Zero Trust med Maks Produktivitet

Hvordan sikre din Organisasjon med et Zero Trust Rammeverk

Jan Vidar Elven

Starter ca 08:45 ☺

Jan Vidar Elven

Cloud Platform & Security Architect

Skill AS

MVP Enterprise Mobility

@JanVidarElven

gotoguy.blog

MVPDAGEN

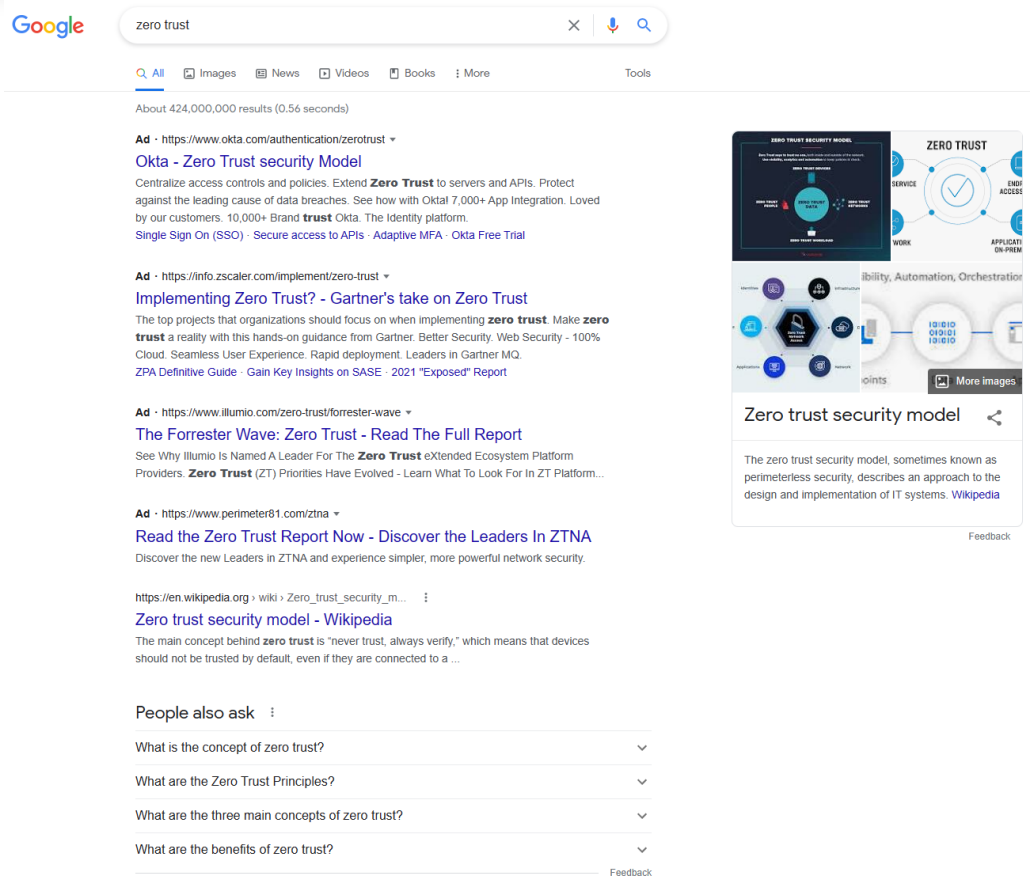
En konferanse der MVPer deler sin kunnskap med deg

SKILL

Zero Trust

- Zero Trust før og nå:
  - John Kindervag (Forrester, 2009)
- Et rammeverk, ikke et produkt
- En reise, visjon, tankesett. Bygg stein på stein.
  -du blir aldri ferdig med det ☺

«NEVER TRUST, ALWAYS VERIFY"



Konseptene i Zero Trust (Kindervag)

Tilgang til alle ressurser skal foregå på en sikker måte uavhengig av lokasjon

Tilgangskontroll gis kun til de som «må ha» og er strengt håndhevet

All trafikk skal inspiseres og logges

Informasjonssikkerhet og Zero Trust

- HUSK: «Tillitt er en sårbarhet»
- -kanskje er dere allerede kompromittert ?!

"Det finnes bare to typer selskaper: de som har blitt hacket, og de som blir det."
- Robert Mueller, FBI Director

COMPUTERWORLD E-helse Olje/energi Bygg/anlegg Offentlig it Fintech

COMPUTERWORLD | MACWORLD | IT-BRANSJEN | TELECOM REVY | EVENT | WHITEPAPER | STILLING LEDIG | E-AVIS

STILLING LEDIG Alle stillinger

Din annonse her
Computer Communications AS

CRM senior konsulenter
Cartagena AS

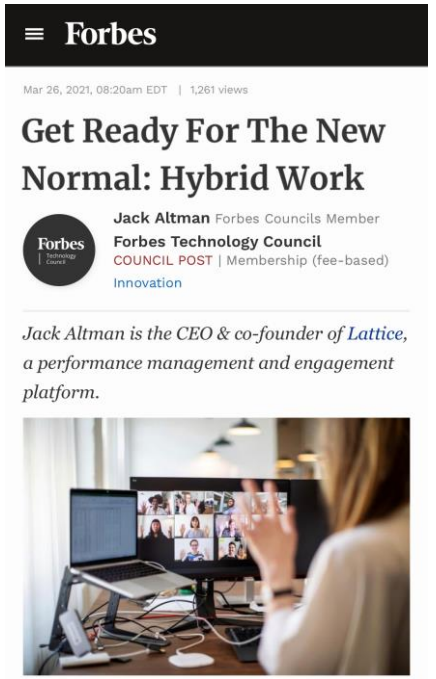
Teamleder Utvikling
Visma Financial Solutions AS

ZERO TRUST: John Kindervag har jobbet med å kvitte verdens it-sikkerhetsstrategier for konseptet "tillit" siden 2008. Det er en tanke som har fått svært mange tilhengere siden da. Opphavet til Zero Trust model var innom Norge i oktober. (Foto: Stig Øyvann)

Tillit er en sårbarhet, mener forskeren bak strategien «Zero Trust model»

Et tiår senere – Hva er hovedtrendene nå?

- Mars 2020 ->
  - #WorkFromHome
  - Hybrid arbeidsplass den nye normalen
- Økte angrep fra nasjon/statlige aktører
  - Mer sofistikert
  - Multi-vector
  - Orkestrert



4-in-5 organizations already have or are working towards a hybrid workplace.

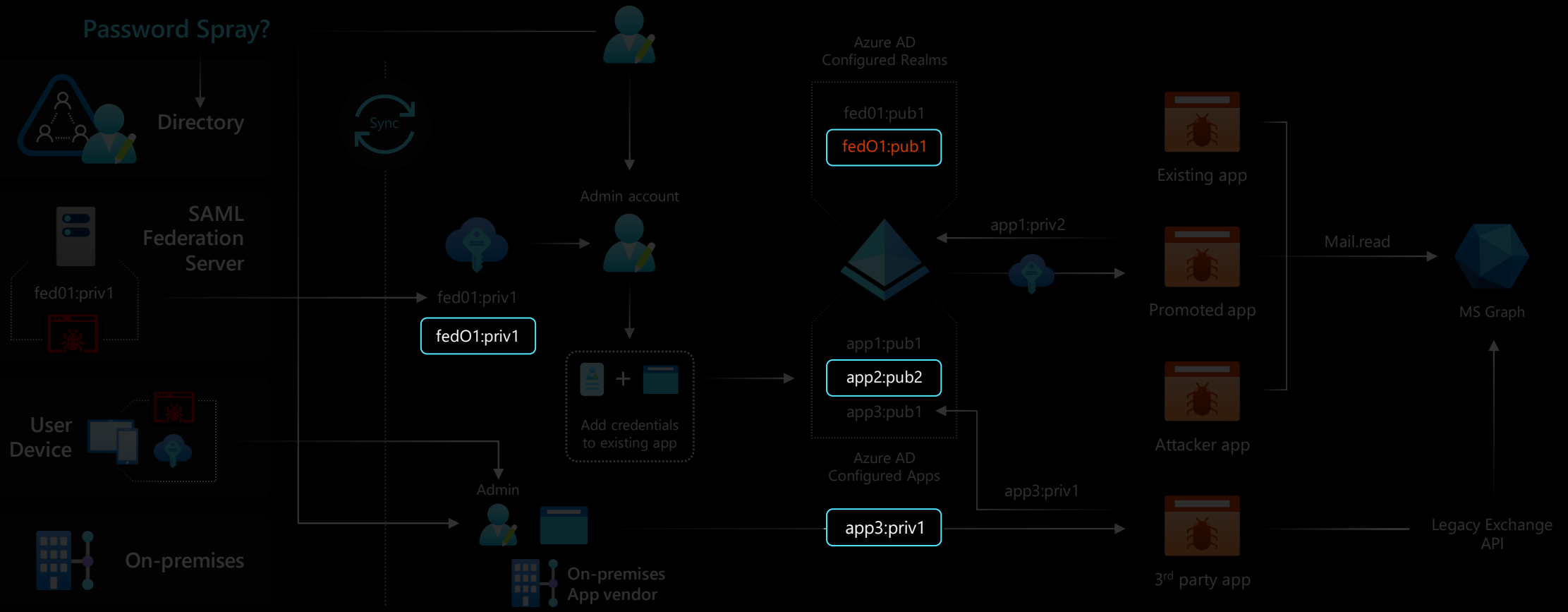
Security is a top concern.

Hybrid Workplace Concerns

Employees downloading unsafe apps	37%
An increase to IT workload	37%
Ransomware attacks	36%
Phishing attacks	35%
Improper use of personal devices	34%
Unauthorized access to data	31%
Inability to manage all devices	30%
Use of personal email accounts	30%
Non-compliance with data regulations	24%

Why the Hybrid Workplace Is a Cybersecurity Nightmare - WSJ

Sophisticated, orchestrated, multi-vector attacks are growing



...and targeting every identity

User Identities

Admin Identities

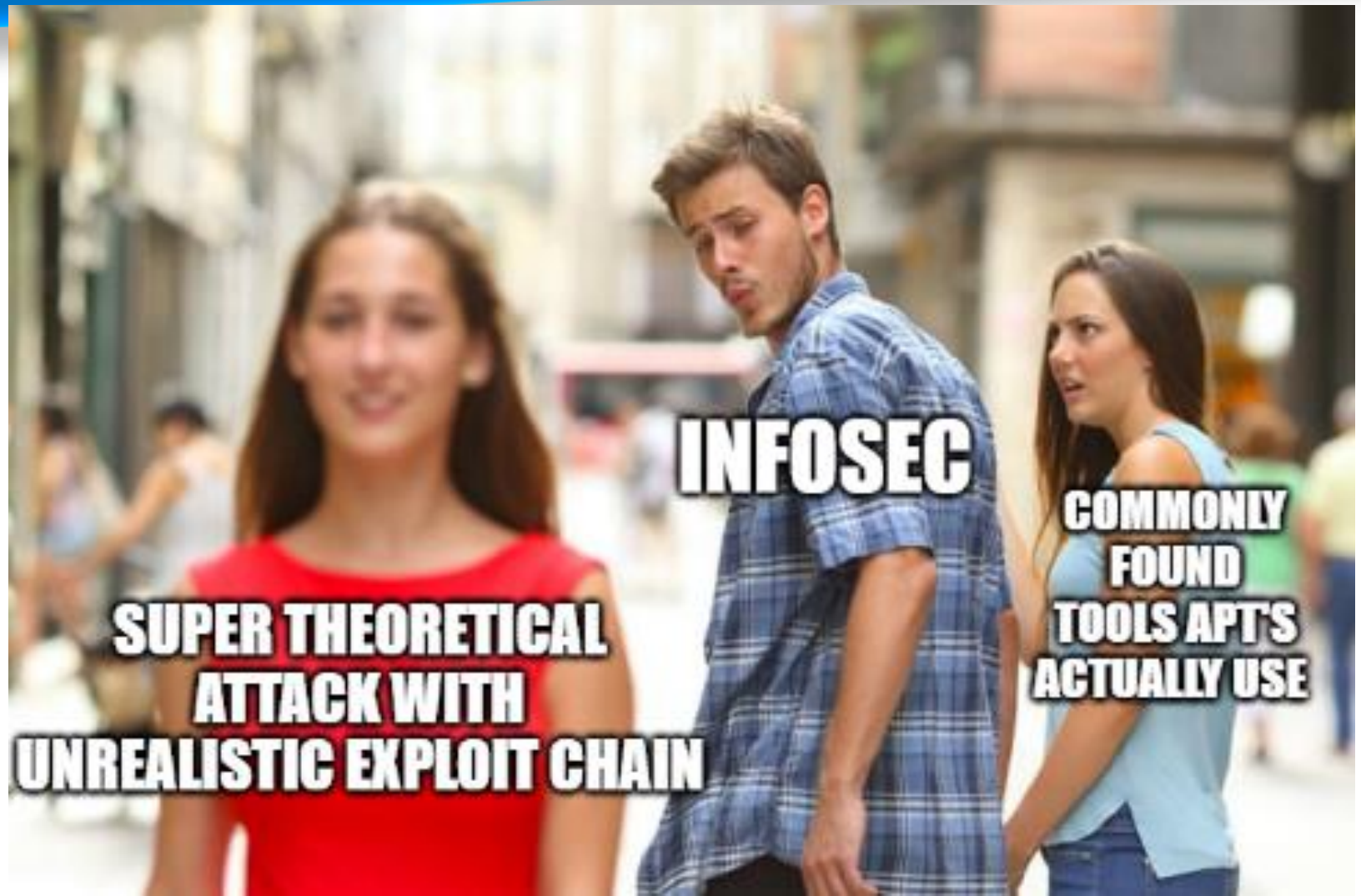
...and targeting every identity

User Identities

Admin Identities

Workload Identities

Men: Fokus på de riktige tingene



We need a better approach

Users are Employees	Employees + Partners +Customers
Corporate Devices	Bring Your Own Device
On-Premises Apps	Explosion of Cloud Apps
Work is Done at Work	Work is Done Anywhere
Criminal Syndicates	Nation State Actors

A Zero Trust strategy is imperative

Verify explicitly

Use least privileged access

Assume breach

Verify explicitly

Use least privileged access

Assume breach

Verify all your identities

Human Identities

- Groups/Role
- Location
- Privileges
- Risk

Verifying explicitly begins with strong authentication

INCLUDING PASSWORDLESS TECHNOLOGY

Phone Authenticator

Windows Hello

FIDO2 security key

Biometrics

Push notification

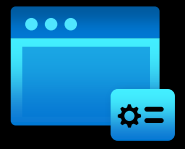
Soft Tokens OTP

Hard Tokens OTP

SMS, Voice

Verify all your identities

Human Identities



Workload Identities

Groups/Role

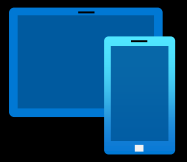
Location

Privileges

Risk

Verify all your devices

Managed endpoints



Personal devices

Managed or BYOD

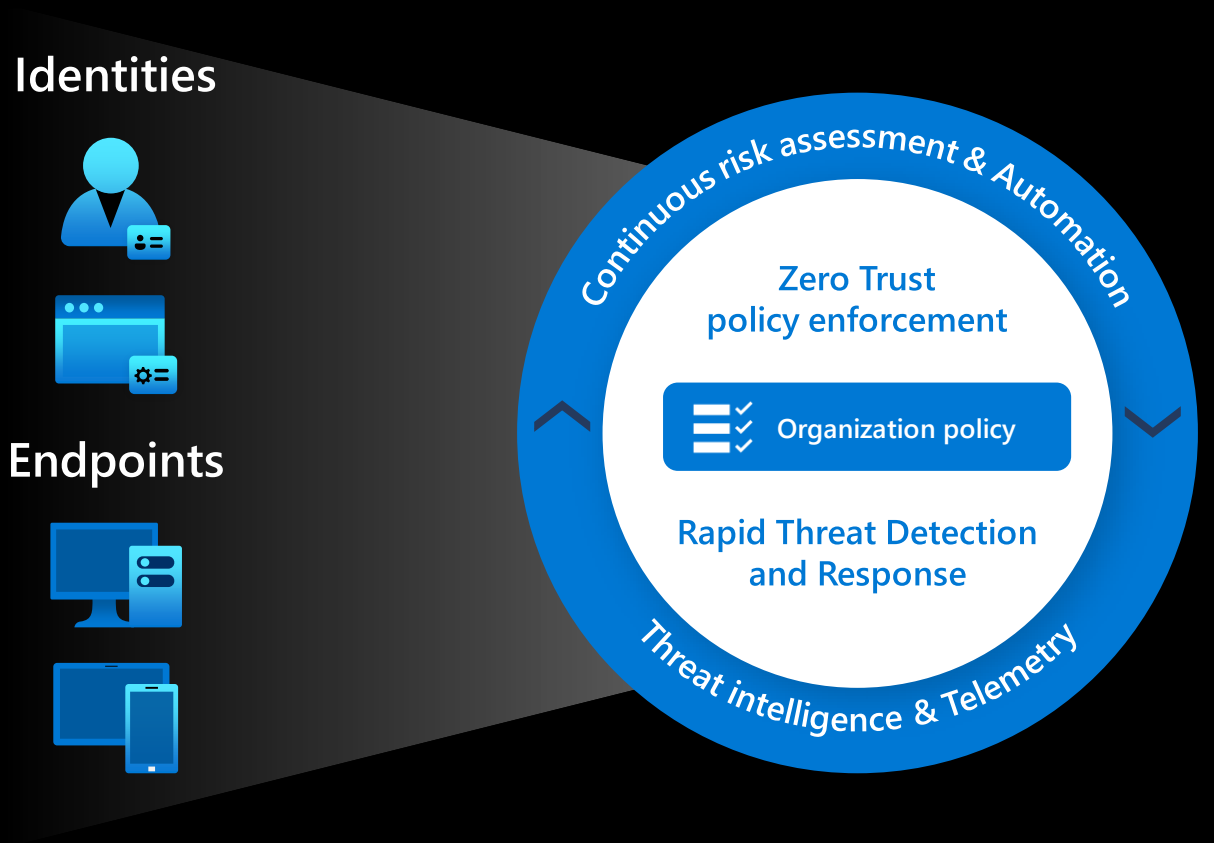
Health & compliance

Type and OS version

Encryption status

Risk

Zero Trust policy enforcement



A Zero Trust strategy is imperative

Verify explicitly

Use least privileged access

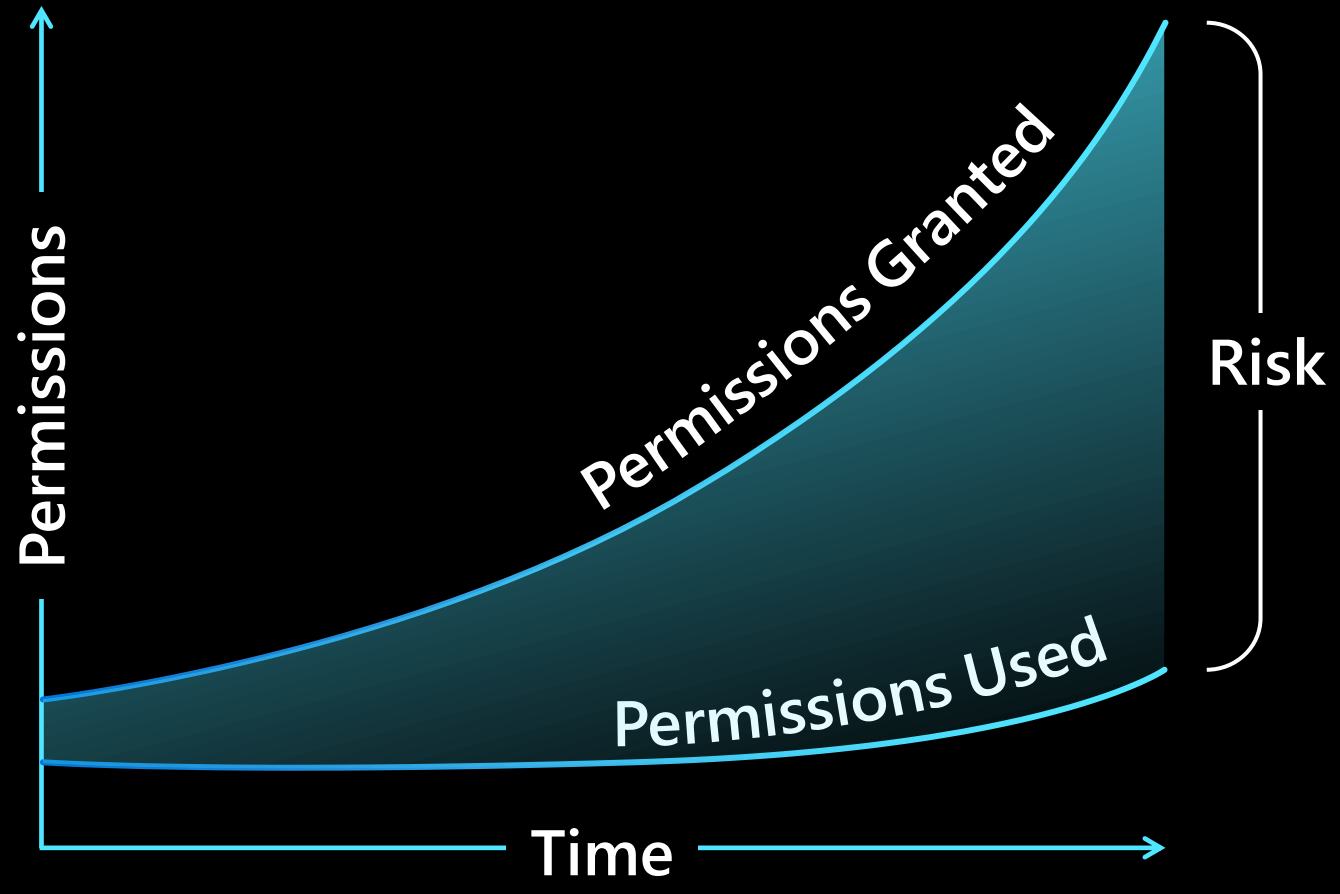
Assume breach

Verify explicitly

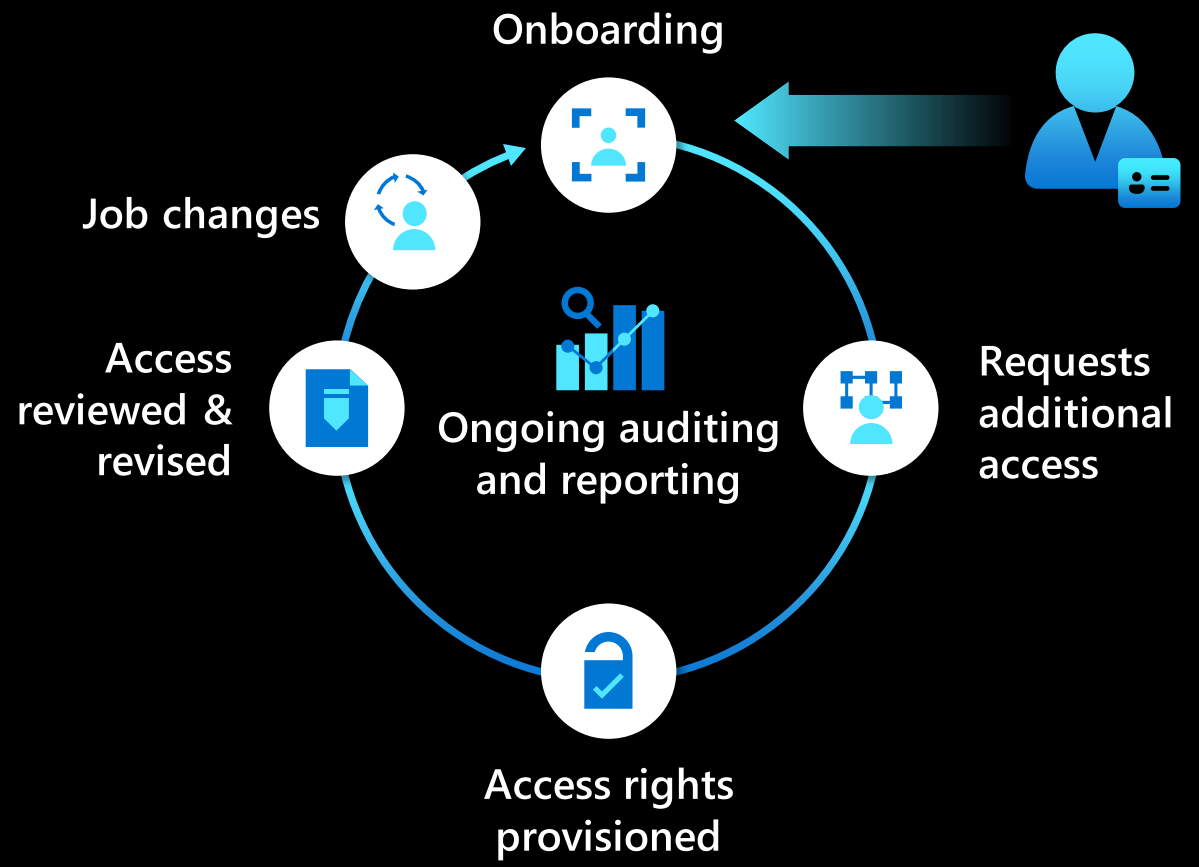
Use least privileged access

Assume breach

Mind the gap

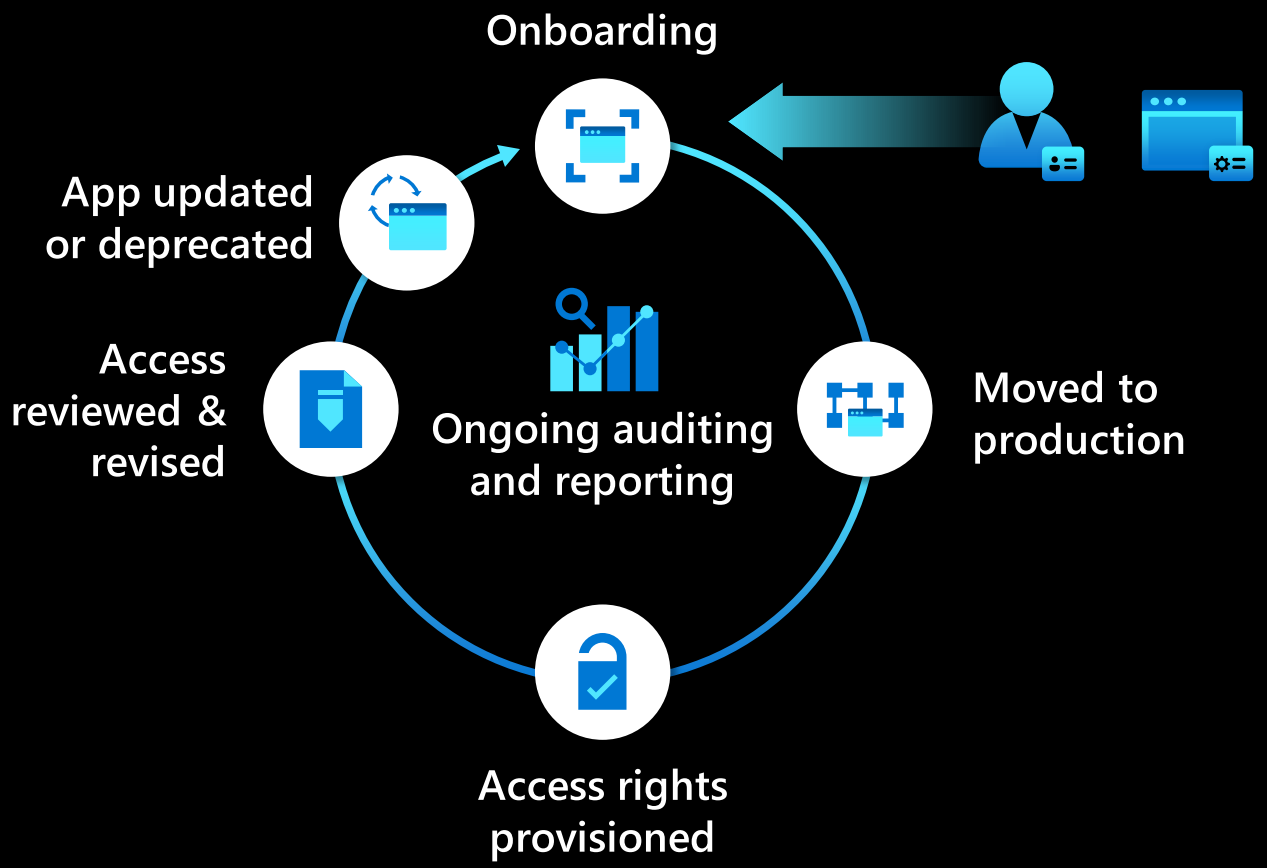

Permissions
Permissions Granted
Permissions Used
Risk
Time

Identities need governance



Identities need governance

...including workload identities



Govern your data

Unified approach

Discover

Classify

Label

Apply policy

Protect

Data loss prevention

Encryption

Access restriction

Conditional access

Govern

Archiving

Retention & deletion

Records management

Disposition reviews

Monitor

Sensitive info detection

Content explorer

Activity explorer

Audit trail

Proof of disposals

Devices

Apps

ISVs, third-party

On-premises

Cloud services

Monitoring your entitlements across everything

A Zero Trust strategy is imperative

Verify explicitly

Use least privileged access

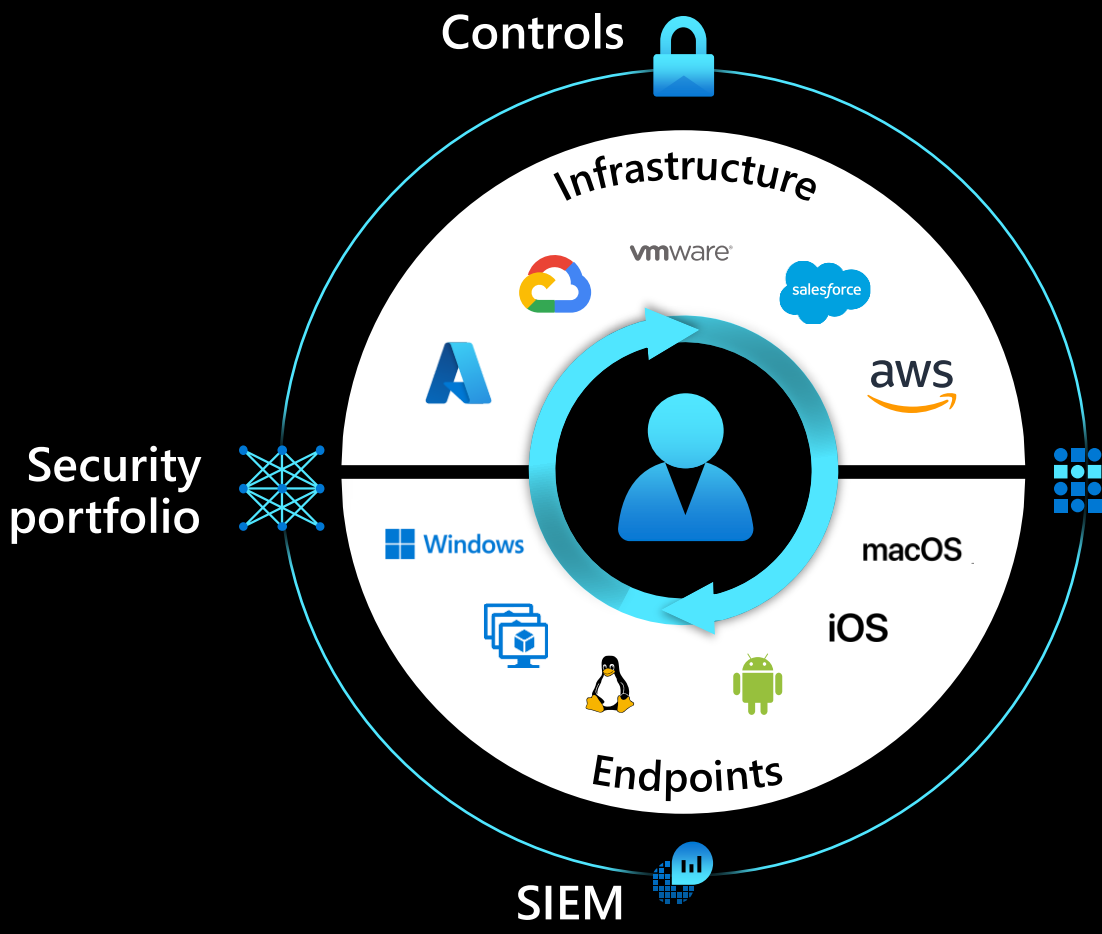
Assume breach

Verify explicitly

Use least privileged access

Assume breach

Monitor comprehensively



ML+AI detections need to adapt and evolve

Token theft

Forged SAML tokens

Workload identity attacks

Automated mitigation and remediation

Threat detection and response

Force MFA

Force password reset

Minimal access mode

Threat response playbooks

Notification

Blocking

Automation

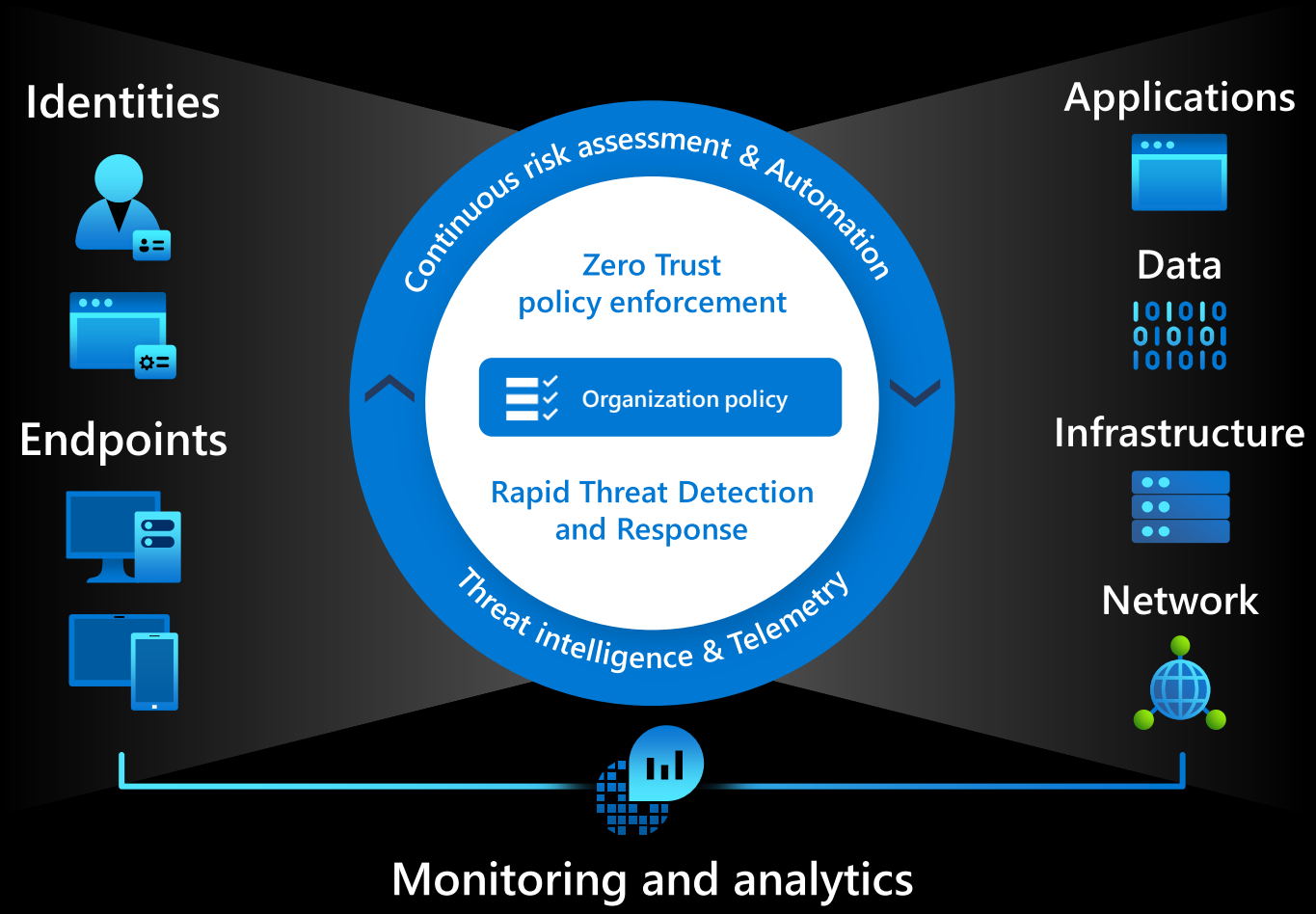
A Zero Trust strategy is imperative

Verify explicitly

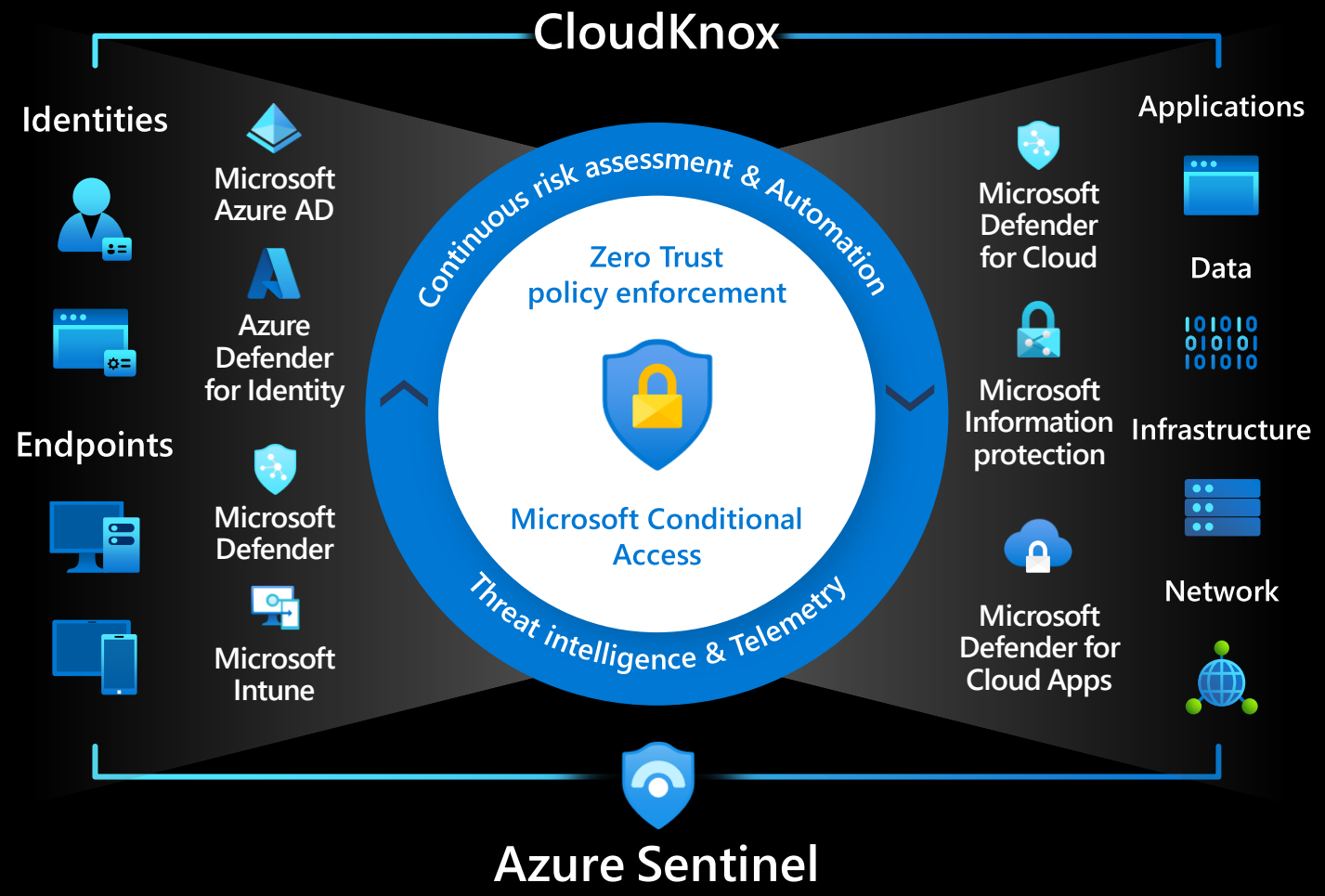
Use least privileged access

Assume breach

Zero Trust approach



Zero Trust from Microsoft



Zero Trust med Maks Produktivitet?

MVPdagen – 5 års jubileum
Fra oss til deg

Sterk Autentisering med Passordfritt

☆☆☆

Dårlig:

PASSORD

123456

picture1

abc123

111111

qwerty

★☆☆

God:

PASSORD OG ...

SMS

Stemme

★★☆

Bedre:

PASSORD OG ...

Microsoft Authenticator

★★★

Best:

PASSORDFRI

Windows Hello

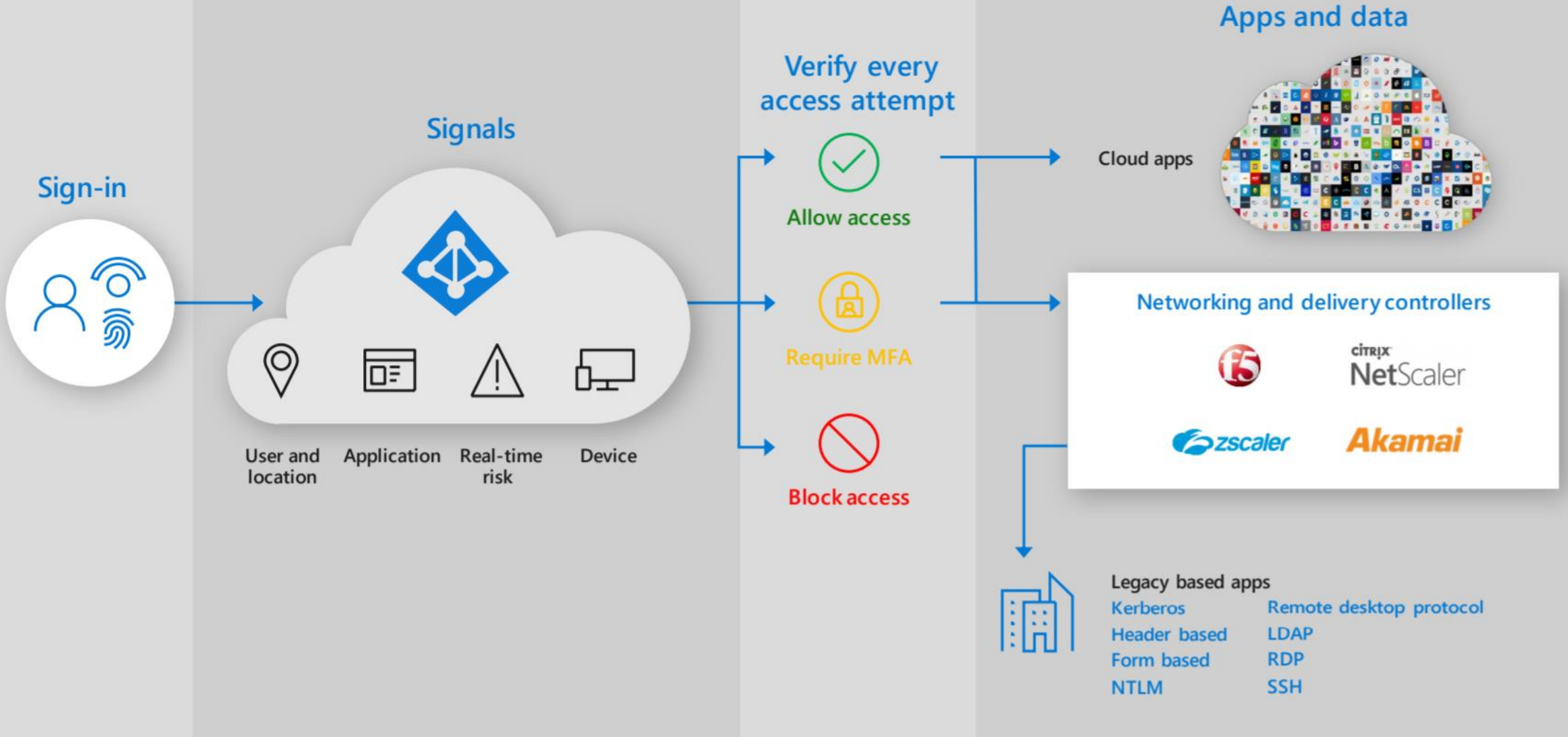
Microsoft Authenticator

Sikkerhetsnøkkel

Microsoft «reisetips» til Zero Trust

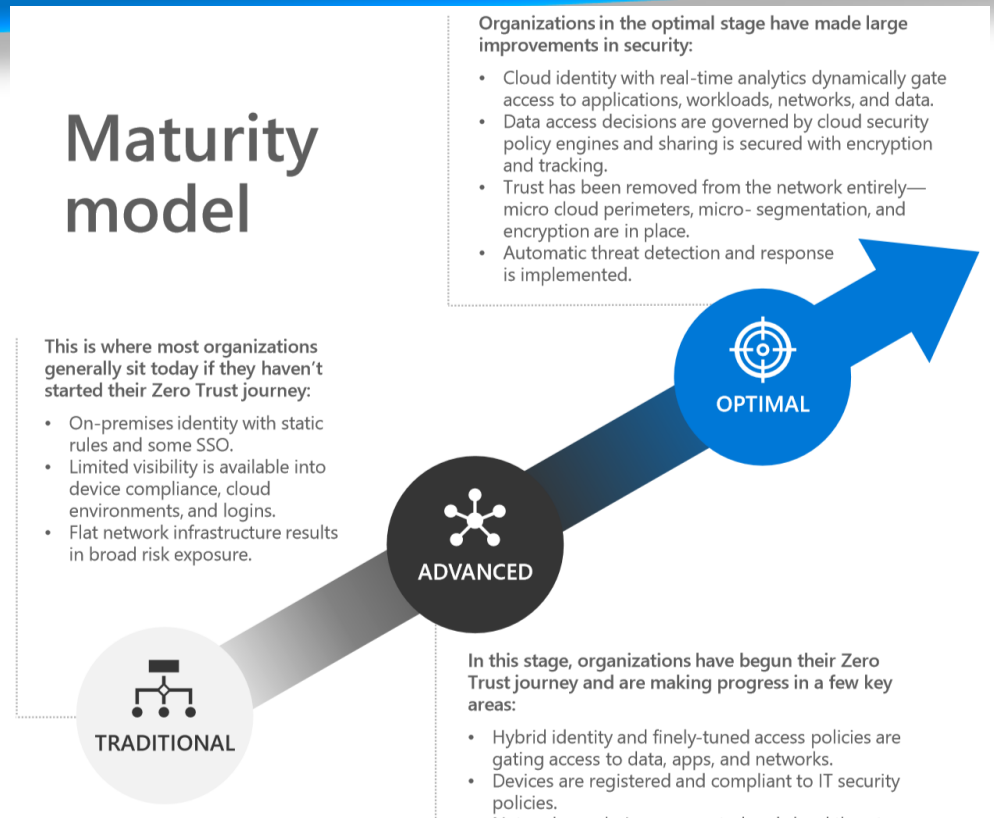
1. **Få et godt grunnlag for sikring av identitet**
2. Implementer betinget tilgang
3. Styrk legitimering av brukeren
4. Planlegg med en «dobbel» perimeter strategi
5. Integrer intelligens og analyse av aktiviteter
6. Minimer angrepsflaten
7. Øk bevissthet rundt sikkerhet
8. Etabler selvhjelp for brukeren
9. Ikke lov for mye (ikke «big bang»)
10. Synliggjør verdi på veien

Zero Trust for Datasenter via Internet



Zero Trust Modning

"Progress over Perfection"



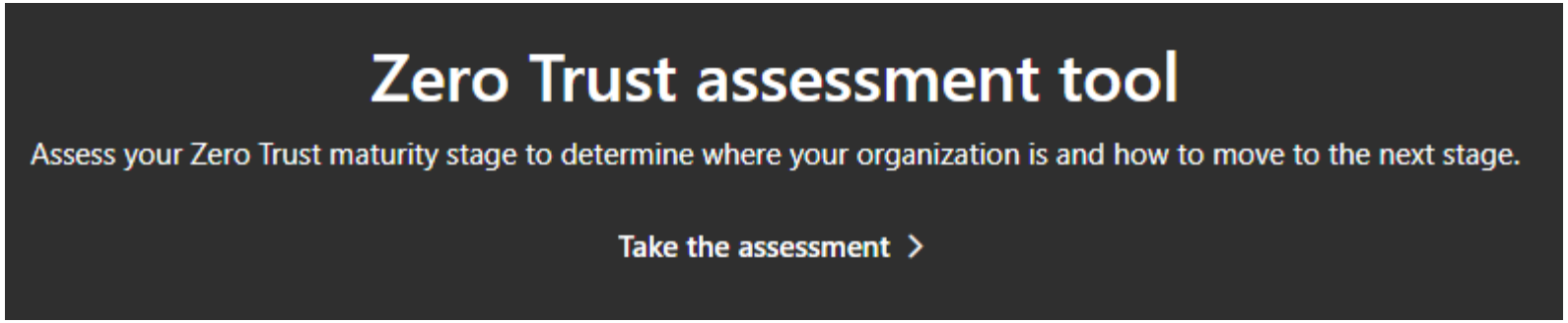
	Traditional	Advanced	Optimal
Identities	On-premises identity provider is in use No SSO is present between cloud and on-premises apps Visibility into identity risk is very limited	Cloud identity federates with on-premises system Conditional access policies gate access and provide remediation actions Analytics improve visibility	Passwordless authentication is enabled User, device, location, and behavior is analyzed in real time to determine risk and deliver ongoing protection
Devices	Devices are domain joined and managed with solutions like Group Policy Object or Config Manager Devices are required to be on network to access data	Devices are registered with cloud identity provider Access only granted to cloud managed & compliant devices DLP policies are enforced for BYO and corporate devices	Endpoint threat detection is used to monitor device risk Access control is gated on device risk for both corporate and BYO devices
Apps	On-premises apps are accessed through physical networks or VPN Some critical cloud apps are accessible to users	On-premises apps are internet-facing and cloud apps are configured with SSO Cloud Shadow IT risk is assessed; critical apps are monitored and controlled	All apps are available using least privilege access with continuous verification Dynamic control is in place for all apps with in-session monitoring and response
Infrastructure	Permissions are managed manually across environments Configuration management of VMs and servers on which workloads are running	Workloads are monitored and alerted for abnormal behavior Every workload is assigned app identity Human access to resources requires Just-In-Time	Unauthorized deployments are blocked and alert is triggered Granular visibility and access control are available across all workloads User and resource access is segmented for each workload
Network	Few network security perimeters and flat open network Minimal threat protection and static traffic filtering Internal traffic is not encrypted	Many ingress/egress cloud micro-perimeters with some micro-segmentation Cloud native filtering and protection for known threats User to app internal traffic is encrypted	Fully distributed ingress/egress cloud micro-perimeters and deeper micro-segmentation ML-based threat protection and filtering with context-based signals All traffic is encrypted
Data	Access is governed by perimeter control, not data sensitivity Sensitivity labels are applied manually, with inconsistent data classification	Data is classified and labeled via regex/keyword methods Access decisions are governed by encryption	Classification is augmented by smart machine learning models Access decisions are governed by a cloud security policy engine DLP policies secure sharing with encryption and tracking

https://aka.ms/Zero-Trust-Vision

MVPDAGEN

Zero Trust Assessment

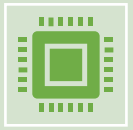
- Sjekk selv hvor du er på Zero Trust reisen
- https://aka.ms/ZeroTrust



Start på veien til “Zero Trust”

Beskytt Identitet

Passwordless! og Sterk Autentisering (Conditional Access & Risk)

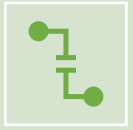


Én felles Identitet

Azure AD SSO

SaaS

Cloud & On-Premises Apps (Leveranseplattform)



Implementer Zero Trust tankesett

“Alt” er på Internett

Verifiser alltid, bruk minst privilegert tilgang, anta brudd.

Beskytt data

Evolusjon (Progress) over Revolusjon (Perfection)

Bli med i vår Power Apps-konkurranse!

Hva med en app for parkering- eller hyttebooking? Eller hva med en app som varsler alle i salgsavdelingen når er ny avtale har blitt signert? Bli med i vår konkurranse og få sjansen til å vinne din egen Power App – ferdig utviklet og publisert! Alt du trenger å gjøre er å sende inn ditt forslag til hvilken app du ønsker deg. Vi tar hånd om resten!

VINNEREN ANNONSERES 15. DESEMBER 2021