

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

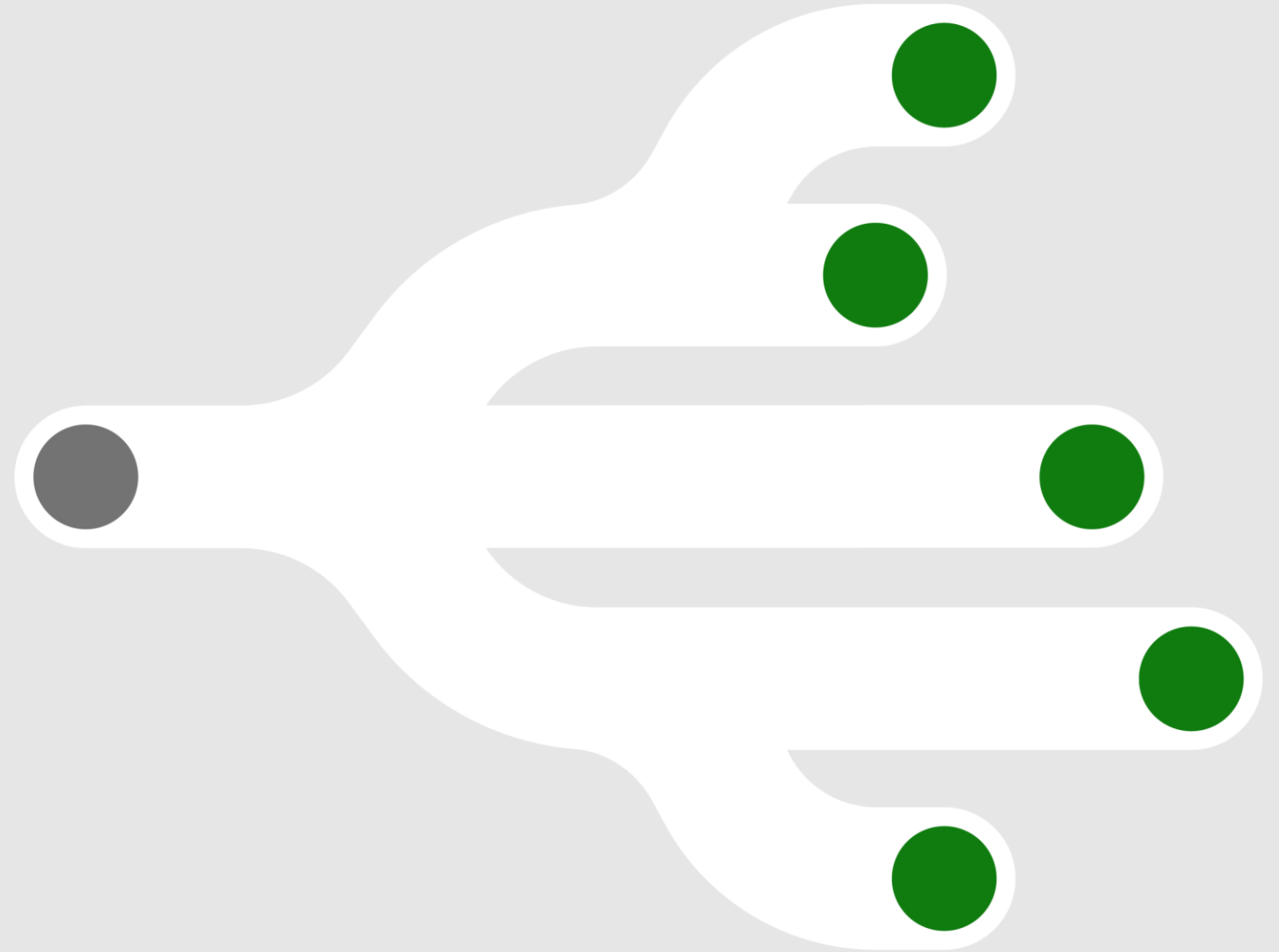
Jeroen Jansen

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.



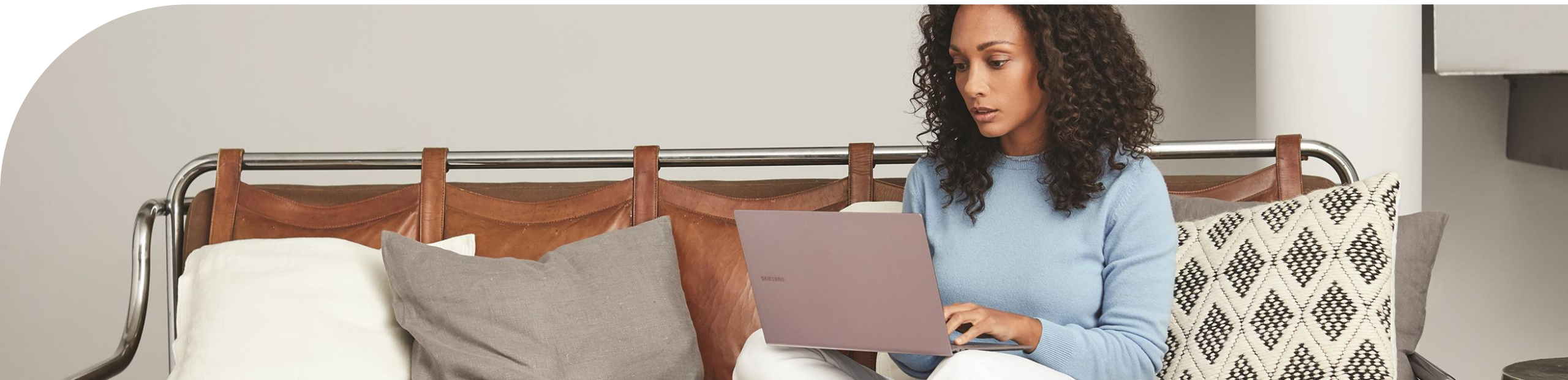
Personal device use at home is difficult to manage and protect, especially when accessing work data through personal devices and/or consumer apps.



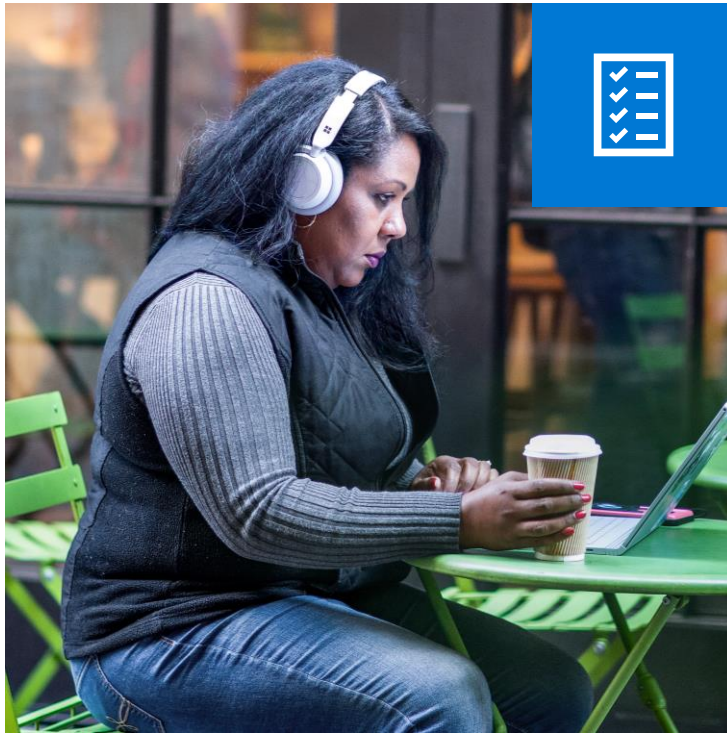
Lack of skilled personnel to keep up with the increased sophistication of attacks.



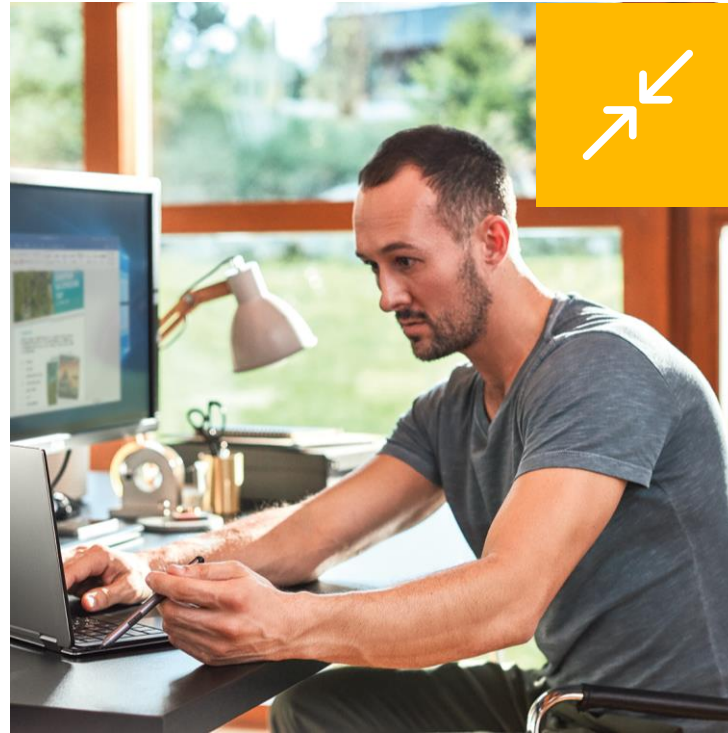
Keeping up with evolving complexity in data privacy or industry regulations.



A new reality needs new principles



Verify explicitly



Use least privilege access

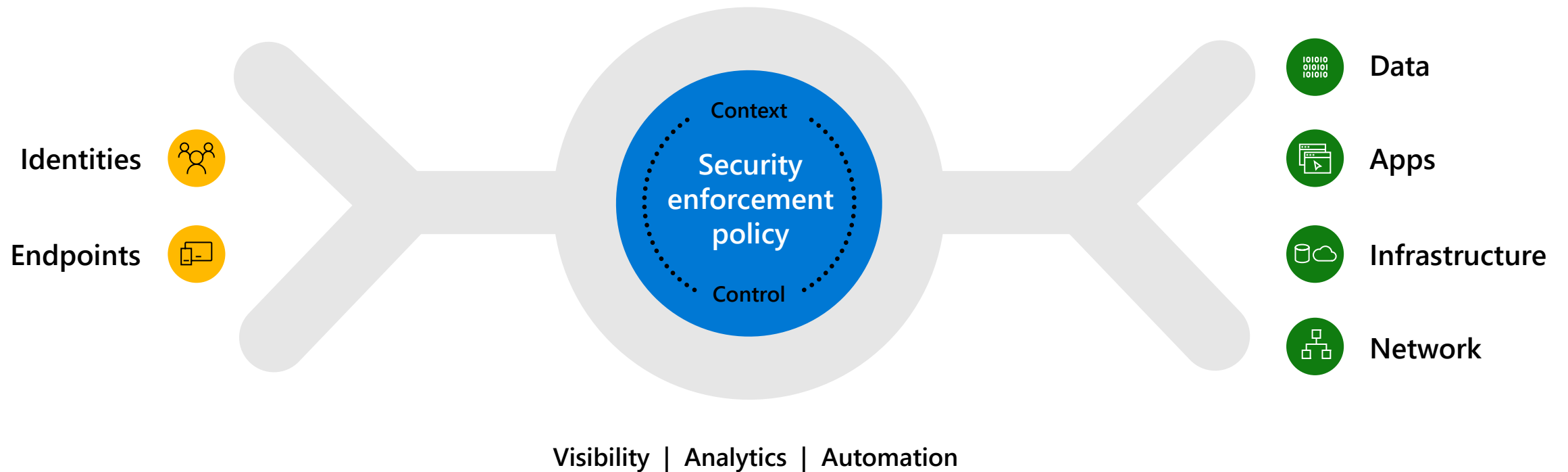


Assume breach

Secure your organization with Zero Trust

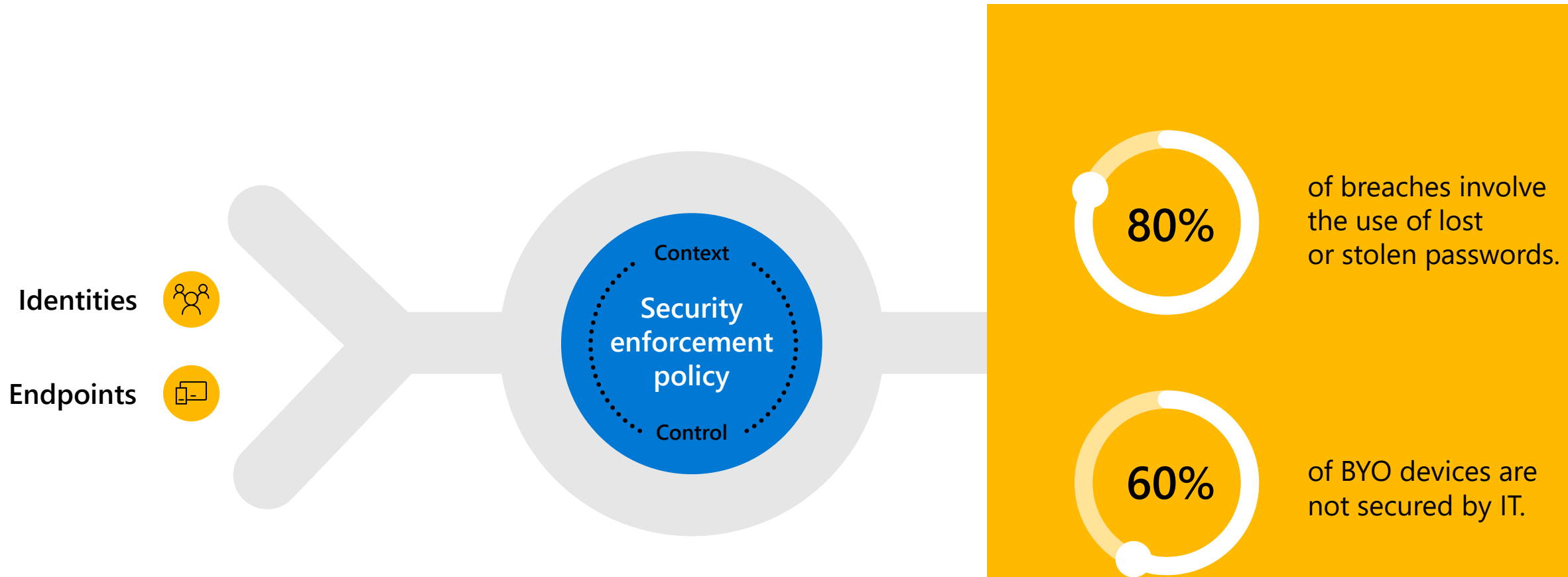
Increase security assurances for your critical business assets

Verify explicitly | Use least privilege access | Assume breach



Building the foundation to Zero Trust

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

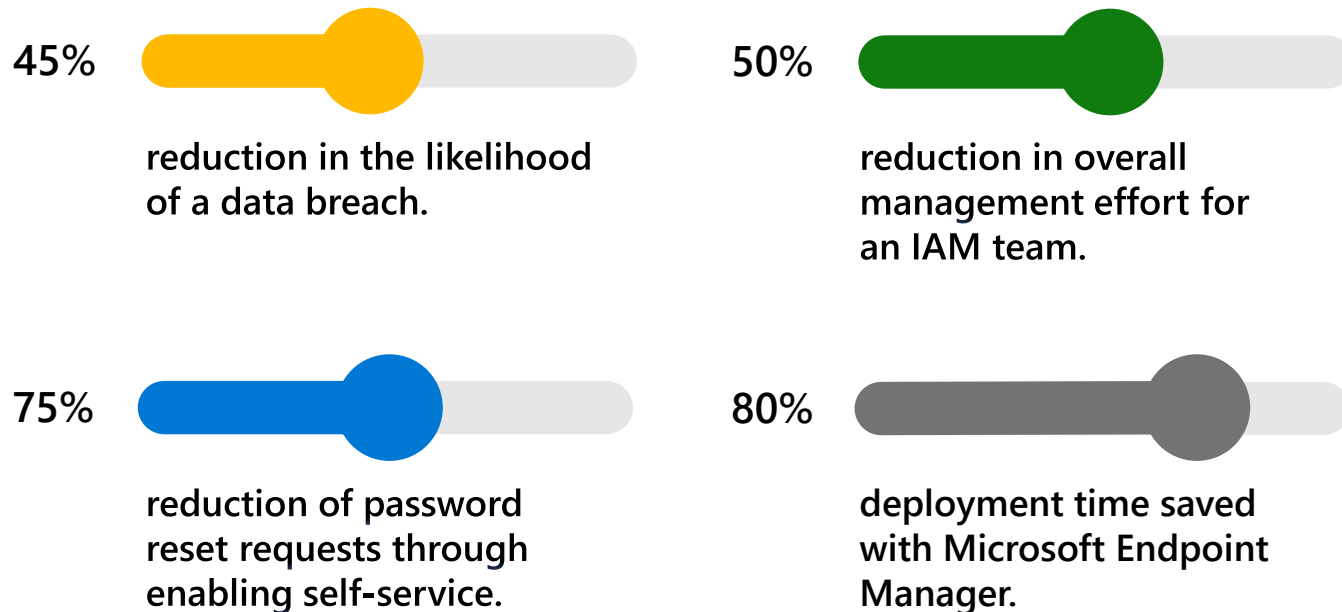


Source: "Verizon 2020 Data Breach Investigations Report"

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



“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





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



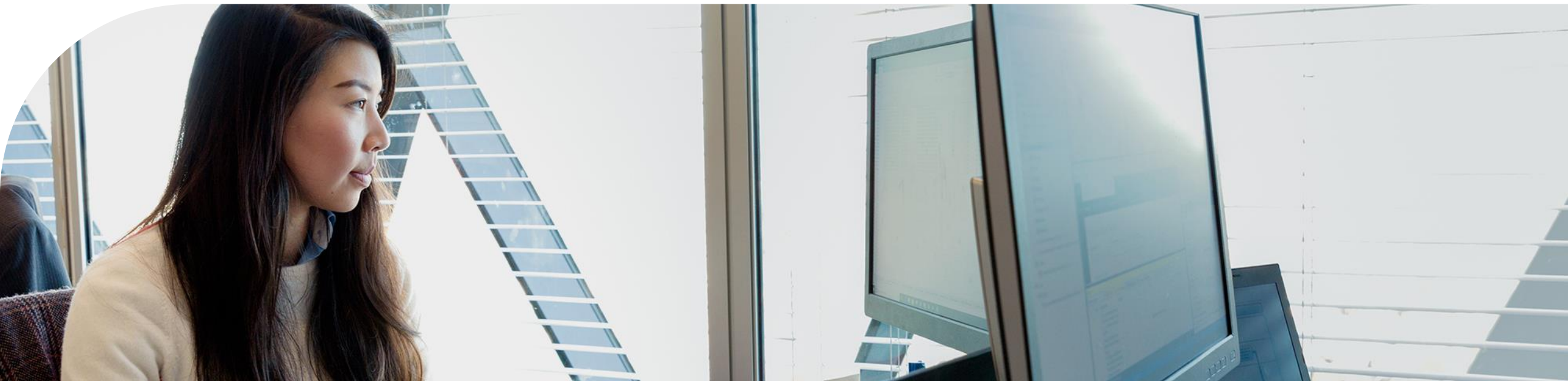
Modernize authentication and manage identities in the cloud.



Manage devices from the cloud at your own pace.

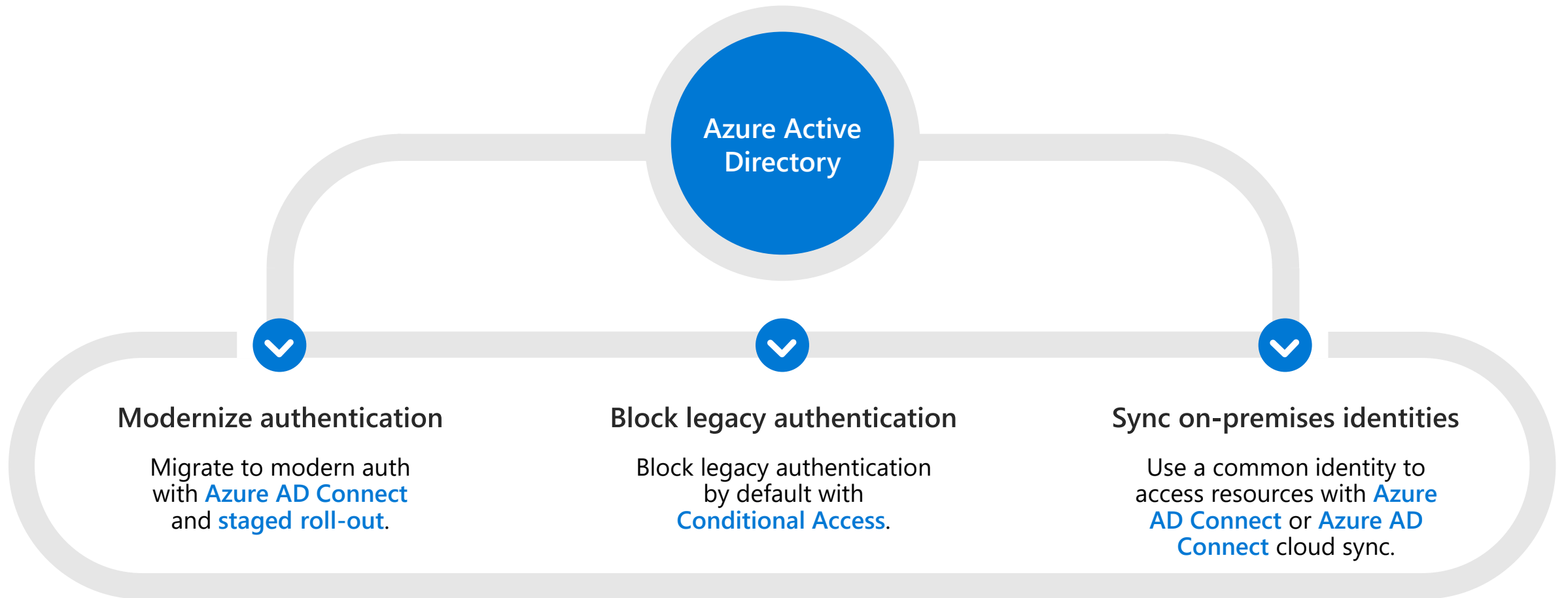


Improve visibility and control by **unifying app management**.



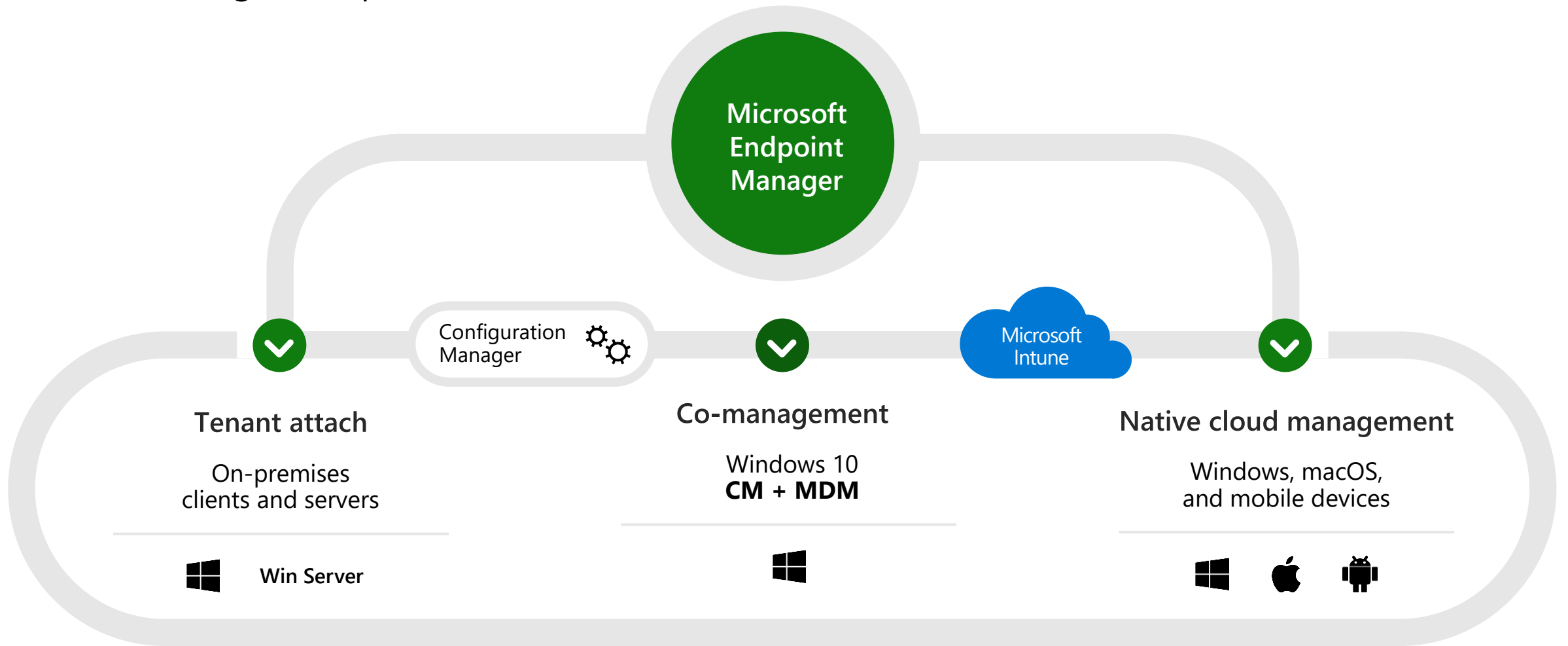
Migrate authentication and identities to the cloud

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



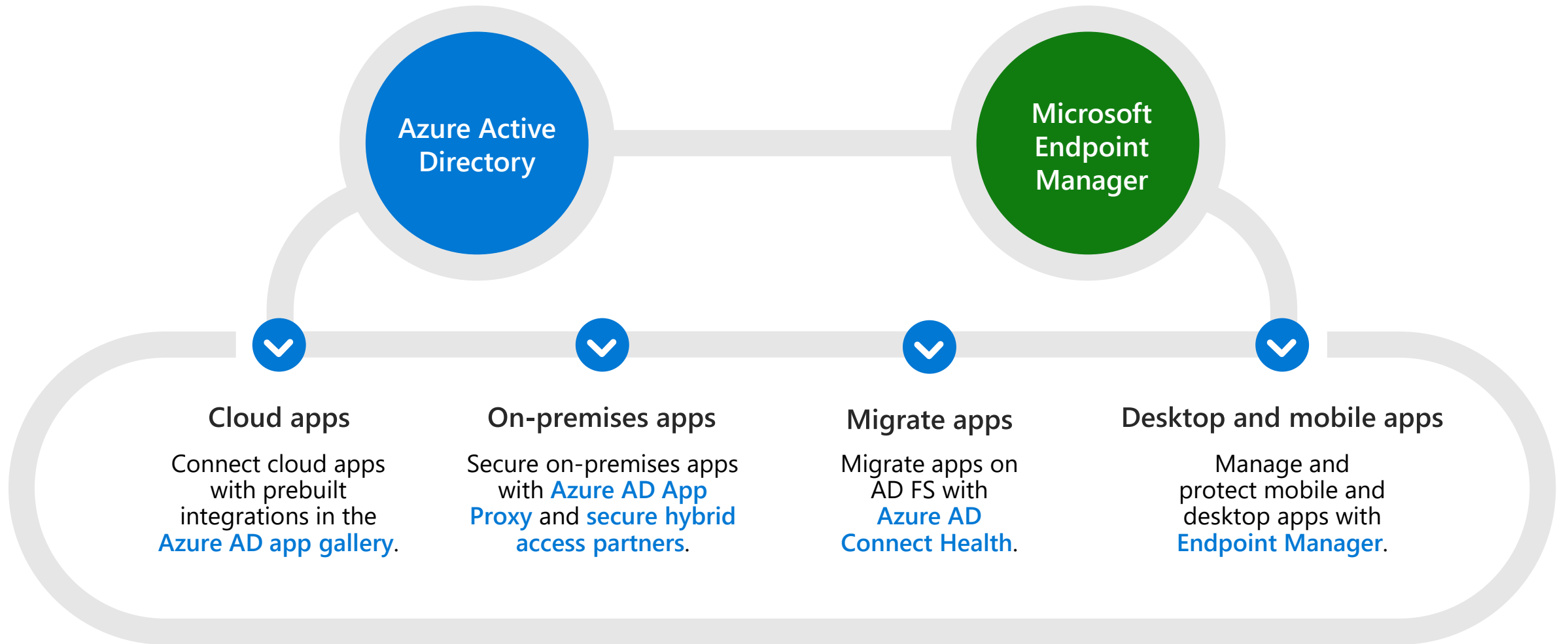
Manage endpoints in the cloud at your own pace

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



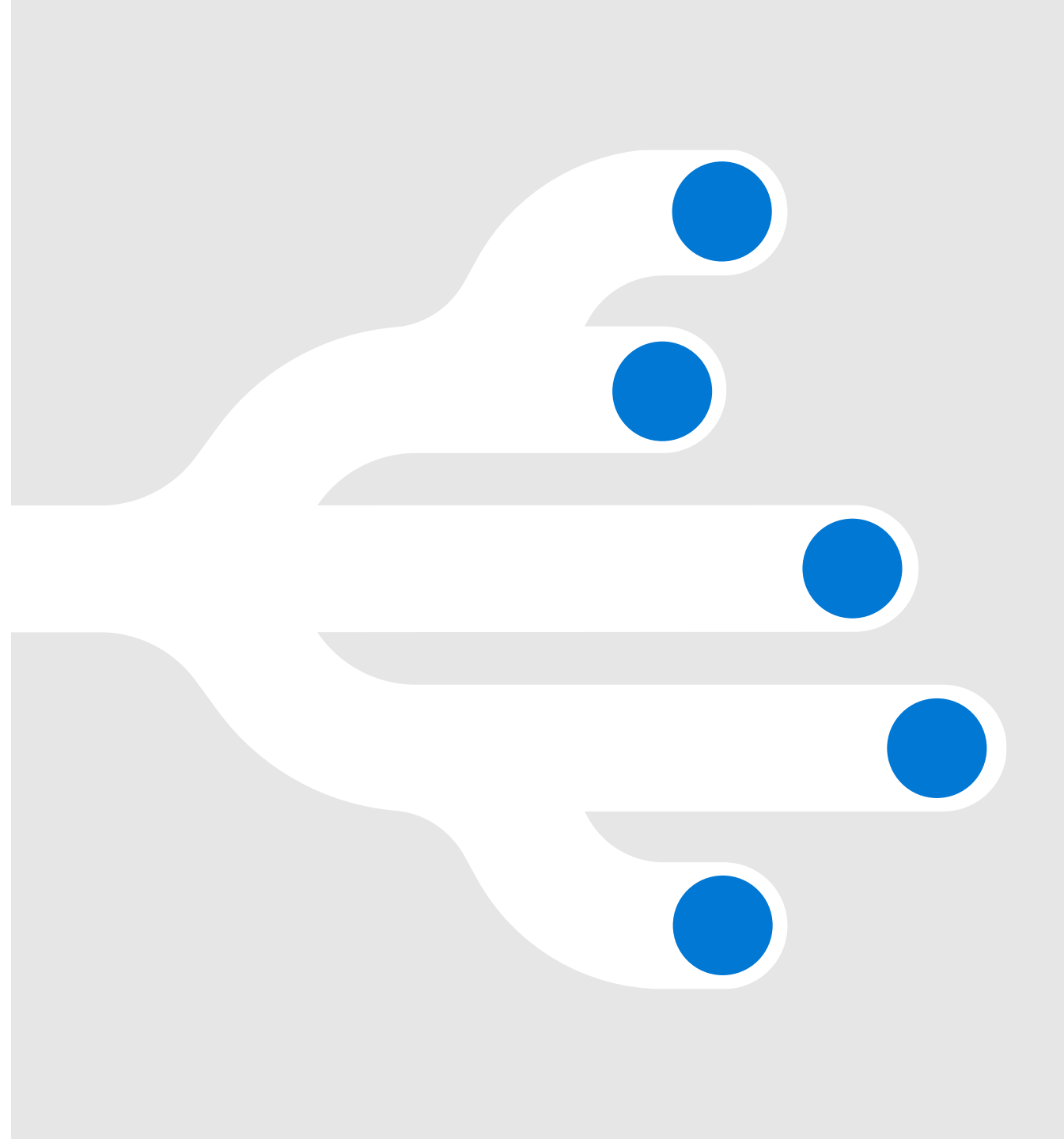
Secure the hybrid workforce



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

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.

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

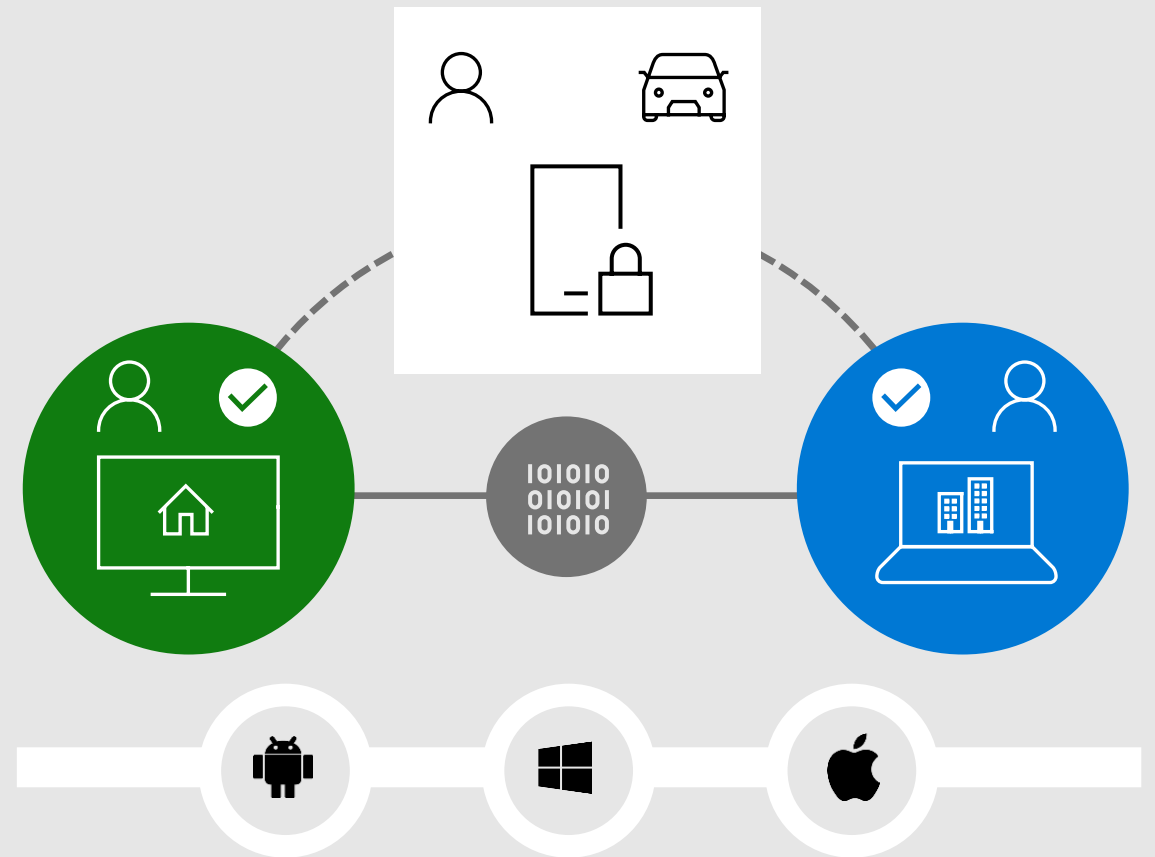
Apply data protection policies on mobile devices and applications.

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.

Microsoft Defender for Business coming soon!



Configure adaptive access policies

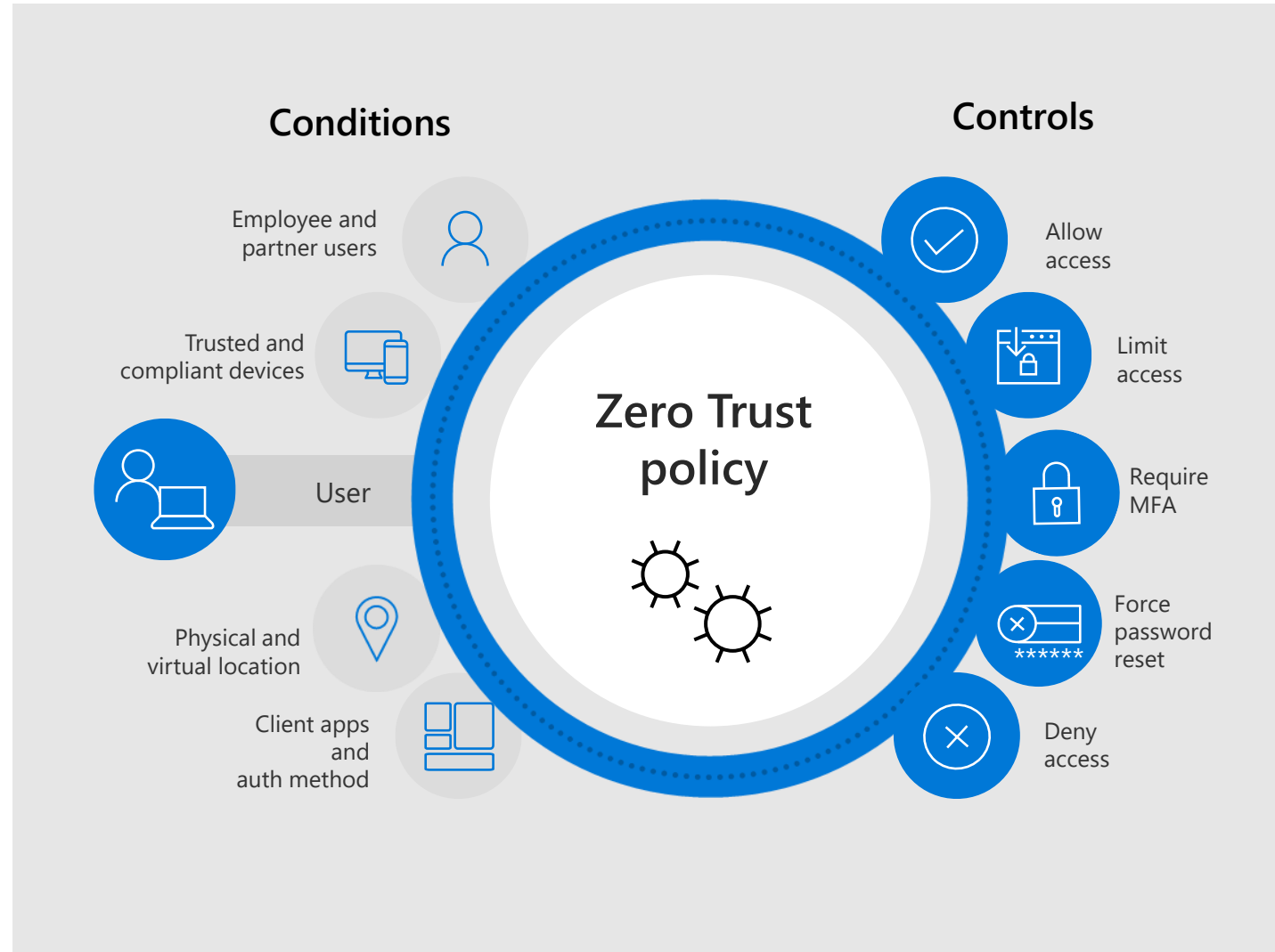
Control access with smart policies and risk assessments

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.



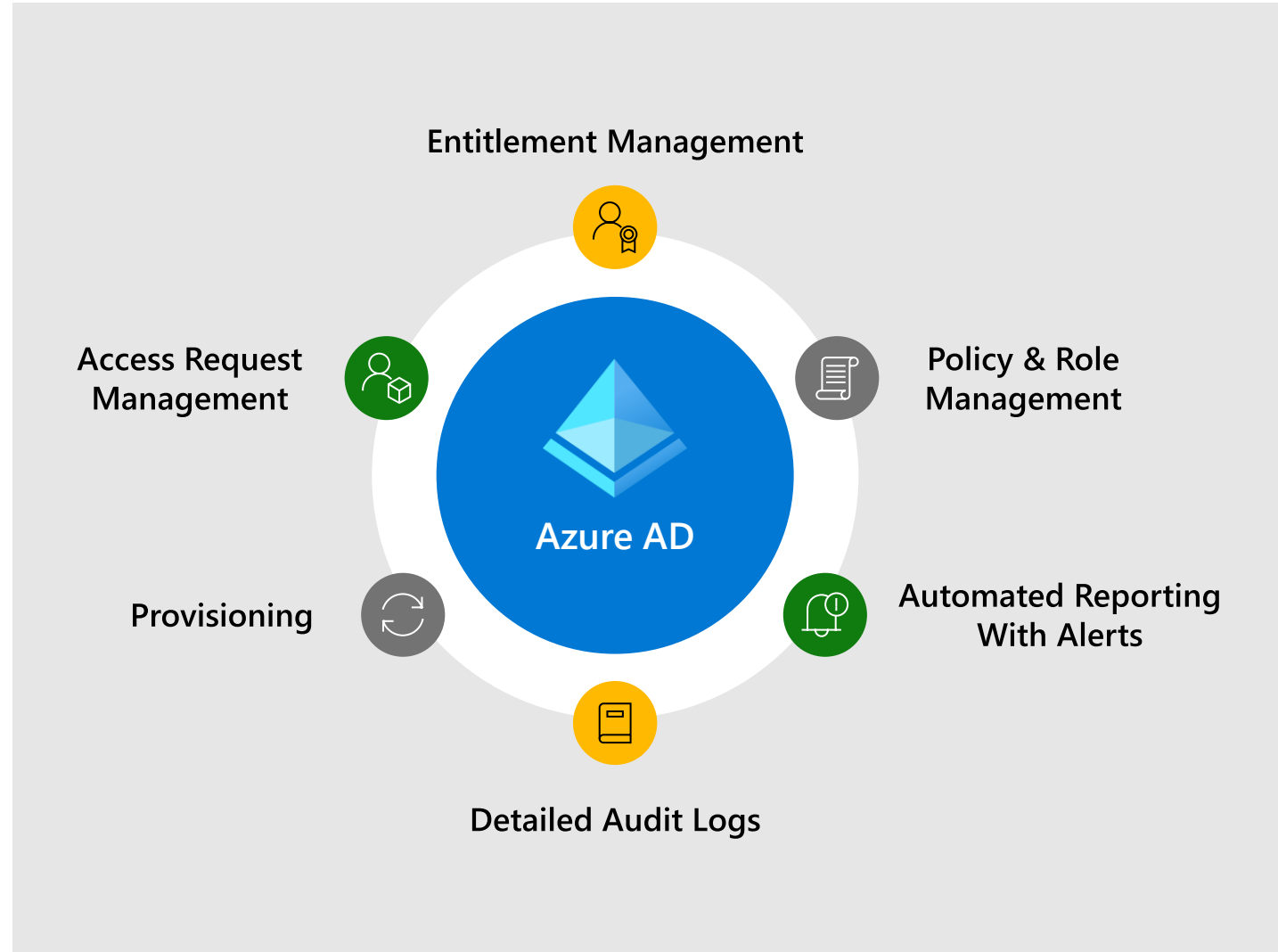
Safeguard resources with access lifecycle management

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



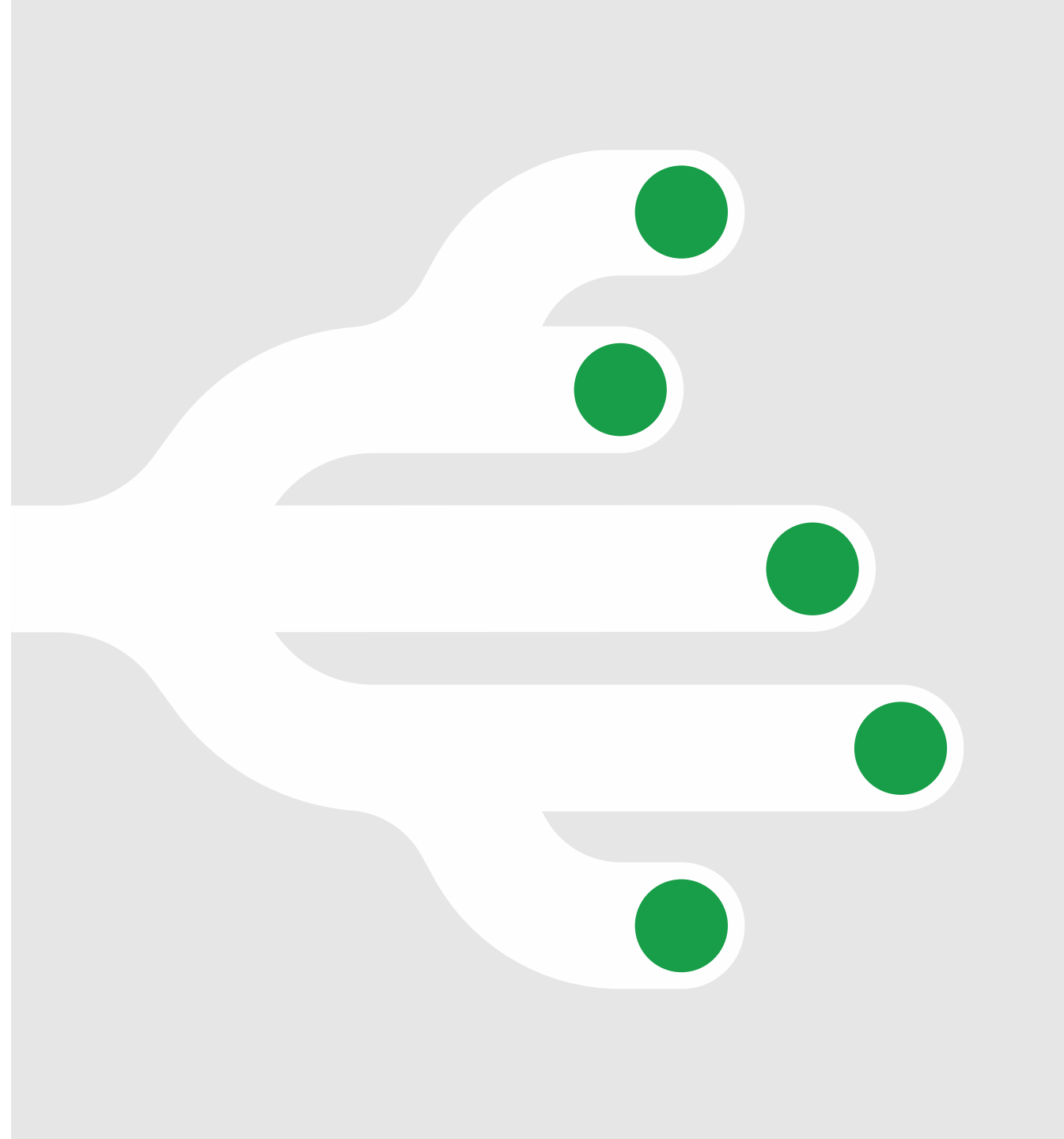
Secure the hybrid workforce



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**.



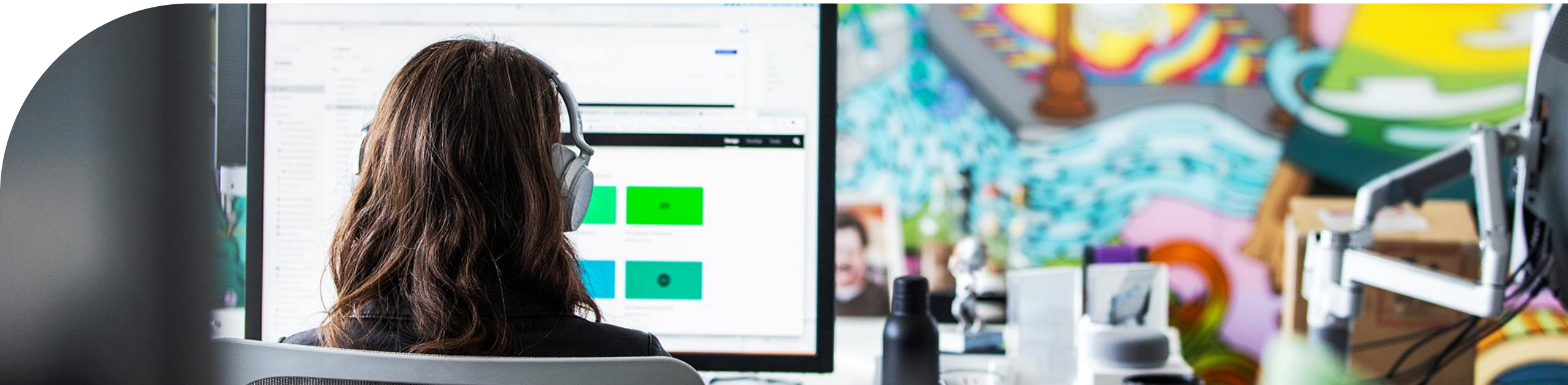
Connect your workforce to all apps with **single sign-on**.



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



Facilitate seamless **collaboration across organizational boundaries**.



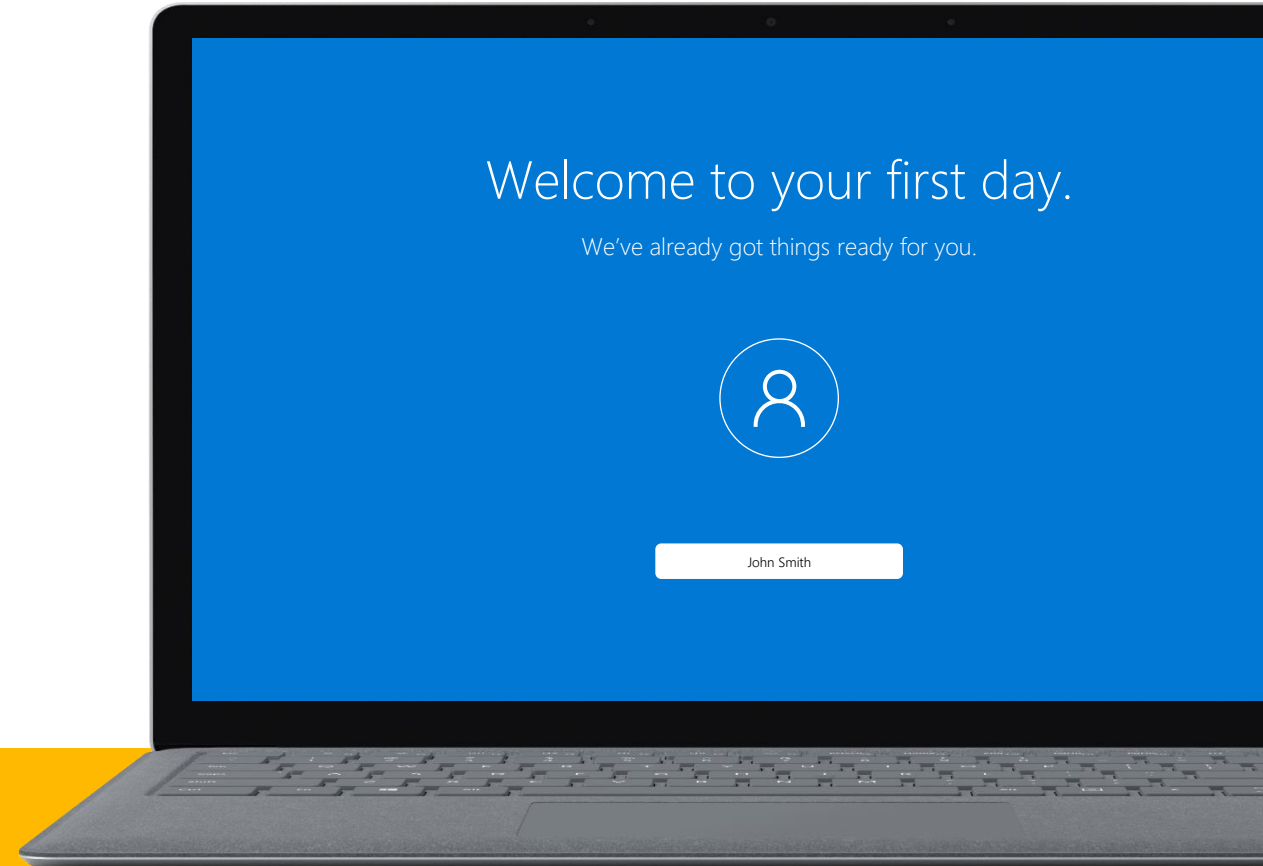
Provision access to resources efficiently

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.



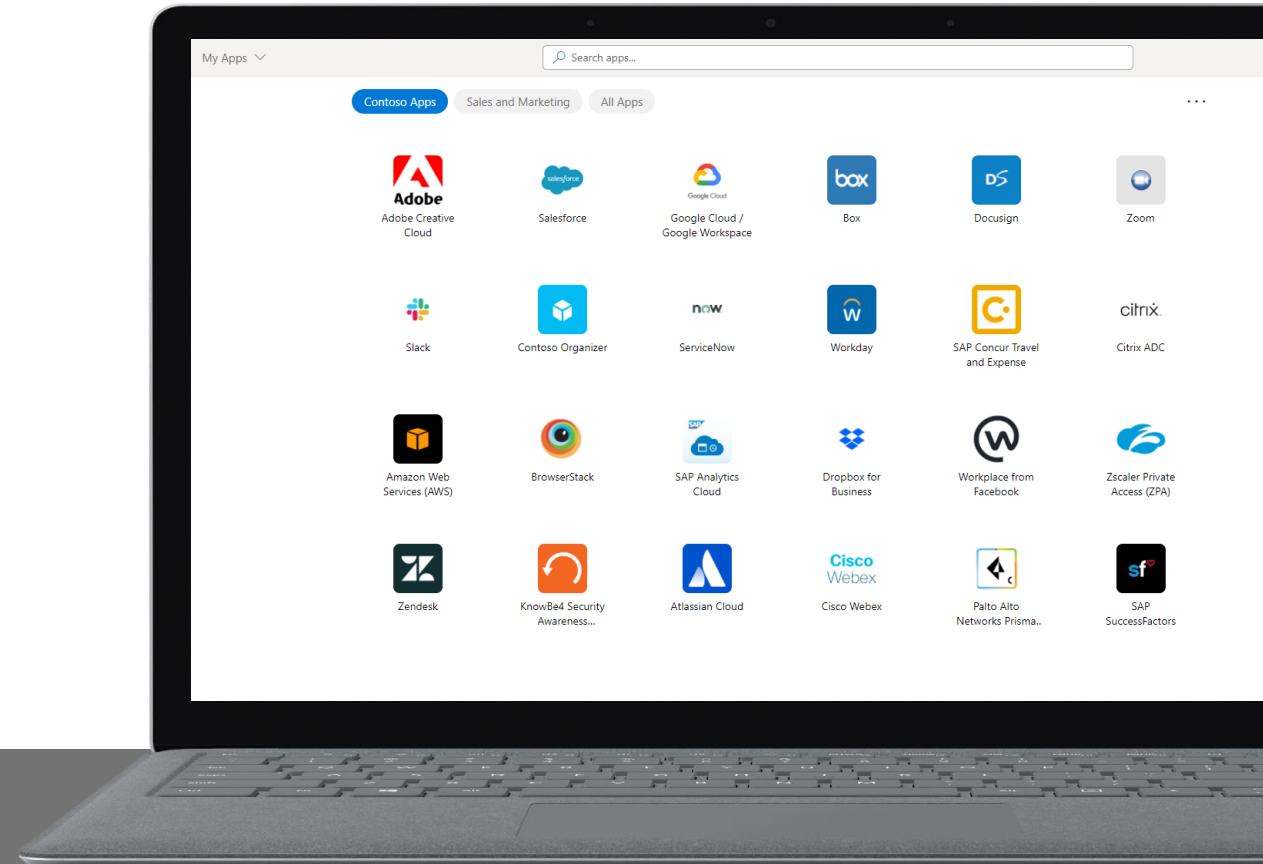
Enable seamless, secure access with single sign-on

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.



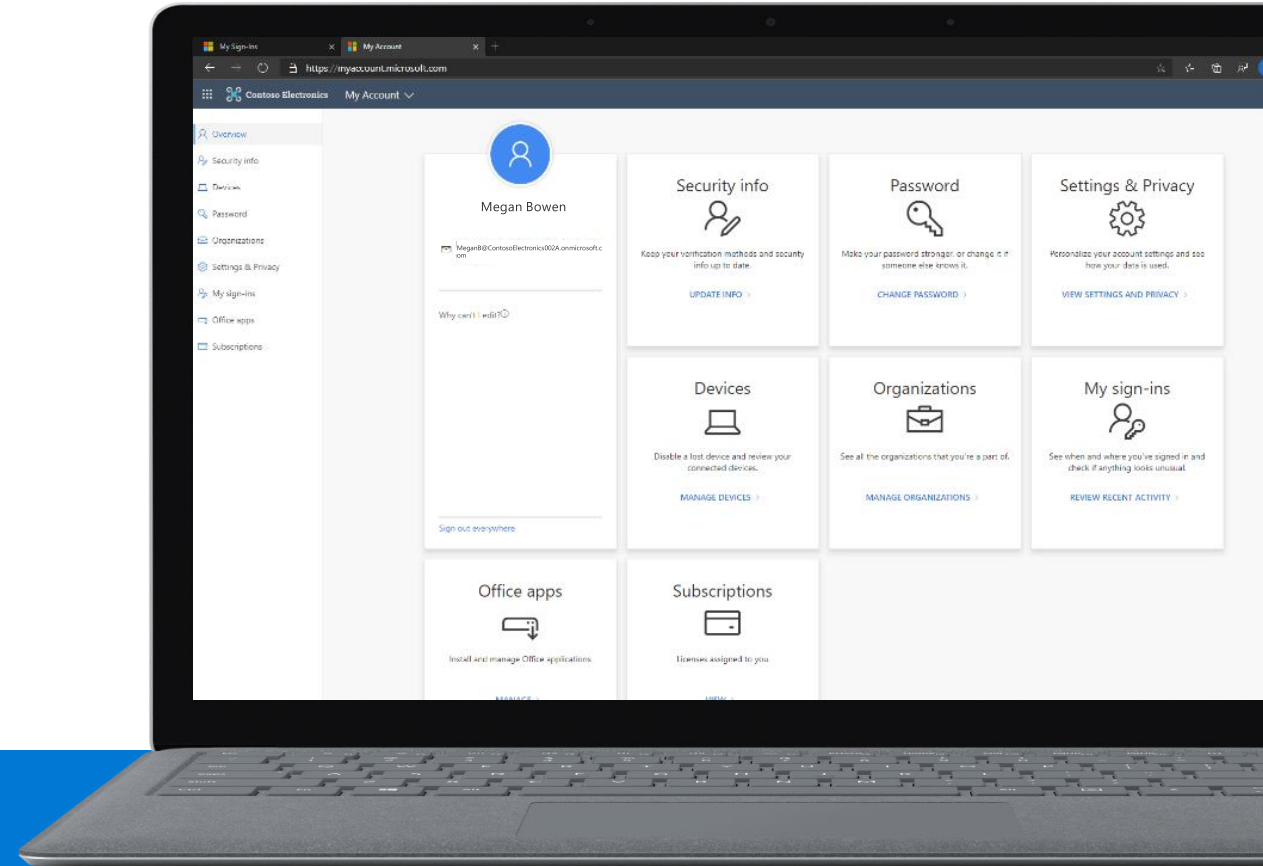
Empower employees to manage their own identity

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.

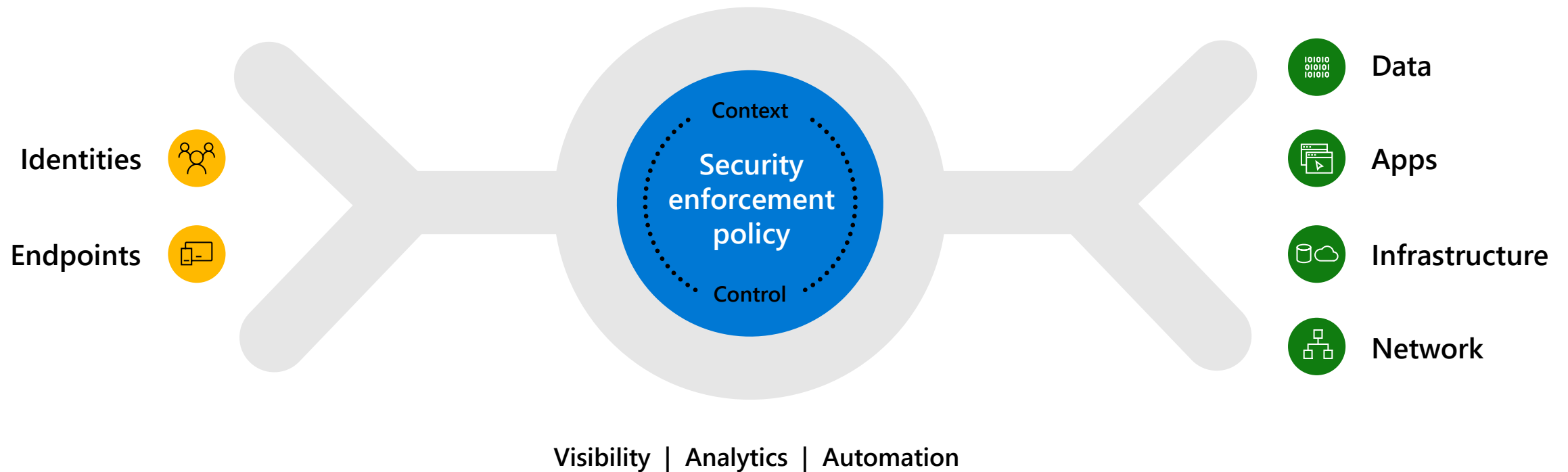
Manage security contact information and detect and report risk sign-in behavior.



Secure your organization with Zero Trust

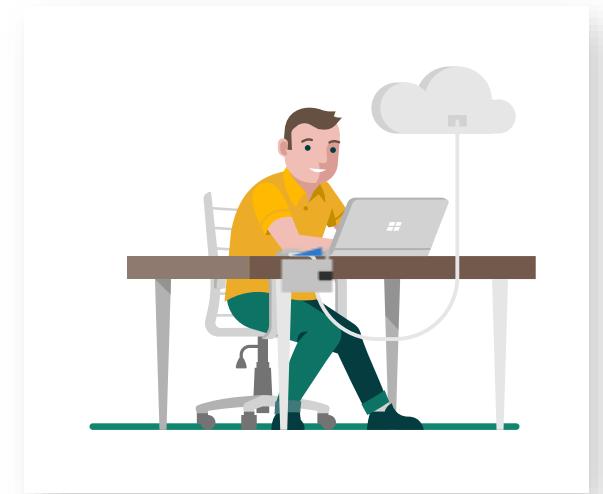
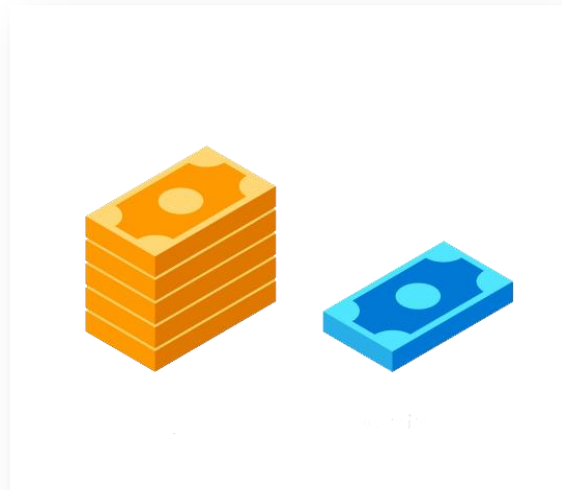
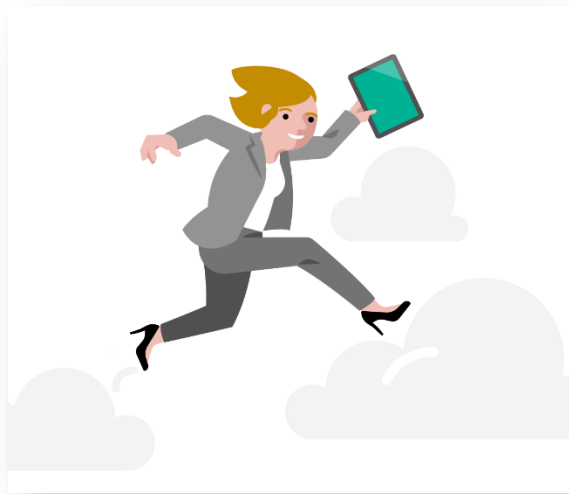
Increase security assurances for your critical business assets

Verify explicitly | Use least privilege access | Assume breach



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



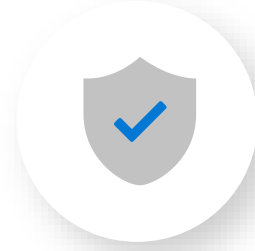
Collaborate in real time

- 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

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 accidentally saves to a personal share which is not secure.**

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

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

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

¹Source: 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](#).

Microsoft 365 Business Basic to Business Premium

Microsoft
Upsell Guide for Partners
Microsoft 365 Business Basic → Microsoft 365 Business Premium
If Partners and Sellers: Use this document to understand the sales journey for Microsoft 365 Business Premium and guide your upsell conversations with customers. Do not share this document directly with customers.

Microsoft 365 Business Premium is a comprehensive productivity and security solution for businesses with 1-300 employees. It includes everything Microsoft 365 Business Basic provides plus advanced security and device management to help you protect your company data across personal and company-owned devices.

Microsoft 365 Business Basic
Cloud Services
Desktop Apps
Advanced Security

Microsoft 365 Business Premium
Cloud Services
Desktop Apps
Advanced Security

HOW TO UPSELL: START WITH DISCOVERY QUESTIONS

1. Did you know that approximately 1/3 of all cyberattacks are targeted at small businesses? [Get the facts](#)
2. Have you had any recent security incidents like phishing or ransomware?
3. How do you protect against lost or stolen devices & passwords, especially for mobile/remote workers?
4. How do you help ensure confidential work and customer data is not accidentally leaked?
5. Do you have a process to secure data when an employee leaves your company?
6. How do you have a way to quickly identify attacks and mitigate risk and liability?
7. Do employees productivity and collaboration impacted due to the variety of applications being used?
8. Are your employees able to seamlessly work and collaborate from multiple devices?

FOLLOW THE SALES JOURNEY BELOW

| DISCOVER NEEDS | PITCH THE SOLUTION | HANDLE OBJECTIONS | MANAGE & DEPLOY |
|---|---|---|--|
| Use the Business Premium guide to ensure customer needs and find the right Microsoft 365 solution. Use the Security Score 365 to help customers understand security posture and risks. | Use these customer facing assets: • EOL Plan Docs • Microsoft Comparison • EOL Plan Docs • Microsoft Comparison • Microsoft Comparison • Microsoft Comparison • Microsoft Comparison • Microsoft Comparison | For objection handling use the Compare Microsoft 365 Business Basic to Business Premium document. Use the FAQ and FAQ to address customer concerns. Use the FAQ and FAQ to address customer concerns. | Review the Top 10 Microsoft 365 Business Premium Upgrade Checklist . Use the FAQ and FAQ to address customer concerns. Use the FAQ and FAQ to address customer concerns. |

For additional resources, go to [Microsoft 365 Business Premium Partner Playbook](#)

Microsoft
Upsell Guide for Partners
Microsoft 365 Business Basic → Microsoft 365 Business Premium
Microsoft 365 Business Premium Additional Capabilities

Secure Devices
Control which devices and users can access business information with [Intune Device Management](#). Apply security policies to protect data on any device. Keep company data within [approved apps](#) on mobile devices. Remove business data from lost or stolen devices with [Intune selective wipe](#).

Protect Business Data
Protect sensitive emails. Block sharing of sensitive information like credit card numbers with [Azure Information Protection](#). Restrict copying and saving of business information. Enable unlimited cloud archiving.

Enhanced Antivirus
Enforce malware protection across Windows 10 devices with [Windows Defender](#), now with management capabilities to give you visibility into active threats in your environment.

Defend against cyberthreats
Activate Microsoft Defender for Office 365 to guard against unsafe attachments, suspicious links, phishing and ransomware with [ATP Safe Links](#). Detect malware with sandbox analysis of email attachments with [ATP Safe Attachments](#). Enable [anti-phishing policies](#). Enable [advanced multi-factor authentication](#).

Enable secure remote access and protect identity
Enable employees to securely access business apps, wherever they work, help protect against lost or stolen passwords with advanced multi-factor authentication. Conditional Access helps provide the right access to the right people, while keeping hackers at bay.

Improve productivity and collaboration
Provide employees with enhanced Office features, helping them create content more easily, access and edit files more often, and gain access to PC-only applications such as Access and Publisher, all while maintaining a high level of security.

Streamline appointment scheduling and management
Help your staff stay on top of their schedules and avoid double bookings. An easy to navigate interface lets your customers find and book appointments around the clock.

Track and report mileage
Maintain an accurate record of your mileage with tracking and reporting in the palm of your hand. Active monitoring in the background as you drive and automatic classification of frequent drives on your behalf. Available US, UK, Canada.

Compare the [Microsoft 365 Business Plans](#) and understand the [upgrade process from Business Standard to Business Premium](#).

Microsoft
Upsell Guide for Partners
Microsoft 365 Business Basic → Microsoft 365 Business Premium
Customer Conversation talking points

1. Comprehensive and cost effective: A complete productivity and security solution, that's easy to manage and deploy and cost effective vs. point solutions.

2. Simple activation: No need to deploy additional products, just activate protection capabilities in the same way as other Office features.

3. Streamlined: Designed for Office apps and Windows, so it protects without hogging system resources or requiring special add-ons.

4. Top rated security vendor: Customer recently released [Magic Quadrant reports](#) across Endpoint Management, Access Management and more and Microsoft was a leader in these.

5. Top rated antivirus capabilities: Microsoft Defender ATP is now ranked as a top AV product by both such as AV Test, AV-comparators, SE labs are more.

6. Designed for a distributed environment: Microsoft 365 Business Premium provides a comprehensive solution for work from anywhere with real time collaboration, online meetings, secure remote access and advanced operational protection to let you run your business from anywhere while helping safeguard your business data.

Simplify your technology investment and help reduce cost

| Security, Identity and Device Mgmt | Microsoft 365 Business Premium |
|------------------------------------|--------------------------------|
| Security & Compliance | \$5 |
| Endpoint Protection | \$5 |
| Cloud App Security | \$5 |
| Customer Access MFA | \$5 |
| Business app protection | \$5 |
| Secure Management | \$5 |
| Collaboration and Productivity | \$20 |
| Productivity app for the office | \$20 |
| Cloud Services | \$20 |

Microsoft 365 Business Premium integrated productivity, collaboration and security solution.

Upsell Guides for Partners

<https://aka.ms/M365BPPlaybook>

Microsoft 365 Business Standard to Business Premium

Microsoft
Upsell Guide for Partners
Microsoft 365 Business Standard → Microsoft 365 Business Premium
If Partners and Sellers: Use this document to understand the sales journey for Microsoft 365 Business Premium and guide your upsell conversations with customers. Do not share this document directly with customers.

Microsoft 365 Business Premium is a comprehensive productivity and security solution for businesses with 1-300 employees. It includes everything that Business Standard offers plus advanced security and device management to help you protect your company data across personal and company-owned devices.

Microsoft 365 Business Standard
Cloud Services
Desktop Apps
Advanced Security

Microsoft 365 Business Premium
Cloud Services
Desktop Apps
Advanced Security

HOW TO UPSELL: START WITH DISCOVERY QUESTIONS

1. Did you know that approximately 1/3 of all cyberattacks are targeted at small businesses? [Get the facts](#)
2. Have you had any recent security incidents like phishing or ransomware?
3. How do you protect against lost or stolen devices & passwords, especially for mobile/remote workers?
4. How do you help ensure confidential work and customer data is not accidentally leaked?
5. Do you have a process to secure data when an employee leaves your company?
6. How do you have a way to quickly identify attacks and mitigate risk and liability?

FOLLOW THE SALES JOURNEY BELOW

| DISCOVER NEEDS | PITCH THE SOLUTION | HANDLE OBJECTIONS | MANAGE & DEPLOY |
|---|---|--|--|
| Use the Business Premium guide to ensure customer needs and find the right Microsoft 365 solution. Use the Security Score 365 to help customers understand security posture and risks. | Use these customer facing assets: • EOL Plan Docs • Microsoft Comparison • EOL Plan Docs • Microsoft Comparison • Microsoft Comparison • Microsoft Comparison • Microsoft Comparison | For objection handling use the Compare Microsoft 365 Business Standard to Business Premium document. Use the FAQ and FAQ to address customer concerns. Use the FAQ and FAQ to address customer concerns. | Review the Top 10 Microsoft 365 Business Premium Upgrade Checklist . Use the FAQ and FAQ to address customer concerns. Use the FAQ and FAQ to address customer concerns. |

For additional resources, go to [Microsoft 365 Business Premium Partner Playbook](#)

Microsoft
Upsell Guide for Partners
Microsoft 365 Business Standard → Microsoft 365 Business Premium
Microsoft 365 Business Premium Advanced Security Capabilities

Secure Devices
Control which devices and users can access business information with [Intune Device Management](#). Apply security policies to protect data on any device. Keep company data within [approved apps](#) on mobile devices. Remove business data from lost or stolen devices with [Intune selective wipe](#).

Protect Business Data
Protect sensitive emails. Block sharing of sensitive information like credit card numbers with [Azure Information Protection](#). Restrict copying and saving of business information. Enable unlimited cloud archiving.

Enhanced Antivirus
Enforce malware protection across Windows 10 devices with [Windows Defender](#), now with management capabilities to give you visibility into active threats in your environment.

Defend against cyberthreats
Activate Microsoft Defender for Office 365 to guard against unsafe attachments, suspicious links, phishing and ransomware with [ATP Safe Links](#). Detect malware with sandbox analysis of email attachments with [ATP Safe Attachments](#). Enable [anti-phishing policies](#). Enable [advanced multi-factor authentication](#).

Enable secure remote access and protect identity
Enable employees to securely access business apps, wherever they work, help protect against lost or stolen passwords with advanced multi-factor authentication. Conditional Access helps provide the right access to the right people, while keeping hackers at bay.

Compare the [Microsoft 365 Business Plans](#) and understand the [upgrade process from Business Standard to Business Premium](#).

Microsoft
Upsell Guide for Partners
Microsoft 365 Business Standard → Microsoft 365 Business Premium
Customer Conversation talking points

1. Comprehensive and cost effective: A complete productivity and security solution, that's easy to manage and deploy and cost effective vs. point solutions.

2. Simple activation: No need to deploy additional products, just activate protection capabilities in the same way as other Office features.

3. Streamlined: Designed for Office apps and Windows, so it protects without hogging system resources or requiring special add-ons.

4. Top rated security vendor: Customer recently released [Magic Quadrant reports](#) across Endpoint Management, Access Management and more and Microsoft was a leader in these.

5. Top rated antivirus capabilities: Microsoft Defender ATP is now ranked as a top AV product by both such as AV Test, AV-comparators, SE labs are more.

6. Designed for a distributed environment: Microsoft 365 Business Premium provides a comprehensive solution for work from anywhere with real time collaboration, online meetings, secure remote access and advanced operational protection to let you run your business from anywhere while helping safeguard your business data.

Simplify your technology investment and help reduce cost

| Security, Identity and Device Mgmt | Microsoft 365 Business Premium |
|------------------------------------|--------------------------------|
| Security & Compliance | \$5 |
| Endpoint Protection | \$5 |
| Cloud App Security | \$5 |
| Customer Access MFA | \$5 |
| Business app protection | \$5 |
| Secure Management | \$5 |
| Collaboration and Productivity | \$20 |
| Productivity app for the office | \$20 |
| Cloud Services | \$20 |

Microsoft 365 Business Premium integrated productivity, collaboration and security solution.

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

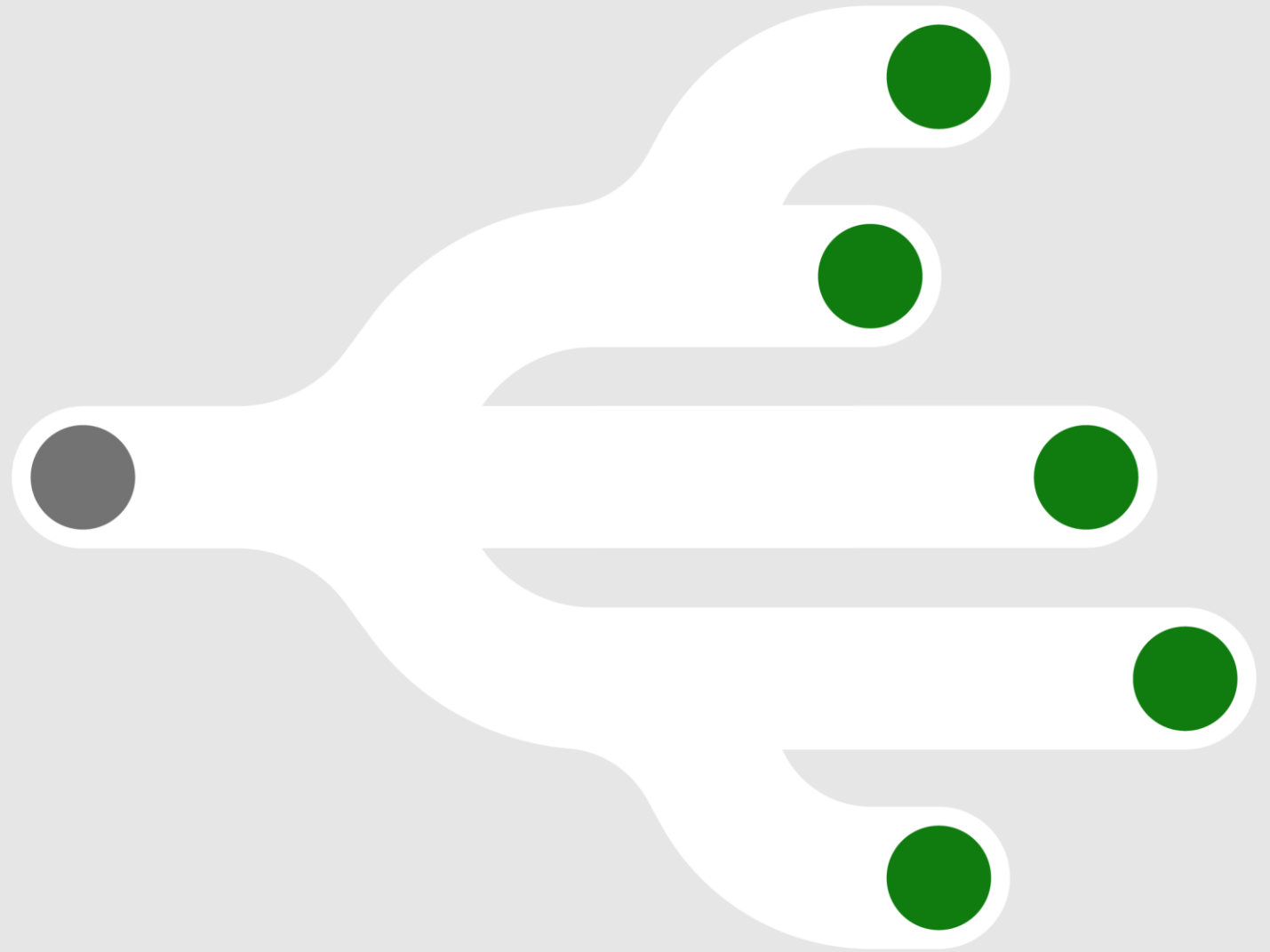


[Glenn Habes | LinkedIn](#)



[Jeroen Jansen | LinkedIn](#)

Q&A



Thank you

