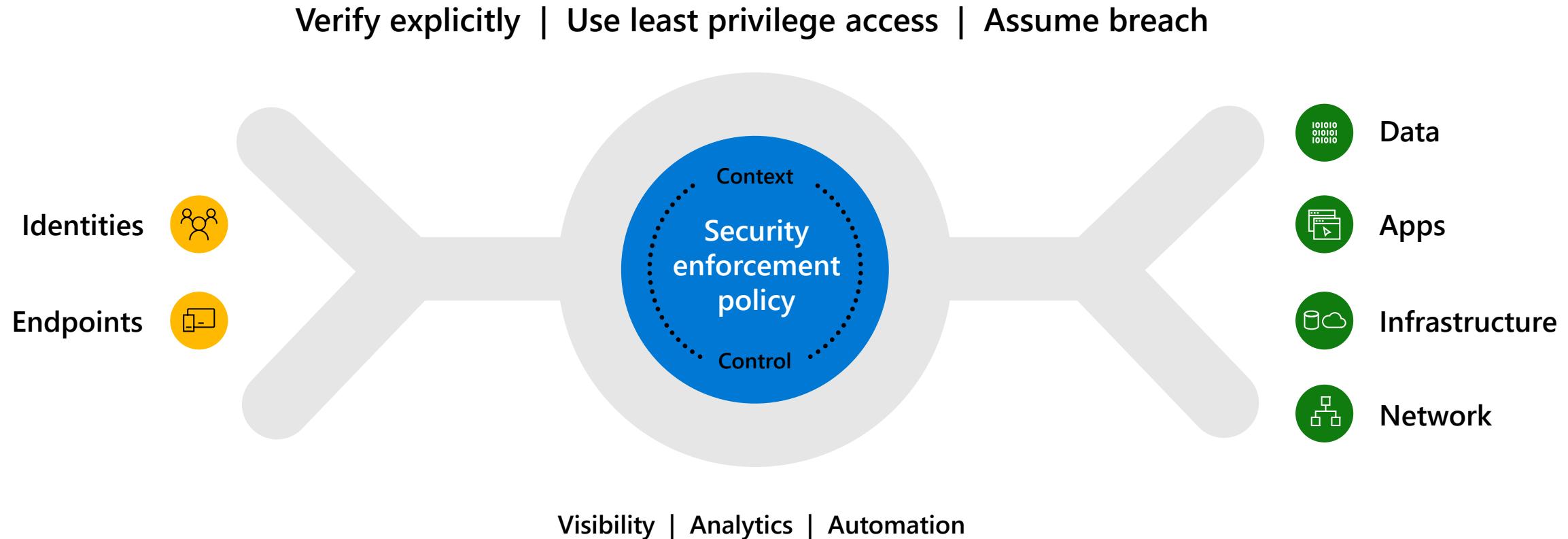
Data Loss Prevention (DLP)

Retention Policies

M365 Discover and Respond (eDiscovery)

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

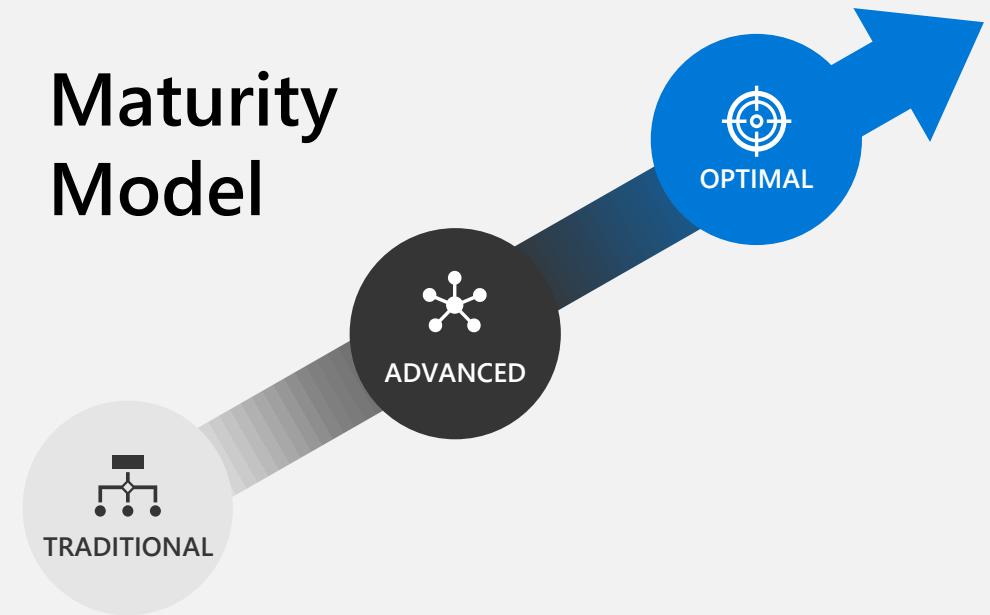
Get started modernizing identities and endpoints with [FastTrack](#).

3

Advance your Zero Trust journey by diving deeper with us on a [specific area](#).

Making Zero Trust a reality

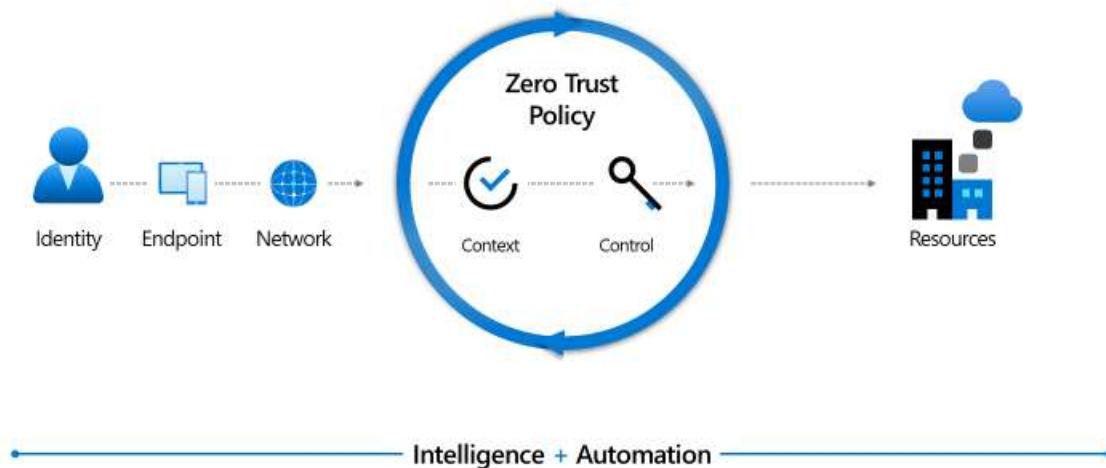
- Do you grok Zero Trust?
- Have you established a v-team with your stakeholders?
- Do you know where you want to arrive?
- Do you know where you are at today?
- Do you have buy-in from C-level to bridge that gap?



Download today at
aka.ms/ztmmodel

Zero Trust networking maturity model

Zero Trust



Traditional

Few network security perimeters and flat open network

Minimal threat protection and static traffic filtering

Internal traffic is not encrypted

Many ingress/egress

Advanced

cloud micro-perimeters with some micro-segmentation

Cloud native filtering and protection for known threats

User to app internal traffic is encrypted

Fully distributed

Optimal

ingress/egress cloud micro-perimeters and deeper micro-segmentation

ML-based threat protection and filtering with context-based signals

All traffic is encrypted

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)

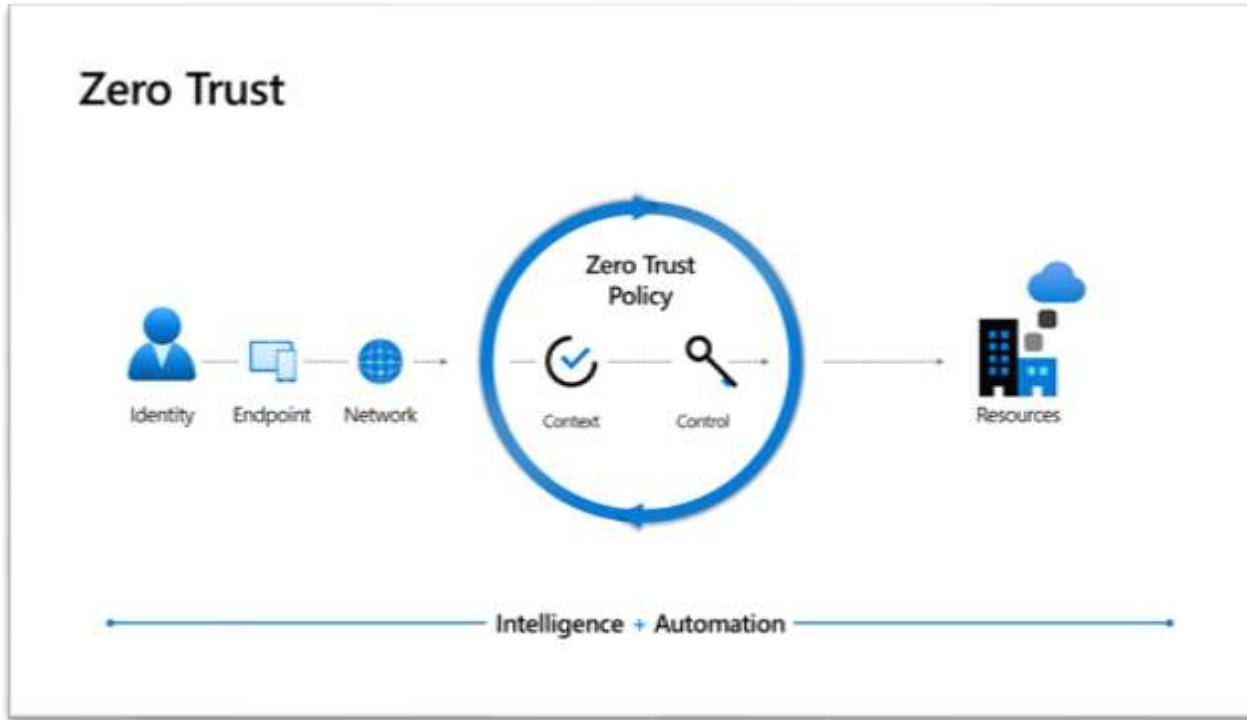


Datacenter &
DevOps Security

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

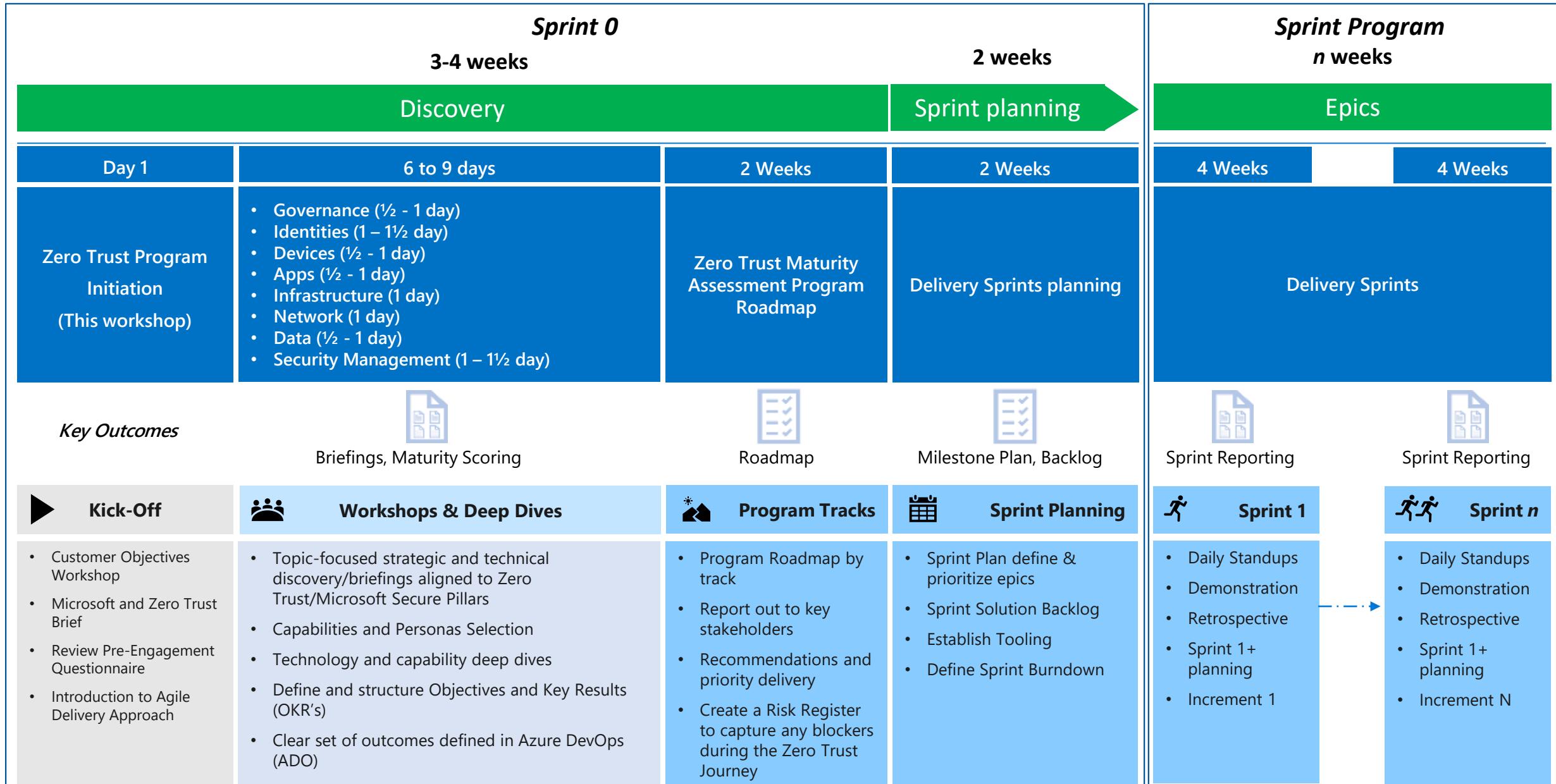
Zero Trust Resources



- 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](#)

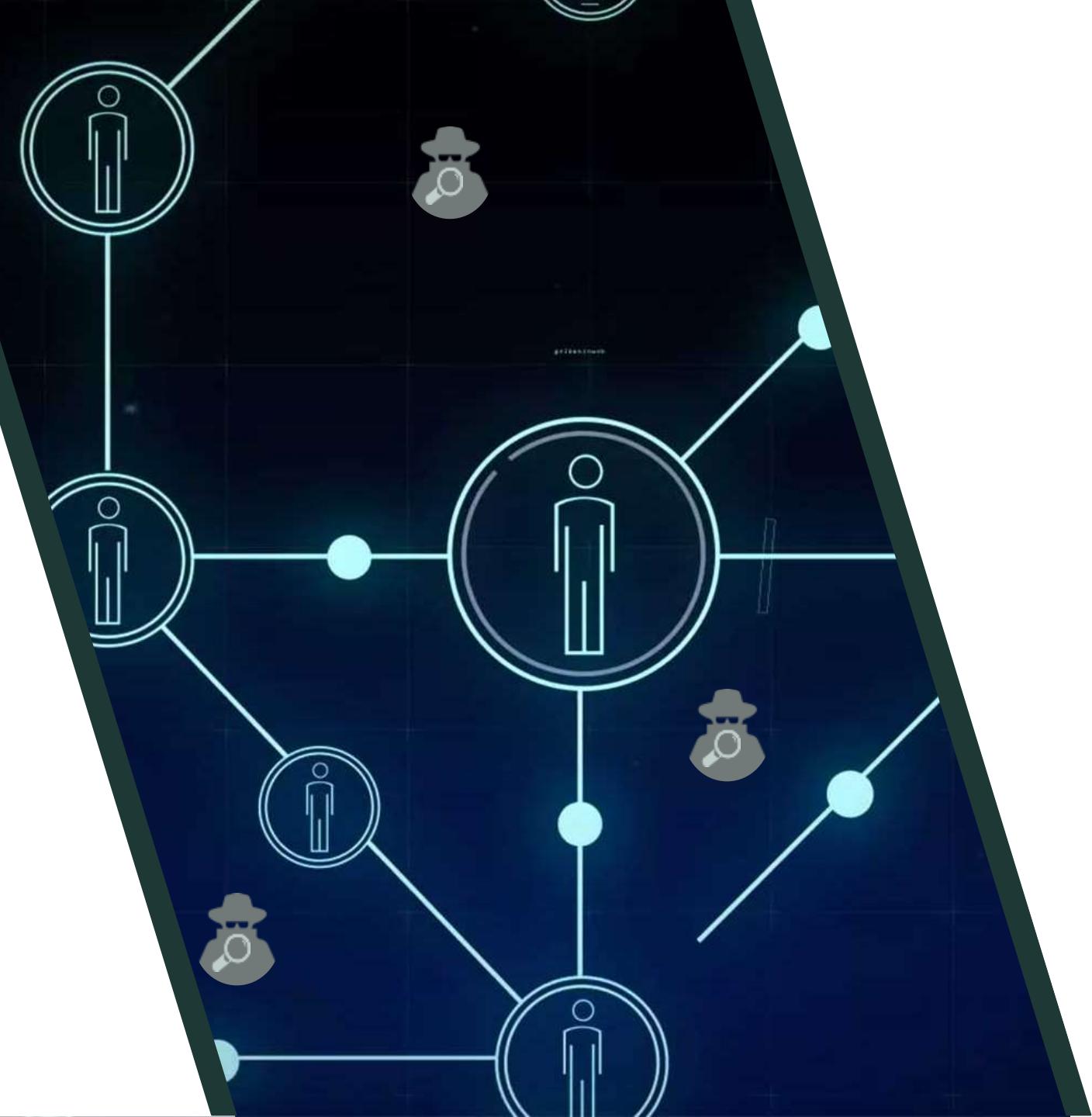
- 
- Zero Trust: Security Through a Clearer Lens session ([Recording](#) | [Slides](#))
 - [CISO Workshop Slides/Videos](#)
 - [Microsoft's IT Learnings](#) from (ongoing) Zero Trust journey

Zero Trust Program Approach (Example)

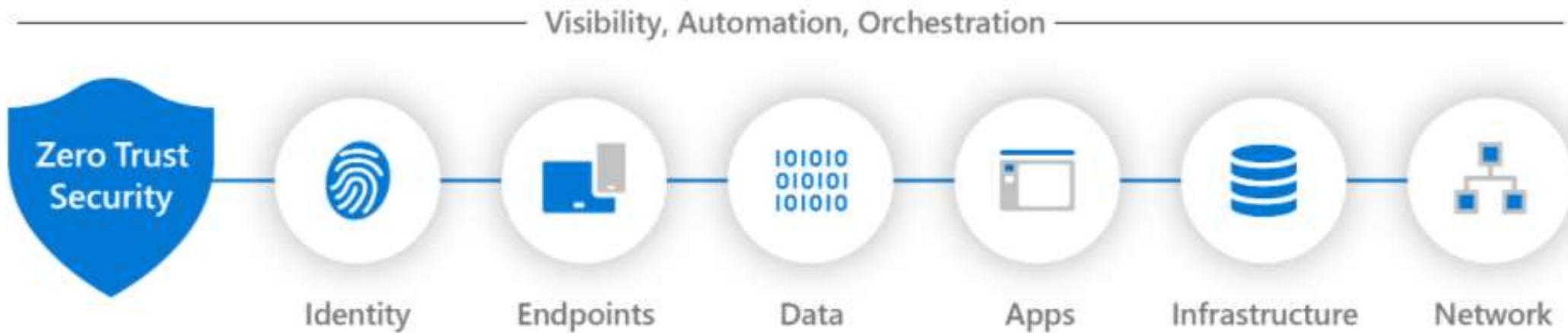




Zero Trust and Microsoft Controls across M365 & Azure



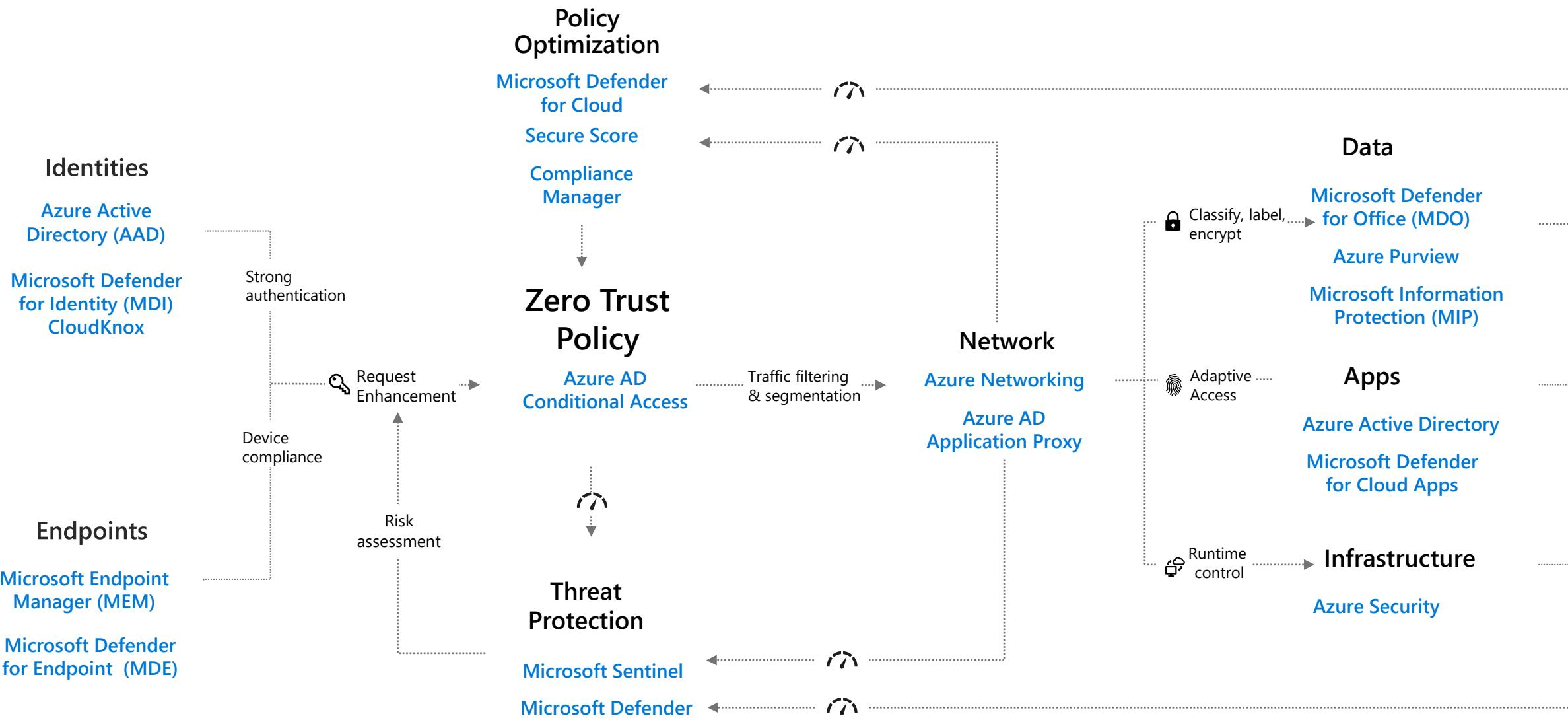
Assess Zero Trust readiness and build a plan



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



Securing identity with Zero Trust

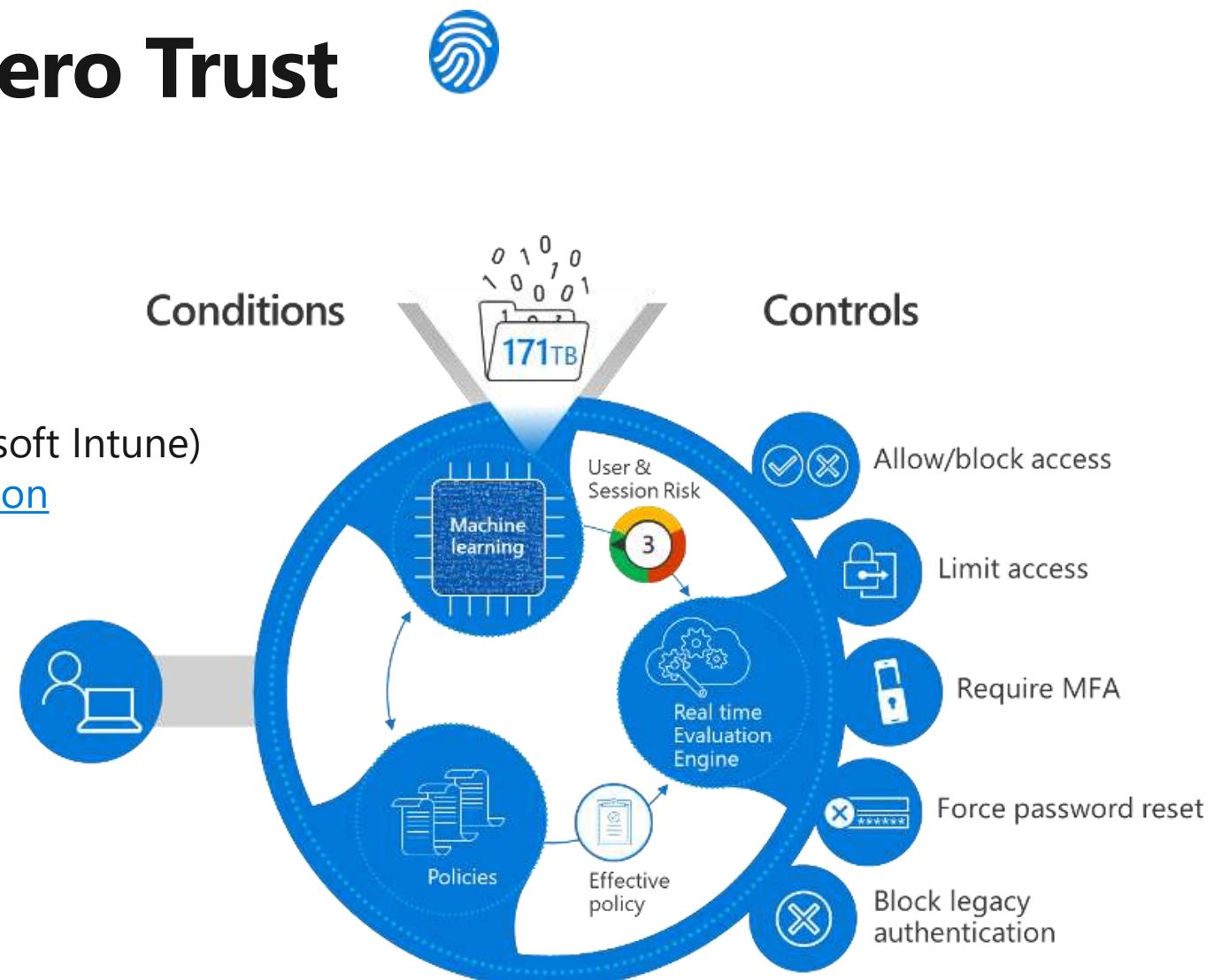


Microsoft Azure

- [Azure Active Directory](#)
- [Azure Advanced Threat Protection](#)

Microsoft 365

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



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](#)

Microsoft Defender ATP



Threat & Vulnerability
Management



Attack surface
reduction



Next-generation
protection



Endpoint detection
and response



Automated investigation
and remediation



Microsoft
Threat Experts

Centralized configuration and administration, APIs

Microsoft Threat Protection

Secure data with Zero Trust

101010
010101
101010

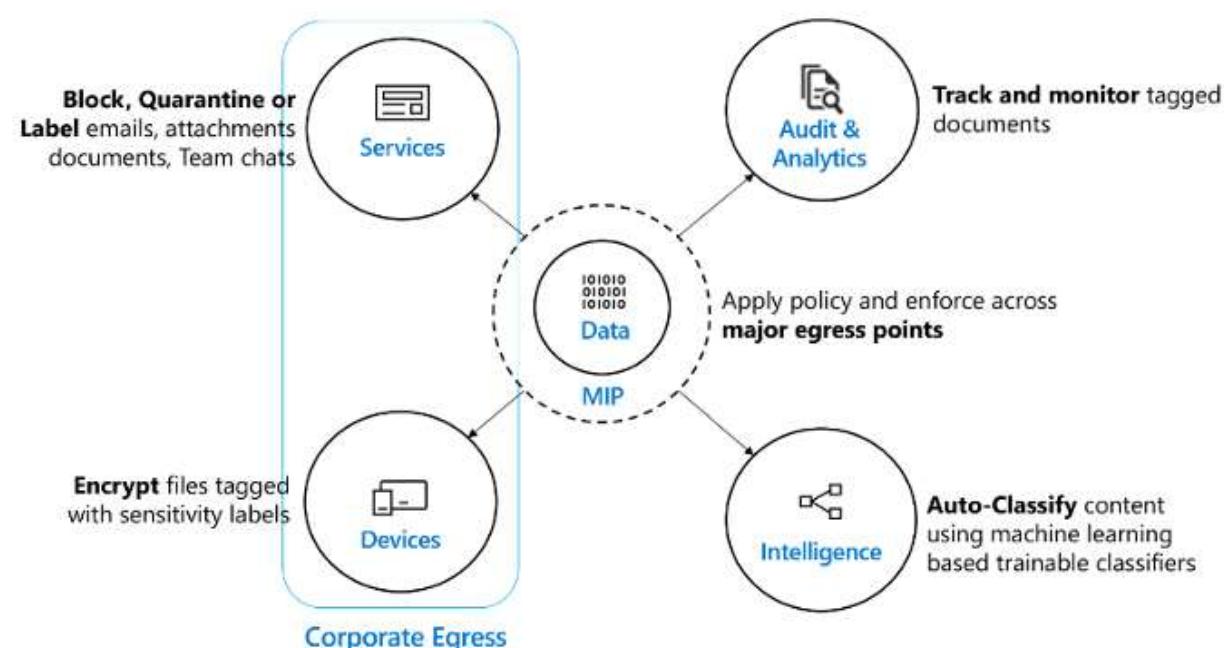
Microsoft Azure

- [Azure Information Protection](#) with Unified Labeling Client and Scanner

Microsoft 365

- [Microsoft Cloud App Security](#)

Microsoft Information Protection (MIP) is a comprehensive, flexible, integrated, and extensible approach to protecting sensitive data.



Secure applications with Zero Trust

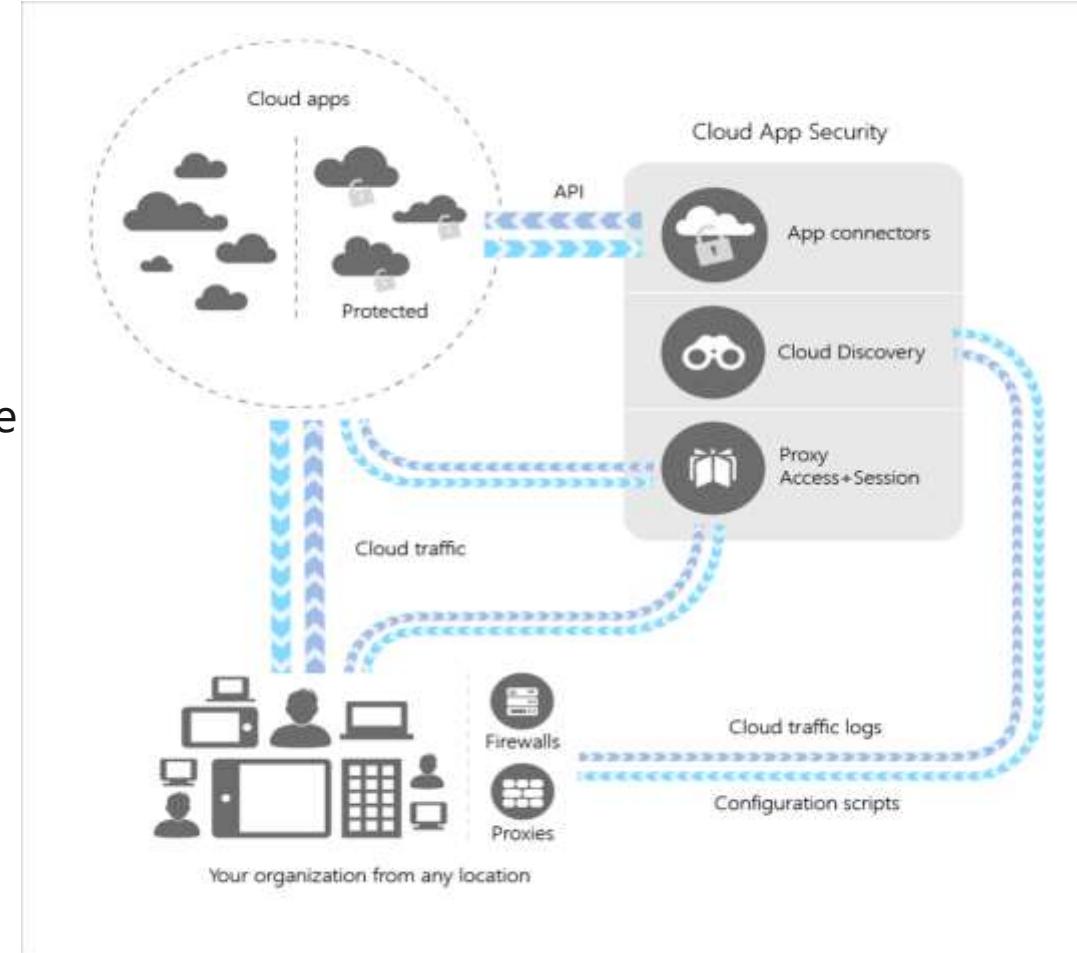


Microsoft Azure

- [Microsoft Azure Active Directory](#)

Microsoft 365

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

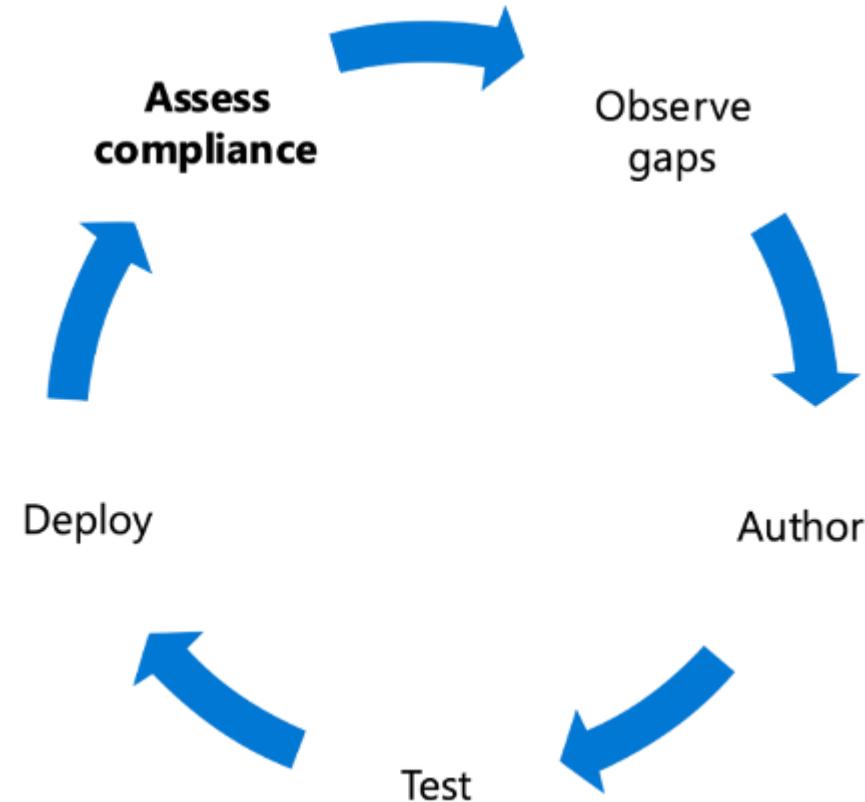


Secure infrastructure with Zero Trust



Microsoft Azure

- [Azure Blueprints](#)
- [Azure Policy](#)
- [Azure Arc](#)
- [Azure Security Center \(ASC\)](#)
- [Azure Sentinel](#)
- [Azure Resource Manager \(ARM\) templates](#)

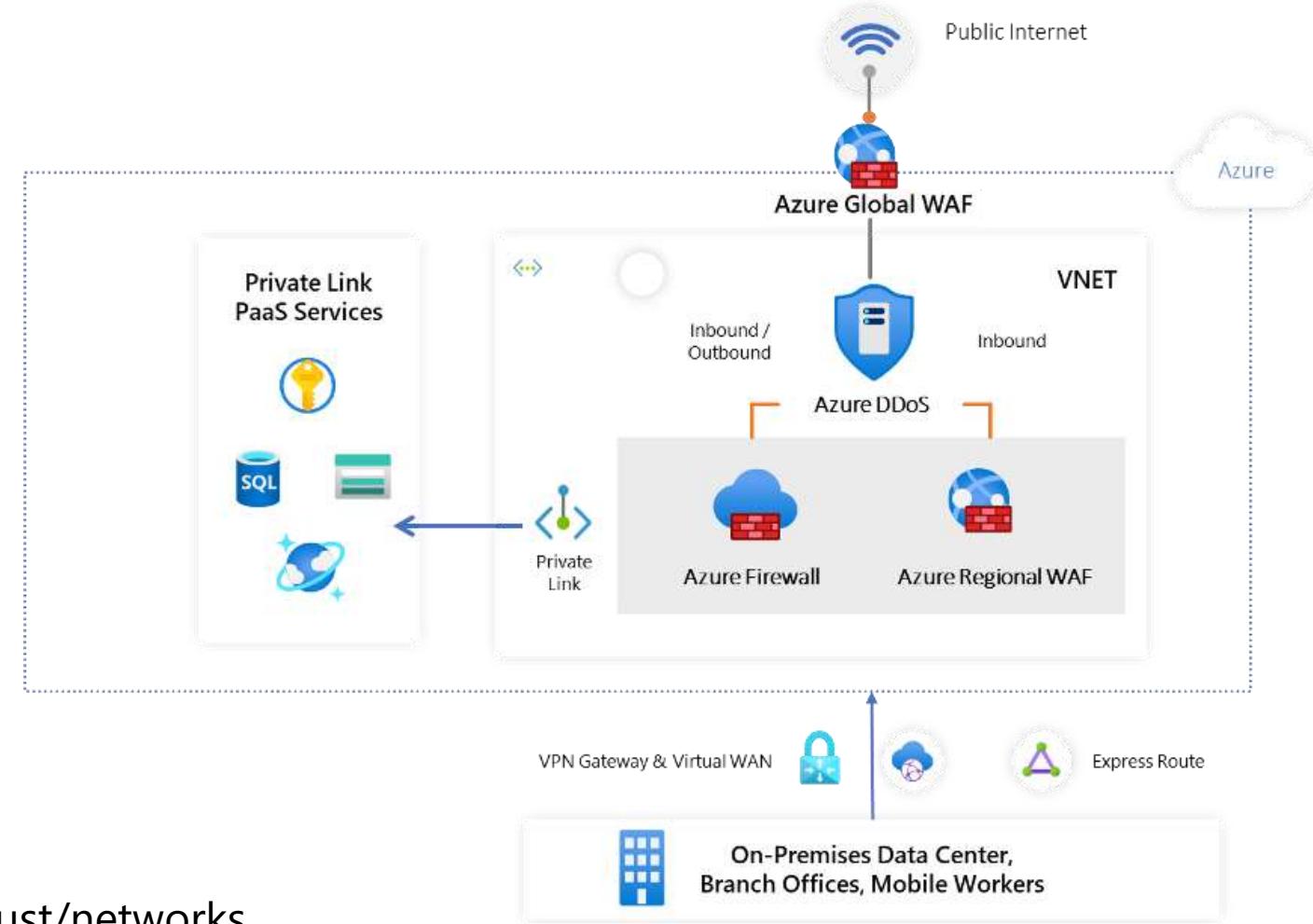


Secure networks with Zero Trust



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](#)



Visibility, automation, and orchestration with Zero Trust



Microsoft Azure

- [Azure Advanced Threat Protection](#)
- [Azure Sentinel](#)

Provide Integrated Capabilities to Manage Threats

Microsoft 365

- [Microsoft Threat Protection](#) - > XDR Capability

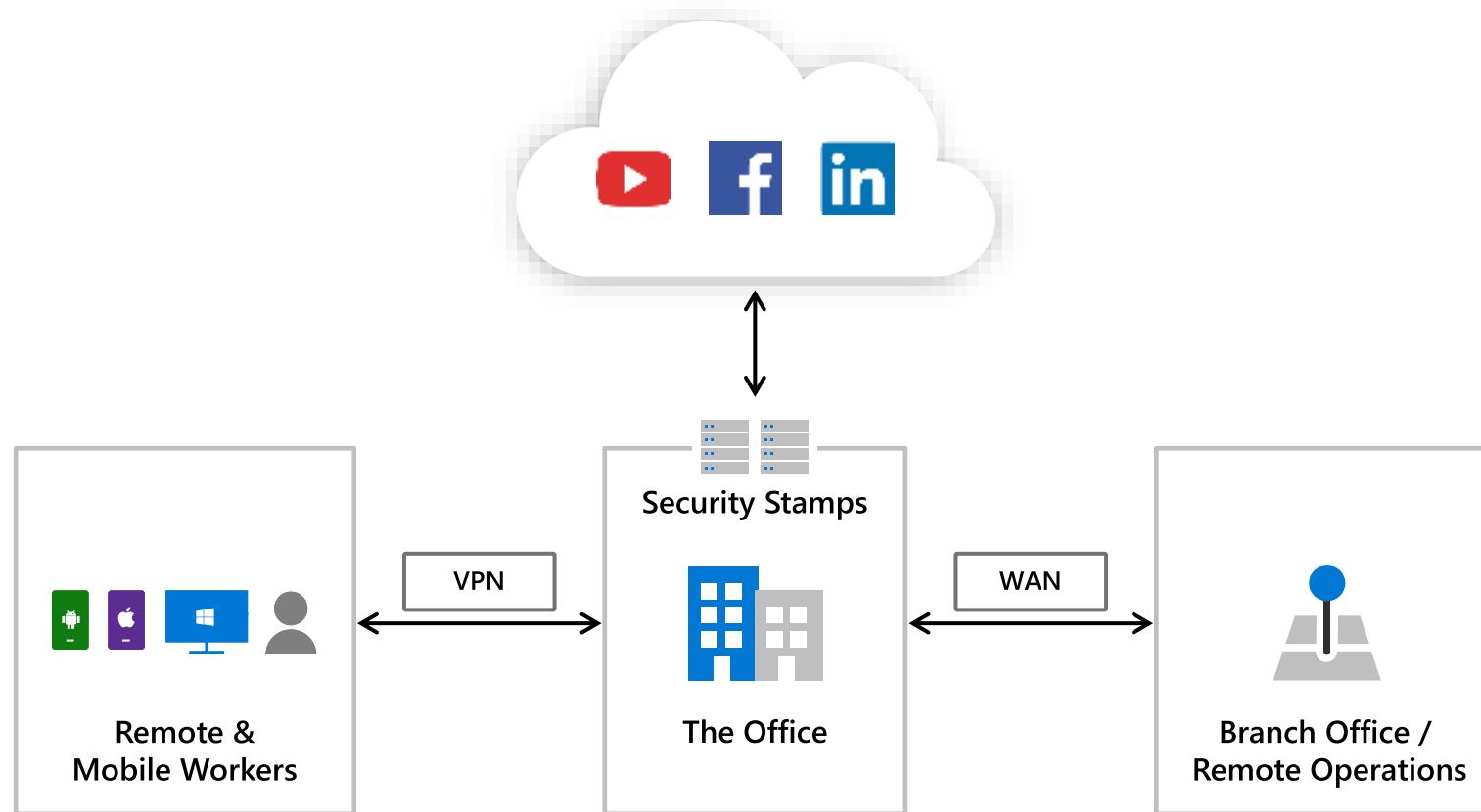


Microsoft Zero Trust Controls

Microsoft control	Build an identity perimeter	Secure the common control plane	Least privilege access to sanctioned apps	Data is protected wherever it 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	✓	✓	✓	✓	✓	✓

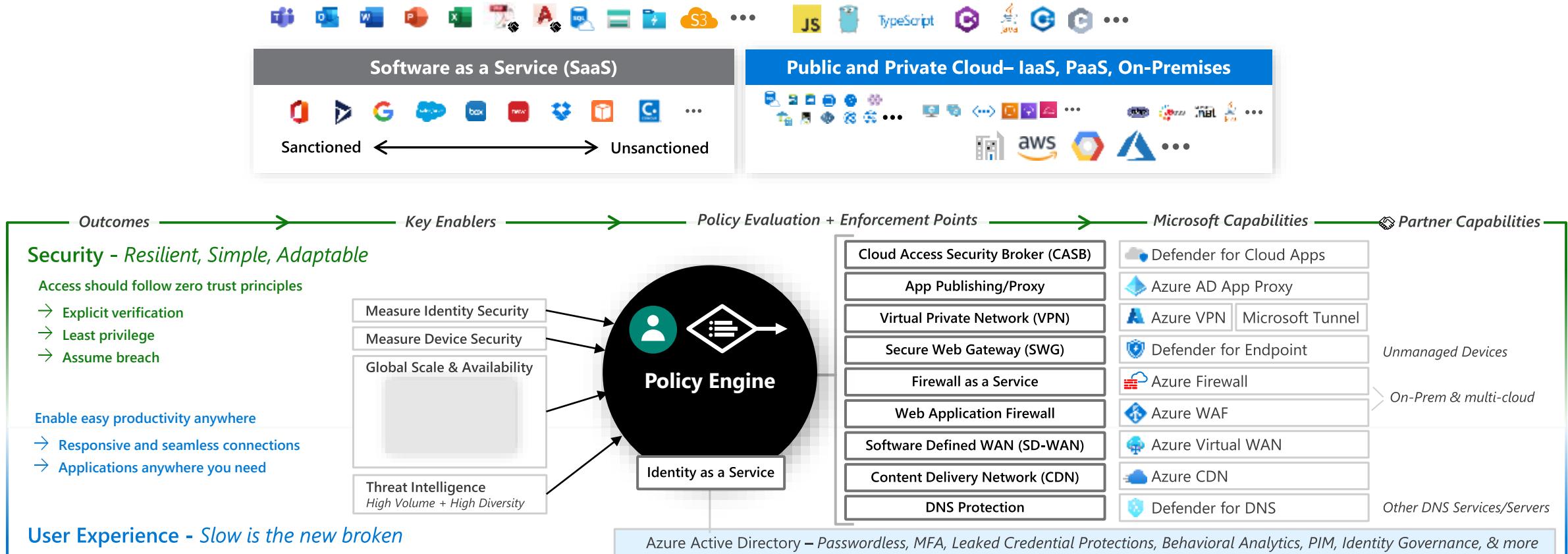
Thank you

Traditional networking model



Secure Access Service Edge (SASE)

Architecture for Secure, Responsive, and Pervasive Productivity



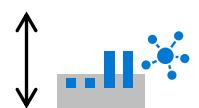
BYOD and Partner Devices/Users



Managed Users and Devices

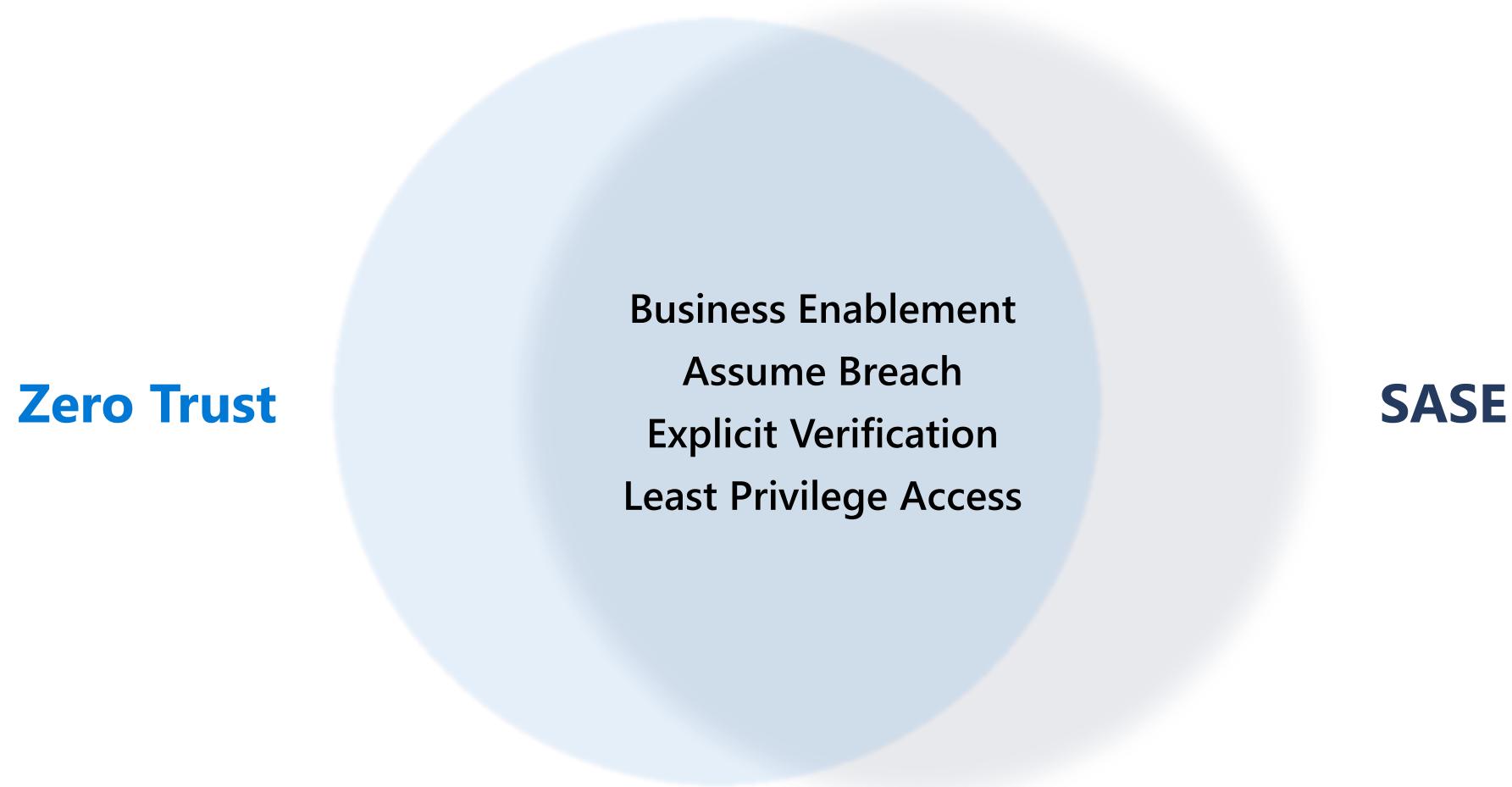


The Office



IoT and OT Environment

Comparing Zero Trust and Secure Access Service Edge (SASE)

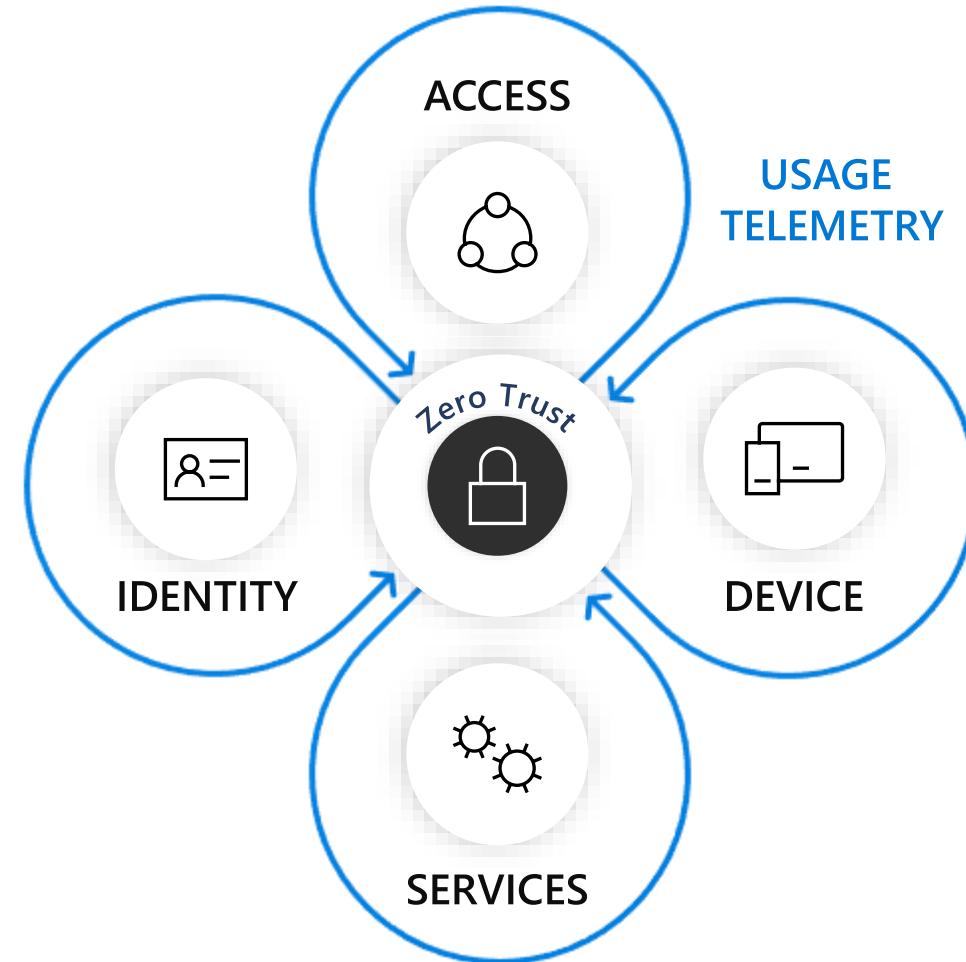


Zero Trust and **Secure Access Service Edge** provide similar approaches to secure a digital estate while enabling productivity

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

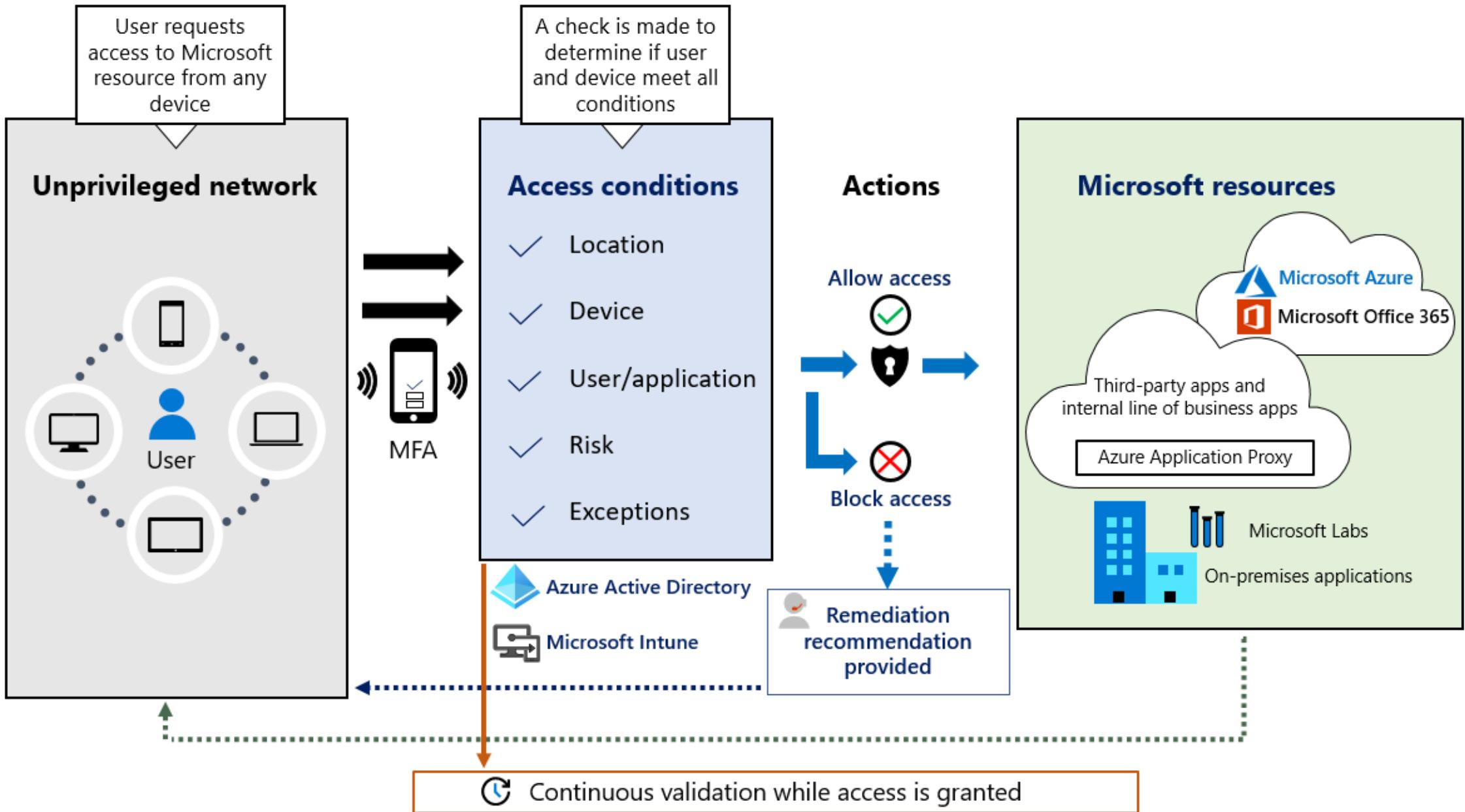


Major phases of zero trust networking

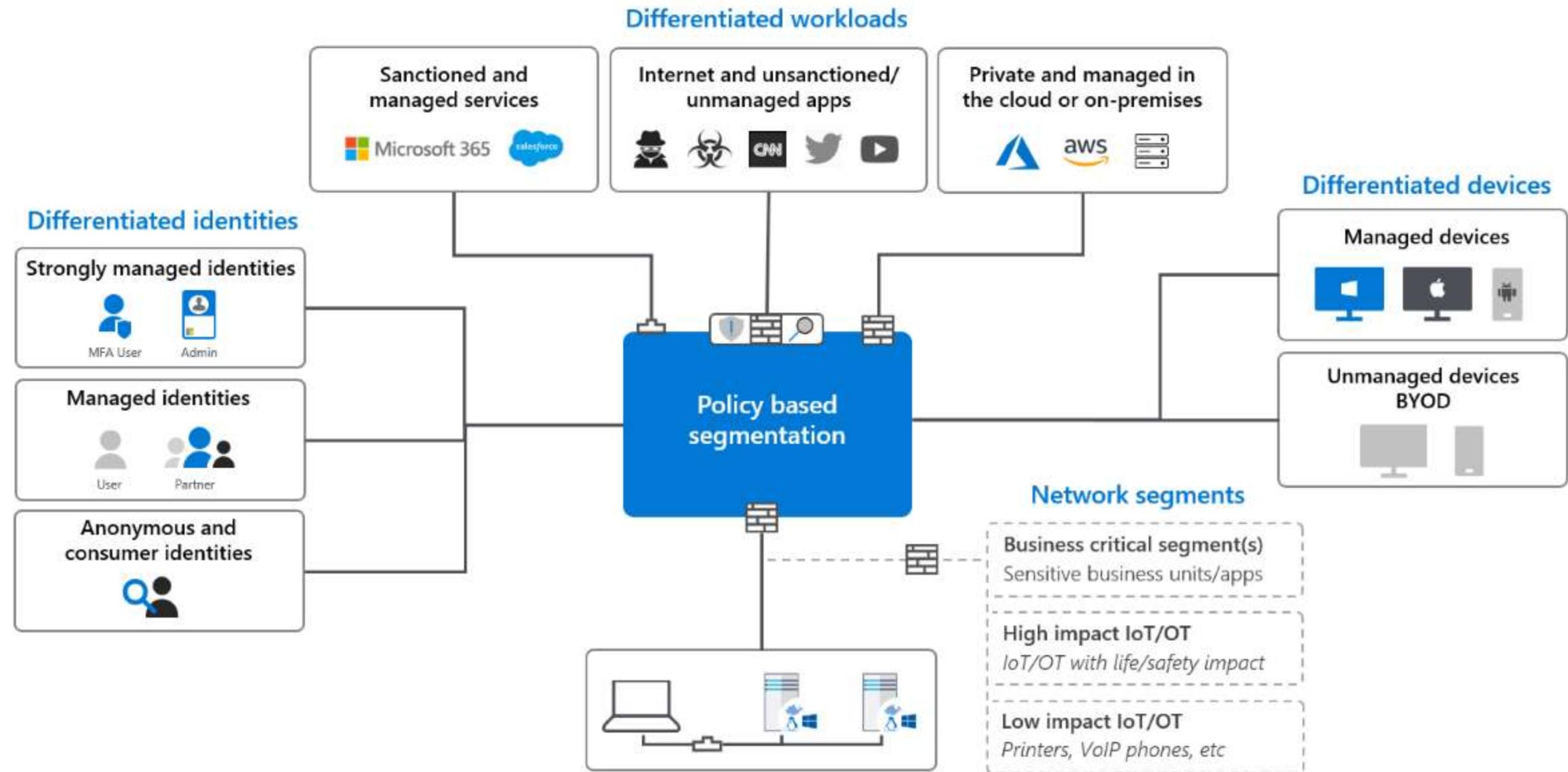
Pre-Zero Trust	Verify identity	Verify device	Verify access	Verify services
<ul style="list-style-type: none"><input checked="" type="checkbox"/> Device management isn't required<input checked="" type="checkbox"/> Single factor authentication to resources<input checked="" type="checkbox"/> Capability to enforce strong identity exists<input checked="" type="checkbox"/> Data classification and information protection exists	 <ul style="list-style-type: none"><input checked="" type="checkbox"/> Strong identity is verified and enforced<input checked="" type="checkbox"/> Passwords are eliminated in favor of biometrics<input checked="" type="checkbox"/> Access to applications and data is limited to minimum required to perform job function	 <ul style="list-style-type: none"><input checked="" type="checkbox"/> Client device health is enforced<input checked="" type="checkbox"/> Unmanaged devices have secure alternative access methods<input checked="" type="checkbox"/> Users don't have administrative permissions on client devices	 <ul style="list-style-type: none"><input checked="" type="checkbox"/> Internet is the default network in all Microsoft office locations<input checked="" type="checkbox"/> Network segmentations are built based on role and function	 <ul style="list-style-type: none"><input checked="" type="checkbox"/> Applications and conditions are enforced using conditional access<input checked="" type="checkbox"/> Applications and services are accessible directly from the internet

Pervasive telemetry

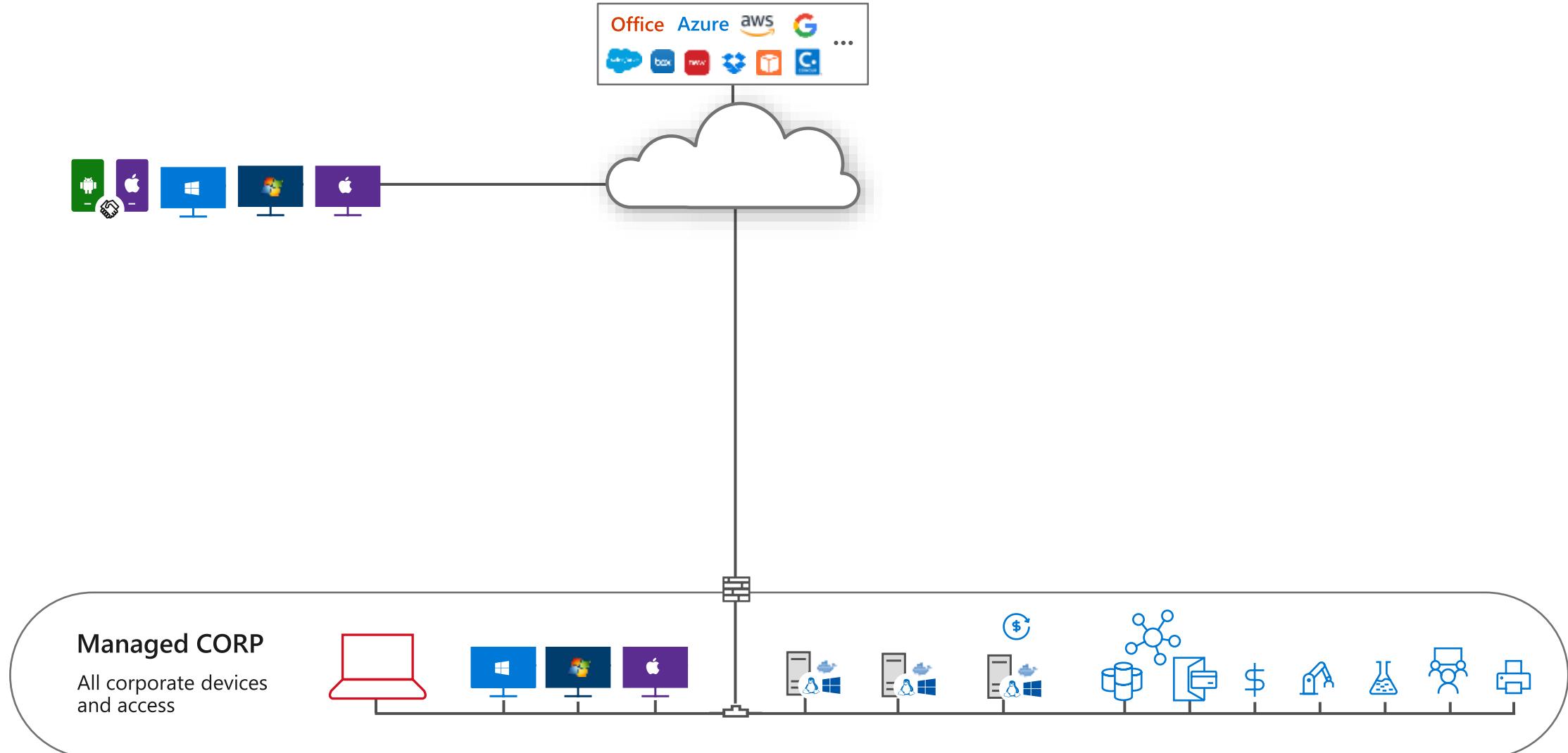
Microsoft's Zero Trust Architecture



Zero Trust- Network segmentation transformation

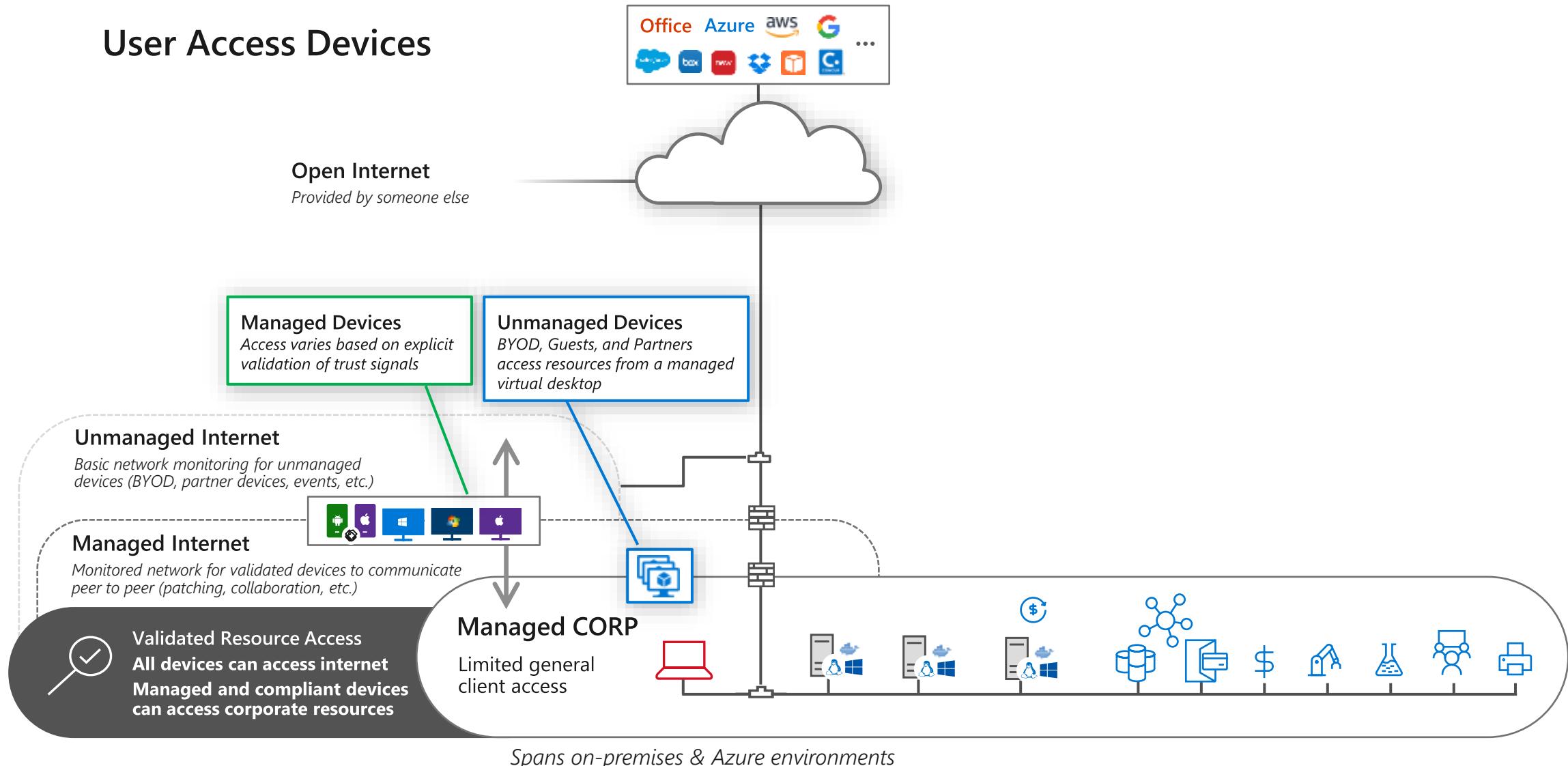


Typical 'Flat' Network



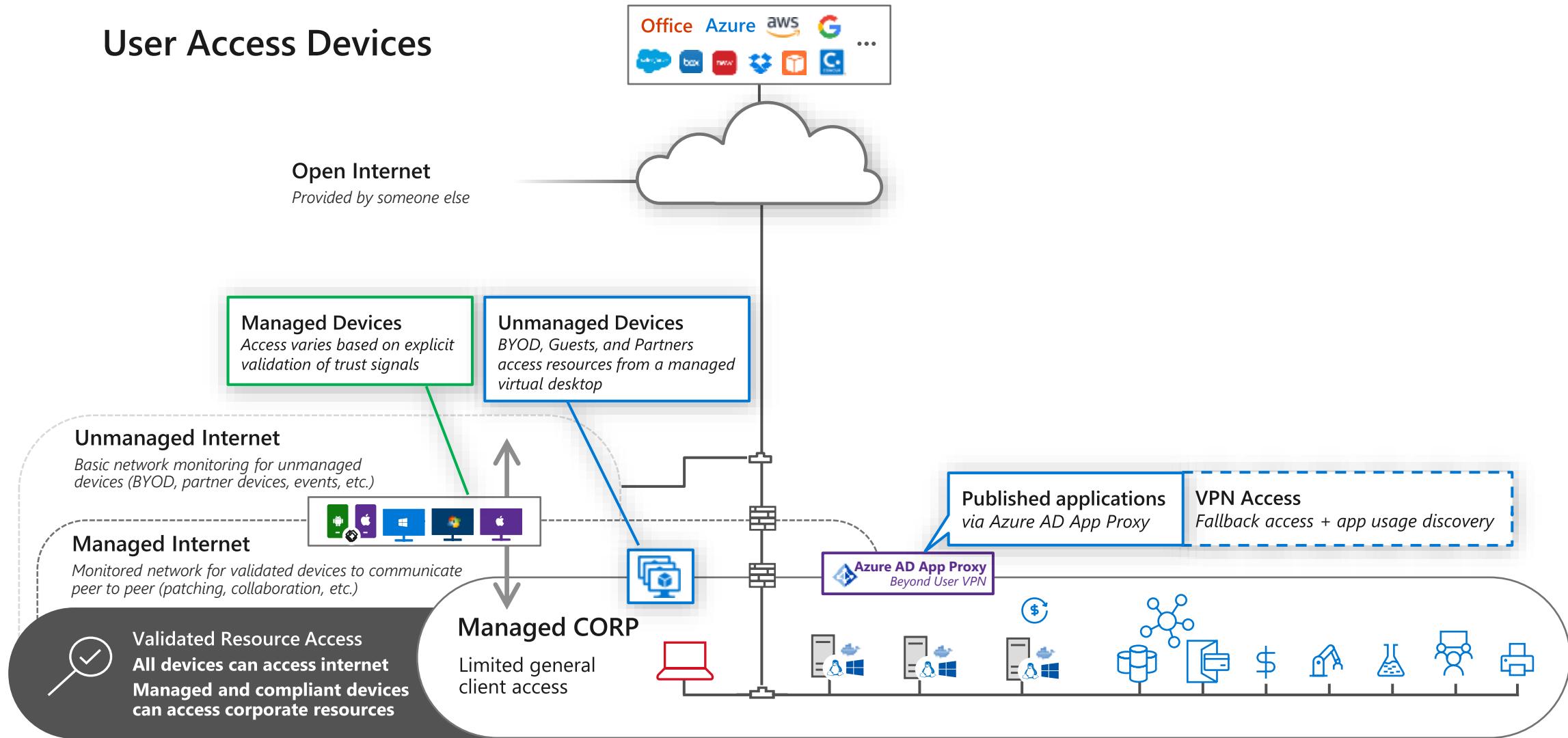
Zero Trust – Client Security Transformation

User Access Devices

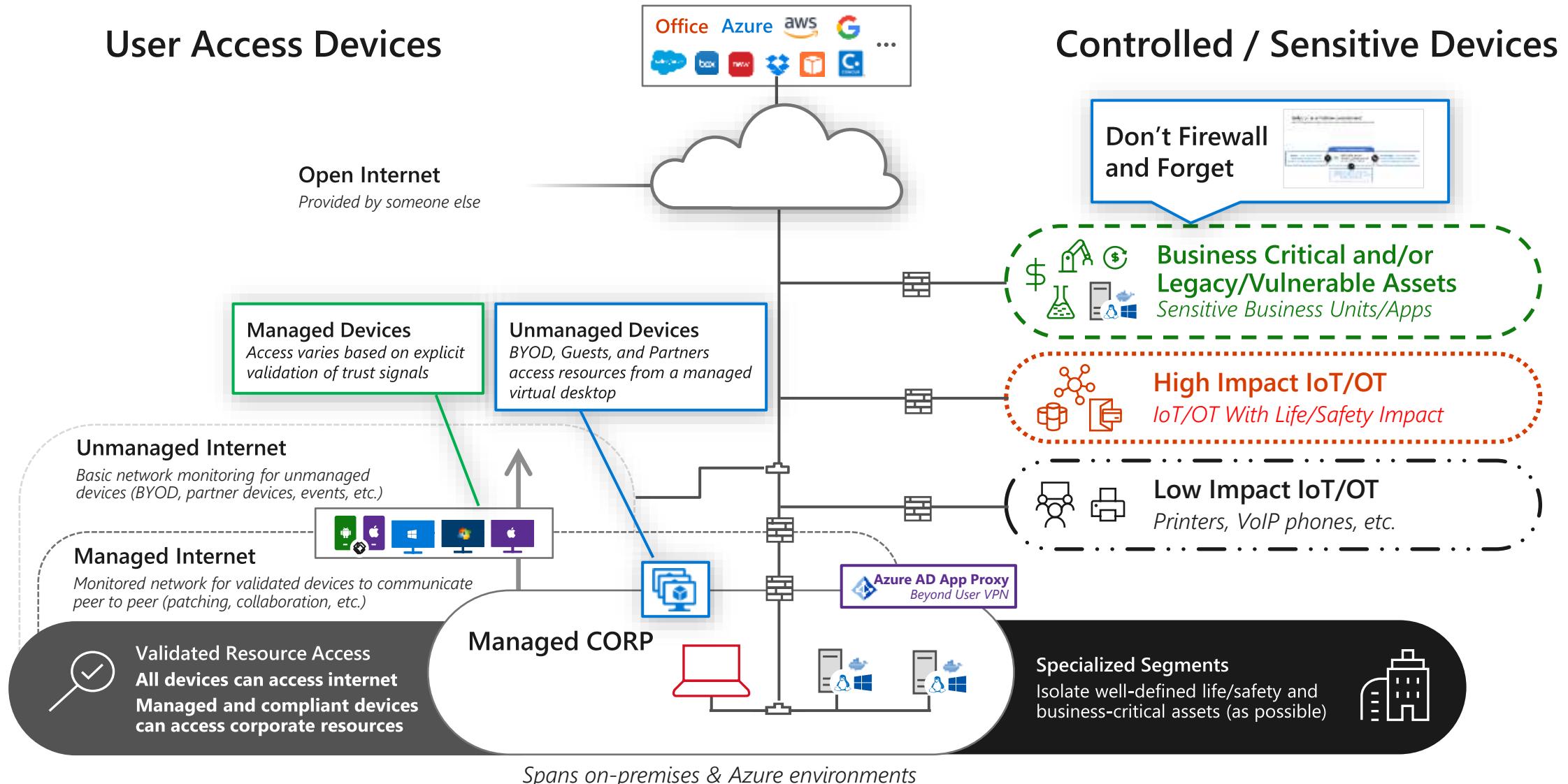


Zero Trust – App Access for Clients

User Access Devices



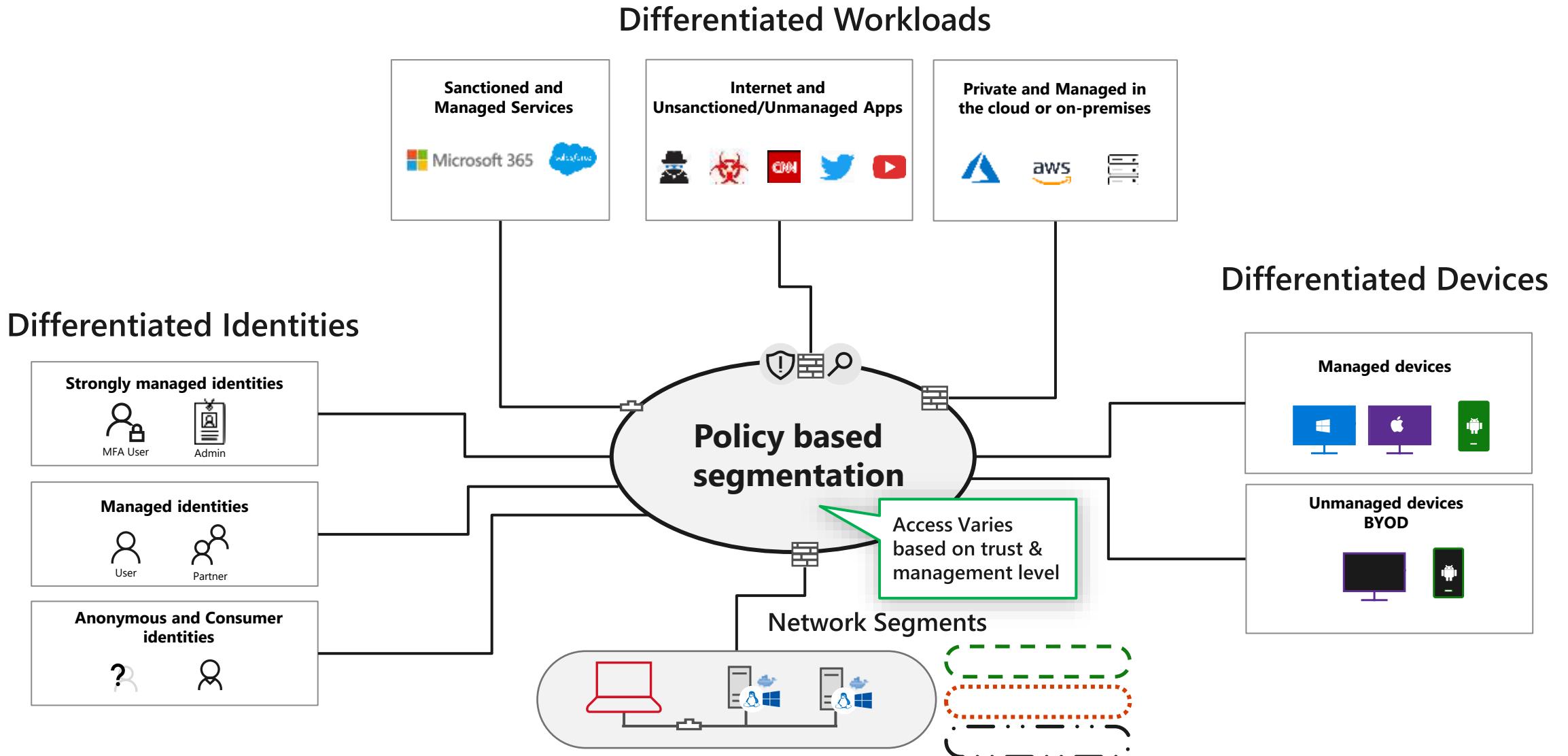
Zero Trust – Network Segment Transformation



Full Zero Trust End State

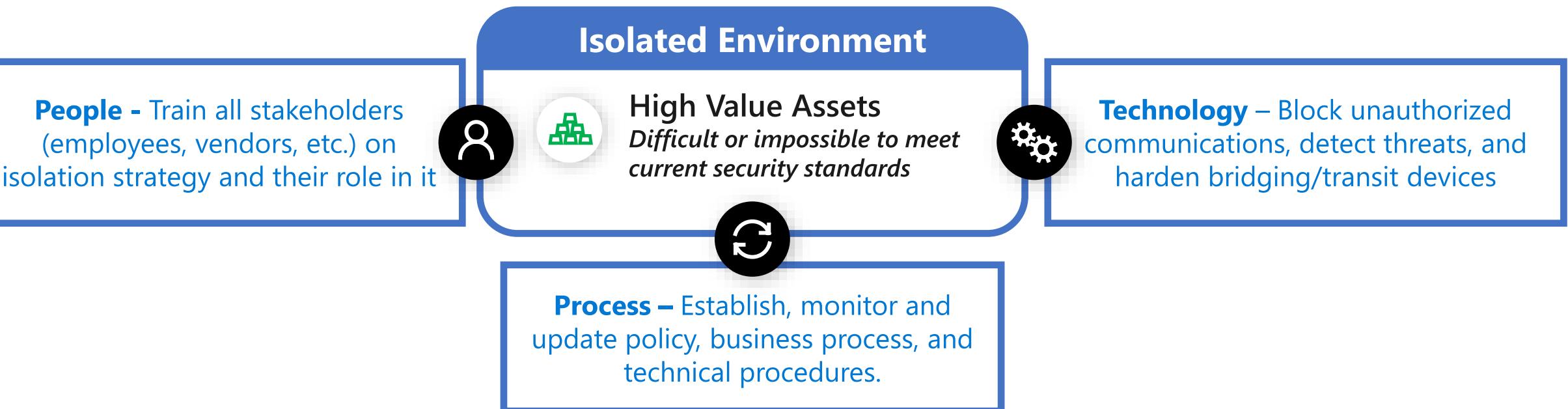
Bringing the best of both worlds

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

Introductions



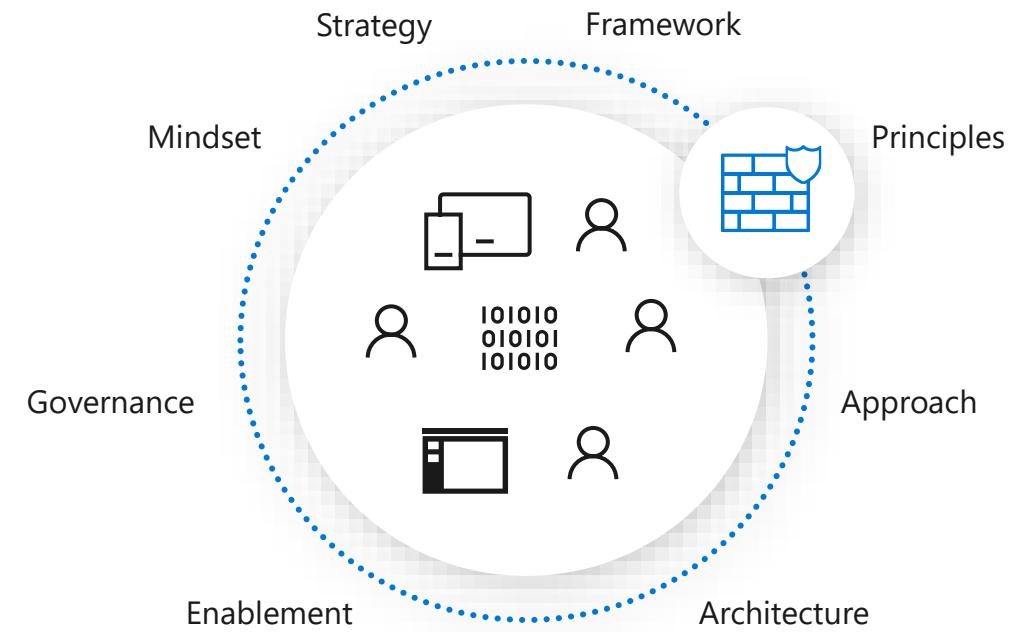
What Does Zero Trust Mean To Your Organization?

Zero Trust (Networking):

- An approach to security which treats every access attempt as if it's originating from an untrusted network.

Microsoft's Zero Trust Approach:

- An integrated approach to securing access with adaptive controls and continuous verification across your entire digital estate.
- Zero Trust isn't a thing you buy or 'do'. It's a security paradigm and architecture (maturity) journey.
- There are certain principles and tenets that shape Zero Trust. These are established by [Microsoft](#) and [NIST](#)
- Microsoft tools integrate across all Zero Trust elements, providing visibility everywhere with signals and analytics across the enterprise. It's risk-based, powered by intelligent security.
- The operating model must break down silos and provide unified security across all domains and elements.
- To be successful, governance must keep up and must drive the right behaviors.
- Assume every resource is on the open internet, where identity is the control plane. Never trust. Always verify.
- Risk-based, powered by intelligent security.
- Integration is key for effectiveness.
- Build on what you have. Integration is key for effectiveness.
- Different approaches for different use cases.
- Network is only important in certain scenarios.
- When done right, it delivers increased security and productivity.



Logical Components of a Zero Trust Architecture



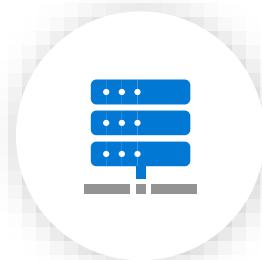
Identity



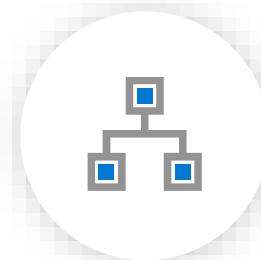
Devices



Apps



Infrastructure



Networking



Data



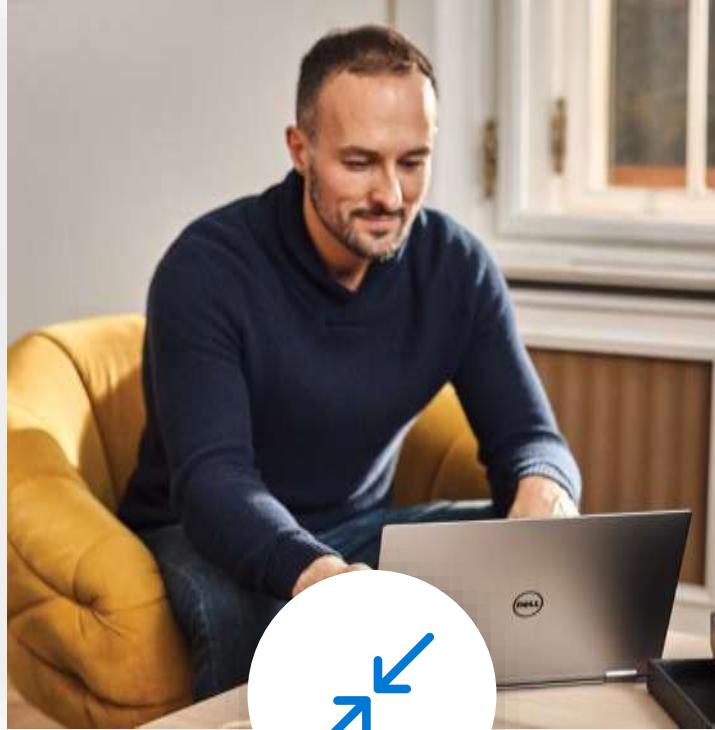
Guiding Principles and Standards

- **Principles** are high-level statements of the values that guide IT and the Business, e.g. "*Information is an asset*". They are universally agreed truths. They guide and shape the lower-level artefacts; standards and policies.
 - Principles change very little – if at all – over time.
 - The objectives should change very little over time, as they are foundations of Zero Trust and an organization's Cybersecurity strategy.
 - Strategies are long-term missions that do not frequently change. Therefore, the Principles are best tied to strategic objectives.
- **Standards** define the specification to which we do something, e.g. "*Data-at-rest must be encrypted using AES 128 bit or better*".
 - Standards change, they improve and become obsolete.
 - They are closer to technology.
- Design decisions are shaped by standards and principles and will prescribe a product and configuration. e.g. "*Disks shall be encrypted using Microsoft BitLocker*".
- Principles are not tangible, so appropriate standards and policies must be defined and enforced in order to implement the Principles.

A new reality needs new principles



Verify explicitly



Use least privilege access



Assume breach

Components of the Zero Trust Model

In an optimal Zero Trust implementation, your digital estate is connected and able to provide the signal needed to make informed access decisions using automated policy enforcement.



Zero Trust Model

Implementing a Zero Trust Model

Migrating to a Zero Trust Security Model allows you to simultaneously improve security over conventional network-based approaches and better enable users where and when they need access.

A Zero Trust model requires:

1. *Signal* to inform decisions,
2. *Policies* to make access decision and,
3. *Enforcement* capabilities to implement those decisions effectively.



Signal to make an informed decision.

Zero Trust considers many signal sources—from identity systems to device management and device security tools—to create context-rich insights that help make informed decisions.

Decision based on organizational policy.

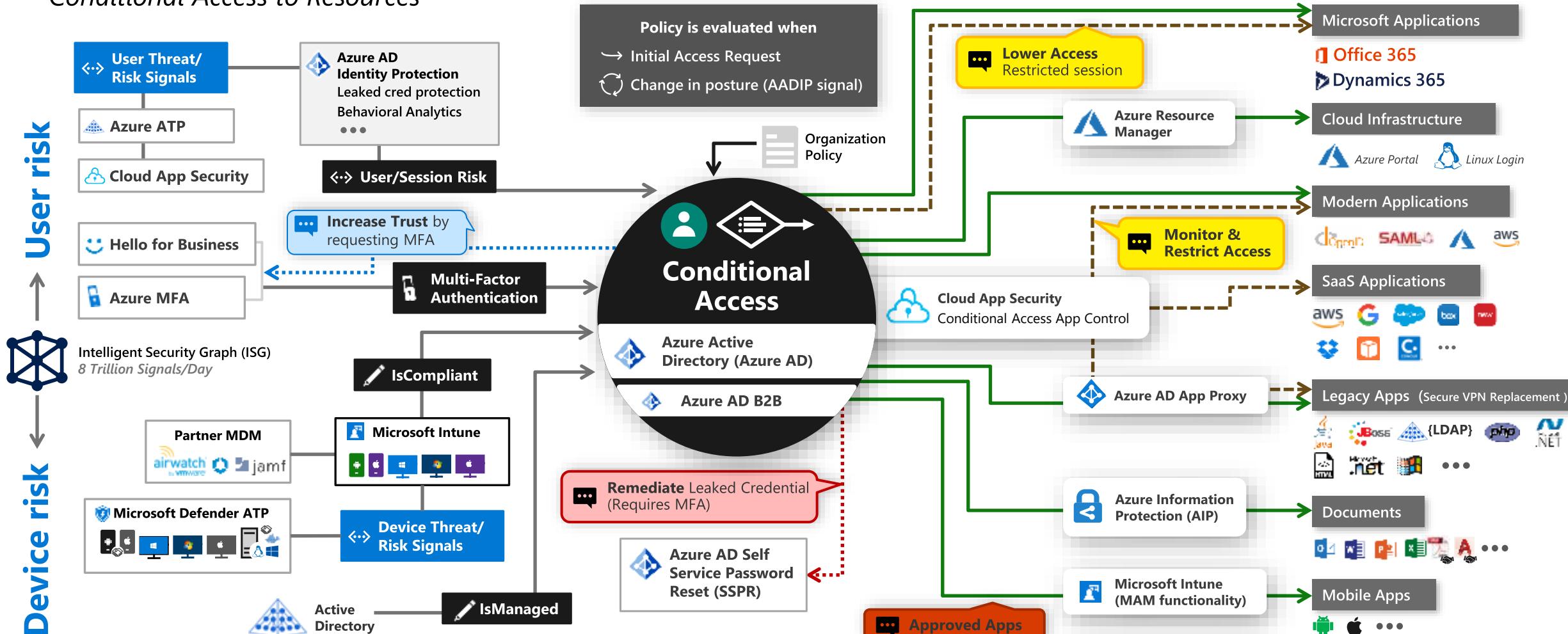
The access request and signal are analyzed to deliver a decision based on finely-tuned access policies, delivering granular, organization-centric access control.

Enforcement of the policy across resources.

Decisions are then enforced across the entire digital estate—such as read-only access to a SaaS app or remediating compromised passwords with a self-service password reset.

Zero Trust User Access

Conditional Access to Resources



Signal

to make an informed decision



Decision

based on organizational policy



Enforcement

of policy across resources

Zero Trust Maturity

Zero Trust Maturity Model Explained

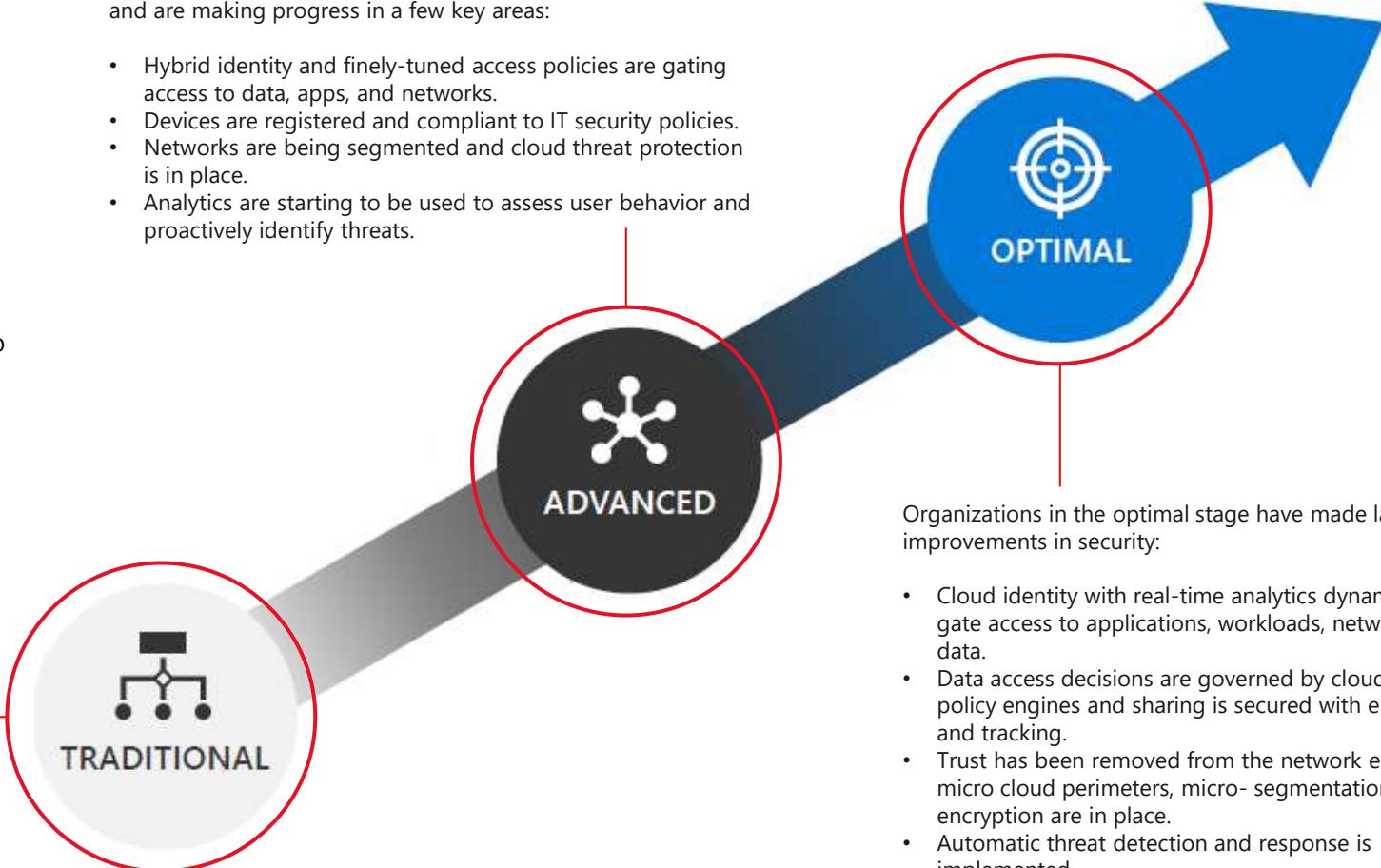
- A three-stage maturity model developed by Microsoft
- Different organizational requirements, existing technology implementations, and security stages all affect how a Zero Trust security model implementation is planned.
- Using our experience in helping customers to secure their organizations as well 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.

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.

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.



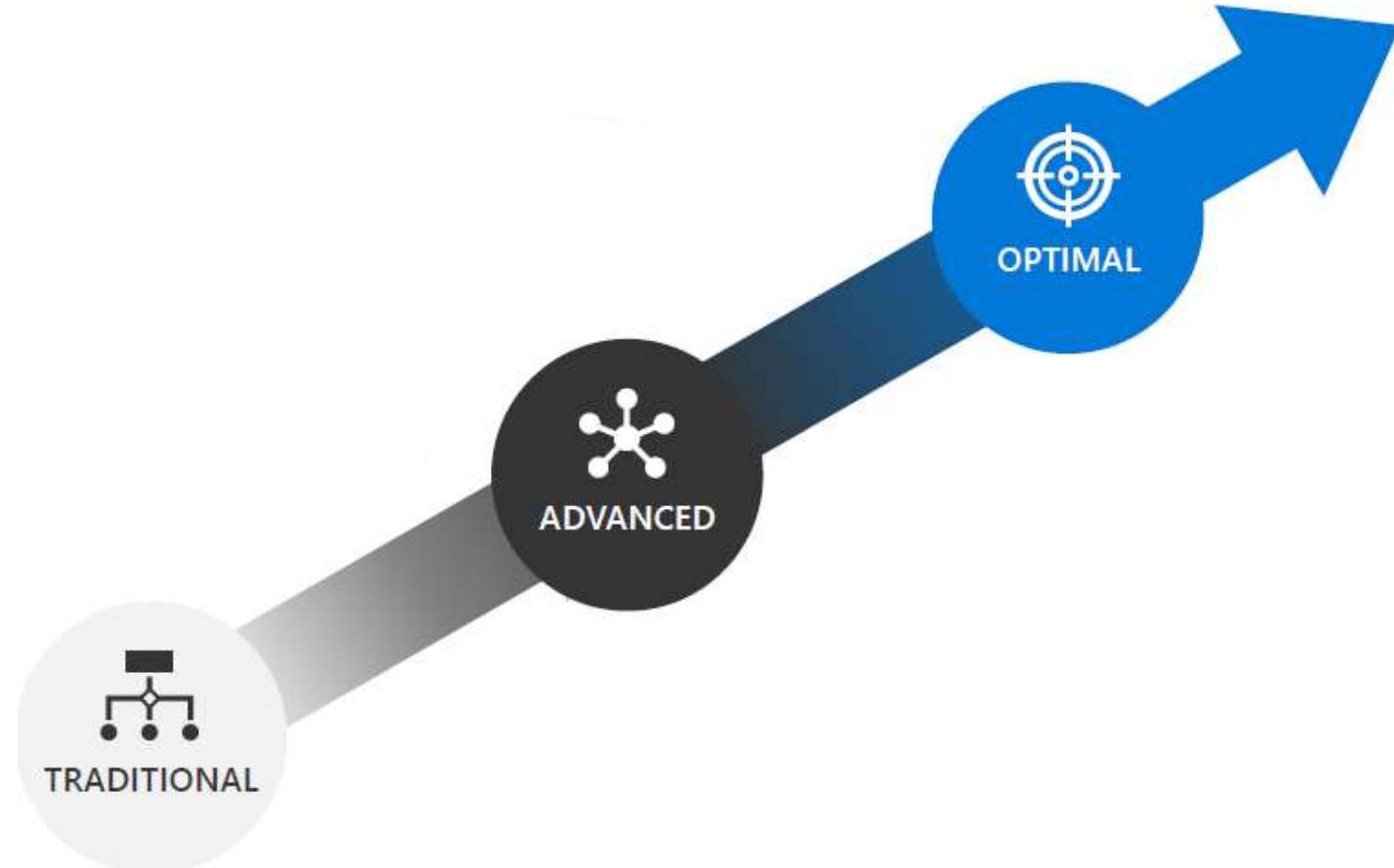
Organizations in the optimal stage have made large improvements in security:

- 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.

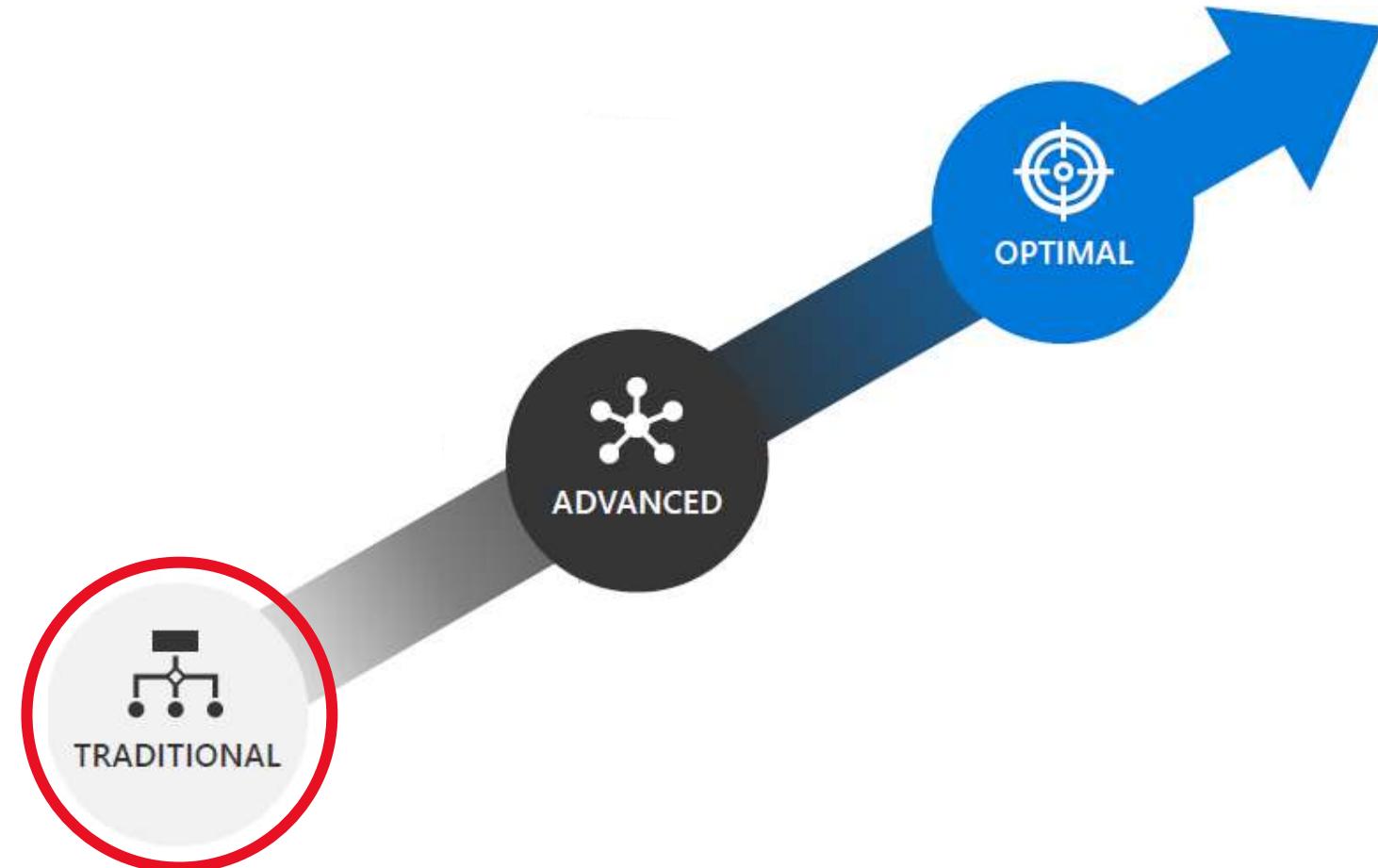


Zero Trust Maturity

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.

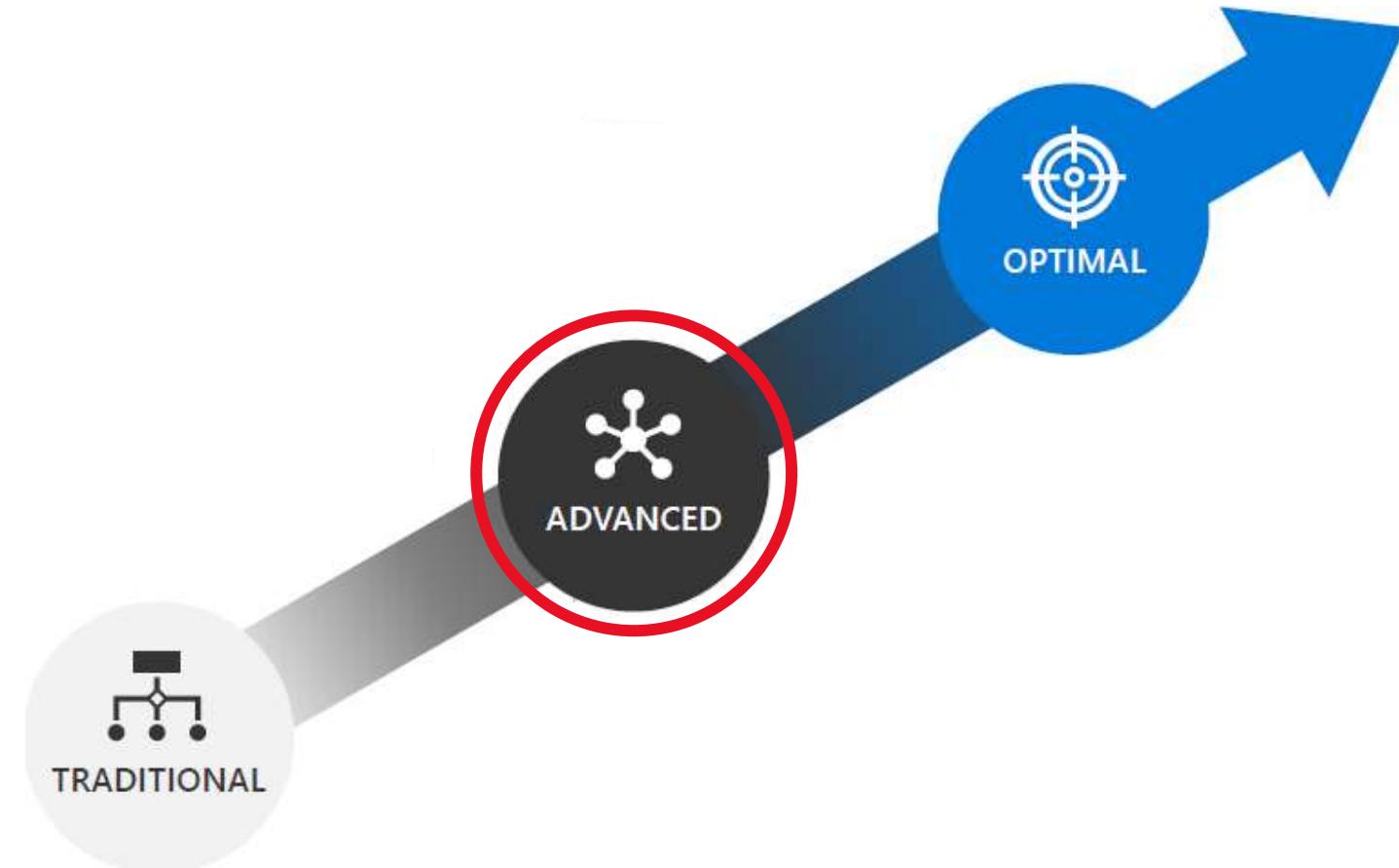


Zero Trust Maturity

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.

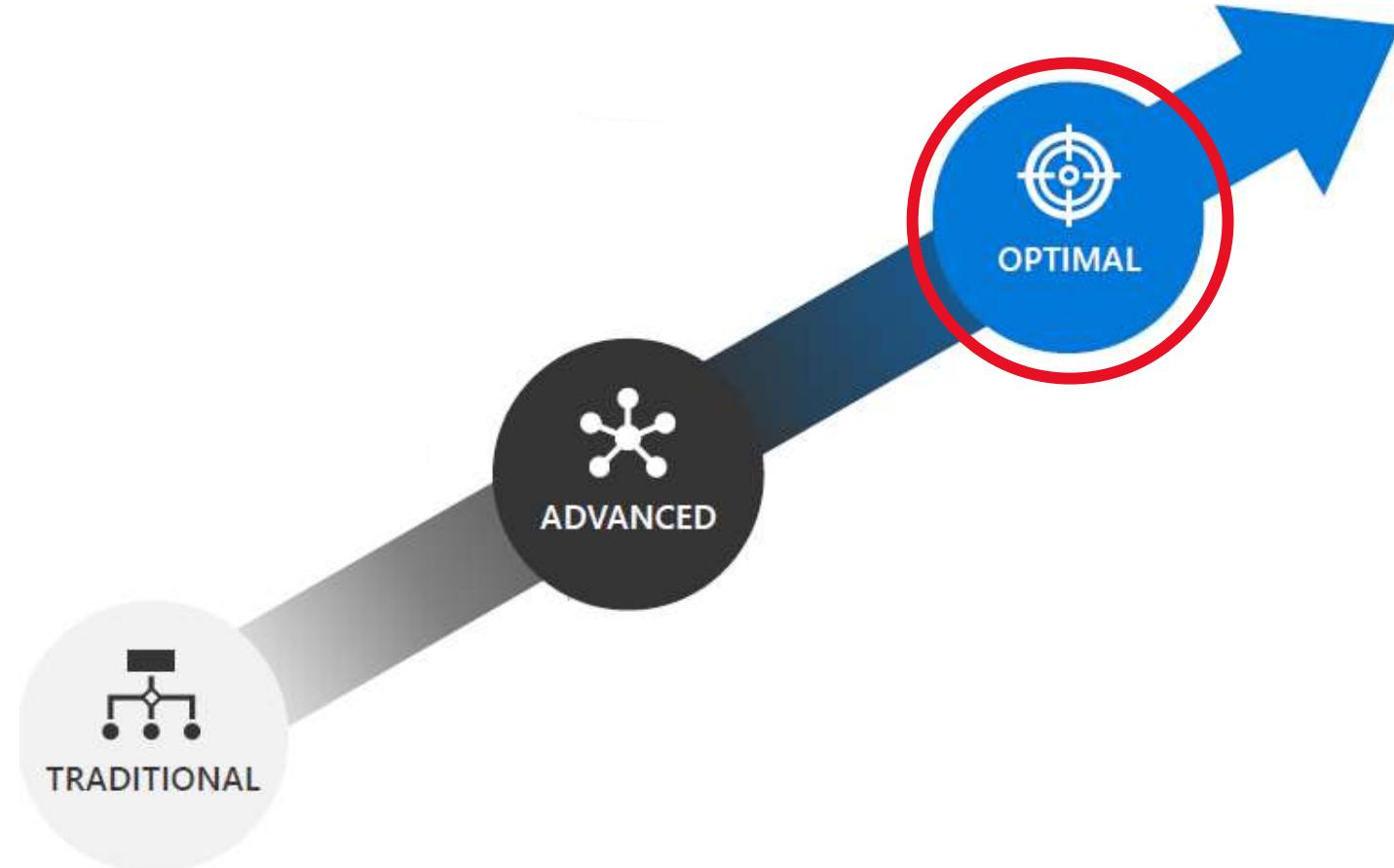


Zero Trust Maturity

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

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

Optimal

Passwordless authentication is enabled

User, device, location, and behavior is analyzed in real time to determine risk and deliver ongoing protection

Zero Trust Maturity

Readiness across the six Foundational Elements – Data



Data

Access is governed by perimeter control, not data sensitivity

Sensitivity labels are applied manually, with inconsistent data classification

Advanced

Data is classified and labeled via regex/keyword methods

Access decisions are governed by encryption

Optimal

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

Zero Trust Maturity

Readiness across the six Foundational Elements – Devices



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

Advanced

Devices are registered with cloud identity provider

Access only granted to cloud managed & compliant devices

DLP policies are enforced for BYO and corporate devices

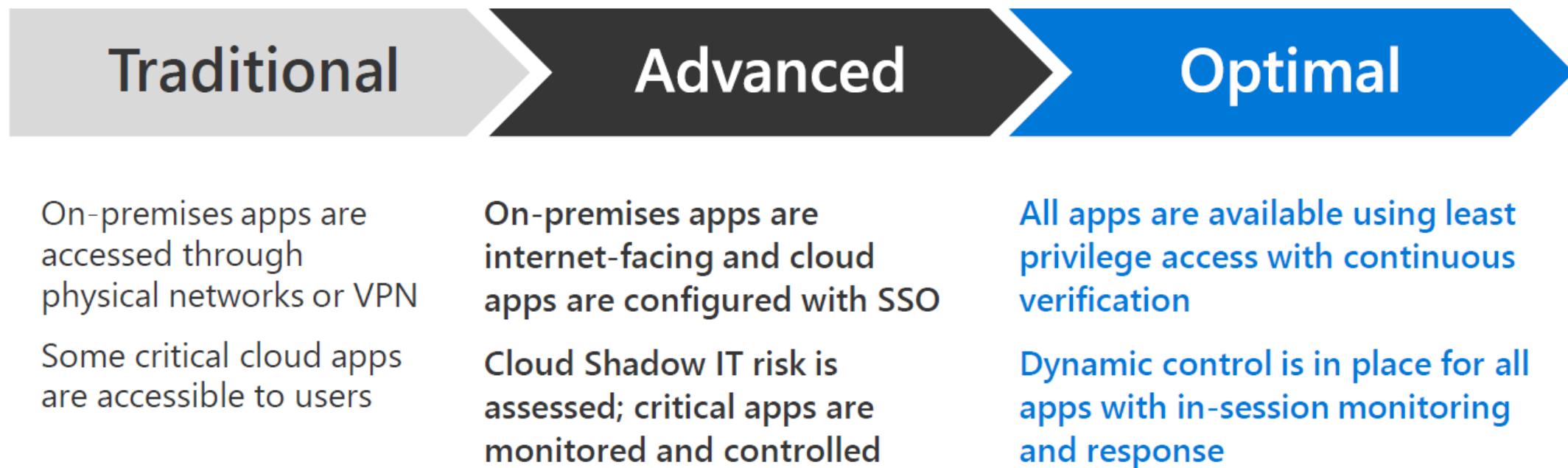
Optimal

[Endpoint threat detection is used to monitor device risk](#)

[Access control is gated on device risk for both corporate and BYO devices](#)

Zero Trust Maturity

Readiness across the six Foundational Elements – Apps



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

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

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	<ul style="list-style-type: none"> On-premises identity provider is in use No SSO is present between cloud and on-premises apps Visibility into identity risk is very limited 	<ul style="list-style-type: none"> Cloud identity federates with on-premises system Conditional access policies gate access and provide remediation actions Analytics improve visibility 	<ul style="list-style-type: none"> Passwordless authentication is enabled User, device, location, and behavior is analyzed in real time to determine risk and deliver ongoing protection
Devices	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> Devices are registered with cloud identity provider Access only granted to cloud managed & compliant devices DLP policies are enforced for BYO and corporate devices 	<ul style="list-style-type: none"> Endpoint threat detection is used to monitor device risk Access control is gated on device risk for both corporate and BYO devices
Apps	<ul style="list-style-type: none"> On-premises apps are accessed through physical networks or VPN Some critical cloud apps are accessible to users 	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Permissions are managed manually across environments Configuration management of VMs and servers on which workloads are running 	<ul style="list-style-type: none"> Workloads are monitored and alerted for abnormal behavior Every workload is assigned app identity Human access to resources requires Just-In-Time 	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Few network security perimeters and flat open network Minimal threat protection and static traffic filtering Internal traffic is not encrypted 	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Access is governed by perimeter control, not data sensitivity Sensitivity labels are applied manually, with inconsistent data classification 	<ul style="list-style-type: none"> Data is classified and labeled via regex/keyword methods Access decisions are governed by encryption 	<ul style="list-style-type: none"> 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)



	Identities	Devices	Apps	Infrastructure	Network	Data
Advanced	<ul style="list-style-type: none"> Cloud identity federates with on-premises system Conditional Access policies gate access and provide remediation actions Analytics improve visibility Identity segmentation Raise attacker cost 	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> Workloads are monitored and alerted for abnormal behavior Every workload assigned app identity Human access to resources requires Just-In-Time 	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> Data is classified and labelled via regular expressions/keyword Access decisions governed by encryption Raise attacker cost
Controls	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> High value assets enrolled into Azure Security Center (ASC) JIT for high value workloads Azure AD PIM Secure Windows Server 2019 build 	<ul style="list-style-type: none"> Cloud adoption framework followed Tier 0 assets segmented Critical legacy protocol triage 	<ul style="list-style-type: none"> 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

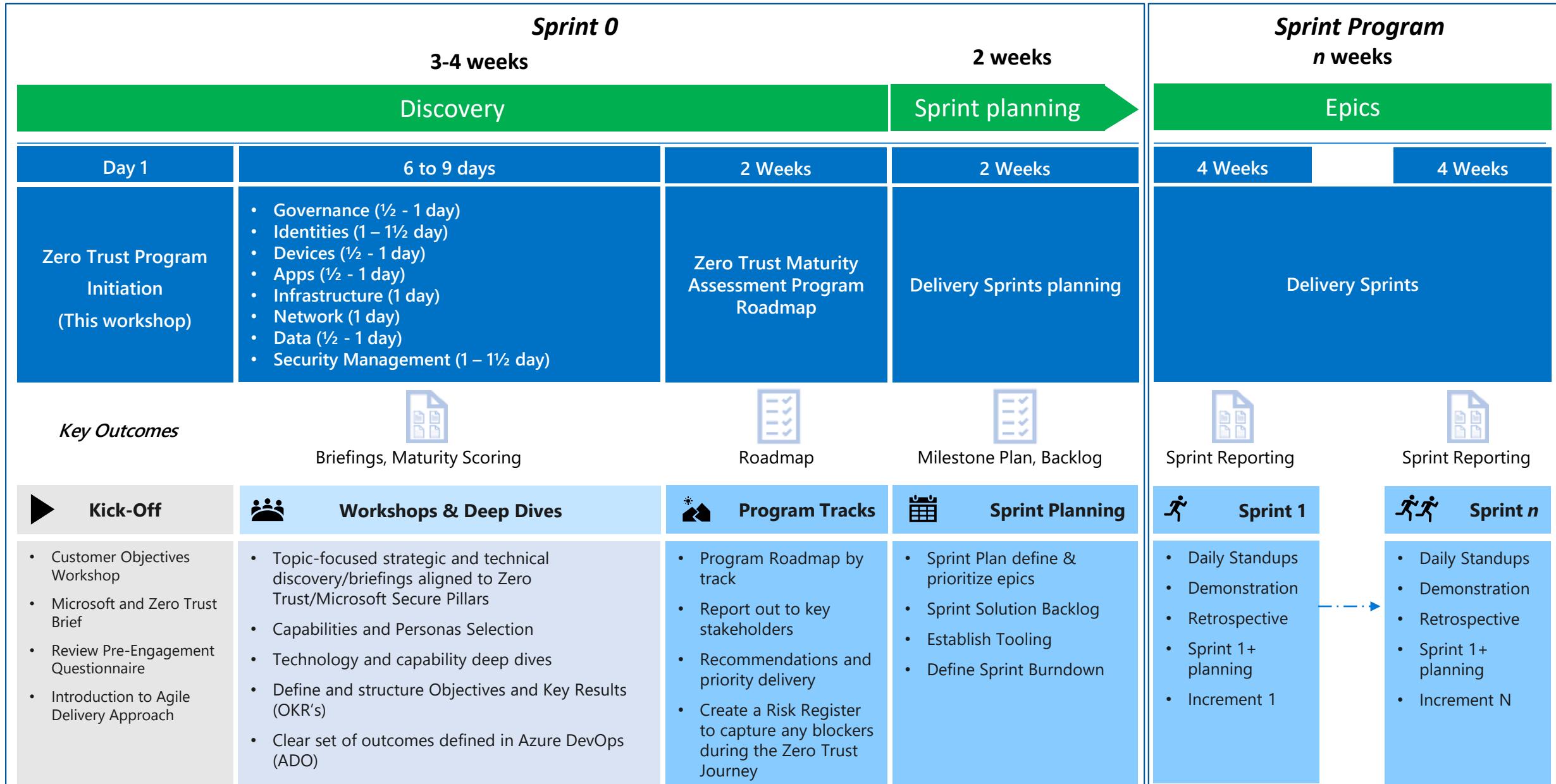
Optimal

	Identities	Devices	Apps	Infrastructure	Network	Data
Optimal	<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • Endpoint threat detection is used to monitor device risk • Access control is gated on device risk for both corporate and BYO Devices 	<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • Azure Security Center (ASC) policies • Identify and remove legacy protocols 	<ul style="list-style-type: none"> • 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 it 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	✓	✓	✓	✓	✓	✓

Microsoft Zero Trust Program Approach



Scrum Framework For The Zero Trust Program





Digital Empathy Is Key

- **Create clarity**
 - Synthesize the complex
 - Ensure shared understanding
 - Value understood
- **Generate energy**
 - Inspire optimism, creativity, and growth
 - Create an environment where everyone does their best work
 - Build organizations/teams that are stronger tomorrow than today
- **Deliver success**
 - Drive innovation that people love
 - Be boundary-less in seeking solutions for the Zero Trust program
 - Tenaciously pursue the right outcomes

Next Steps

- Prepare, engage and unify key stakeholders across your organization on your vision for Zero Trust.
- Start the discovery of your current state and objectives for the Zero Trust program.
- Identify personas for your Zero Trust program.
- Work together with Microsoft to Identify capabilities and technical security gaps in your existing environment.
- Document and prioritize in a solution backlog prior to Program/Sprint planning.



Education, Learning and Certification on Zero Trust

ADOPTING ZERO TRUST

Arm yourself with the knowledge and skills required to adopt Zero Trust at your organization. Create the business case for Zero Trust and learn how to build alignment around a common imperative, terminology, and set of tools to mobilize lasting change.

Adopting Zero Trust is available as a one-time course experience or as part of Forrester Decisions for [Technology Executives](#) and [Security & Risk](#).

The next course begins on October 3. Register by September 30.

Forrester account required for registration. Sign in or create an account.

[REGISTER NOW \(\\$2260\)](#)

[Download course catalog](#)

CERTIFIED
ADOPTING
ZERO TRUST

FORRESTER®

Topics Covered In Adopting Zero Trust

The Zero Trust eXtended Framework

Understand Zero Trust as a holistic approach that includes people, processes, and technologies.

Five Steps To A Zero Trust Network

Quickly begin and iterate on a five-step journey to realize the benefits of a Zero Trust strategy.

The Business Case For Zero Trust

Enroll Your Team In An Upcoming Course

Oct 3

Register by Sep 30

Nov 7

Register by Nov 4

<https://www.forrester.com/certification/zero-trust/#zt>

Based on CSA's bi-annual conferences and training tracks.

MEMBER LOGIN

Membership STAR Program Certificates & Training Research

SEARCH

Zero Trust

Advancement Center

Leading the development of tools and resources to guide zero trust implementation.

ZERO TRUST

Advancement Center

HOME PARTNERS WORKING GROUP EVENTS RESOURCE HUB

Home > Research > Zero Trust Advancement Center

Zero Trust is one of the most widely talked about cybersecurity trends today. Zero Trust says no part of a computer and networking system can be implicitly trusted, including the humans operating it. Therefore, we must put measures in place to provide assurance that the systems and their components are operating appropriately, typically under a "least privilege" model and continuously verified.

Creating an industry "north star" for Zero Trust has huge implications in raising the cybersecurity baseline across the board and eliminating significant systemic risk. CSA's mission is to create research, training, professional credentialing and provide an online center for additional curated Zero Trust resources. These tools will enable enterprises to understand and implement Zero Trust principles into business planning, enterprise architectures and technology deployments. Using CSA's agile programs for research, training and certification, as well as our global footprint of industry experts, chapters, webinars and conferences, we are uniquely positioned to build and evangelize authoritative Zero Trust best practices and tools. If you're interested in learning more, you can read the press release or contact us at zt@cloudsecurityalliance.org.

Submit Zero Trust Content to the Resource Hub

<https://cloudsecurityalliance.org/zt/>

Help write the exam questions for the Certificate of Zero Trust Knowledge D [Inbox](#) [Print](#) [Email](#)

Danielle Catteddu <outgoing@e.cloudsecurityalliance.org> [Unsubscribe](#)

Fri, 9 Sept, 02:14 (5 days ago) [Star](#) [Reply](#) [More](#)

to me ▾

Dear Colleagues,

We are still looking for subject matter experts to help write the exam questions for the Certificate of Zero Trust Knowledge (CZTK). Experts will receive payment for their contributions to the development of this program. If interested please email us at training@cloudsecurityalliance.org, to learn more.

We are looking for candidates who have 3-5 years of experience in the relevant field(s): Zero Trust, Zero Trust architecture design/ implementation/ management, governance, authentication and authorization, identity, credential and access management, cloud security and are certified in a relevant subject area.

Relevant certifications (not an exhaustive list):

- Certified Information Security Manager (CISM)
- Certified in Risk and Information Systems Control (CRISC)
- Certificate of Cloud Security Knowledge (CCSK)
- Certificate of Cloud Auditing Knowledge (CCAK)
- SANS certificates (ex: GIAC)
- Penetration Testing (ex: GCPN)
- CREST certification (ex: CPSA)

<https://www.pluralsight.com/paths/zero-trust-architecture-zta>

The screenshot shows a learning path titled "Zero Trust Architecture (ZTA)" on Pluralsight. The path consists of three courses: "Zero Trust Architecture (ZTA): Getting Started", "Establishing a Zero Trust Architecture (ZTA)", and "Determining deployment scenarios and use cases for Zero Trust Architecture (ZTA)". Each course has a brief description, duration, and a star rating. The "Zero Trust Architecture (ZTA): Getting Started" course is currently expanded, showing its details.

PLURALSIGHT

SKILLS Why Skills? Courses View plans For individuals

LEARNING PATHS

Zero Trust Architecture (ZTA)

3 courses 2 hours Skill IQ

This skill will teach you a basic understanding and applicability of Zero Trust Architecture (ZTA).

Courses in this path

Zero Trust Architecture (ZTA) courses

The intention of this skill is to help you understand the foundational concepts of Zero Trust Architecture (ZTA), when and how to employ it, as well as understanding the resource implications and related decisions that need to be made. We also cover determining the deployment scenarios and use cases for ZTA, as well as migrating to and maturing associated programs.

You will gain a full understanding of the subject by studying the following courses:

- Zero Trust Architecture (ZTA): Getting Started
- Establishing a Zero Trust Architecture (ZTA)
- Determining deployment scenarios and use cases for Zero Trust Architecture (ZTA)
- Migrating to and maturing Zero Trust Architecture (ZTA)

Zero Trust Architecture (ZTA): Getting Started
by Dr. Lyron H. Andrews 55m 4.5 (22)

<https://www.cybrary.it/course/zero-trust-networks/>

The screenshot shows a course titled "Zero Trust Networks" on Cybrary. The course page includes a summary, ratings, and a "Create Free Account" button. Below the course details, there's a section for team training and a table comparing time, difficulty, and CEU/CPE credits.

Get 2 months of Cybrary for Teams FREE
Get the first 2 months of your Cybrary for Teams annual subscription for free!

CYBRARY Training Library Solutions Resources Company Pricing

Zero Trust Networks

CYBRARY COURSE

The Zero Trust model of network security is stronger than traditional approaches that focus only on perimeter security. If you have basic knowledge of network security architecture, take this Zero Trust certification course to learn how the Zero Trust model is applied to users, devices, applications, and network traffic.

Create Free Account ★★★★★ 4.0 813 Share

NEED TO TRAIN YOUR TEAM? LEARN MORE

TIME	DIFFICULTY	CEU/CPE
1 hour 17 minutes	Beginner	2

<https://www.pluralsight.com/paths/zero-trust-architecture-zta>

<https://www.cybrary.it/course/zero-trust-networks/>

Order your copy now using this link
<https://routledge.pub/Zero-Trust-Journey>

CRC Press
Taylor & Francis Group

**ZERO TRUST JOURNEY
ACROSS THE
DIGITAL ESTATE**

Abbas Kudrati
Binil Pillai

GRAB YOUR COPY TODAY
WWW.ROUTLEDGE.COM/9781032125497

ABOUT THE BOOK

Zero Trust is increasingly becoming the critical security approach of choice for many enterprises and governments; however, security leaders often struggle with the significant shifts in strategy and architecture required to holistically implement Zero Trust.

This book seeks to provide an end-to-end view of the Zero Trust approach across organizations' digital estates that includes strategy, business imperatives, architecture, solutions, human elements, and implementation approaches that could significantly enhance these organizations' success in learning, adapting, and implementing Zero Trust. The book concludes with a discussion of the future of Zero Trust in areas such as artificial intelligence, blockchain technology, operational technology (OT), and governance, risk, and compliance.

The book is ideal for business decision makers, cybersecurity leaders, security technical professionals, and organizational change agents who want to modernize their digital estate with the Zero Trust approach.

ENJOY 20% DISCOUNT
ENTER
'FLE22'
AT CHECKOUT
VALID ON routledge.com
BOOKS ONLY