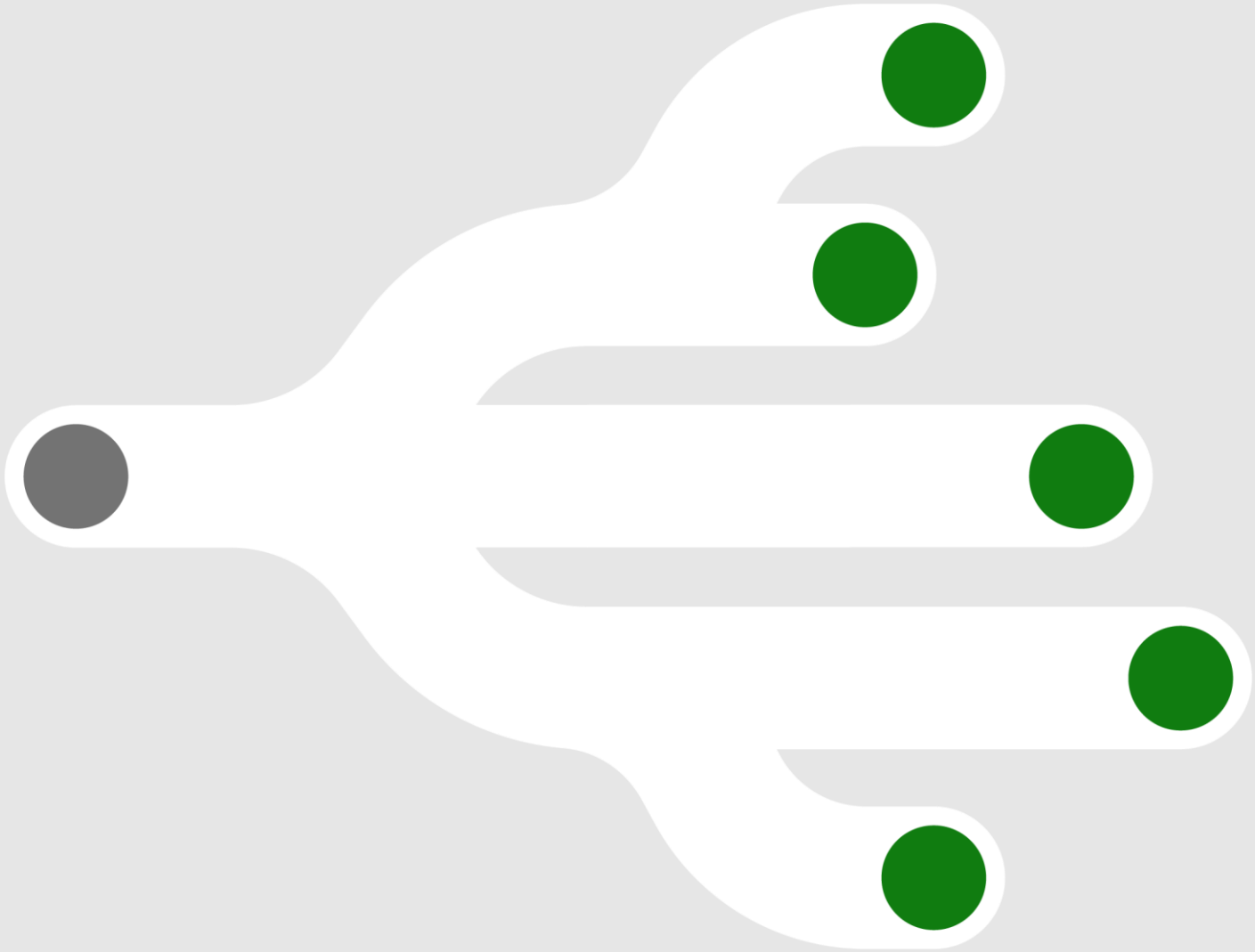
Microsoft Security

Vertrouwen is goed maar beveiligen is beter, implementeer Microsoft Zero Trust en beveilig vertrouwen



Jeroen Jansen
Product Marketing Manager

Glenn Habes
Channel Sales Manager

#SecurityLifeHacks

Today’s challenges: evolving risks

Surge of cyber attacks during the pandemic, especially ransomware and phishing attacks.

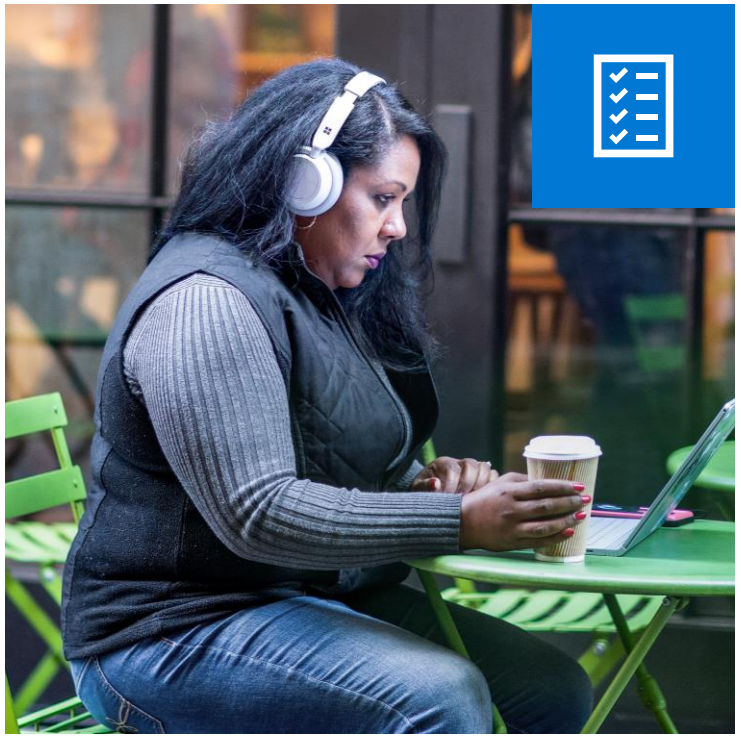
Continuous security vulnerabilities to be re-evaluated after last year’s rush to scale remote work services.

Personal device use at home is difficult to manage and protect, especially when accessing work data through personal devices and/or consumer apps.

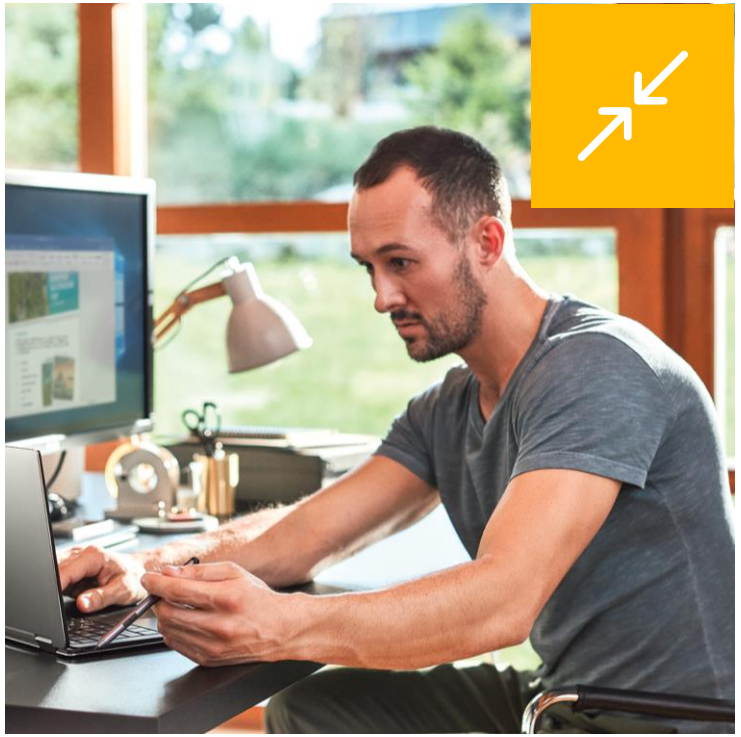
Lack of skilled personnel to keep up with the increased sophistication of attacks.

Keeping up with evolving complexity in data privacy or industry regulations.

A new reality needs new principles



Verify explicitly

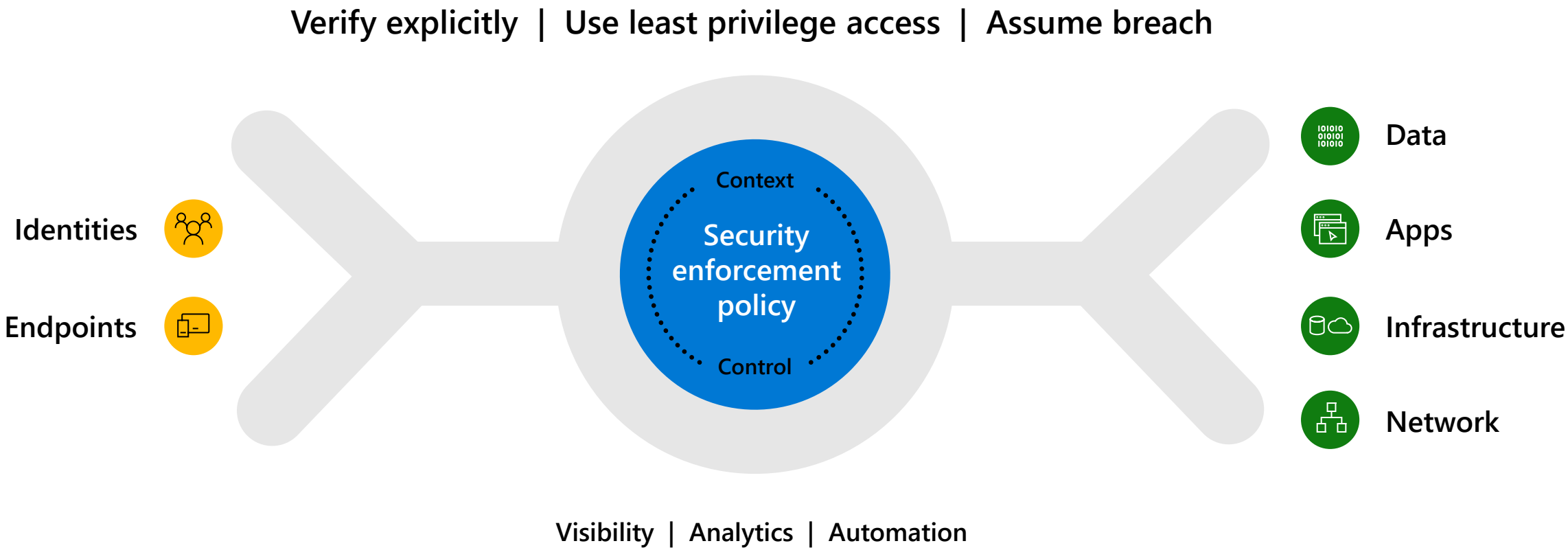


Use least privilege access

Assume breach

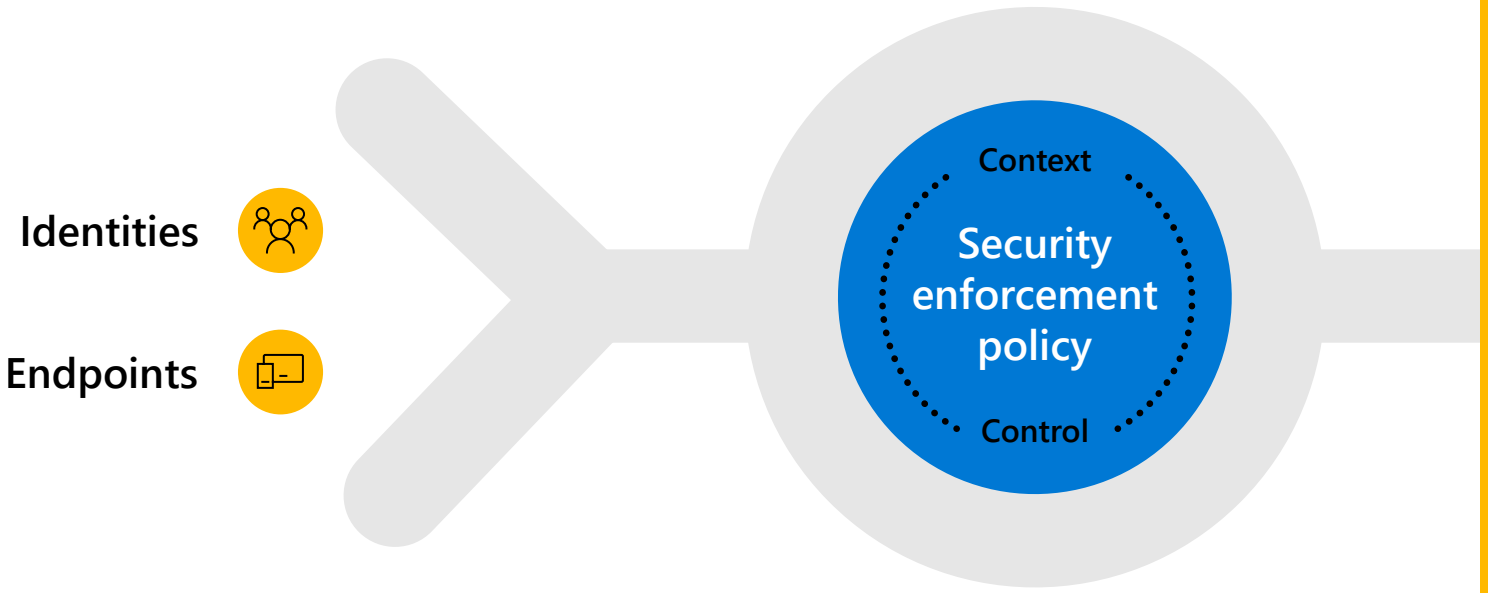
Secure your organization with Zero Trust

Increase security assurances for your critical business assets



Building the foundation to Zero Trust

Zero Trust starts with securing the people and the devices they use to get work done



80%

of breaches involve the use of lost or stolen passwords.

60%

of BYO devices are not secured by IT.

Source: "Verizon 2020 Data Breach Investigations Report"
Source: "Mobile security—the 60 percent problem" Brian Peck, Zimperium, April 7, 2020

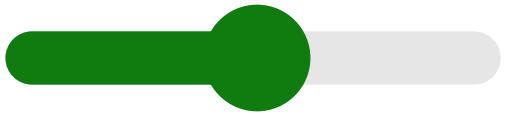
The business value of securing your identities and endpoints

Increased security and productivity

45%

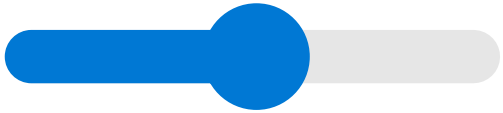
reduction in the likelihood of a data breach.

50%



reduction in overall management effort for an IAM team.

75%



reduction of password reset requests through enabling self-service.

80%

deployment time saved with Microsoft Endpoint Manager.

Sources:
The Total Economic Impact™ Of Securing Apps With Microsoft Azure Active Directory, a commissioned study conducted by Forrester Consulting, August 2020.
The Total Economic Impact™ Of Microsoft Endpoint Manager, a commissioned study conducted by Forrester Consulting, April 2021.
Forrester based all savings estimates on the composite organizations developed for its TEI studies.

"Digital transformation is something many companies like ours are considering. Based on our experience with Azure AD, whenever I think about the cloud, I now think about identity management as the foundation. This foundation must be strong to easily transition to cloud services."

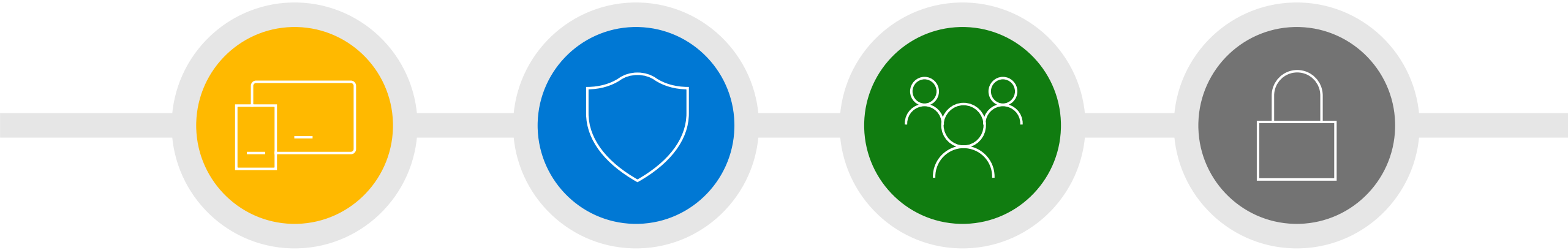
Mr. Ichinose
IT Manager
Mitsui & Co.

"Since implementing a Zero Trust strategy using Microsoft 365 technologies, our employees can fulfill their company duties from anywhere in the world while maintaining tight control over core security needs."

Igor Tsyganskiy
Chief Technology Officer
Bridgewater Associates

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

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

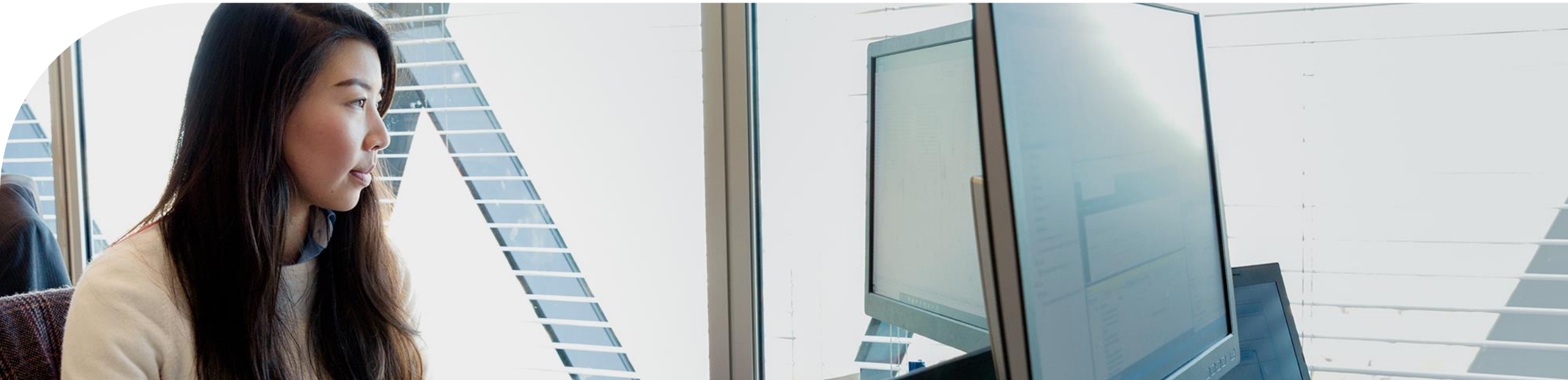
Enable business agility and efficient allocation of resources.

Strategies for modernization

Modernize authentication and manage identities in the cloud.

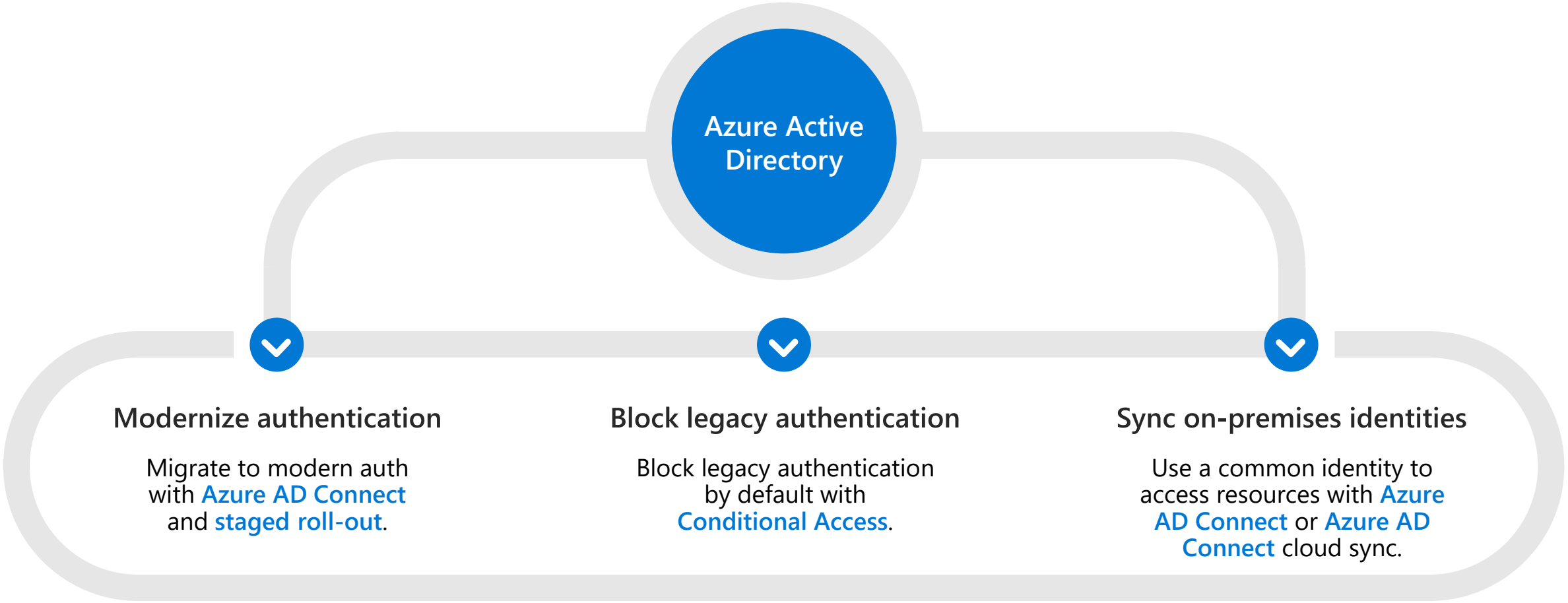
Manage devices from the cloud at your own pace.

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



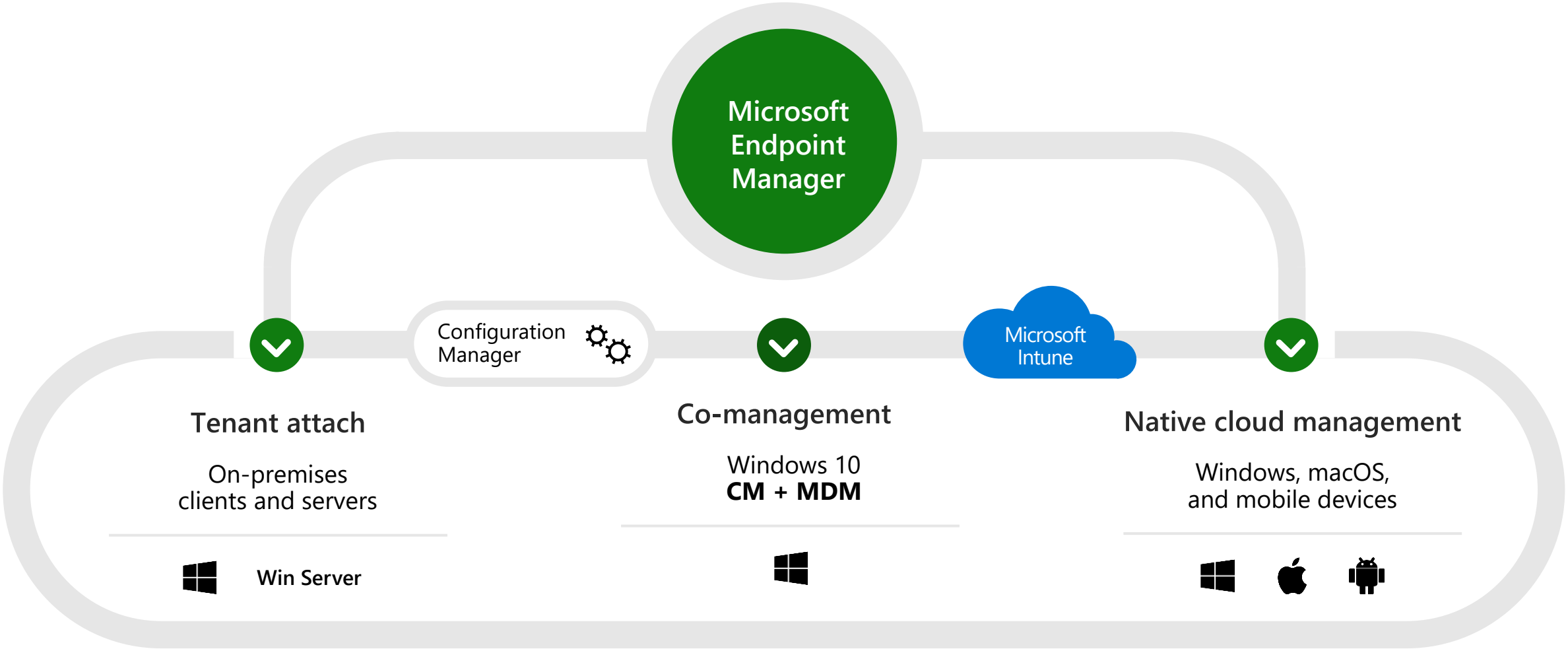
Migrate authentication and identities to the cloud

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



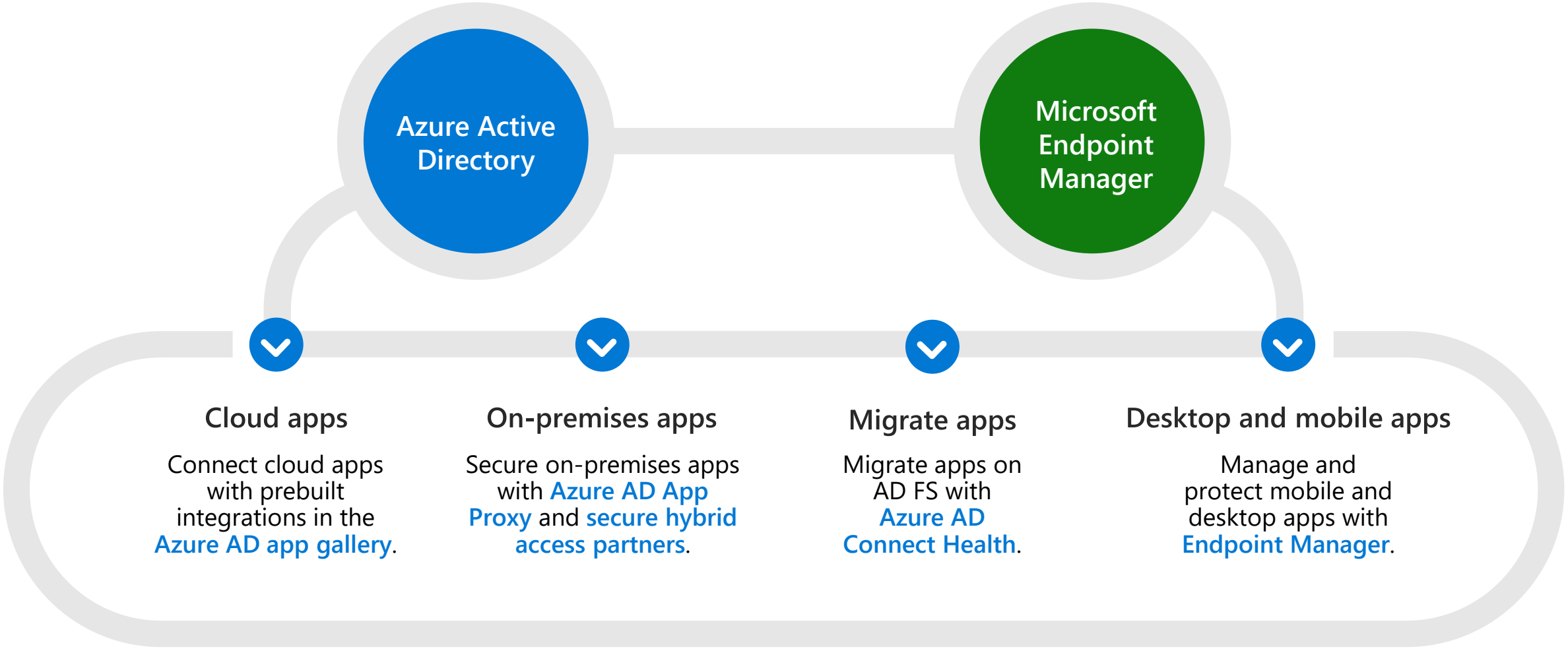
Manage endpoints in the cloud at your own pace

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

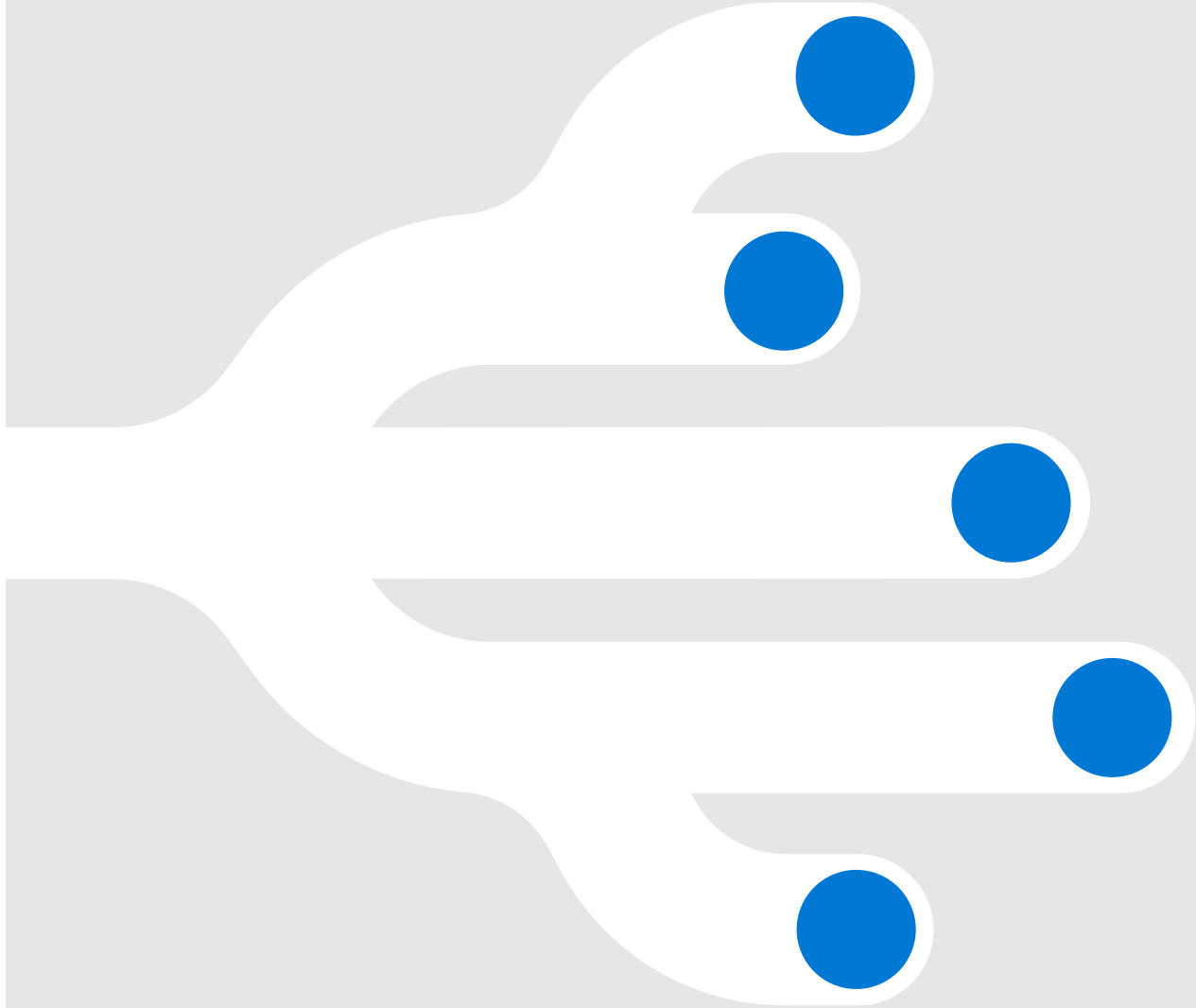


Modernize identities and endpoints

Secure the hybrid workforce

Transform employee experiences

Customize secure access for all user types



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

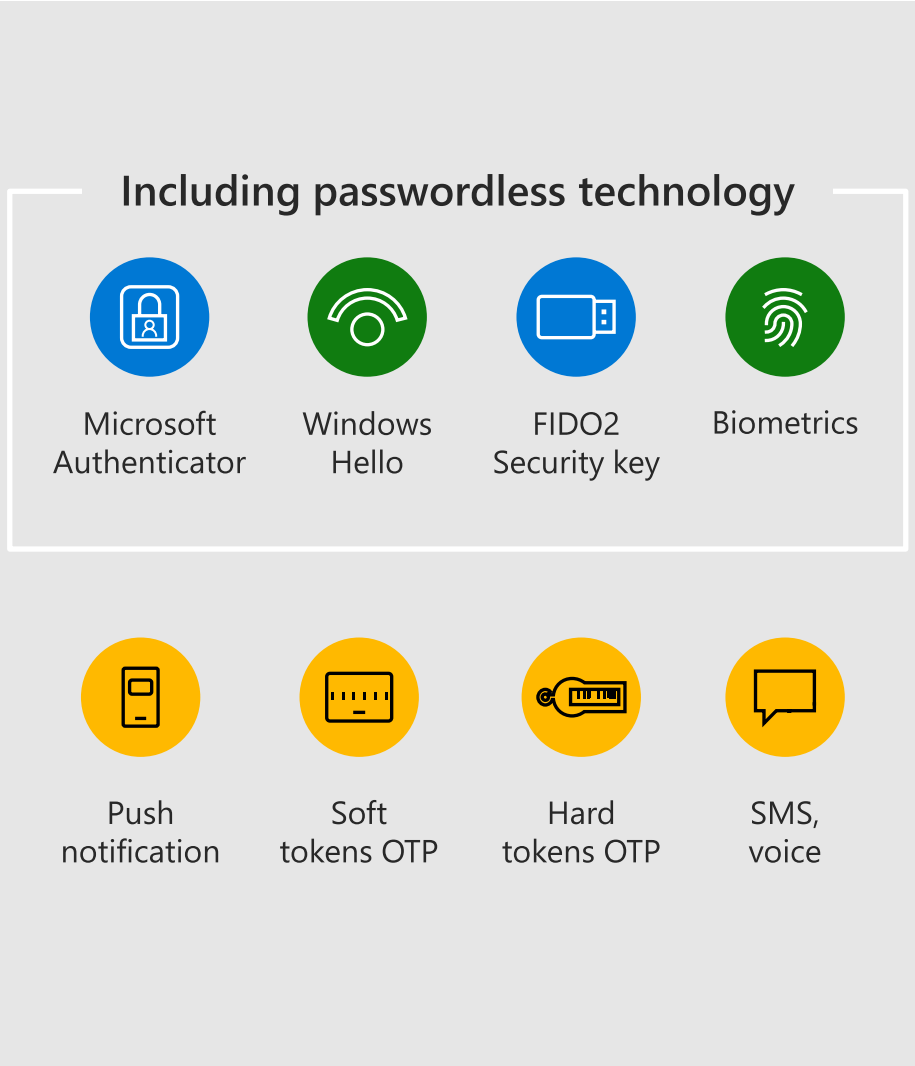
Secure access to resources with multifactor authentication

Passwords are the weakest link in a security chain.

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

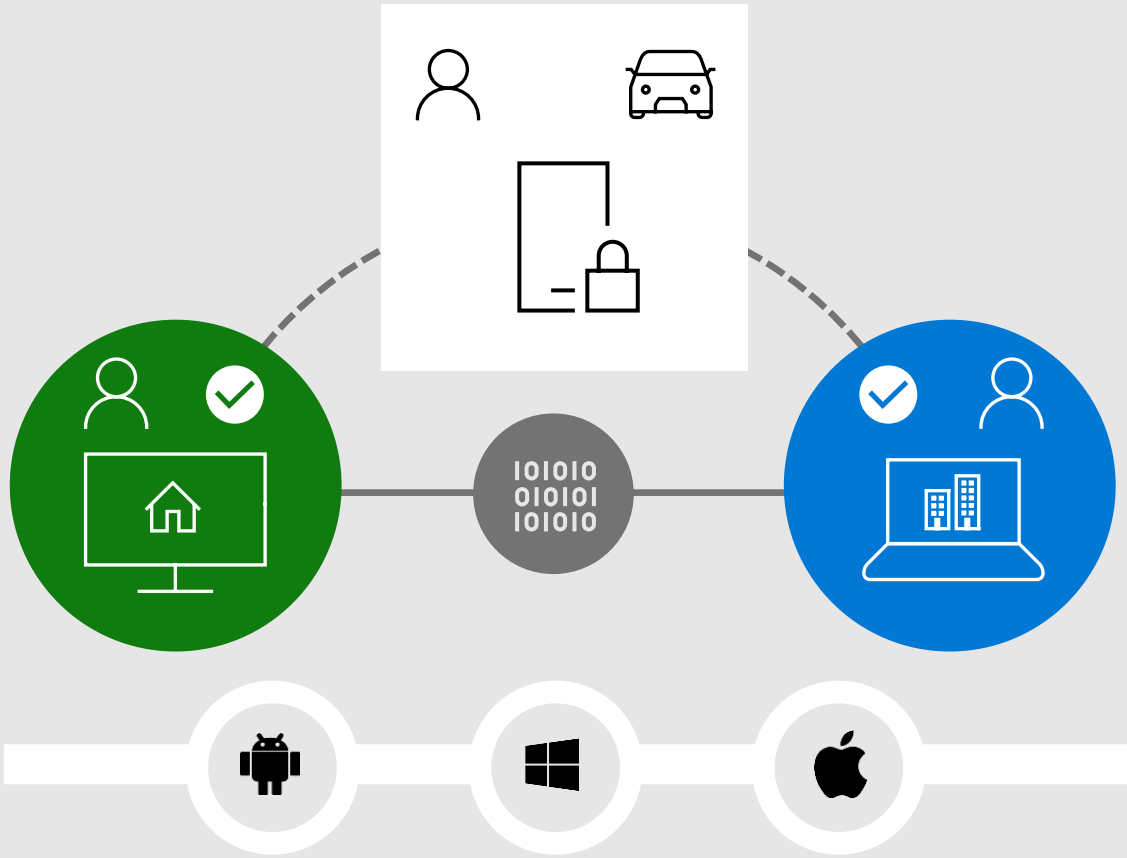
Apply data protection policies on mobile devices and applications.

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.

Microsoft Defender for Business coming soon!



Configure adaptive access policies

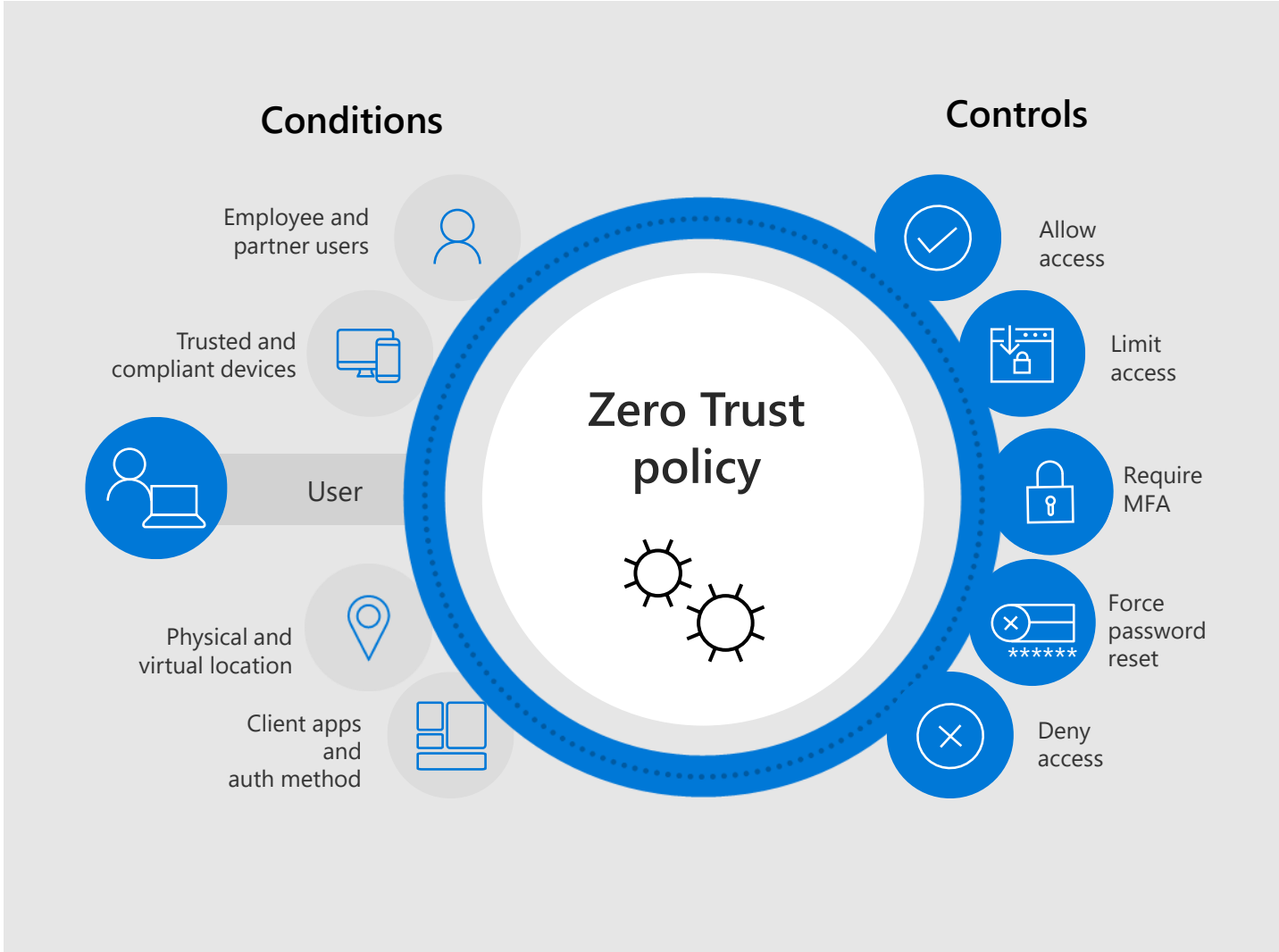
Control access with smart policies and risk assessments

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.



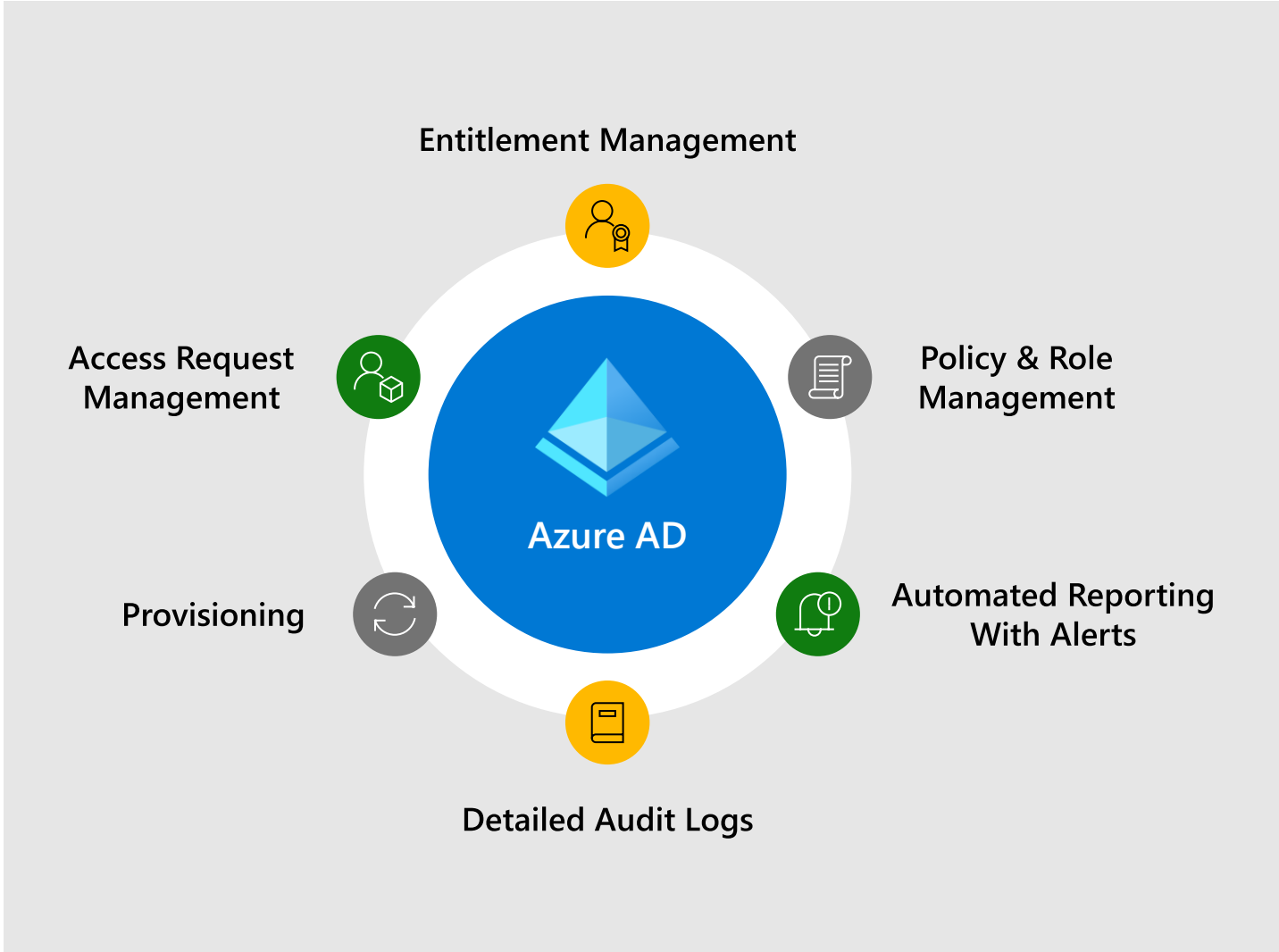
Safeguard resources with access lifecycle management

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.

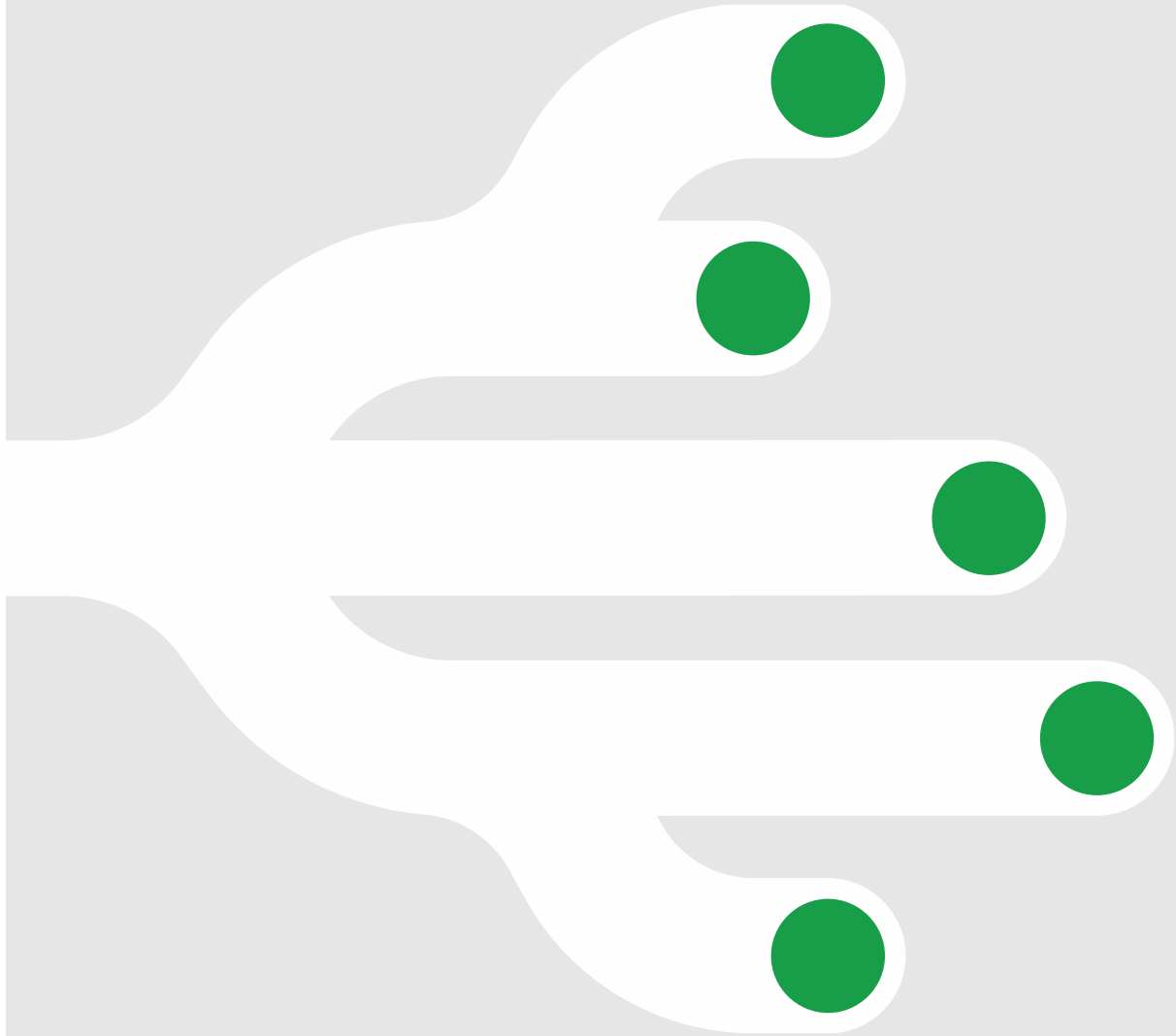


Modernize identities and endpoints

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**.

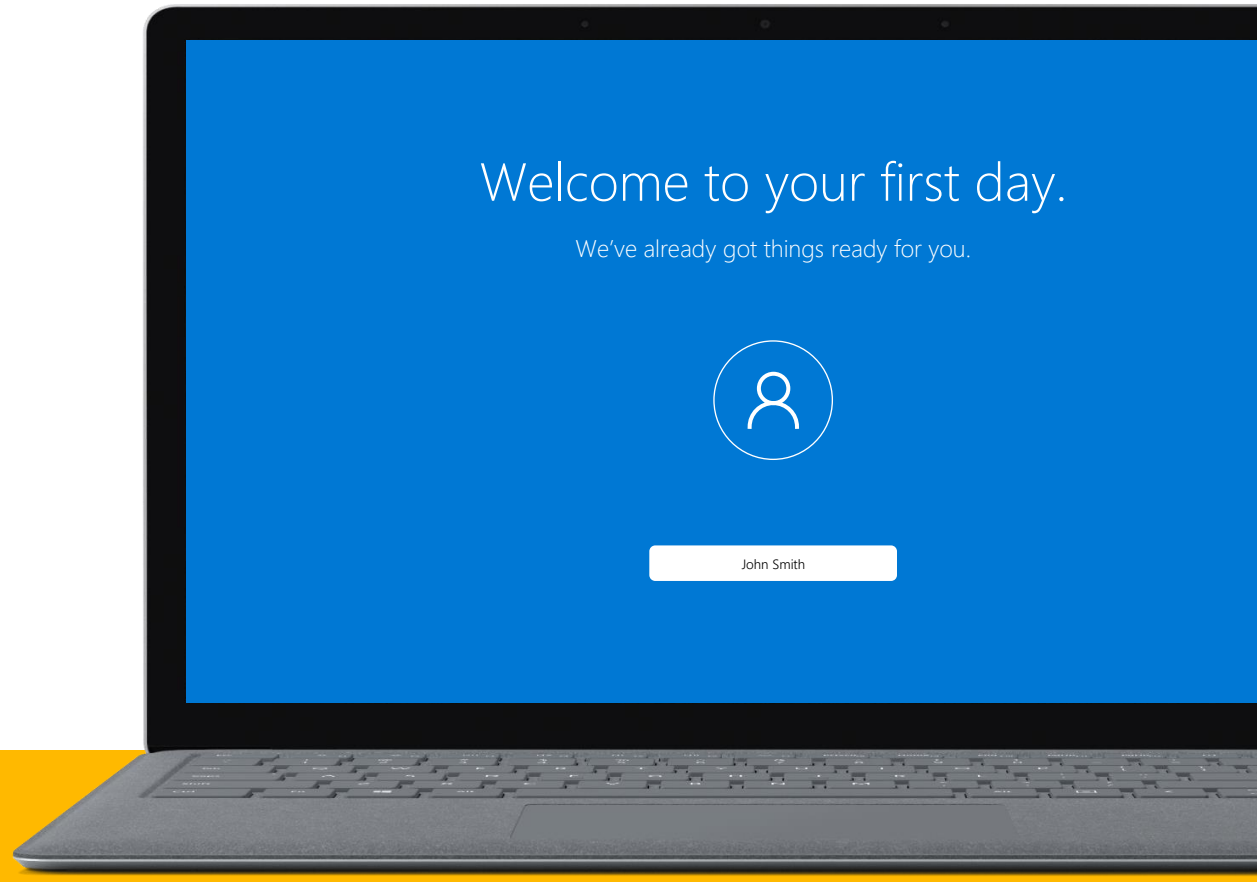
Provision access to resources efficiently

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.



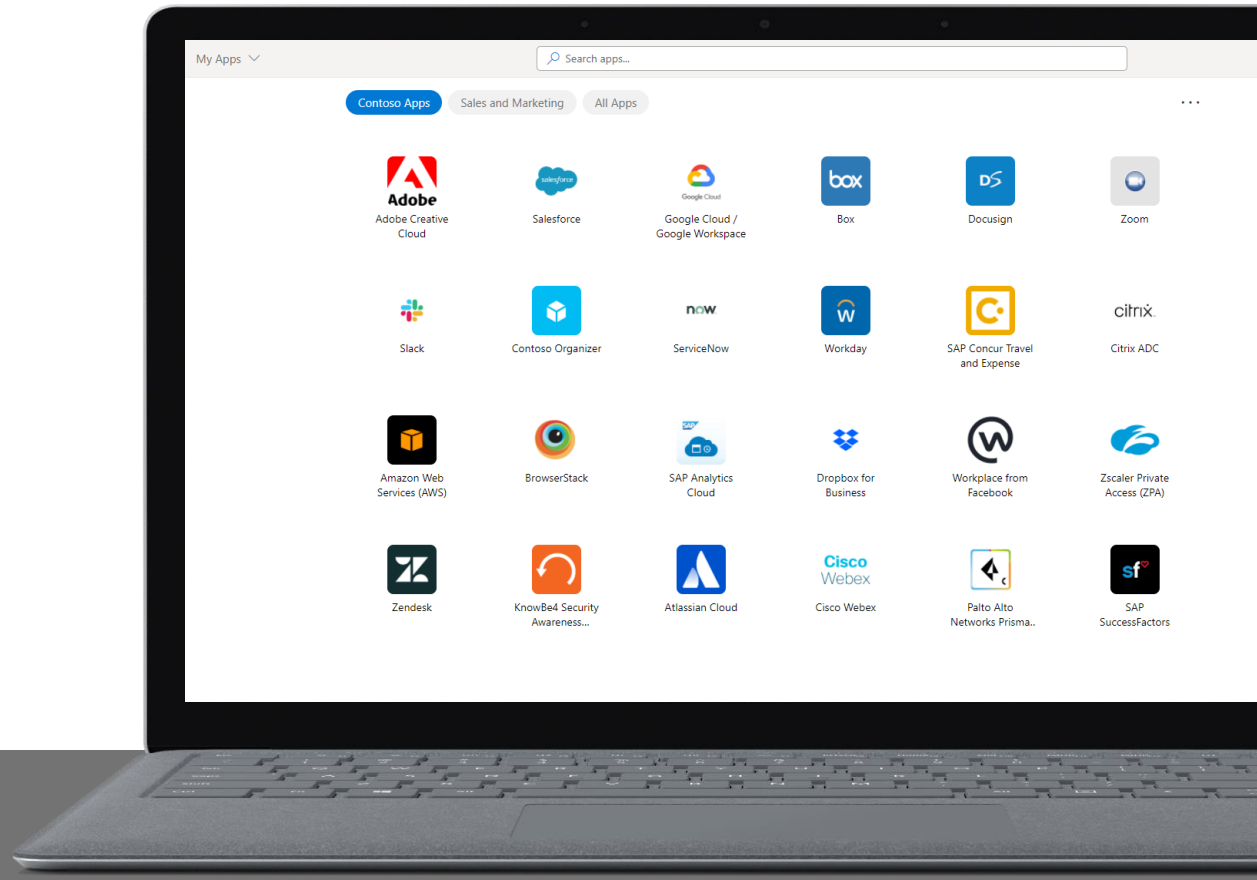
Enable seamless, secure access with single sign-on

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.



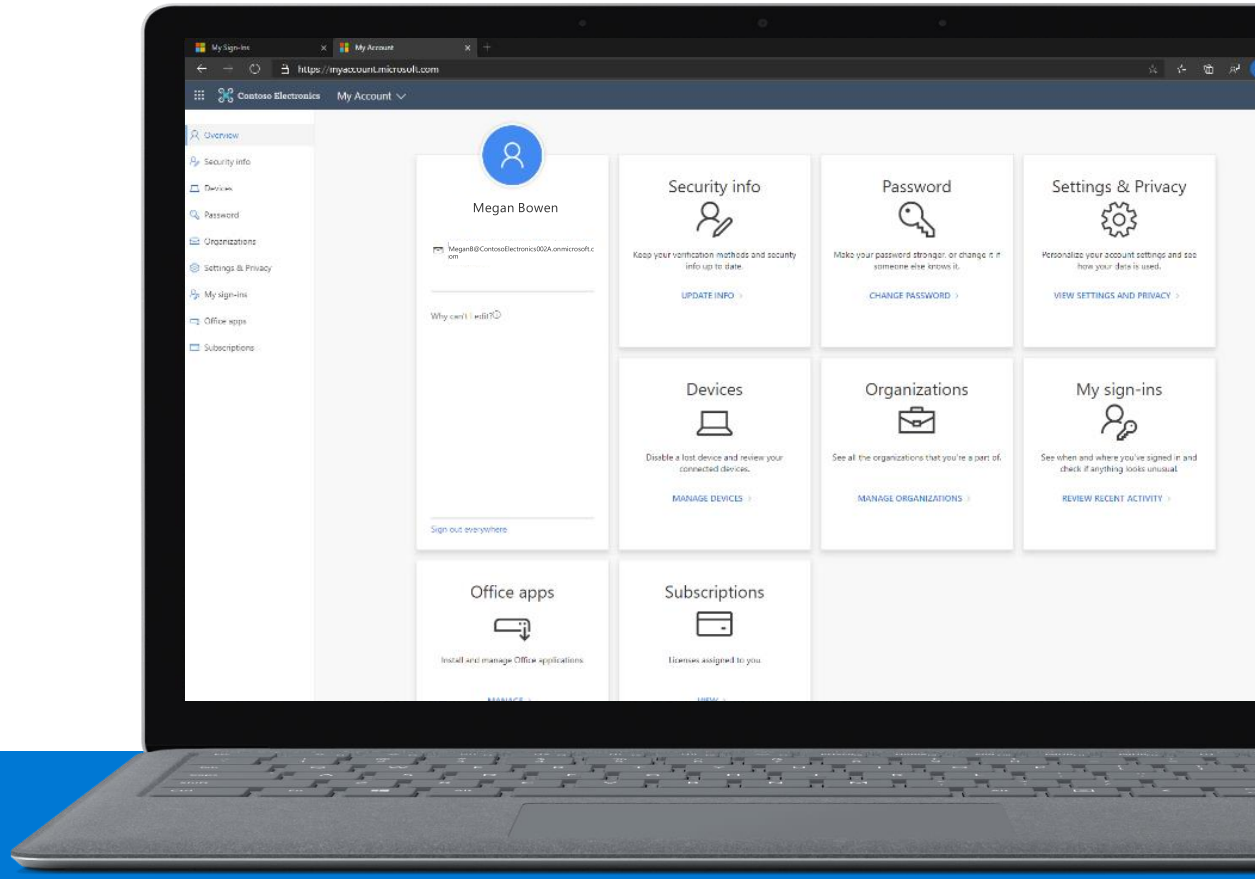
Empower employees to manage their own identity

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

Enable employees to self-service password resets.

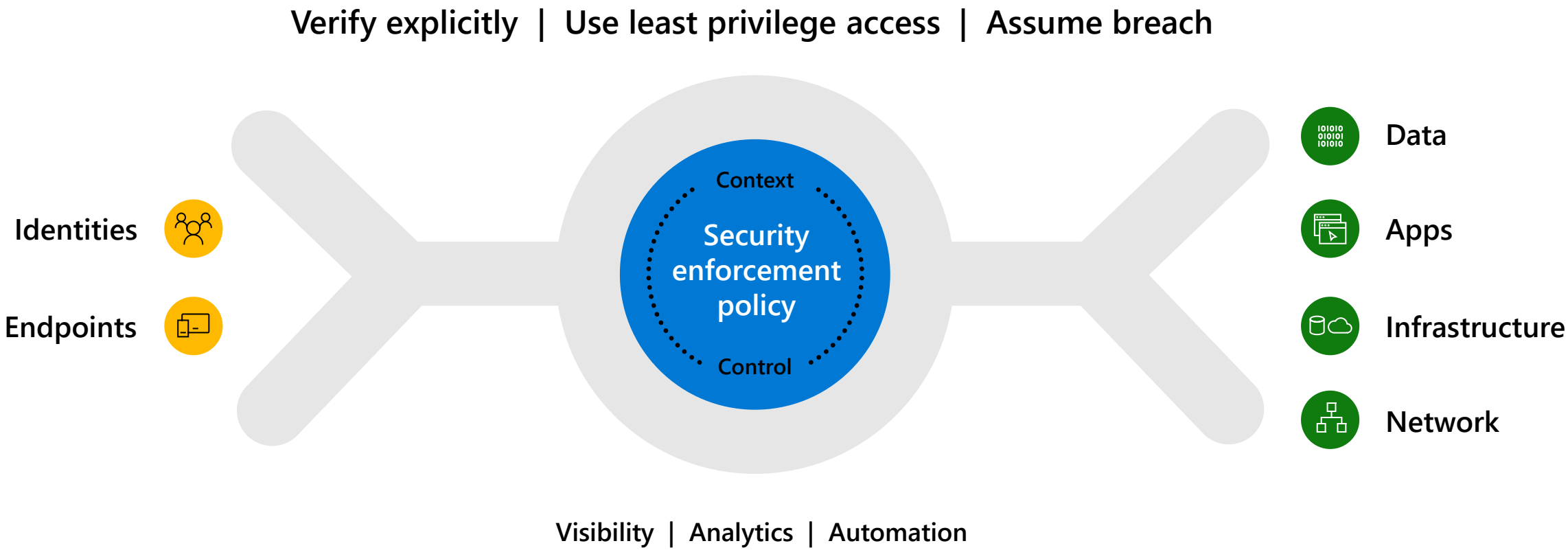
Empower employees and guests to manage and request access packages.

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



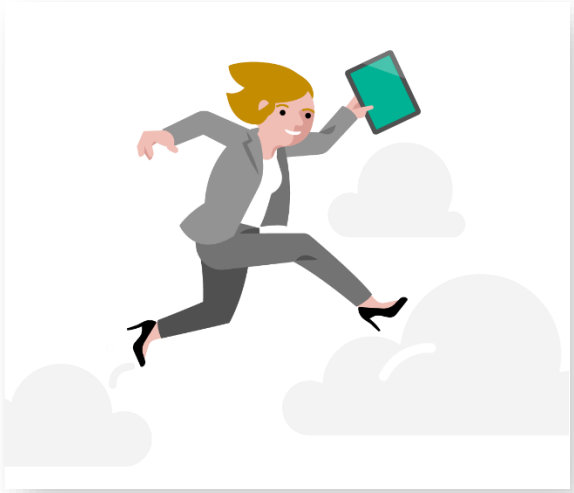
Secure your organization with Zero Trust

Increase security assurances for your critical business assets



Microsoft 365 Business Premium

One solution to run your business from anywhere, with peace of mind

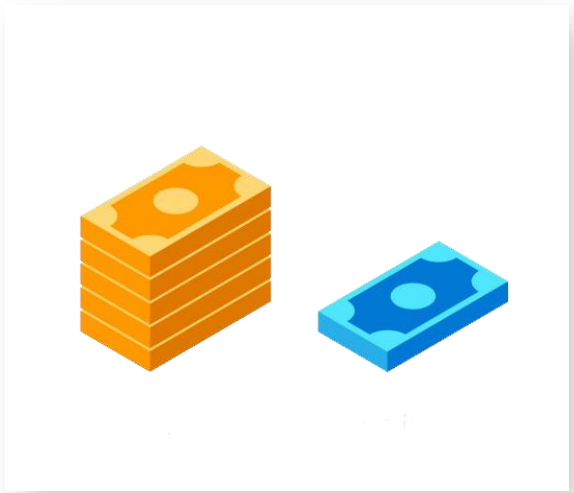


Comprehensive and easy to use

One solution for productivity and security

Cloud platform simplifies deployment

Gets you up and running quickly

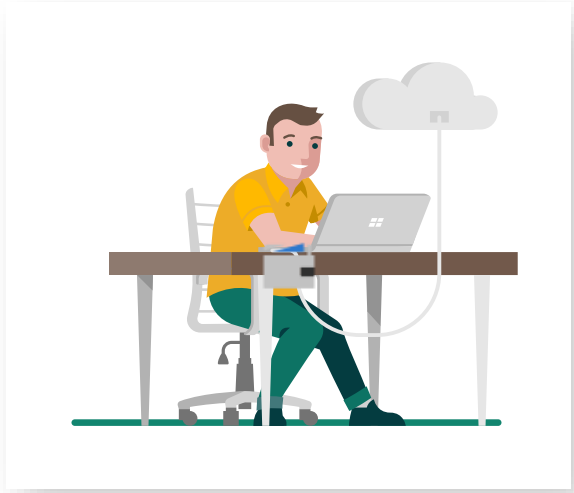


Reduces costs

Eliminates costs of multiple point solutions

Reduces helpdesk costs

Eases licensing complexity



Enterprise grade technology

Advanced security; trusted by enterprises

AI powered threat intelligence

Top rated security vendor

Microsoft 365 Business Premium

Collaborate in real time

- Video Conferencing
- Group Chat
- Easy access to files, Co-authoring
- Phone system (Business Voice add-on)
- App integrations

Enable secure access and protect Identity

- MFA
- Conditional Access
- App Proxy
- Dynamic Groups
- Azure Virtual Desktop

Defend against cyberthreats and data loss

- Microsoft Defender for Office 365
- Azure Information Protection
- Office 365 DLP
- Cloud App Discovery
- Coming soon! Microsoft Defender for Business

Easily Secure and Manage Devices

- Intune Device Management
- Intune Mobile App Management
- Autopilot

Challenge

Work data on personal devices

A Northwind Traders marketing manager is using her personal phone to check company email. She receives a confidential business plan and saves it for later reference. **She accidently saves to a personal share which is not secure.**

64% of SMBs allow employees to access work data on personal phones and computers.[1]

[1]*Source: Microsoft Internal Research of SMBs (2-299 employees)*

Solution

Protect work data on personal devices

With Microsoft 365 Business Premium, you can set up Intune App Protection Policies, so work apps can be separated from personal apps. Administrators can specify that work documents and attachments are only saved on authorized and secure work share like OneDrive for Business, safeguarding sensitive work information.

58% of employee devices on average are configured with proper security protocols and fewer than **1 in 5** saying that all employees undergo security training.[1]

[1]*Source: A commissioned study conducted by Forrester Consulting on behalf of Microsoft, October 2019 survey of SMBs (1-499 employees)*

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.

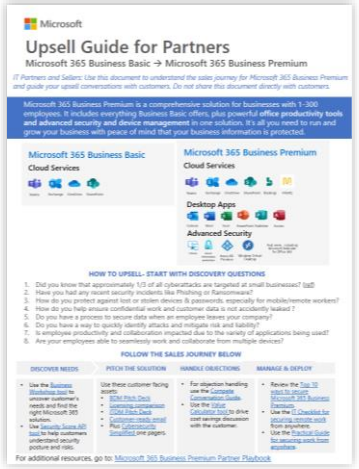
3

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

Upsell Guides for Partners

https://aka.ms/M365BPPlaybook

Microsoft 365 Business Basic to Business Premium


Microsoft

Upsell Guide for Partners

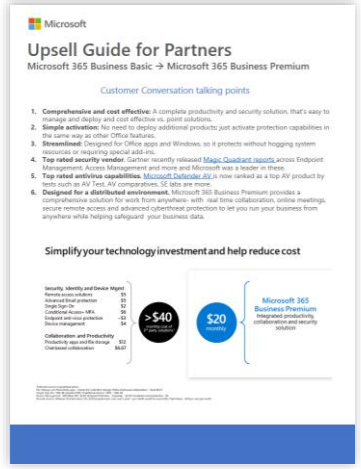
Microsoft 365 Business Basic → Microsoft 365 Business Premium


Microsoft

Upsell Guide for Partners

Microsoft 365 Business Basic → Microsoft 365 Business Premium

Microsoft 365 Business Premium Additional Capabilities


Microsoft

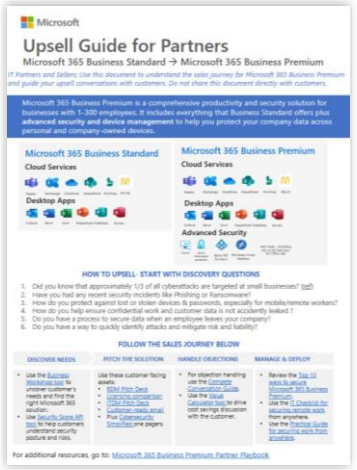
Upsell Guide for Partners

Microsoft 365 Business Basic → Microsoft 365 Business Premium

Customer Conversation talking points

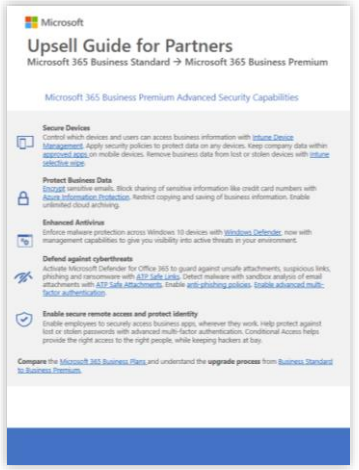
Simplify your technology investment and help reduce cost

Microsoft 365 Business Standard to Business Premium


Microsoft

Upsell Guide for Partners

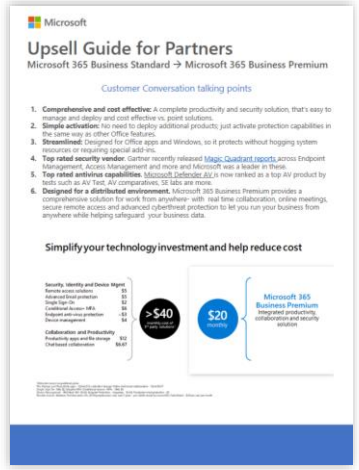
Microsoft 365 Business Standard → Microsoft 365 Business Premium


Microsoft

Upsell Guide for Partners

Microsoft 365 Business Standard → Microsoft 365 Business Premium

Microsoft 365 Business Premium Advanced Security Capabilities


Microsoft

Upsell Guide for Partners

Microsoft 365 Business Standard → Microsoft 365 Business Premium

Customer Conversation talking points

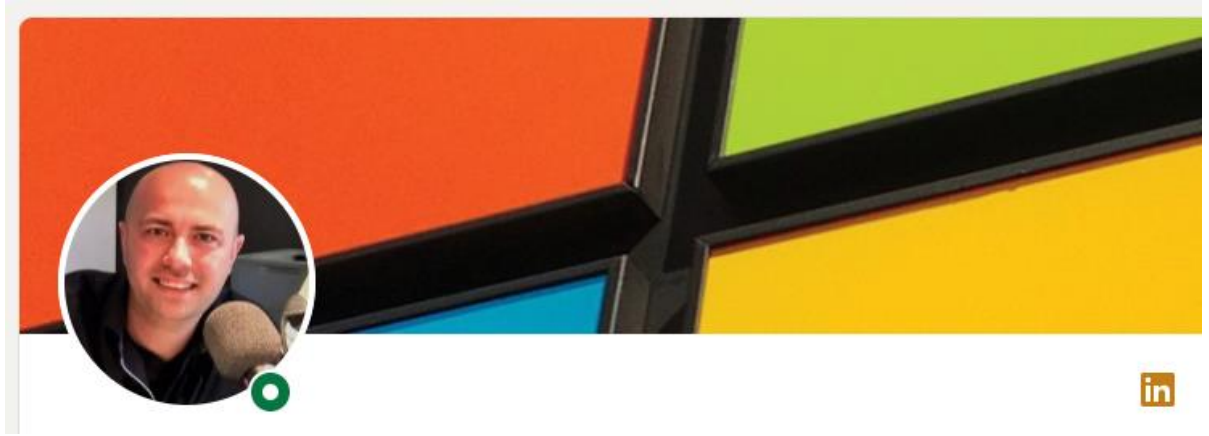
Simplify your technology investment and help reduce cost

Volg ons op LinkedIn voor meer informatie over Microsoft Security Champ Wanted!

Registreer je voor de volgende sessies via:

aka.ms/thenextmicrosoftsecuritychamp
aka.ms/sellingamazingvirtually

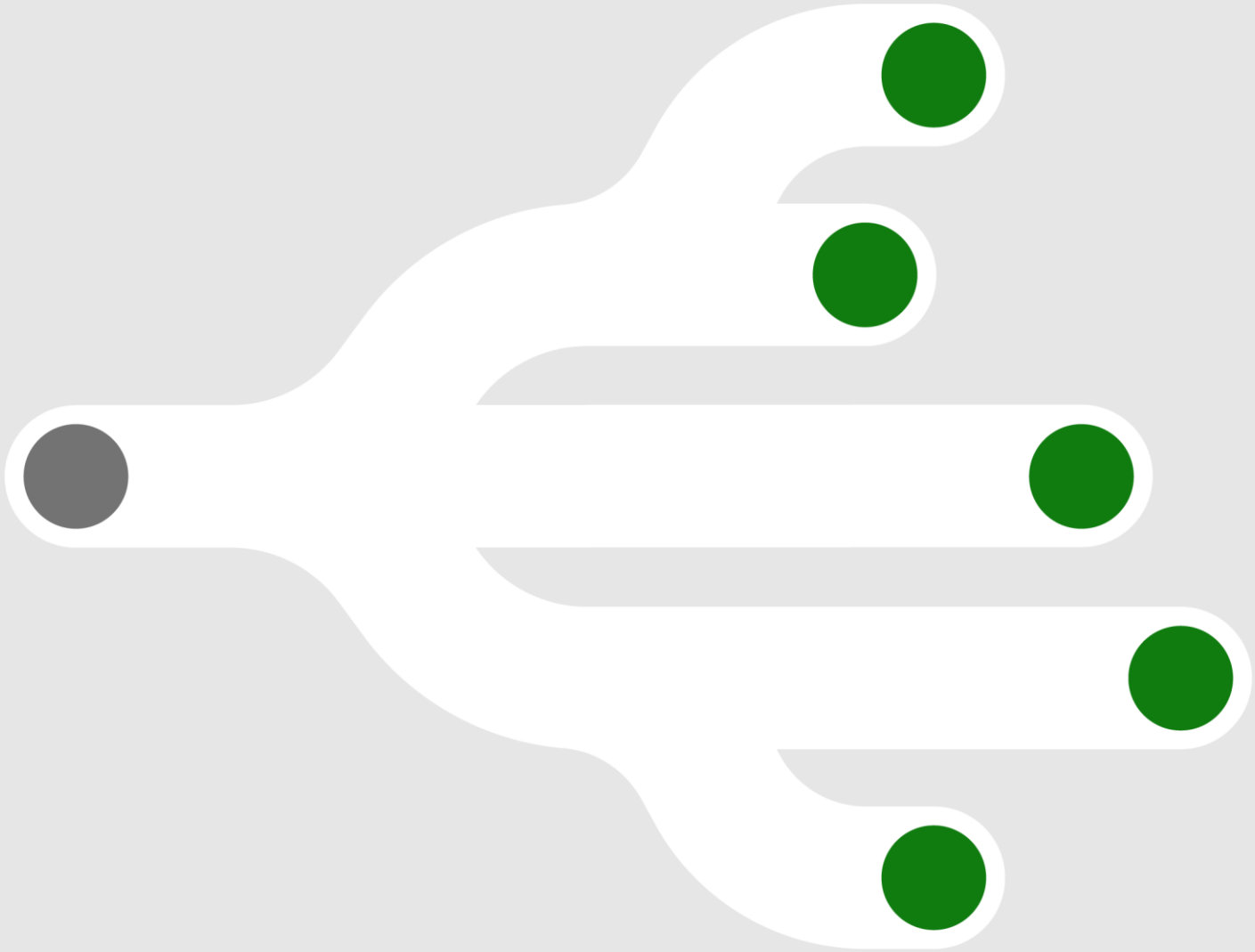
[Glenn Habes | LinkedIn]



[Jeroen Jansen | LinkedIn]

Microsoft Security

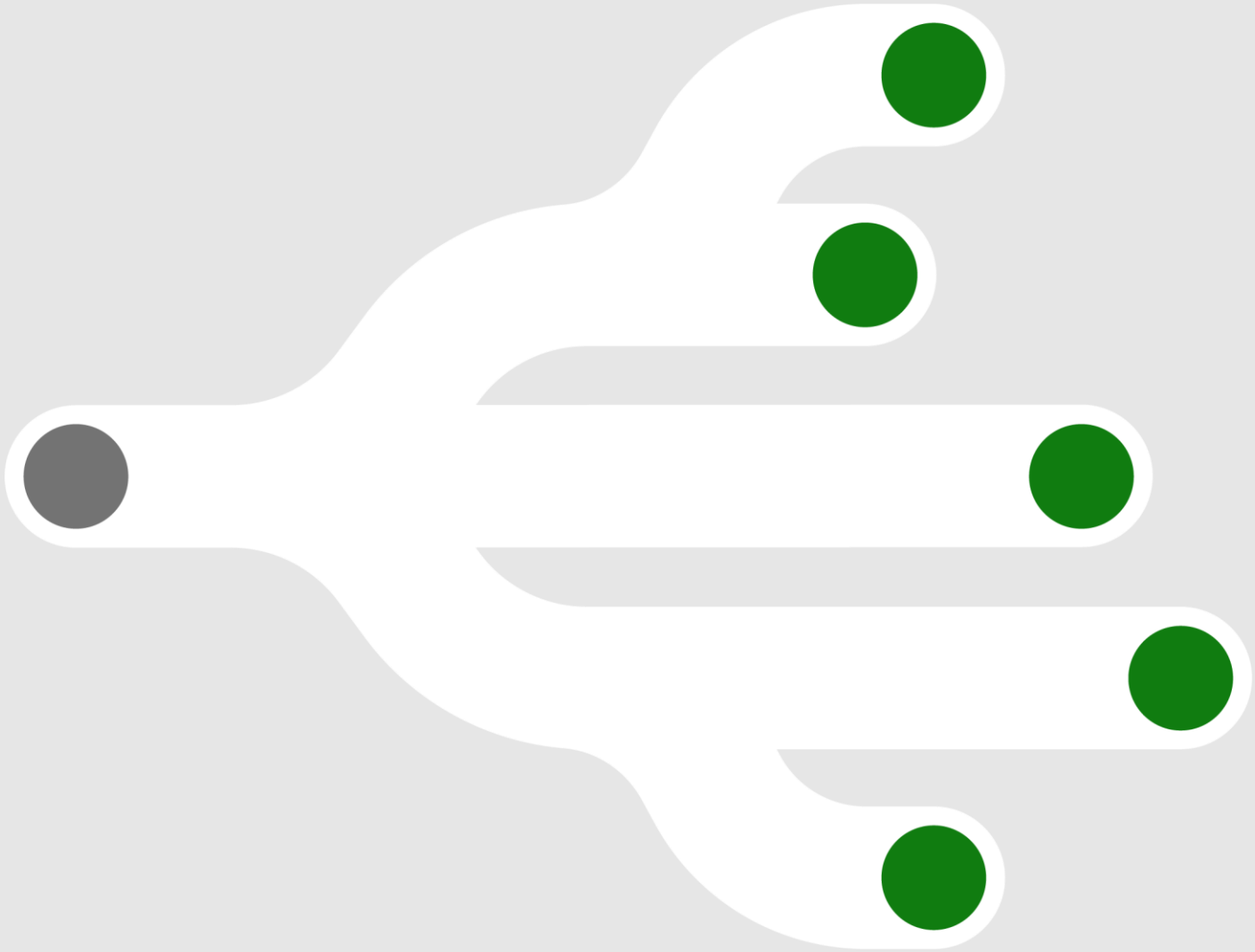
Q&A



#SecurityLifeHacks

Microsoft Security

Thank you



#SecurityLifeHacks