SecWise IDENTITY

Microsoft IAM jump-start Solutions

Koen.Jacobs@secwise.be

Gold
Microsoft Partner
Security
Microsoft

SecWise

Introduction

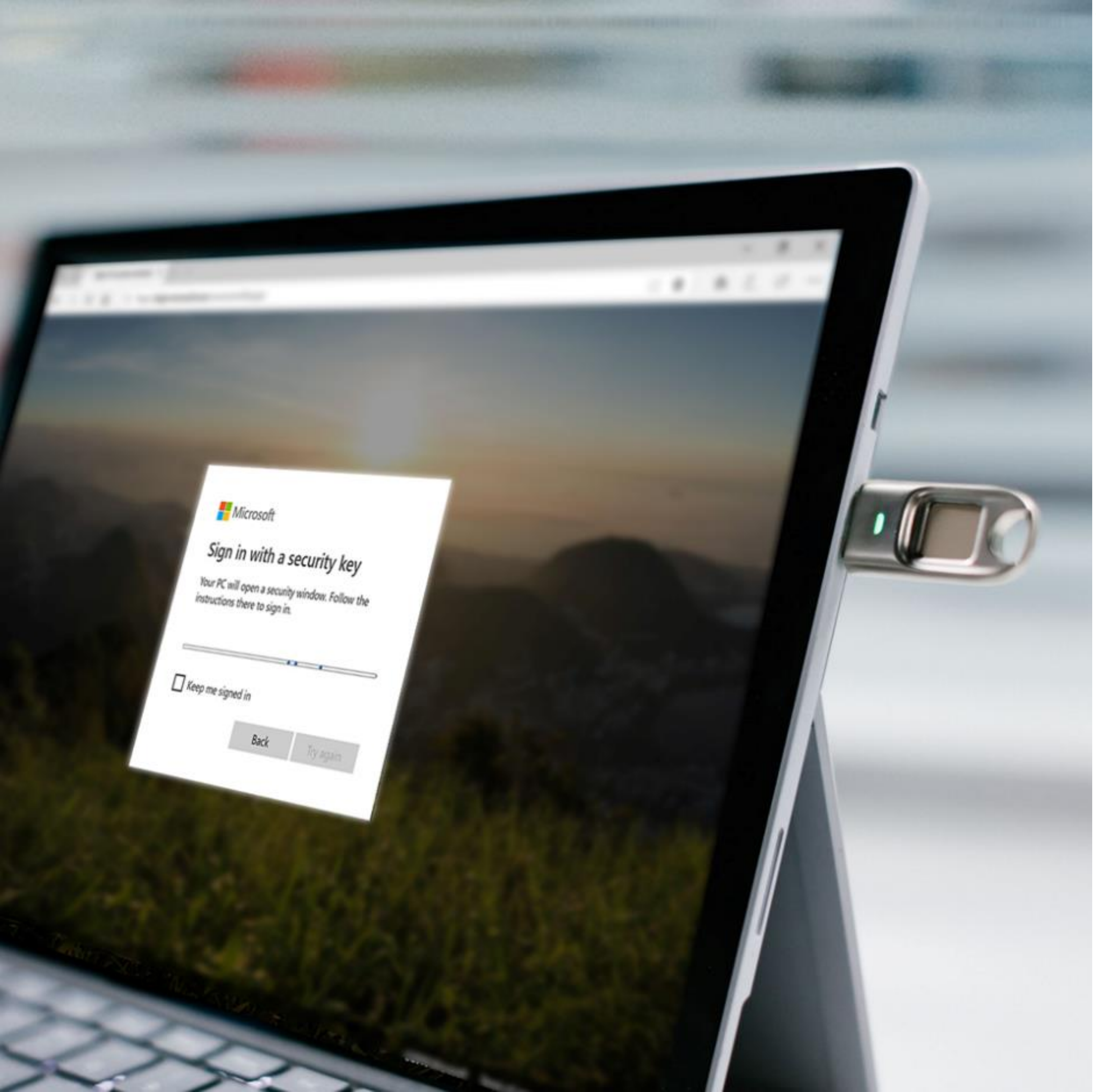
SecWise

- Cyber Security & Information Protection consultancy & service
  - Identity & Access Management
  - Device Management
  - Threat Protection & Detection
  - Information & Data Protection
  - Managed Security Service
  - Azure IaaS / PaaS security
- Experts in Microsoft Cloud Security: act as a Trusted Advisor
- Part of The Cronos Group

engie COLRUYT GROUP NATO OTAN TVH EQUIPMENT imec ING FLANDERS INVESTMENT & TRADE Vlaanderen is internationaal ondernemen

GO! onderwijs van de Vlaamse Gemeenschap isabel group CHRISTELIJKE MUTUALITEIT

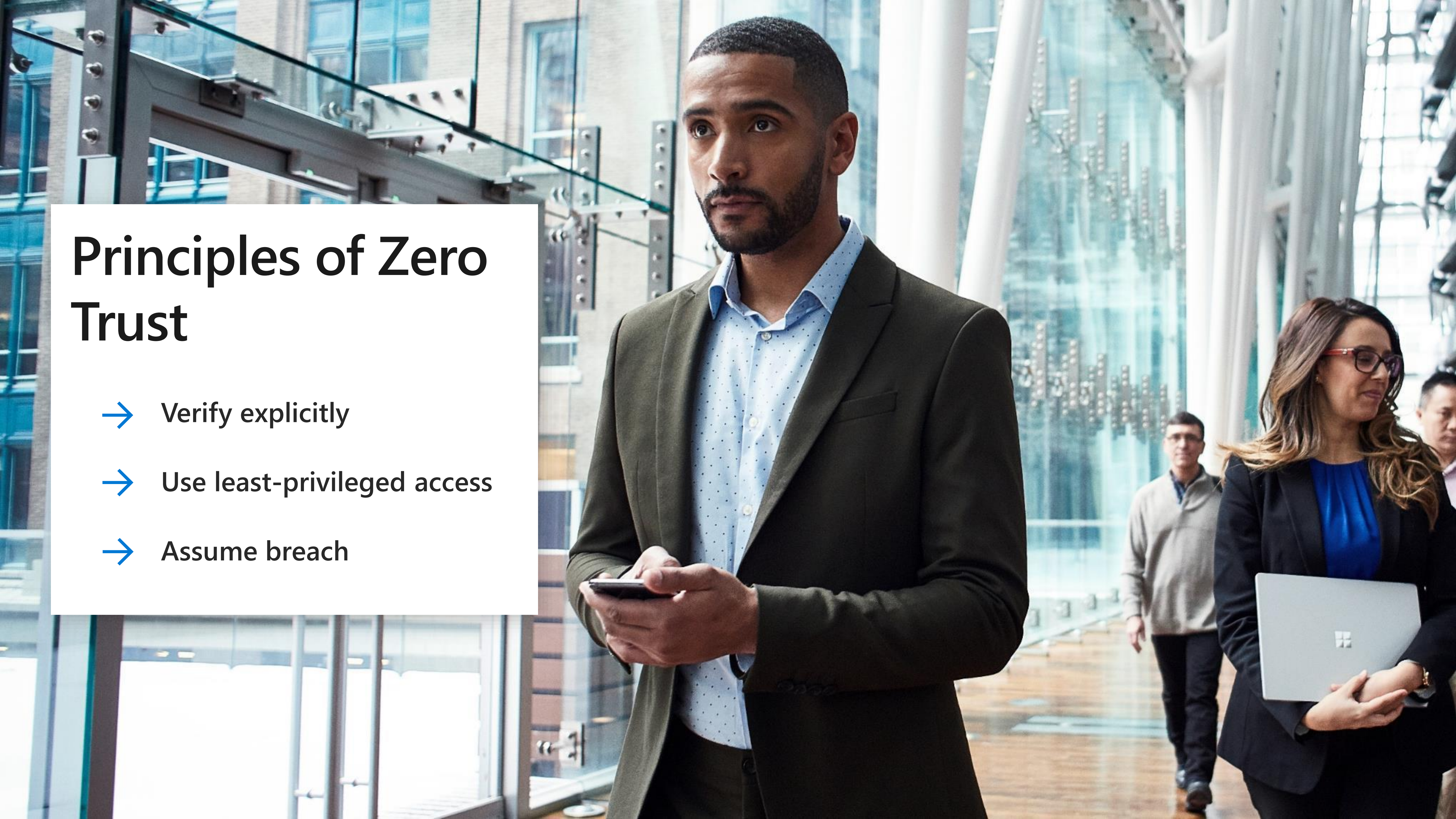
SecWise


Microsoft
Sign in with a security key
Your PC will open a security window. Follow the instructions there to sign in.
□ Keep me signed in
Back
Try again

Agenda

- Zero Trust
- SecWise Solutions
- SecWise Identity offering

SecWise



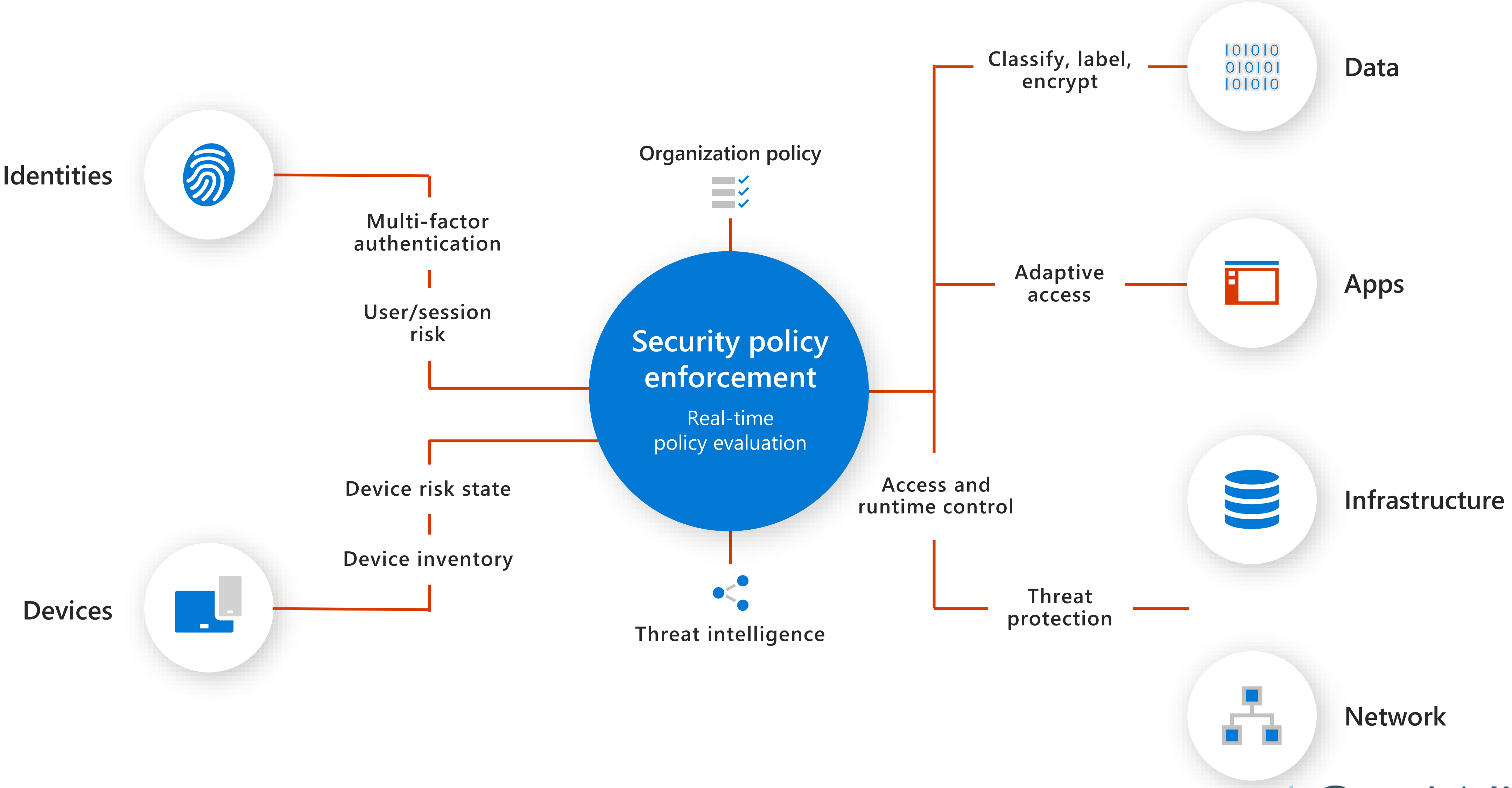
Principles of Zero Trust

→ Verify explicitly

→ Use least-privileged access

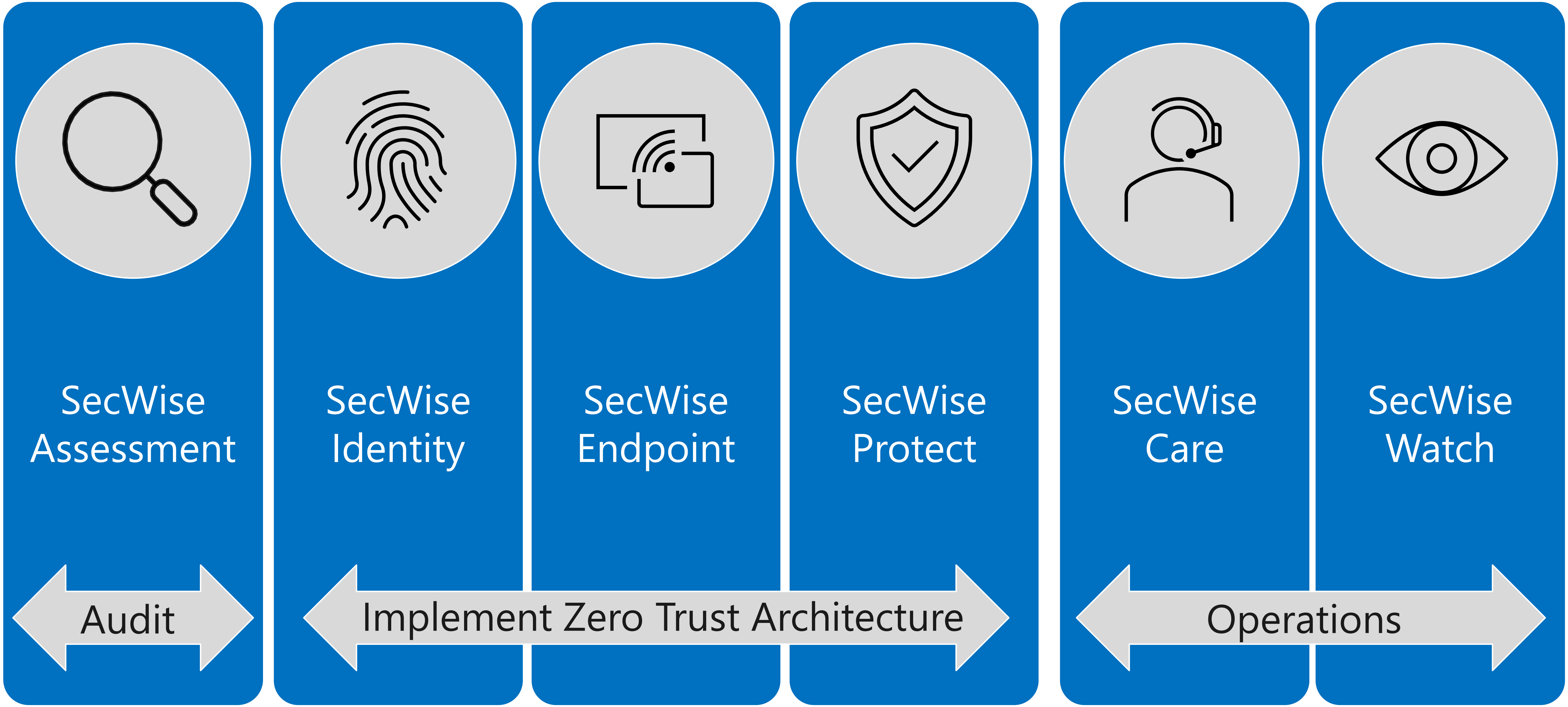
→ Assume breach

Zero Trust architecture



SecWise

SecWise Solutions Offering



SecWise Assessment

SecWise Identity

SecWise Endpoint

SecWise Protect

SecWise Care

SecWise Watch

Audit

Implement Zero Trust Architecture

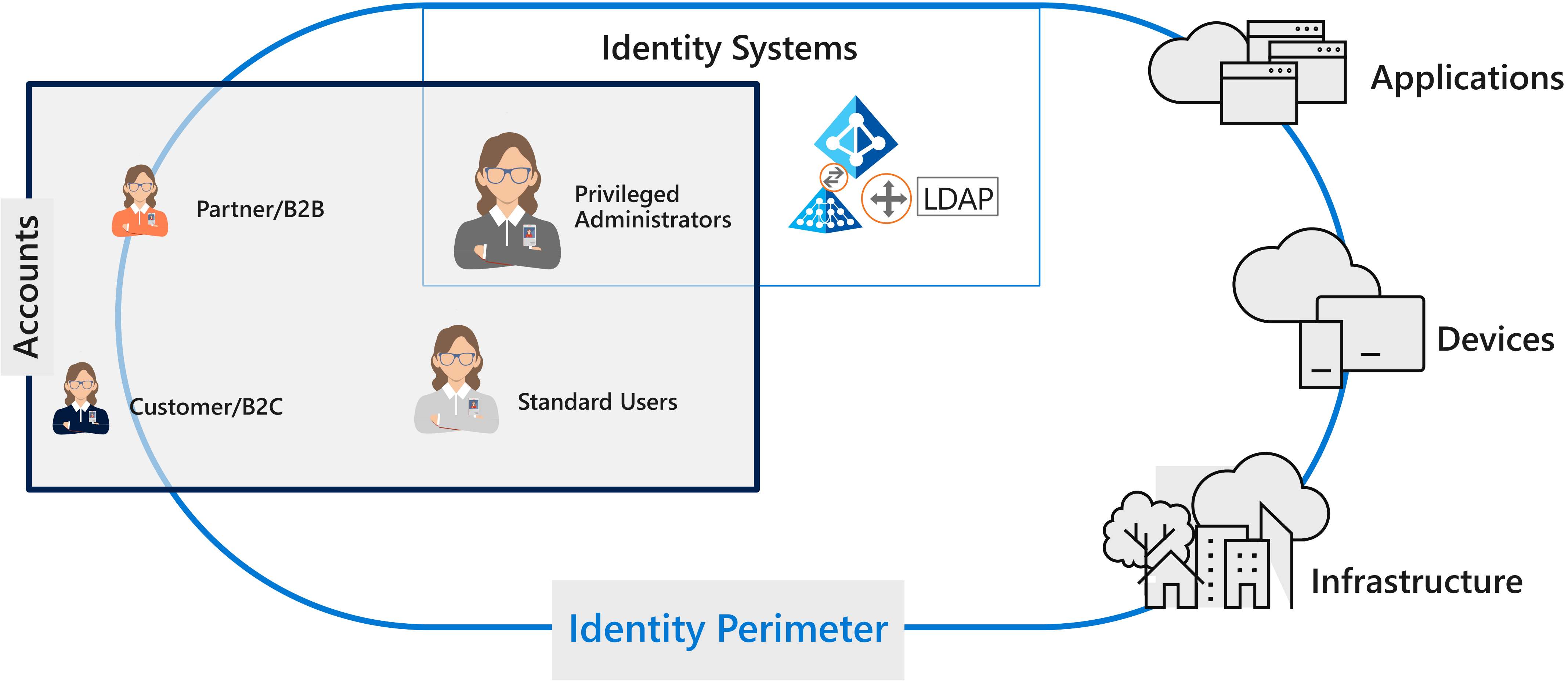
Operations

SECWISE IDENTITY

MODERN IAM - HOW TO DETECT AND PROTECT AGAINST IDENTITY-BASED ATTACKS?

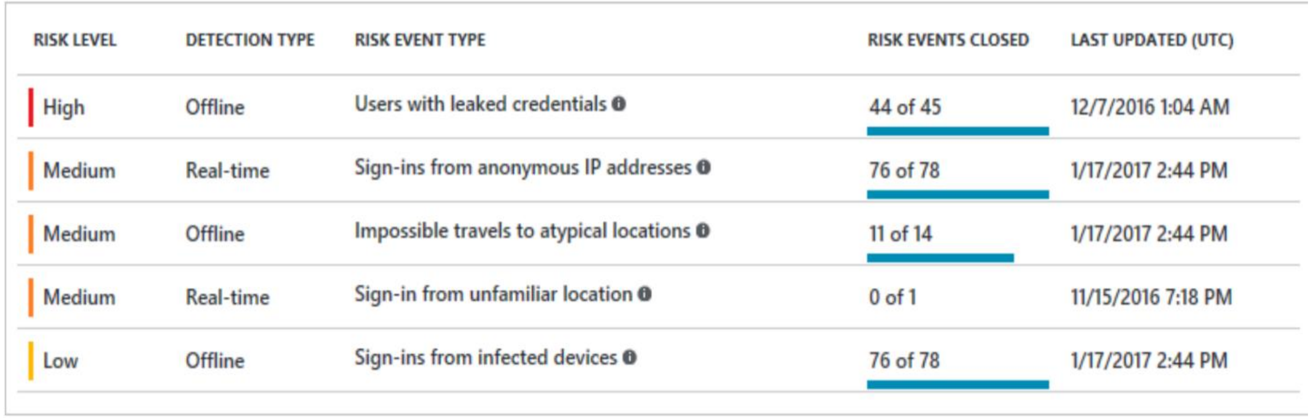
SecWise

What is Identity Access Management?



Why do you need Identity Access Management?

- Most security breaches take place when attackers gain access to an environment by stealing a user’s identity
- Azure Active Directory Identity Protection provides you with capabilities for:
  - Detecting vulnerabilities and risky accounts
  - Investigating risk events
  - Building risk-based conditional access policies, allowing automated responses on suspicious activity
    - Multi-factor authentication registration not configured
    - Unmanaged cloud apps
    - Security Alerts from Privileged Identity Management
    - Azure Active Directory risk events
    - Users with Leaked credentials
    - Sign-ins from anonymous IP address
    - Impossible travel to atypical locations
    - Sign-in from unfamiliar locations
    - Sign-ins from infected devices
    - Sign-ins from IP addresses with suspicious activity



RISK LEVEL	DETECTION TYPE	RISK EVENT TYPE	RISK EVENTS CLOSED	LAST UPDATED (UTC)
High	Offline	Users with leaked credentials	44 of 45	12/7/2016 1:04 AM
Medium	Real-time	Sign-ins from anonymous IP addresses	76 of 78	1/17/2017 2:44 PM
Medium	Offline	Impossible travels to atypical locations	11 of 14	1/17/2017 2:44 PM
Medium	Real-time	Sign-in from unfamiliar location	0 of 1	11/15/2016 7:18 PM
Low	Offline	Sign-ins from infected devices	76 of 78	1/17/2017 2:44 PM

SecWise

SecWise Identity offering:

Solution Description

❖Review and Redesign authentication flows and integration of Active Directory /Azure Active Directory

❖Identity protection best practices testing and enrolment using Conditional access policies

- ❖MFA
- ❖Identity Protection

❖Disable legacy authentication protocols

❖Review & improvement of Azure Active Directory security settings

❖Azure Active Directory Password Protection Policies

Service Options

❖ Light

❖ Elevated

❖ Advanced

Solution Goal

❖Better identity protection & privileged admin access

❖Improve authentication, accountability, auditing and visibility

❖Improve compliance enforcement

❖Improve manageability of identities and devices

SecWise

SecWise Identity flavours

Light

- Implement Hybrid join or Cloud-only identity best practices
- SSO experience for end-users in Edge & Chrome browsers
- Enable smart MFA for 20 users
- Enable SSPR for 20 users
- Block Legacy Protocols
- Password Management best practices

Elevated

- Risk based access Policies
- Privileged Identity Management
- Access Management & Review
- Cloud Application Governance

Advanced

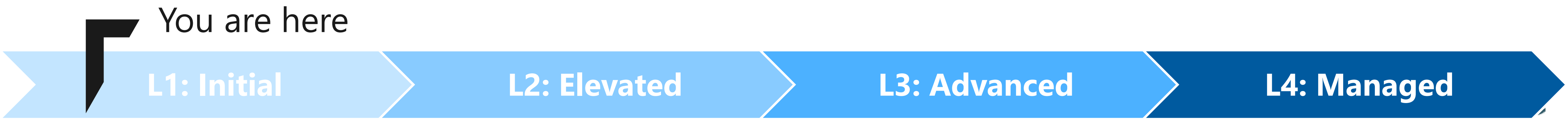
- Password-less strategy WHFB
- Azure Active Directory password protection
- Device compliancy-based access policies
- B2B guest user Governance using entitlement management

SecWise Watch

- Monitoring Identity based attacks
- Monitoring Identity security posture

SecWise Care

- Change requests
- Security Questions/assistance


You are here

L1: Initial

L2: Elevated

L3: Advanced

L4: Managed

een) -

Thank You!

Contact: Koen Jacobs
koen.Jacobs@secwise.be
+32 473 784 295

SecWise