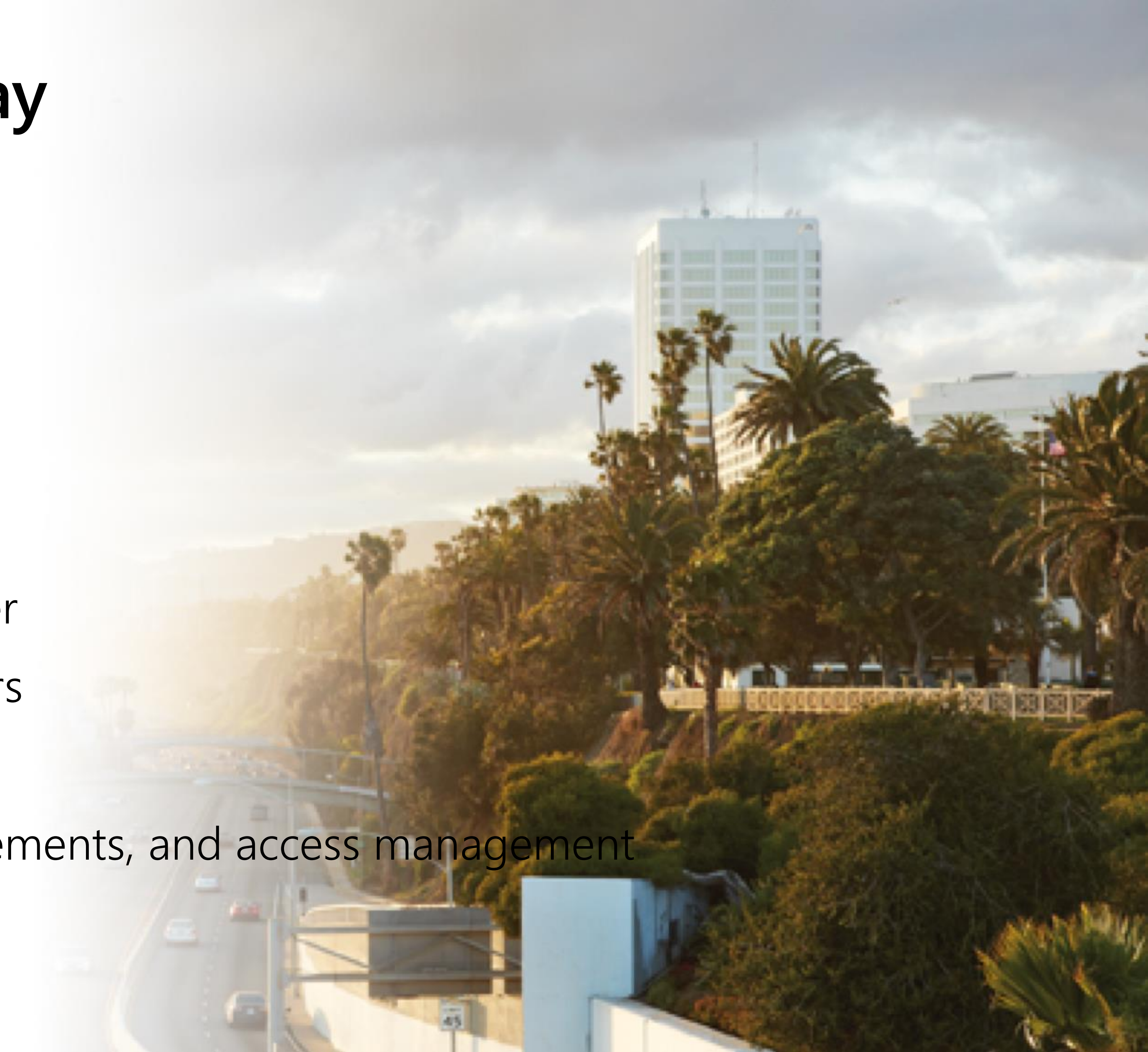
Microsoft

Speaking of security: Identity management

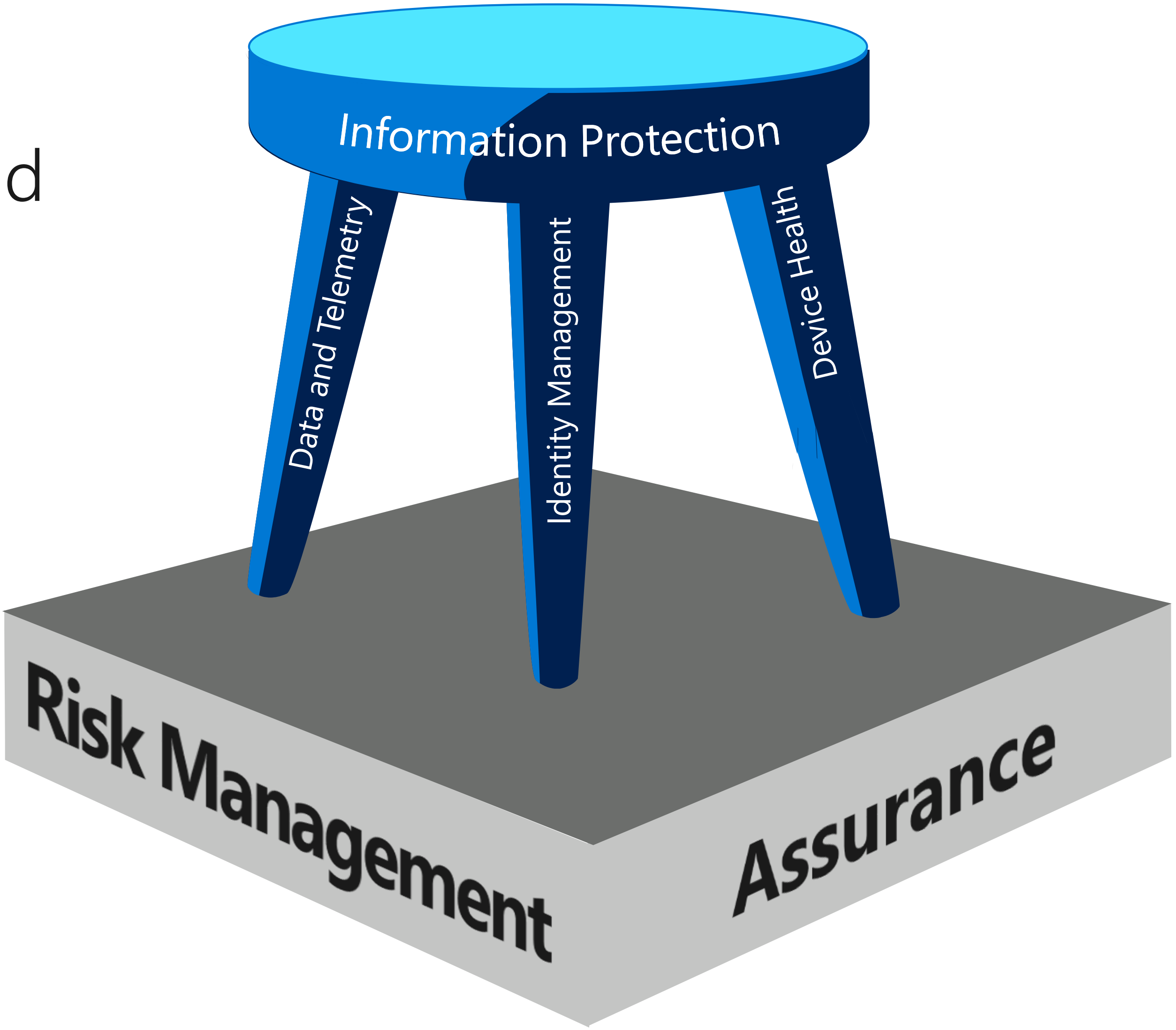
What we’ll cover today

- Security focus
- Digital security strategy
- Security world view
- Why identity is important
- Increasing complexity
- Identity is the new perimeter
- Protecting our administrators
- Eliminating passwords
- Simplify provisioning, entitlements, and access management
- Insights



Security focus

Balancing identity management, device health, data and telemetry, and information protection with risk management and assurance as the foundation.

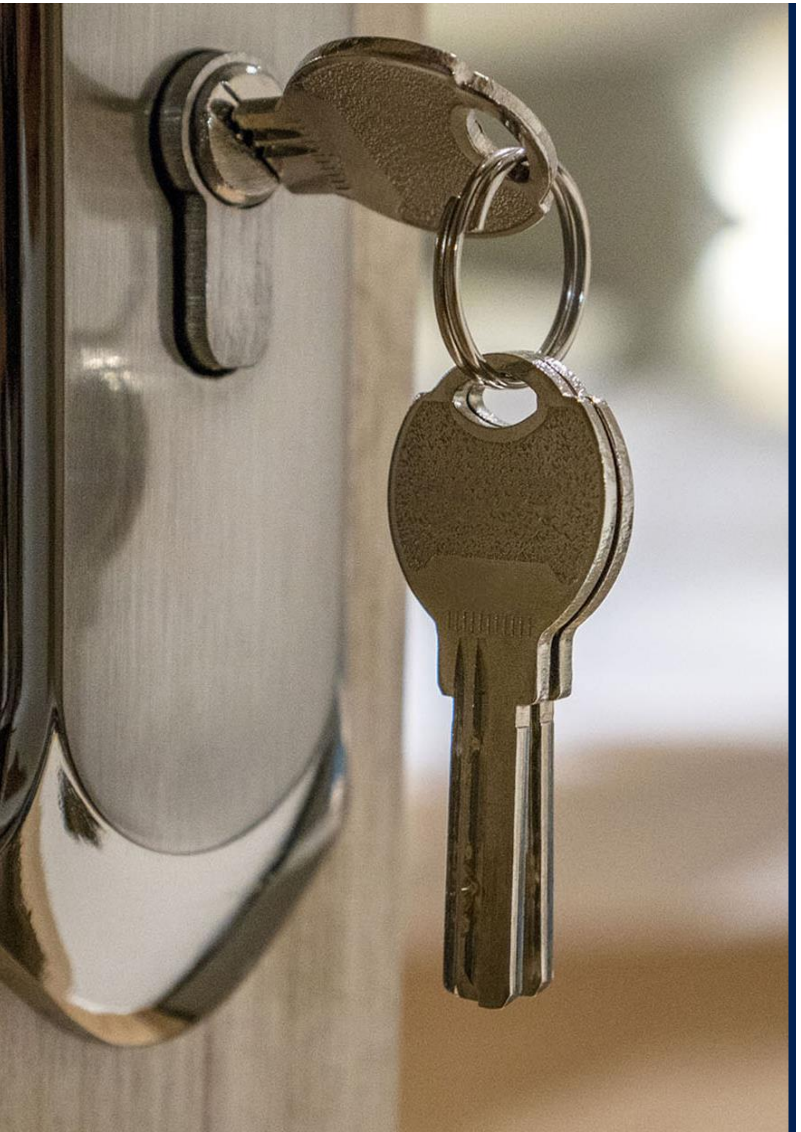


2019 Digital security strategy

	Risk Management	Assurance	Identity Management	Device Health	Data & Telemetry	Information Protection
EPICS	All internet facing interfaces are compliant Tier 1 critical services are resilient	Accelerate cloud security capabilities	Eliminate passwords Protect the administrators Simplify provisioning, entitlements, and access management	Evolve endpoint protection Only allow access from healthy devices Zero trust networks	Detect threats through user behavior anomalies	All Microsoft data is classified, labeled and protected
SERVICES	Business response and crisis management Compliance Enterprise business continuity management Enterprise security governance and risk Security education and awareness Security incident response Security standards and configuration	App & Infrastructure security Emerging security products External assessments Red team penetration testing Supply chain security	Administrator role services Authentication Certificate management Credential management Provisioning, entitlement management, and synchronization	Endpoint protection Phishing protection SAW HRE Vulnerability management Virtualization	Data intelligence Security intelligence platform Security monitoring Threat intelligence	Data loss prevention Insider threat

Security tools engineering

Security world view



→ Opportunities

Globalization: more markets, customers, and business potential

Always-on access provides **more productivity**

Ability to **analyze massive data** sets at scale and speed

Scalable, cloud based storage: efficient, cost effective, and secure

Modern engineering: allows for more agility in building capabilities, features, and in responding to threats

! Risks

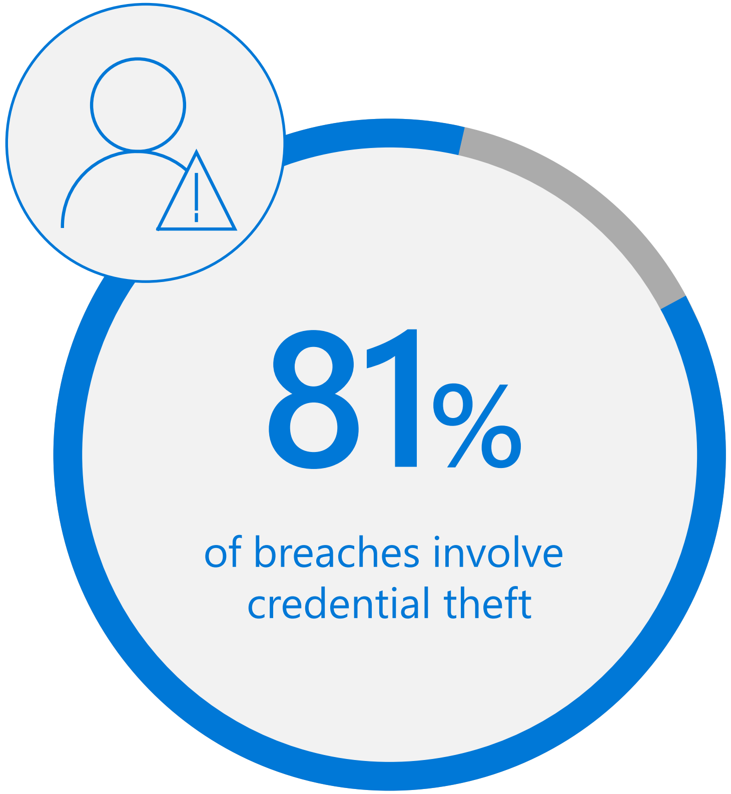
Globalization can lead to **"digital xenophobia"**

More lucrative targets give rise to more **dangerous threat actors**

More surface area for attacks/exposure to harm, including **supply chain**

The client-to-cloud world requires a control shift
(Identity is the new perimeter)

Why identity is important?



81%

of breaches involve credential theft

73%

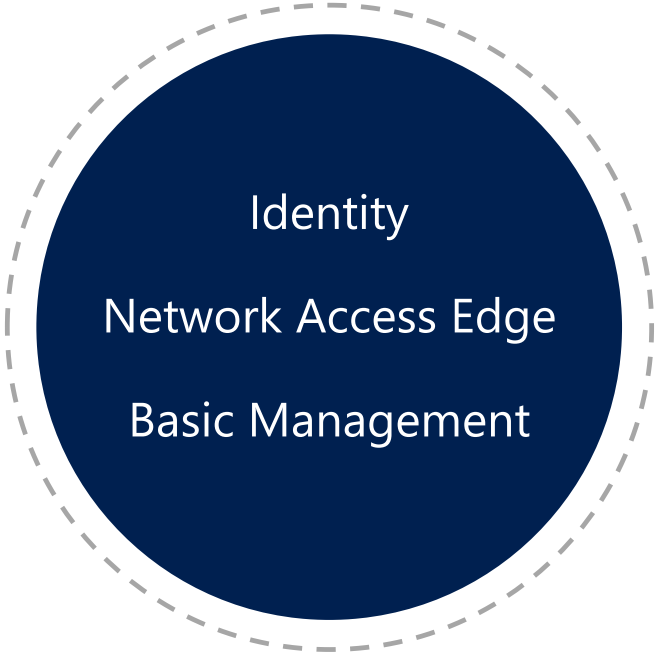
of people re-use passwords across multiple accounts

80%

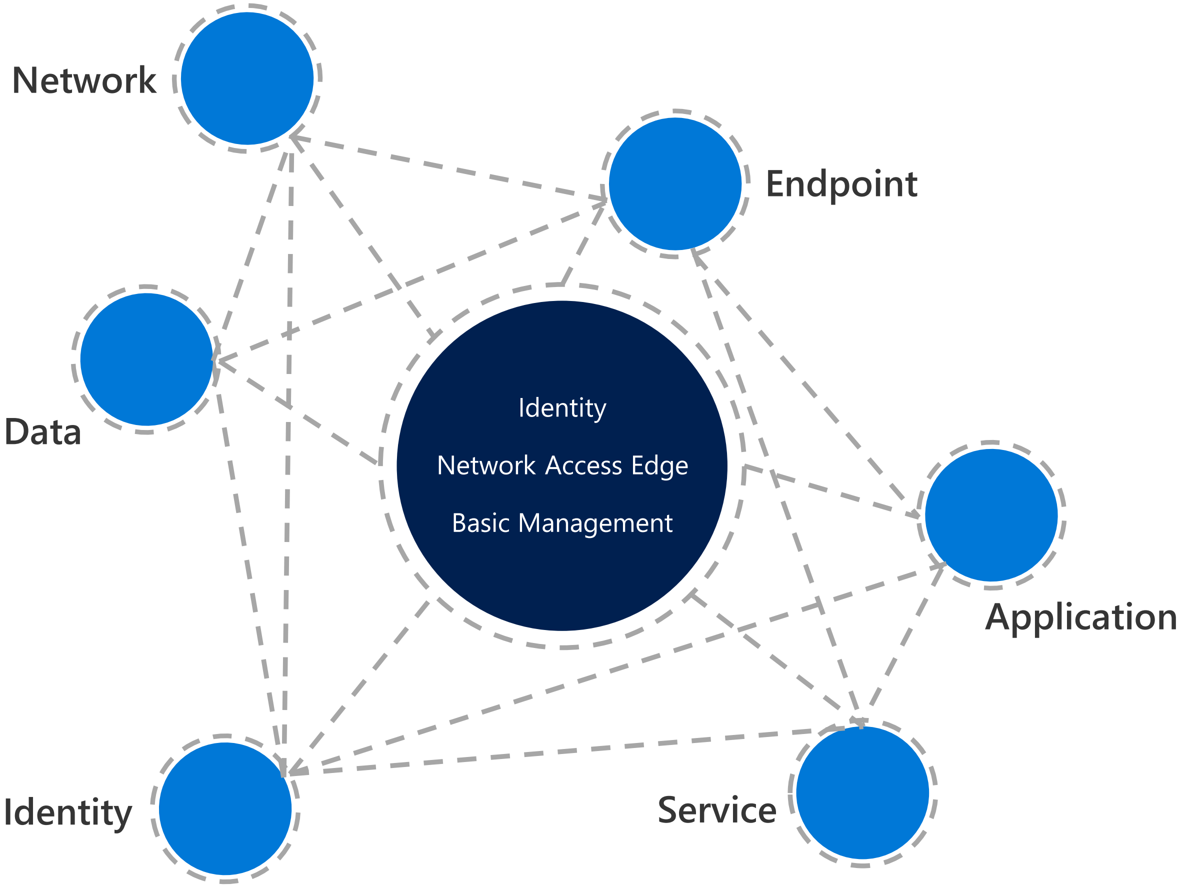
of employees use non-approved apps for work

Increasing complexity

The past



Current reality



Identity is the new perimeter

Key investment areas

Protect the admins

Protect customers and services from malicious use of elevated privileges

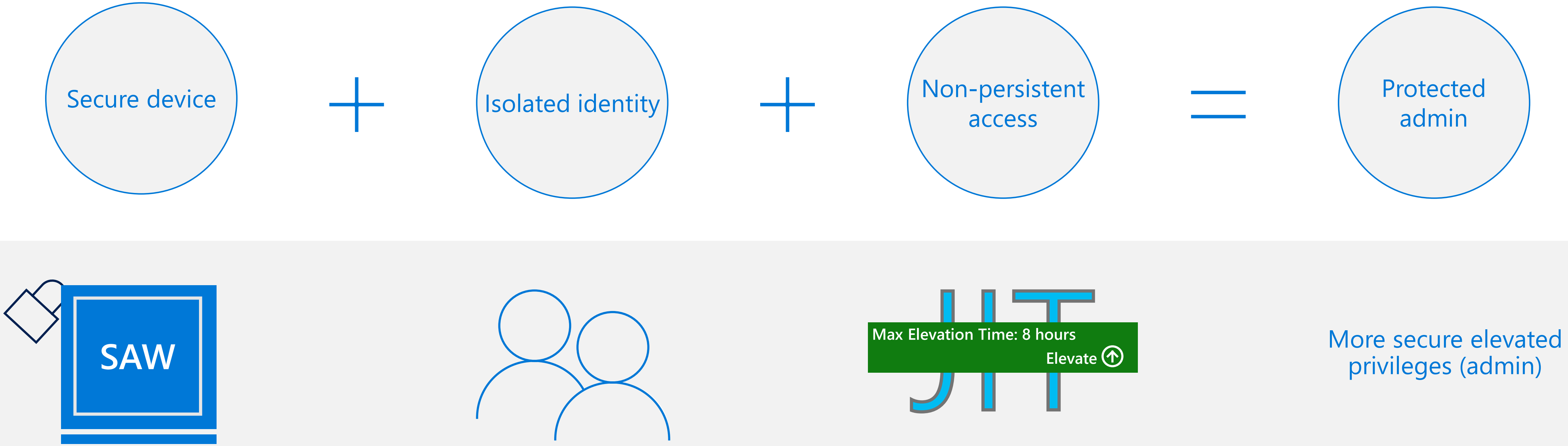
Eliminate passwords

Eliminate passwords through multi-factor authentication

Simplify provisioning

Simplify provisioning, entitlements, and access management

Protecting our administrators



Secure device + Isolated identity + Non-persistent access = Protected admin

SAW

JIT

Max Elevation Time: 8 hours

Elevate

More secure elevated privileges (admin)

Accessing critical resources only from a **Secure Device**

While logging in with an isolated smartcard based **ALT Account**

Only when performing non-standard user duties, non persistently, through **Elevation**

Eliminate passwords

"One of the biggest security issues is passwords." ~ Satya Nadella

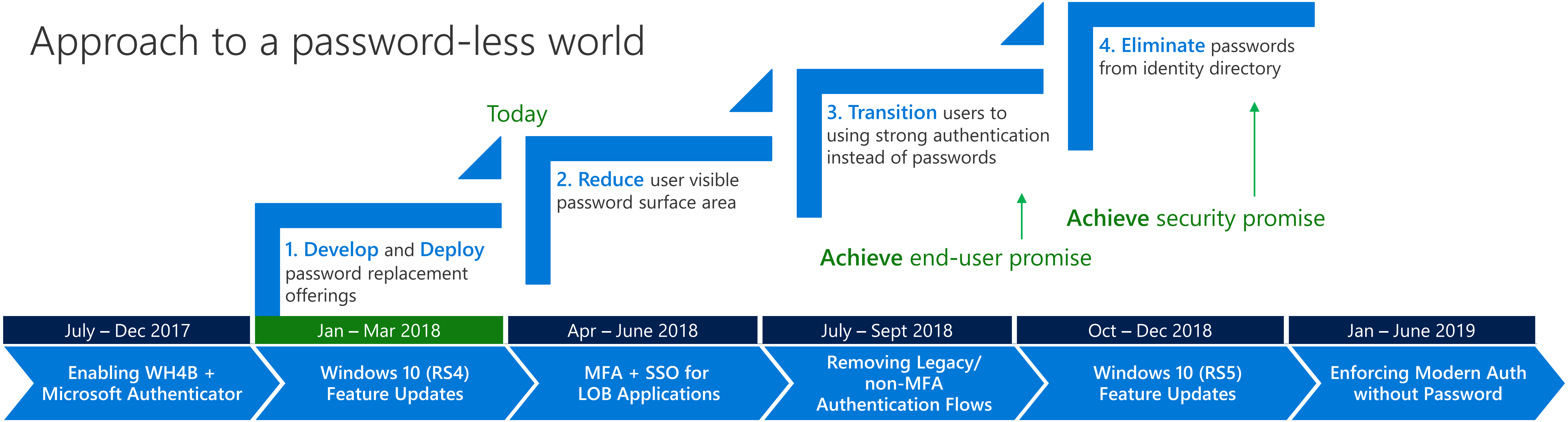
Through strong and Multi-factor Authentication (MFA)

Biometric on Device — Windows Hello for Business – Available on all Windows 10 Machines **TODAY** with improvements coming in RS4 and RS5

Microsoft Authenticator — Microsoft Authenticator – Available **TODAY** across all mobile platforms, integral in corporate bootstrapping of MFA

Device + Biometric — FIDO 2.0 Devices – Enabling ultimate flexibility for users and increase security across all forms of Identity and Auth *(Coming soon)*

Approach to a password-less world



1. Develop and **Deploy** password replacement offerings

Today

2. Reduce user visible password surface area

3. Transition users to using strong authentication instead of passwords

4. Eliminate passwords from identity directory

Achieve end-user promise

Achieve security promise

July – Dec 2017	Jan – Mar 2018	Apr – June 2018	July – Sept 2018	Oct – Dec 2018	Jan – June 2019
Enabling WH4B + Microsoft Authenticator	Windows 10 (RS4) Feature Updates	MFA + SSO for LOB Applications	Removing Legacy/ non-MFA Authentication Flows	Windows 10 (RS5) Feature Updates	Enforcing Modern Auth without Password

Simplify provisioning, entitlements, and access management

Identity provisioning

Access requests and lifecycle

Identity governance

Insights

- Plan for enterprise level cultural shifts
- Think beyond the device
- Security starts at provisioning
- The user-experience matters

Resources

Access all IT Showcase resources at Microsoft.com/ITShowcase

- Webinar: Speaking of security: A discussion with Bret Arsenault, CISO at Microsoft
- Video: How Microsoft protects against identity compromise
- Case study: Microsoft 365 helps create a secure modern workplace
- Case study: Implementing strong user authentication with Windows Hello for Business
- Blog: No more passwords: the relentless commitment to creating a password-less world at Microsoft
- Webinar: IT Expert Roundtable: How Microsoft secures elevated access with tools and privileged credentials
- Article: Protecting high-risk environments with secure admin workstations
- Improving security by protecting elevated-privilege accounts at Microsoft

Microsoft

Microsoft IT Showcase

How Microsoft does IT

Visit the website
http://www.microsoft.com/itshowcase