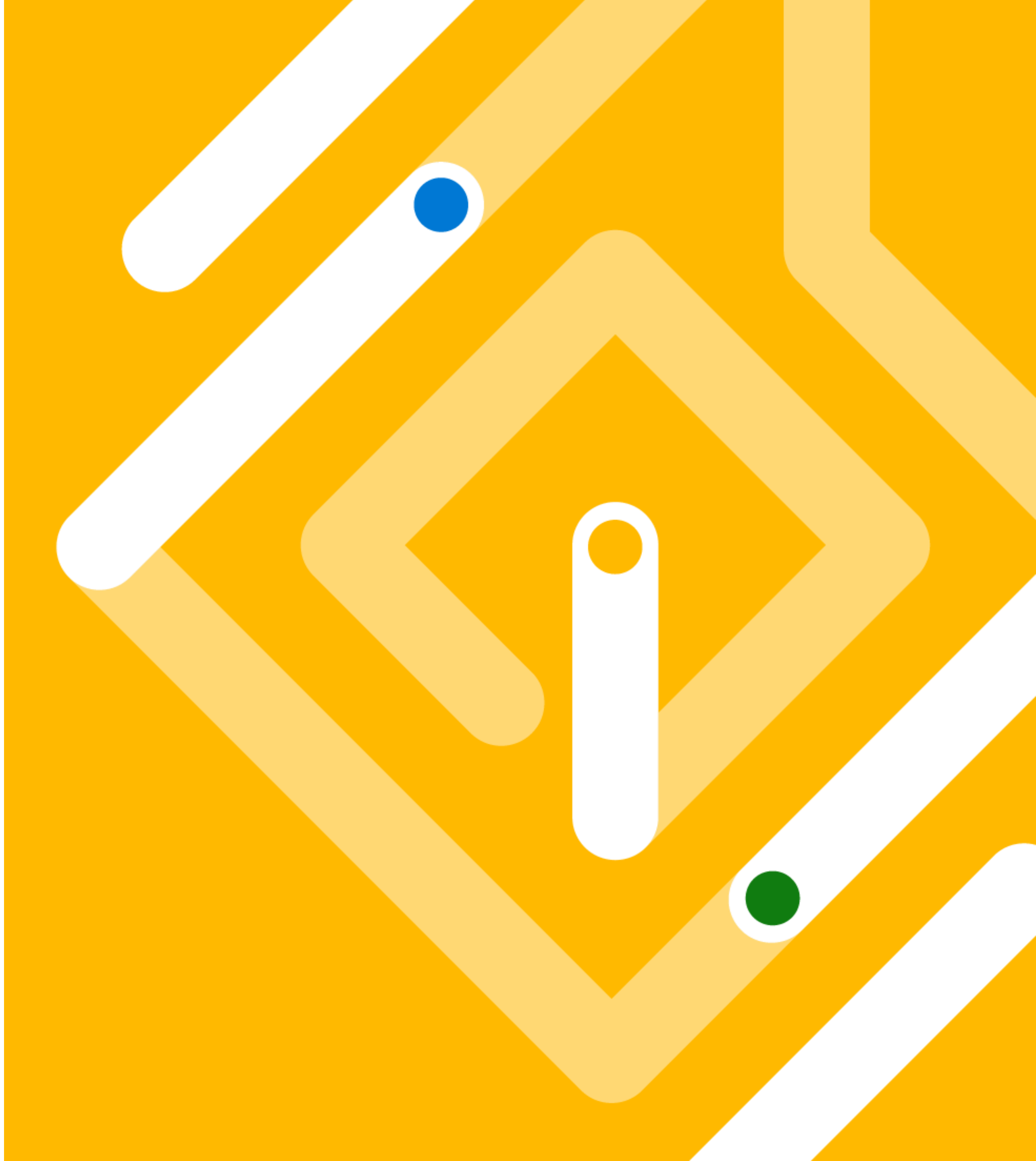
Microsoft Security

acloud

Zero Trust Identity

Azure Active Directory

Current landscape



Identity challenges for today’s organizations

Explosion of apps, on and off the corporate network, **needing secure access**

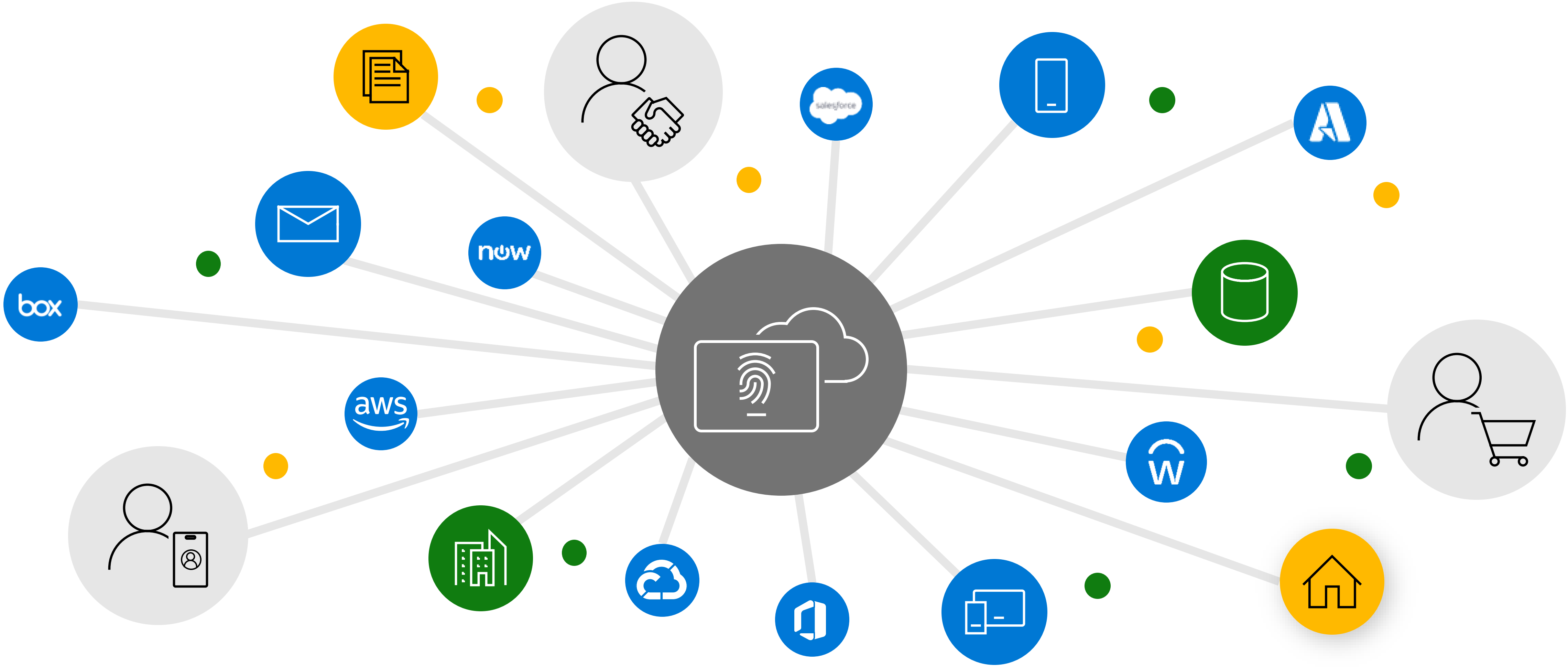
Adapt to the new hybrid work requiring seamless, flexible experiences

Evolving compliance regulations with data privacy and security implications

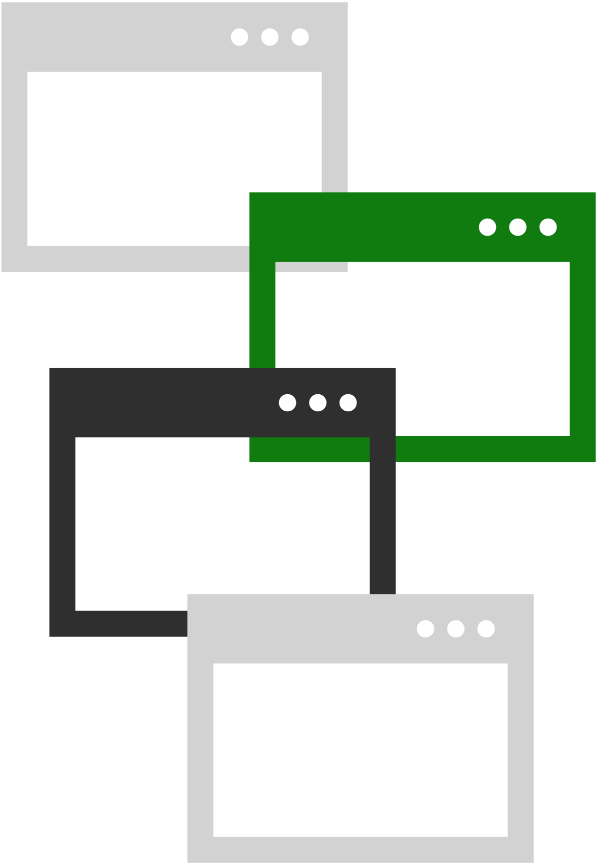
Demands for increased productivity, security, and IT modernization

Identity is the control plane

Secure access for a connected world

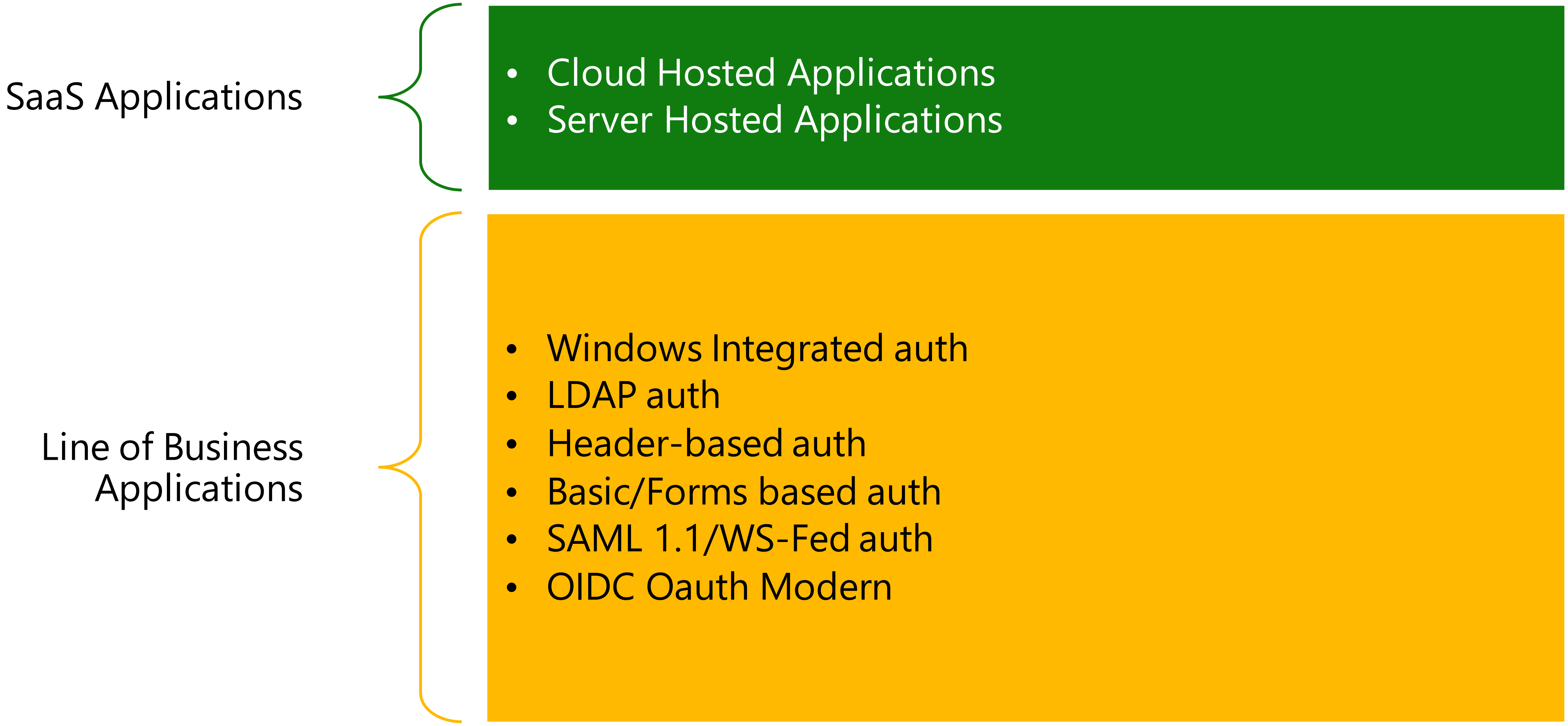


Your app story today



- Traffic may not traverse corp network
- Data may reside off premises
- Legacy identity stores
- Insecure network traffic
- Outdated infrastructure

How we see applications



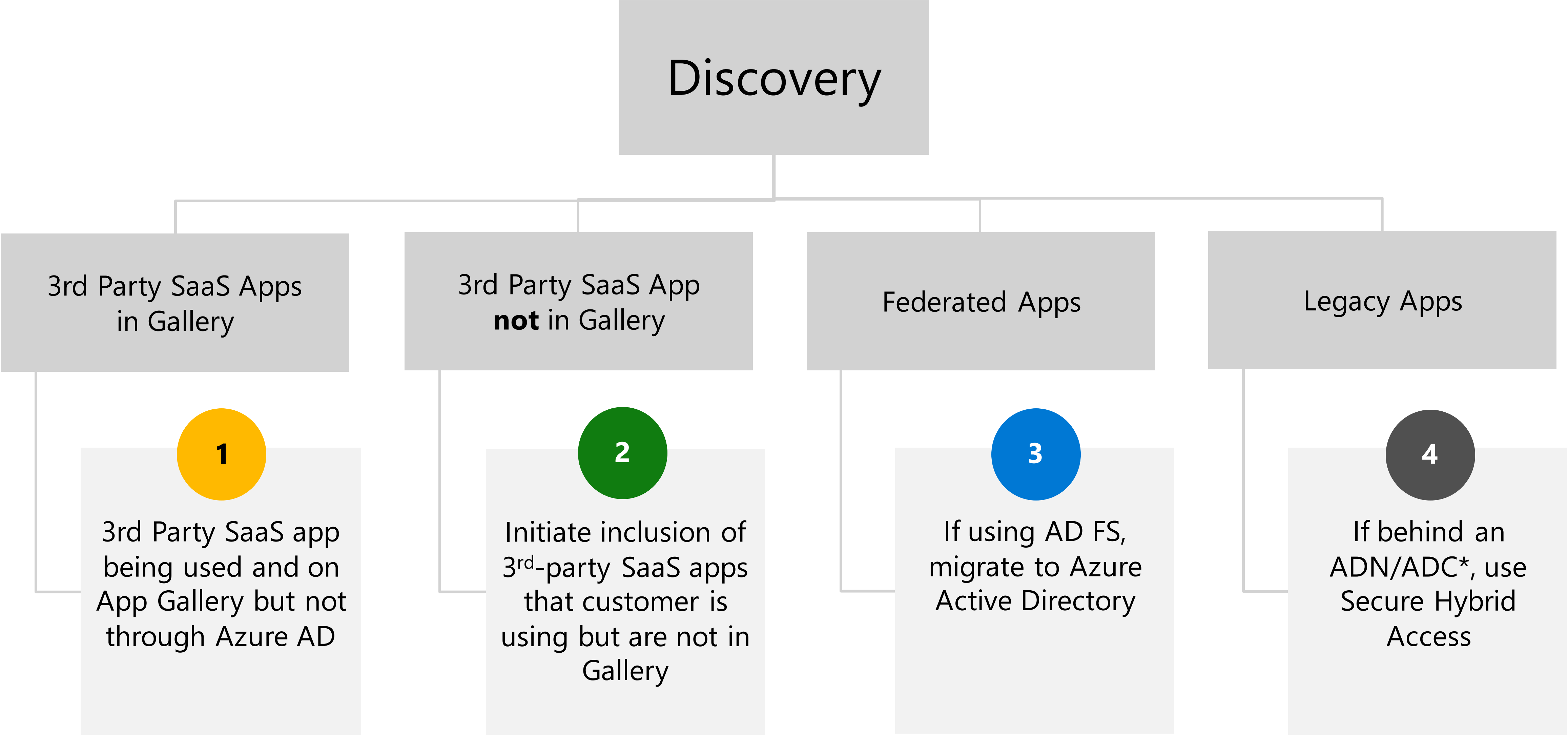
SaaS Applications

- Cloud Hosted Applications
- Server Hosted Applications

Line of Business Applications

- Windows Integrated auth
- LDAP auth
- Header-based auth
- Basic/Forms based auth
- SAML 1.1/WS-Fed auth
- OIDC Oauth Modern

Application prioritization



Discovery

3rd Party SaaS Apps in Gallery

3rd Party SaaS App **not** in Gallery

Federated Apps

Legacy Apps

1 3rd Party SaaS app being used and on App Gallery but not through Azure AD

2 Initiate inclusion of 3rd-party SaaS apps that customer is using but are not in Gallery

3 If using AD FS, migrate to Azure Active Directory

4 If behind an ADN/ADC*, use Secure Hybrid Access

* Application Delivery Network/Application Delivery Controller

Example

Application Classification and Prioritization

Application Name	Categorization Priority	Location and Application Type	Current IDP	Plan to decommission / Modernize?
Example Application	High	On-premises, 3rd party developed	Active Directory	

Identities

Zero Trust Objective

Protect identities against compromise and secure access to resources

Verify and secure every identity with strong authentication

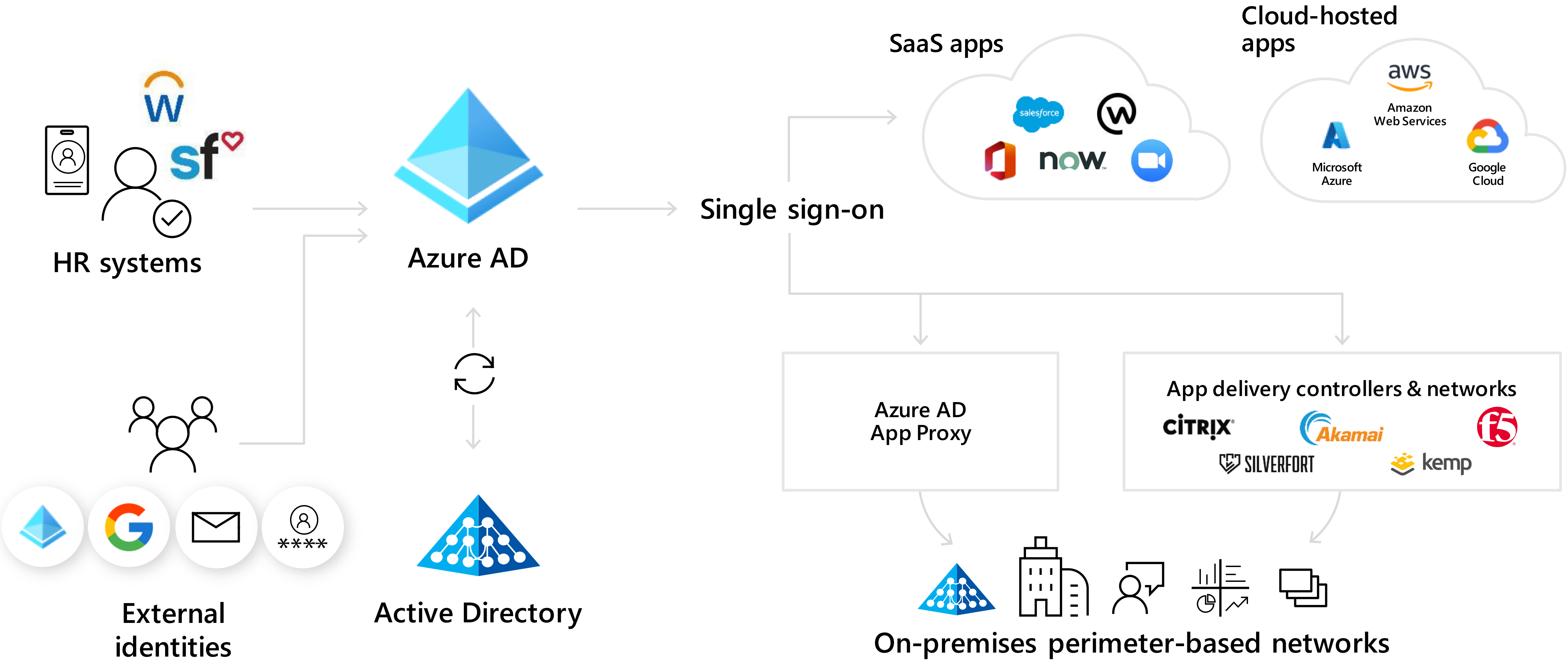
Secure access to all applications with single sign-on

Verify identities with Multi-factor authentication (MFA)

Control access with smart policies and risk assessments

Enforce least privileged access with strong governance

Secure access to all applications with single sign on



HR systems

External identities

Azure AD

Active Directory

Single sign-on

SaaS apps

Cloud-hosted apps

Amazon Web Services

Microsoft Azure

Google Cloud

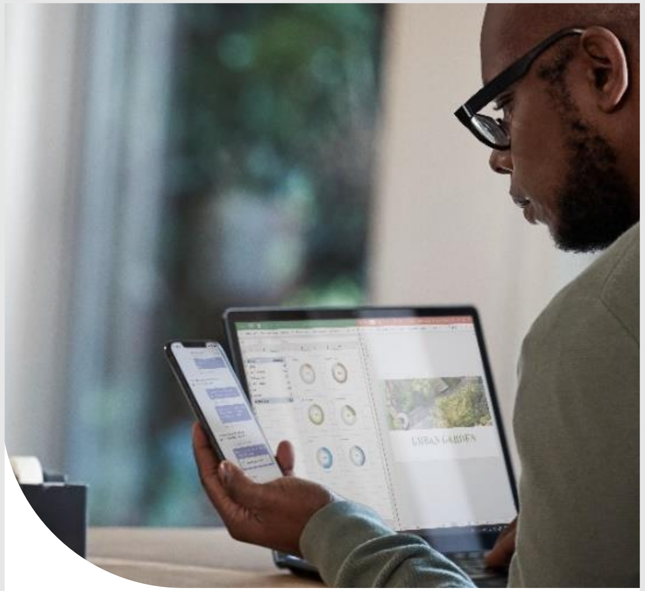
Azure AD App Proxy

App delivery controllers & networks

On-premises perimeter-based networks

Multi-factor authentication

Verify user identities with strong authentication



We support a **broad range of multi-factor authentication options**

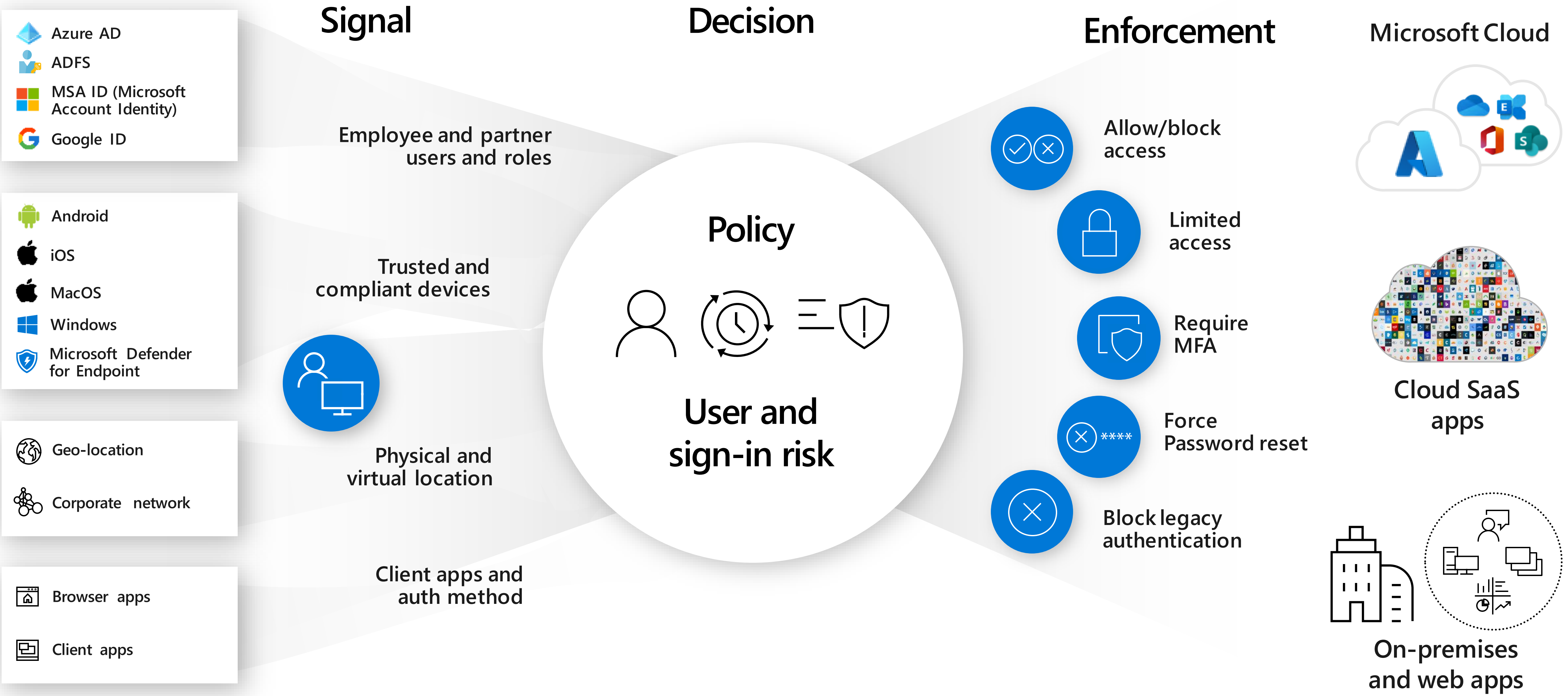
Including passwordless technology

- Microsoft Authenticator
- Windows Hello
- FIDO2 Security key
- Biometrics

- Push Notification
- Soft Tokens OTP
- Hard Tokens OTP
- SMS, Voice

Multi-factor authentication **prevents 99.9% of identity attacks**

Control access with smart policies and risk assessments



Signal

Decision

Enforcement

Microsoft Cloud

Azure AD

ADFS

MSA ID (Microsoft Account Identity)

Google ID

Employee and partner users and roles

Android

iOS

MacOS

Windows

Microsoft Defender for Endpoint

Trusted and compliant devices

Geo-location

Corporate network

Physical and virtual location

Browser apps

Client apps

Client apps and auth method

Policy

User and sign-in risk

Allow/block access

Limited access

Require MFA

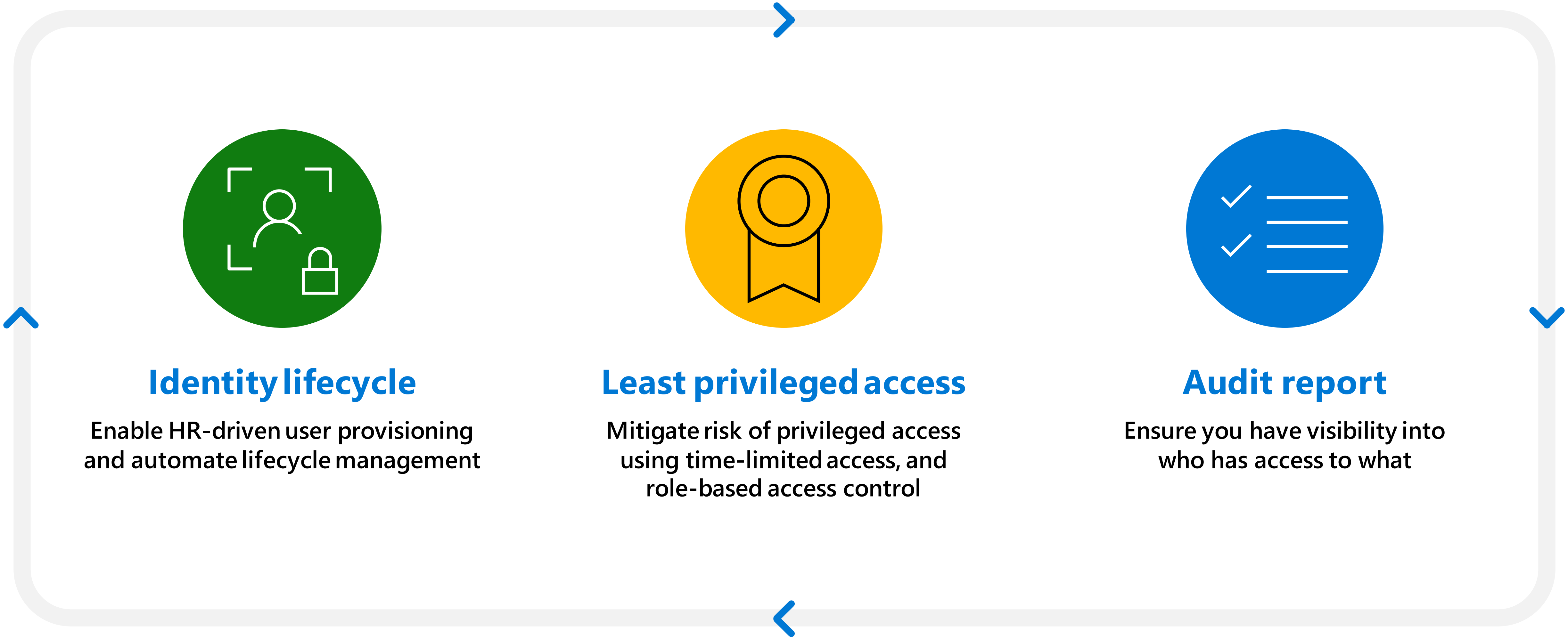
Force Password reset

Block legacy authentication

Cloud SaaS apps

On-premises and web apps

Enforce least privileged access with strong governance



Identity lifecycle

Enable HR-driven user provisioning and automate lifecycle management

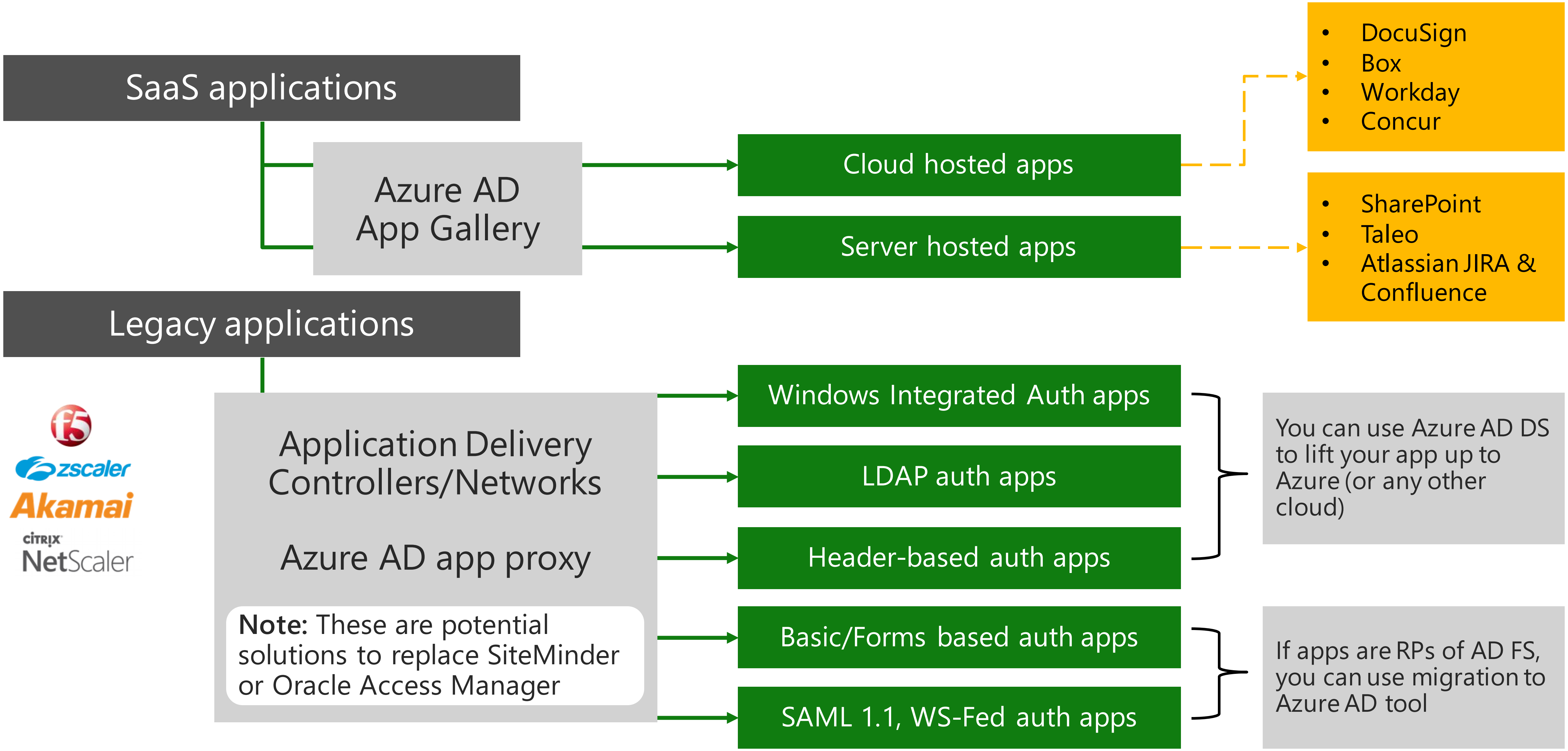
Least privileged access

Mitigate risk of privileged access using time-limited access, and role-based access control

Audit report

Ensure you have visibility into who has access to what

Azure AD App Auth integration overview



SaaS applications

Azure AD App Gallery

Cloud hosted apps

- DocuSign
- Box
- Workday
- Concur

Server hosted apps

- SharePoint
- Taleo
- Atlassian JIRA & Confluence

Legacy applications

f5

zscaler

Akamai

CiTRiX NetScaler

Application Delivery Controllers/Networks

Azure AD app proxy

Note: These are potential solutions to replace SiteMinder or Oracle Access Manager

Windows Integrated Auth apps

LDAP auth apps

Header-based auth apps

You can use Azure AD DS to lift your app up to Azure (or any other cloud)

Basic/Forms based auth apps

SAML 1.1, WS-Fed auth apps

If apps are RPs of AD FS, you can use migration to Azure AD tool

Integrate private apps with Secure Hybrid Access Partners

- Leverage your existing application delivery controllers and networks, VPNs or software defined perimeters
- Support for broad range of legacy protocols:

  Kerberos

  Header-based Auth

  NTLM

  LDAP

  RDP

  Radius

  SSH

  non-HTTP

New partners

Silverfort

Datawiza

Perimeter 81

Strata

App Delivery Controllers and Networking providers

citrix

f5

kemp

Akamai

VPNs and Software Define Perimeter partners

paloalto NETWORKS

CISCO

zscaler

FORTINET

Pulse Secure

SILVERFORT

datawiza

perimeter 81

STRATA

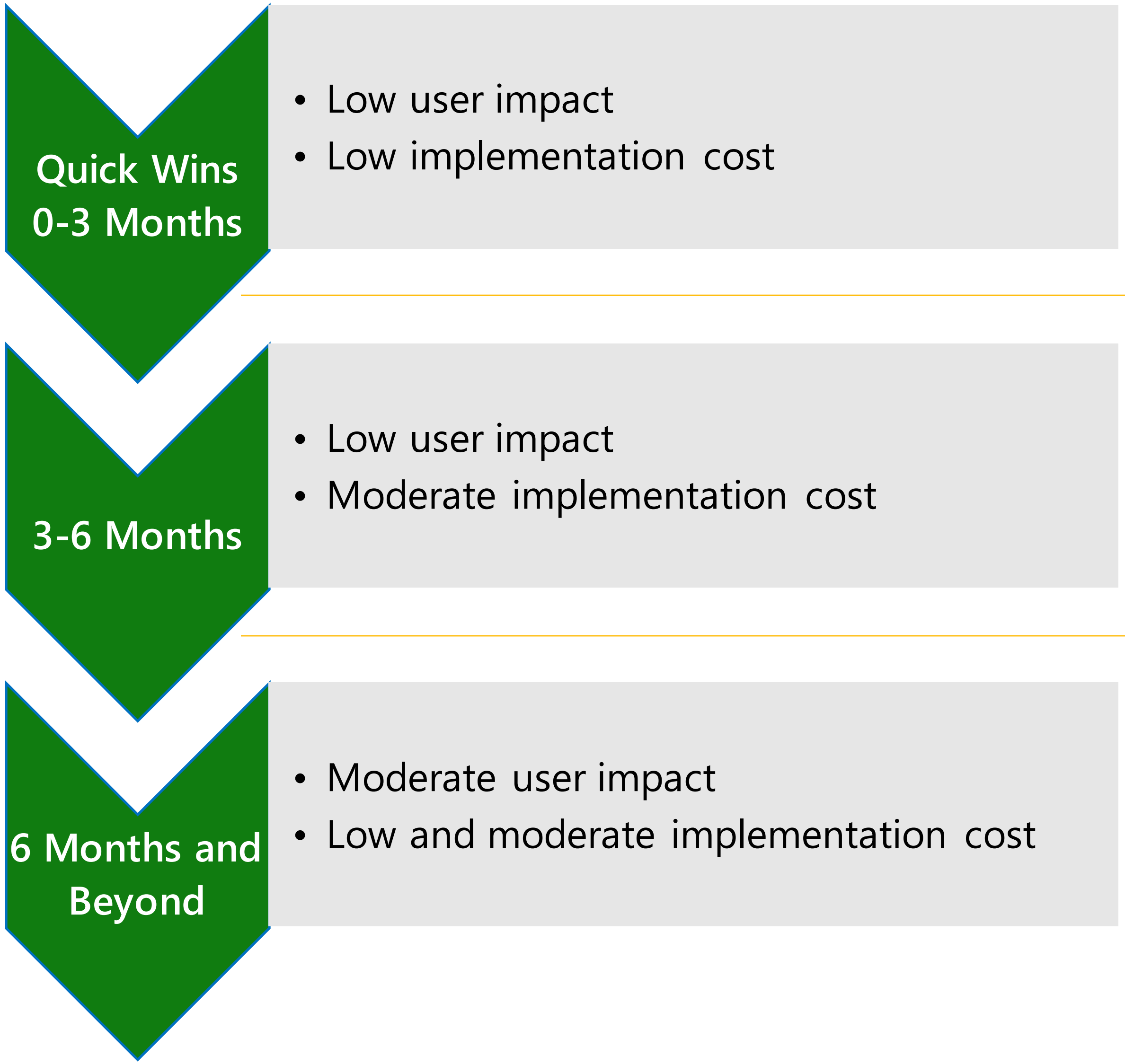
Example

Application Classification and Prioritization Plan

Application Name	Categorization Priority	Location and Application Type	Current IDP	Target IDP	Migration Path
Example Application	High	On-premises, 3rd party developed	Active Directory	Azure AD	Azure AD App Proxy

Example

Recommended Strategy



Quick Wins 0-3 Months

- Low user impact
- Low implementation cost

3-6 Months

- Low user impact
- Moderate implementation cost

6 Months and Beyond

- Moderate user impact
- Low and moderate implementation cost

Quick Wins 0-3 months

Enable MFA for all global admins

Ensure all users can complete multi-factor authentication for secure access

Enable policy to block legacy authentication

Turn on sign-in risk policy

3-6 Months

Enable self-service password reset

6 Months and Beyond

Enable MFA for all users

Do not expire passwords

Stop clear text credentials exposure

Use limited administrative roles

Example

High-level Deployment Plan

1. Work out a draft concept of MFA that you want to deploy in your organization.
2. Use the "Design Decision Points" spreadsheet to define MFA requirements and settings:
   a. Choose way to enable MFA
   b. Choose users and cloud applications that will need MFA
   c. Choose allowed second authenticator factors
   d. Determine other MFA configuration factors
   e. Decide if you need other types of controls (such as Terms of Use or custom)
3. Choose small set of test users.

   NOTE: if necessary, a choose different sets of test users for different conditional access policies
4. If hardware security keys are to be used, obtain and distribute them to test users.
5. Enable MFA to the test set of users and allow enough time to verify that it works as expected.
6. Use feedback from test users to modify you MFA deployment plan, if necessary.
7. Run awareness campaign that MFA will be coming to your organization.
8. If hardware security keys are to be used, obtain and distribute them to remaining users.
9. Enable MFA to users and cloud applications in scope.
10. Monitor, troubleshoot and adjust your MFA deployment.

Azure AD—the world's largest cloud identity service

Thousands of organizations, millions of active users, billions of daily requests

300K+

Azure AD
Premium organizations

425M+

Azure AD
Monthly active users

30B+

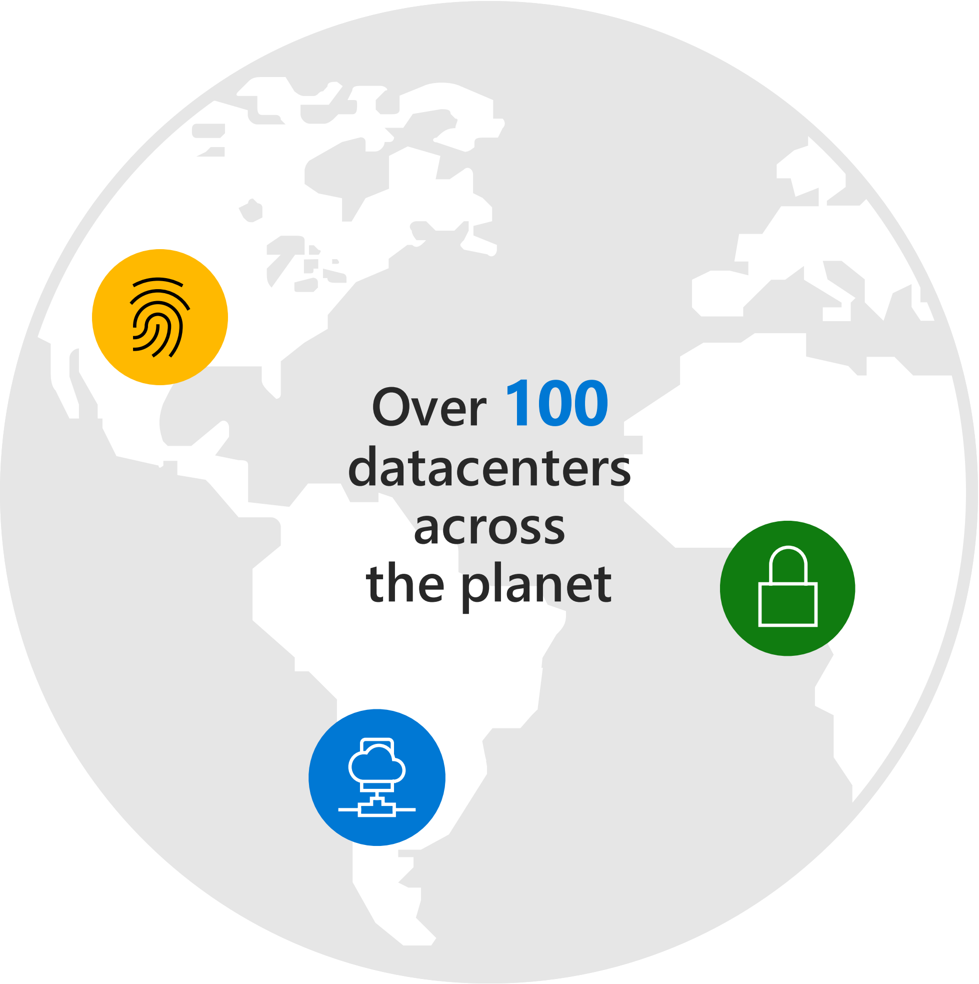
Azure AD
Daily authentication requests

Engineered for availability and security

Cloud-native, hyper-scale, multi-tenant architecture

Each **physical datacenter** protected with world-class, multi-layered protection, and engineered for maximum availability

Global cloud infrastructure with secure hardware and data segregation



Over **100** datacenters across the planet

99.99%

New Azure AD Service Level Agreement

(in effect from April 1st, 2021)

Secured with cutting-edge **operational security**

→ Restricted access

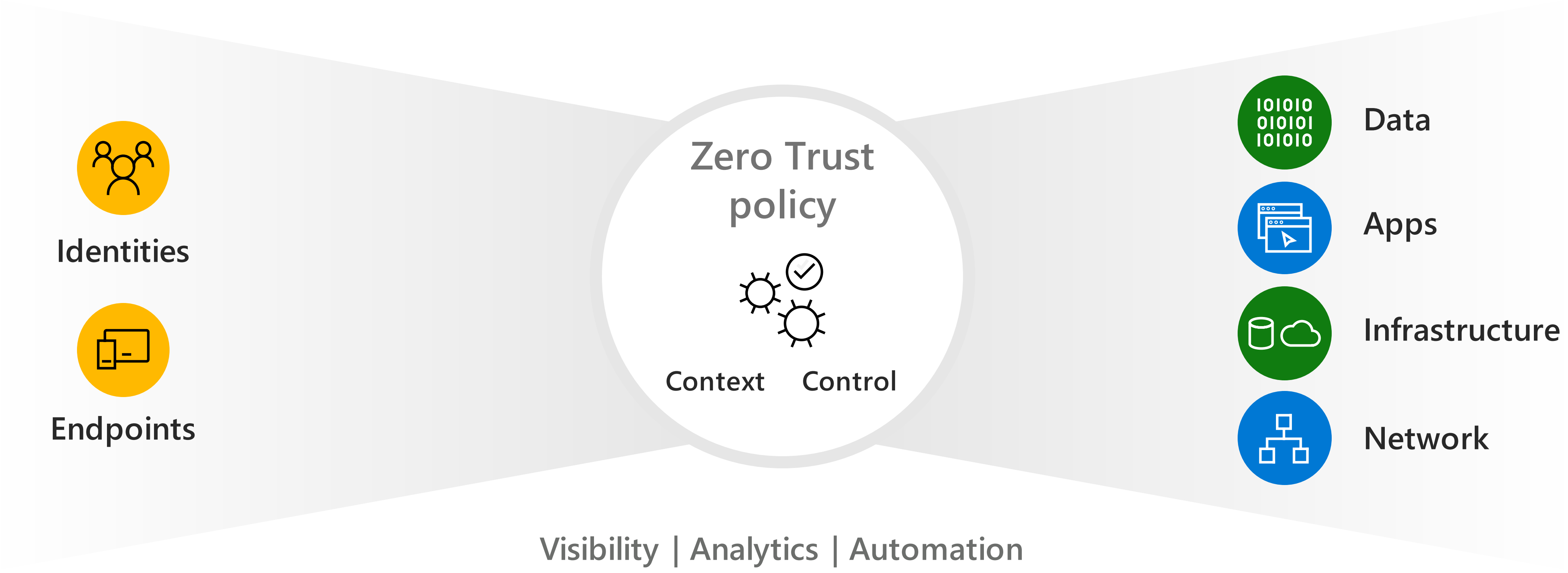
→ 24x7 monitoring

→ Global security experts

Secure your organization with Zero Trust

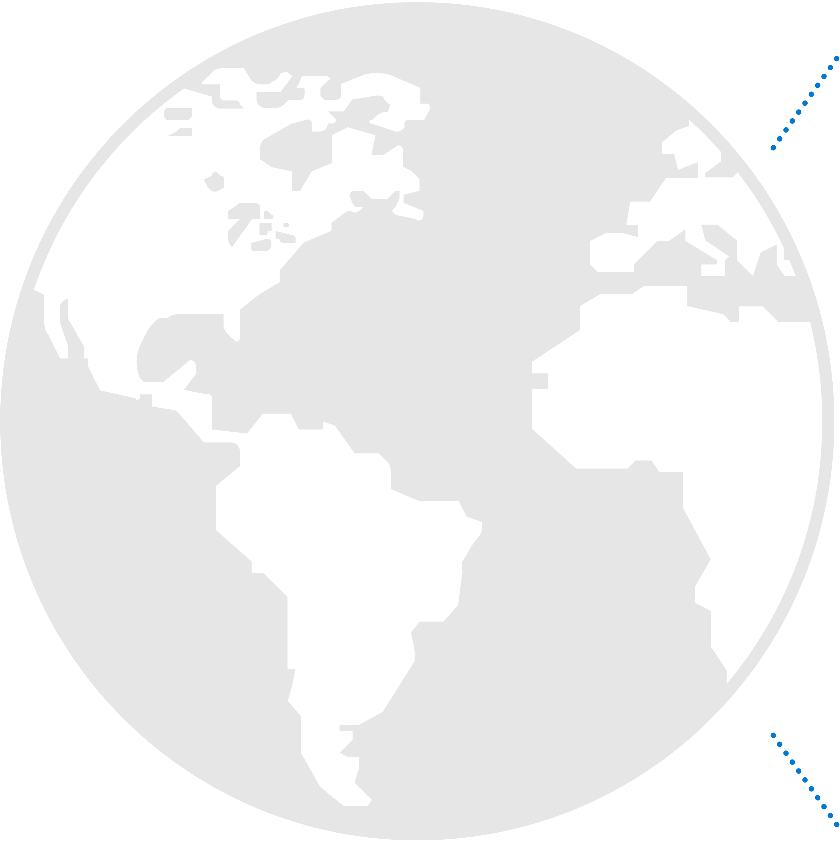
A modern security framework with identity as its foundation

Verify explicitly | Use least-privileged access | Assume breach



Visibility | Analytics | Automation

Open and interoperable ecosystem



✓ Single sign-on

OAUTH 2

SAML v2.0

OpenID Connect

✓ Provisioning

SCIM

✓ Passwordless

fido ALLIANCE

WebAuthn

✓ Decentralized identity

DIF

W3C®

fido CERTIFIED FIDO2

Open and interoperable ecosystem

Passwordless Authentication

ensurity yubico THALES

HID FEITIAN WE BUILD SECURITY OneSpan

AUTHENTREND TRUSTKEY SOLUTIONS

nymi

Human Capital Management

workday. Aquera

successfactors™ An SAP Company

Pre-integrated SSO and user provisioning

zendesk cisco Webex

Adobe now

ATLASSIAN SAP

Identity Governance

SAVIYNT Omada

N8IDENTITY SailPoint

imprivata

Secure Hybrid Access

Akamai CITRIX

f5 kemp

SILVERFORT

Identity Verification

LexisNexis RISK SOLUTIONS onfido

IDEMIA jumio.

Socure VU

Customer success stories across every industry

Financial Services and insurance

“Moving to the cloud with Azure AD has benefitted both our employees and our IT Department. Thanks to Azure AD and Windows Hello for Business, employees can now use face recognition to streamline access to the services they need. Meanwhile, our IT department has freed up more resources, now that it no longer has to maintain an on-premises server or AD FS.”

Mitsui & Co.

MITSUI & CO.

AXA

Erie Insurance

Government

“That's the power of the solution for us. It supports the integration of legacy applications, in whatever state they are in, to talk to the new identity management component.”

New Zealand Ministry of Education

SANDEFJORD KOMMUNE

MINISTRY OF EDUCATION
TE TĀHUHU O TE MĀTAURANGA

DURHAM COUNTY

Healthcare

“Conditional Access in Azure AD is essential for us. Having that level of security across domains, being able to lock down identities from countries we don’t deal with but are known for malware, and using multifactor authentication improves our security posture and reduces stress for my team.”

MVP Health Care

Newfoundland & Labrador Centre for Health Information

MVP HEALTH CARE

Canadian Mental Health Association
Peel Dufferin
Mental health for all

Education

"We had four weeks to accelerate the university’s remote working solution to a viable, user-friendly, and resilient state that could be utilized by all staff and students. Using Azure AD played an enormous part in achieving this.
It’s a much better user experience and so much more powerful in terms of what we can do with security."

Durham University

Microsoft DigiGirlz

Durham University

PALMERSTON NORTH BOYS' HIGH SCHOOL

Retail

“Microsoft’s commitment to improving security and the cloud is clear. It is the relationship that has allowed us to securely implement Azure AD at our scale.”

Walmart

MATTRESSFIRM

asos

Walmart
Save money. Live better.

Professional Services

“We used to require multi-factor authentication whenever anyone was outside the office, but now with [Azure AD] Conditional Access we can take more factors into consideration and provide a much simpler sign-in experience in many cases.”

Burns & McDonnell

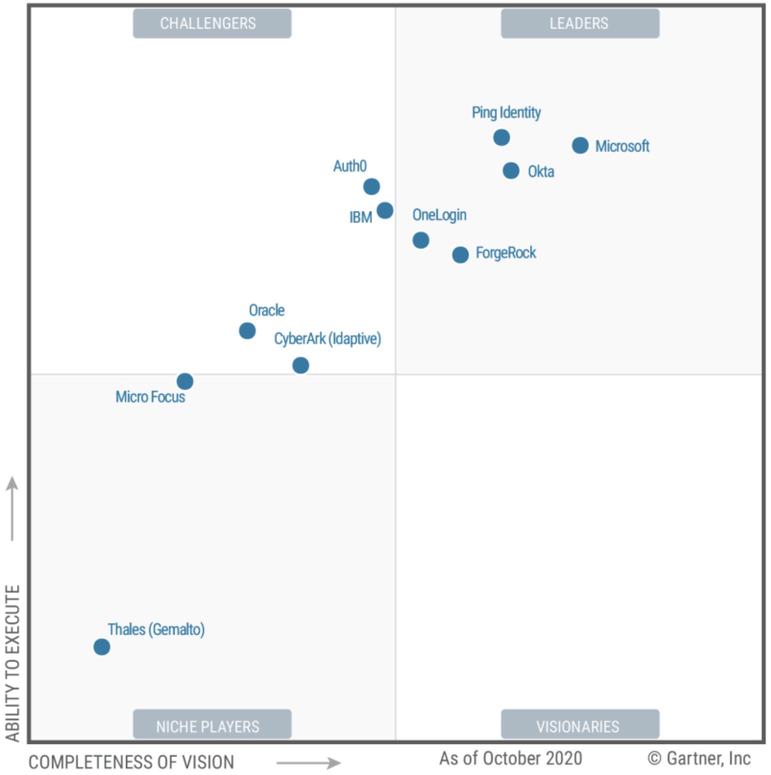
BURNS & McDONNELL

jetBlue

Telefónica

Gartner®

Microsoft—a Leader in Gartner Magic Quadrant for Access Management



*Gartner "Magic Quadrant for Access Management," by Michael Kelley, Abhyuday Data, Henrique Teixeira, November 2020

This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from Microsoft. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally, and is used herein with permission. All rights reserved.

Azure Active Directory

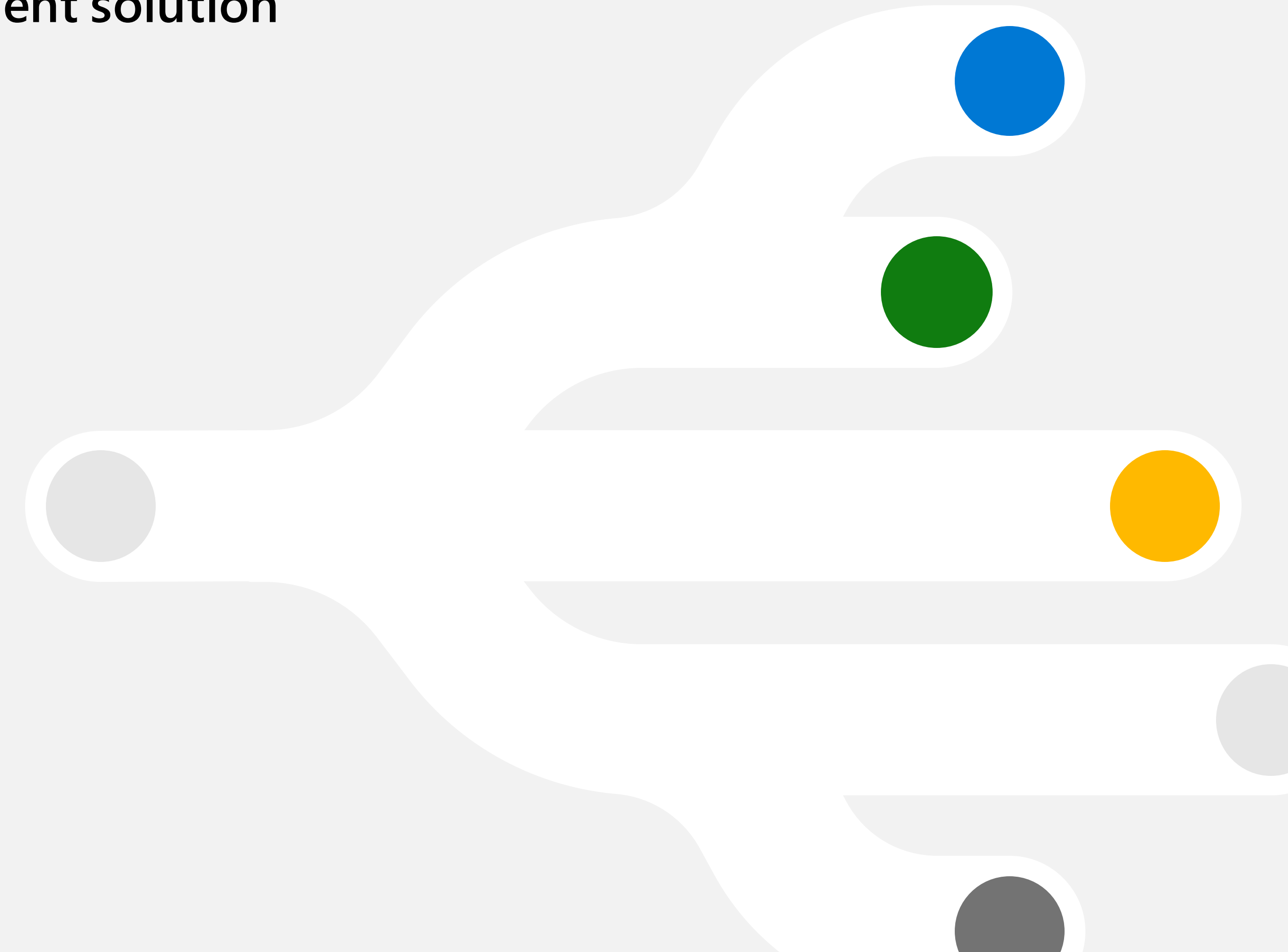
Your complete identity and access management solution with integrated security

Secure adaptive access

Seamless user experiences

Unified identity management

Simplified access governance



Pro Tips

- Start small with securing your most important digital assets (e.g. enforce 2FA for all your Office 365 administrator)
- Always ask the apps vendor if they can support your IAM for SSO and Identity provisioning (make this a default apps onboarding policy)

Next steps and actions

Party responsible	Completion date	Next step, action	Notes