
VELKOMMEN
Webinaret om Cybersikkerhed
starter om et øjeblik
timengo.
PULS
24. november 2020 – Cybersikkerhed

Godt at vide

Webinaret bliver optaget.

Præsentation og optagelsen deles med jer efterfølgende.

Spørgsmål skrives i chatten.

timengo.
enter the cloud

Program

09.10 Effektiv cybersikkerhed nu og i fremtiden

09.40 Når cloud skaber sikkerhed og tillid

10.00 Cybersikkerhed ud fra et zero-trust princip

10.45 Konstant opdateret cyberforsvar – som en service

11.00 Opsamling og anbefalinger til dit “næste skridt”

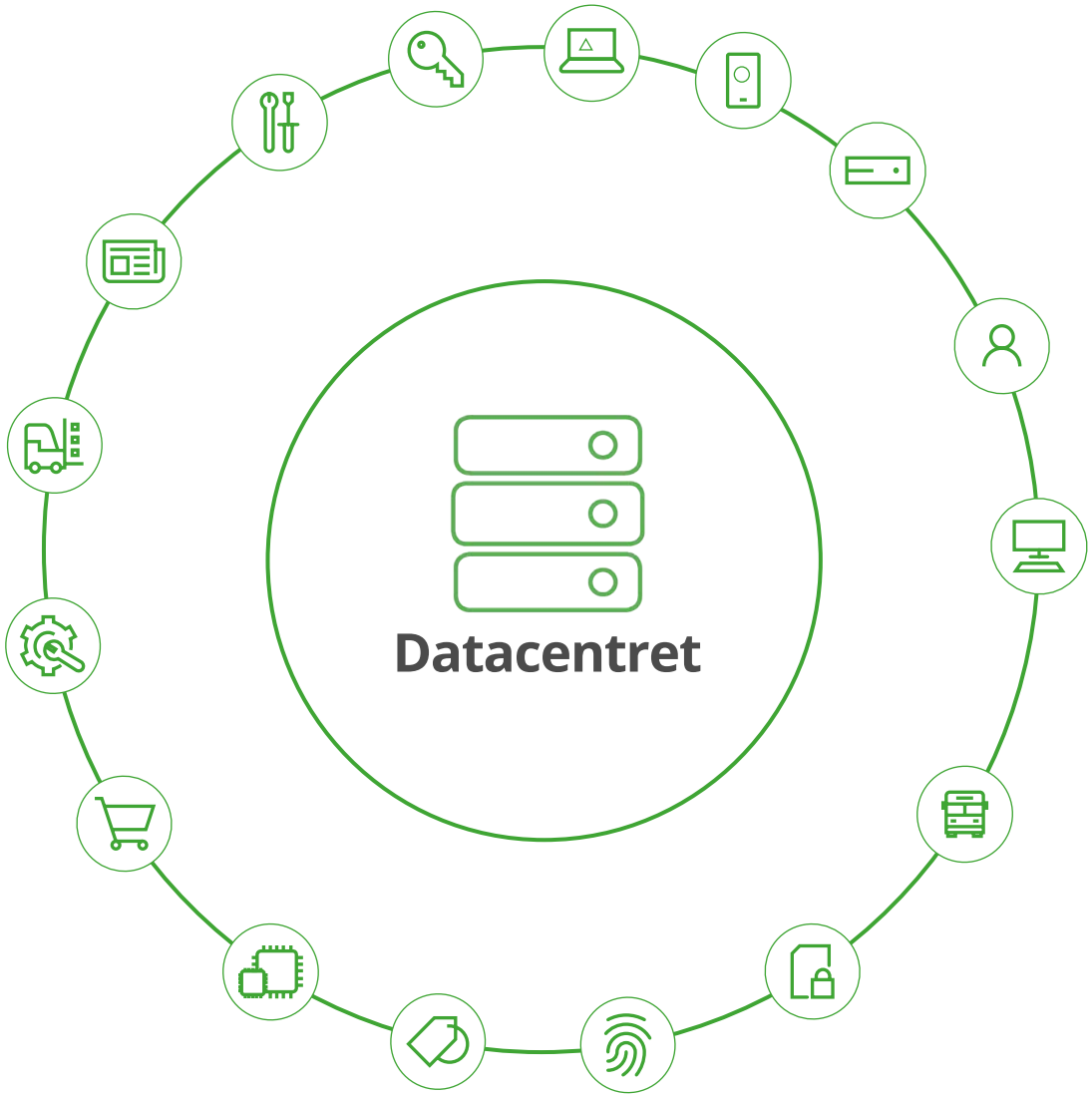
Effektiv cybersikkerhed nu og i fremtiden

Martin Lundsgaard,
Partner og CTO i timengo

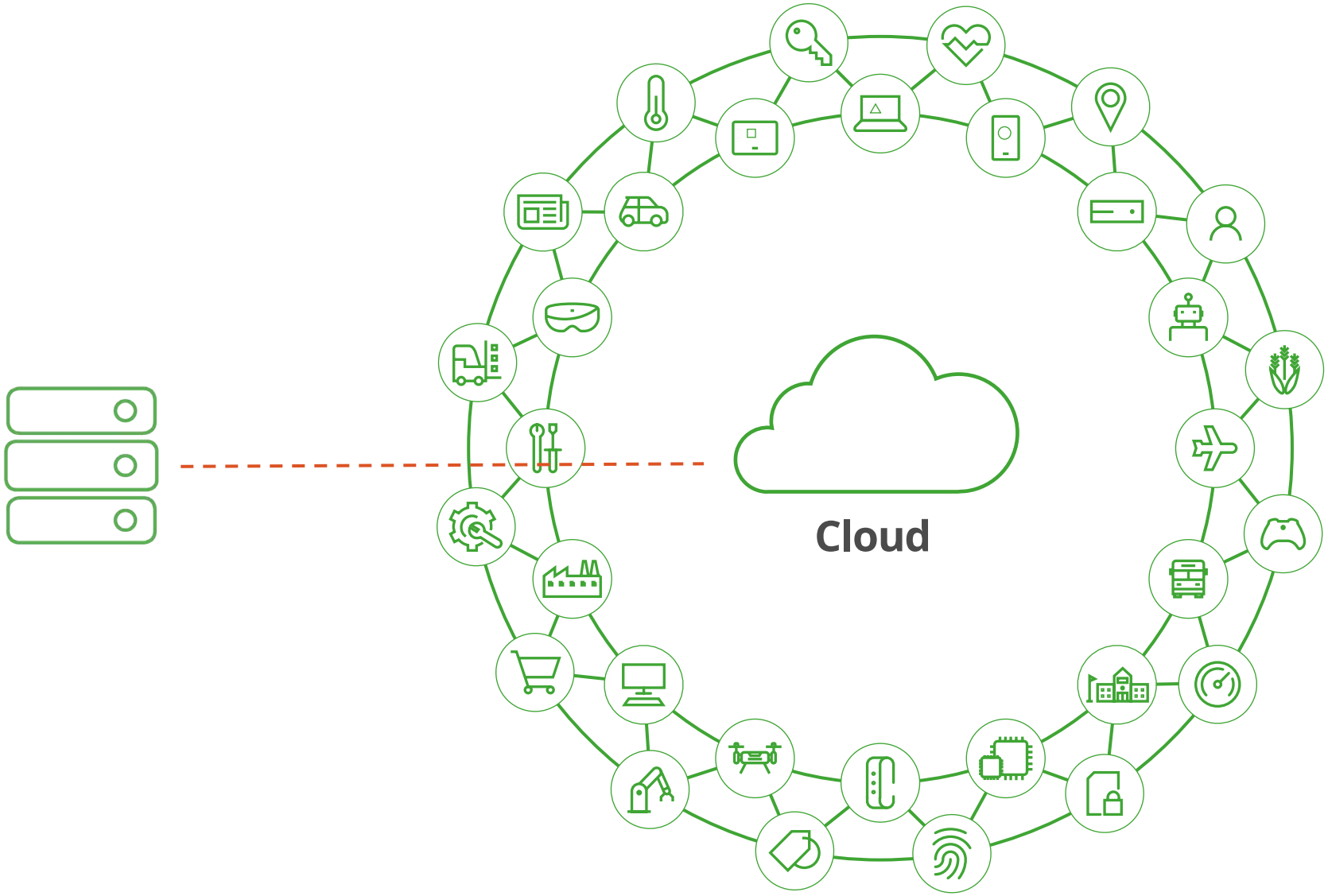
timengo.
enter the cloud

Sikkerhed I en digital verden

Internettet



timengo.
enter the cloud



timengo.
enter the cloud

Udfordringerne i en Zero Trust verden

Identitetsbaserede angreb er steget med >800% siden 2018

Information er det mest attraktive mål for angreb

96% af alt malware er bygget til at ændre sig selv konstant

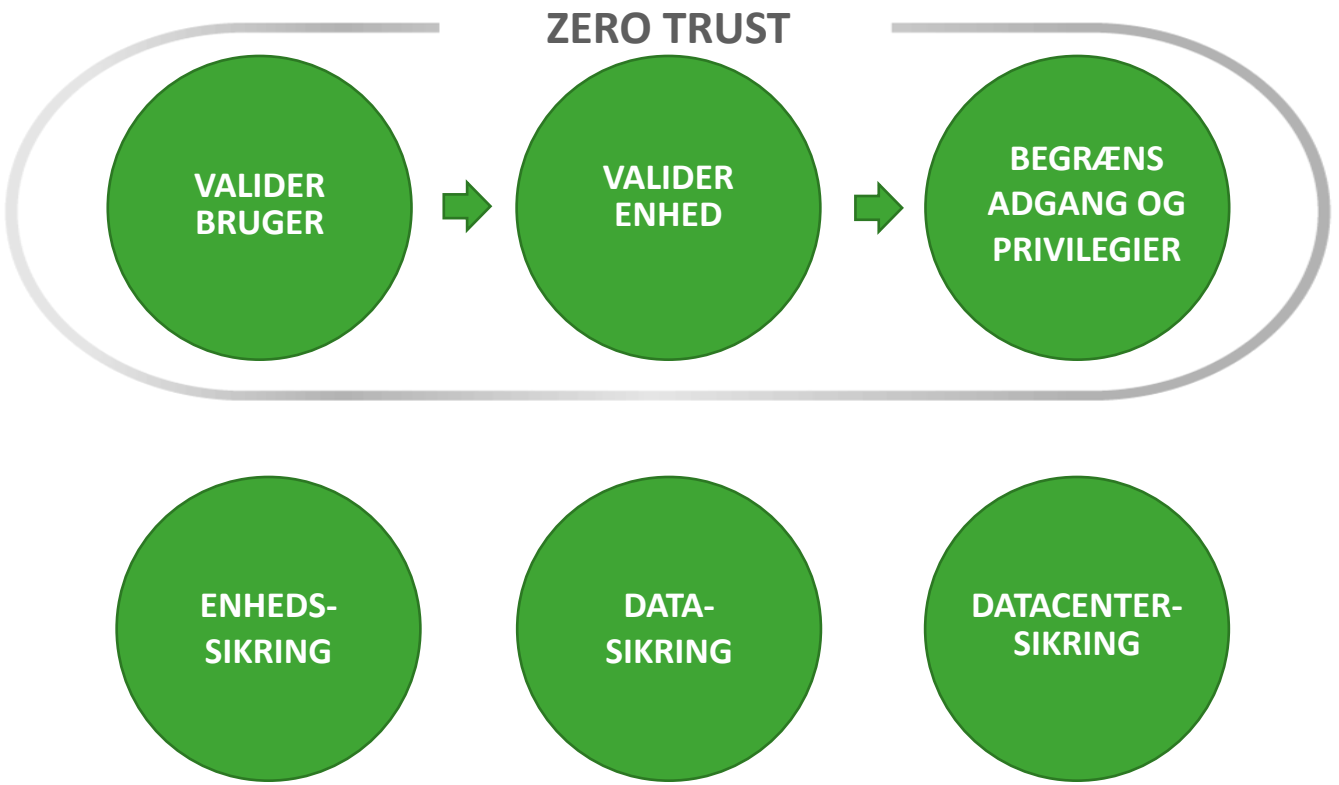
Firmaer bruger i gennemsnit 34 forskellige IT sikkerhedsløsninger

Udfordringer

Løsninger

Identitetsbaserede angreb er steget med >300% I 2018	Benyt identitetsbaseret beskyttelse
Information er det mest attraktive mål for angreb	Beskyttelse skal følge data
96% af alt malware er bygget til at ændre sig selv konstant	Opdag angreb hurtigt, reagér automatisk og beskyt enheder
Firmaer bruger i gennemsnit 34 forskellige IT sikkerhedsløsninger	Højeste sikkerhed = svageste led – Brug få integrerede løsninger

Essensen i Zero Trust og cybersikkerhed



timengo.
enter the cloud

timengo.
enter the cloud

Våbenkapløbet
anno 2020

"På 1 måned i 2019 introduceres der flere nye cyberangrebsmetoder, end der gjorde tilsammen fra 2014 til 2017"

Cyber angreb er big business. Et ukendt hul i ex Windows har en markedsværdi på ca.
1 mia DKK.

Microsoft365 er den platform, som flest angreb rettes mod.

Hjemmearbejde har acceleret cyberkriminalitet eksponentielt

Hvis William Demant og Mærsk kan blive ramt…..

42.8%

Af alle phishing angreb er baseret på et Microsoft document format.

30 %+

af alle PC'ere I danske virksomheder er ikke beskyttet mod kendte huller (exploits).

667%

Stigning i angreb på én måned af Covid 19 pandemien.

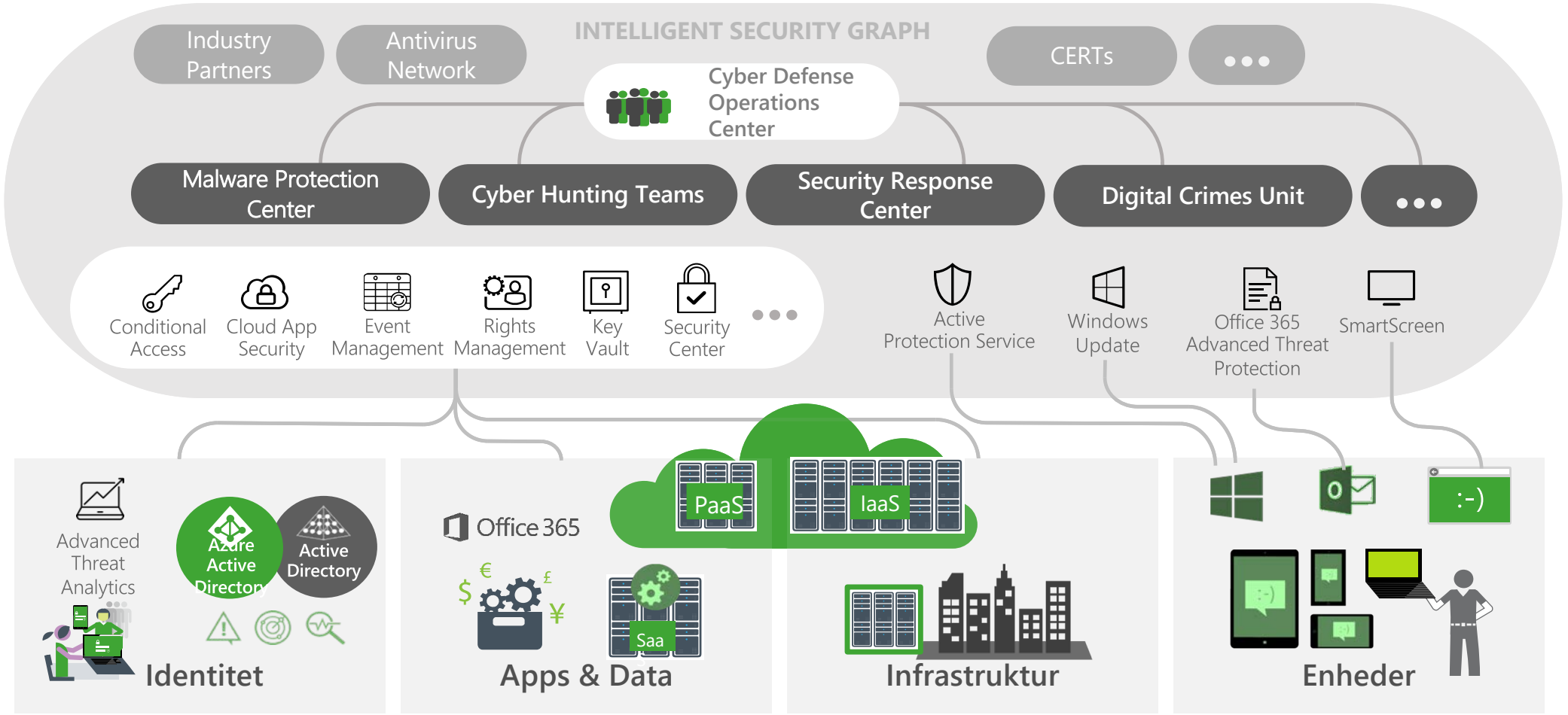
€26.2 mia

I realiserede tab (EU 2019), direkte relateret til email baserede angreb af virksomheder.

Hvad kan den enkelte virksomhed gøre ved det?

Viden
tid
økonomi

Hvad gør Microsoft ved det i skyen ?



M365 Ex kunder udnytter typisk <20% af sikkerheden

Det store paradoks

75% af sikkerheden udnyttes ikke

Microsoft har taget udfordringen op, og bygget cloud platforme, der kan levere en meget komplet løsning på cybersikkerhed og Zero Trust udfordringerne.

Der indgår hundredvis af sikkerhedsteknologier, fra Windows 10 til Azure, til globale sikkerheds AI'er. De skal dog designes og konfigureres rigtigt, og i sammenhæng før virksomheder kan realisere værdien af dem.

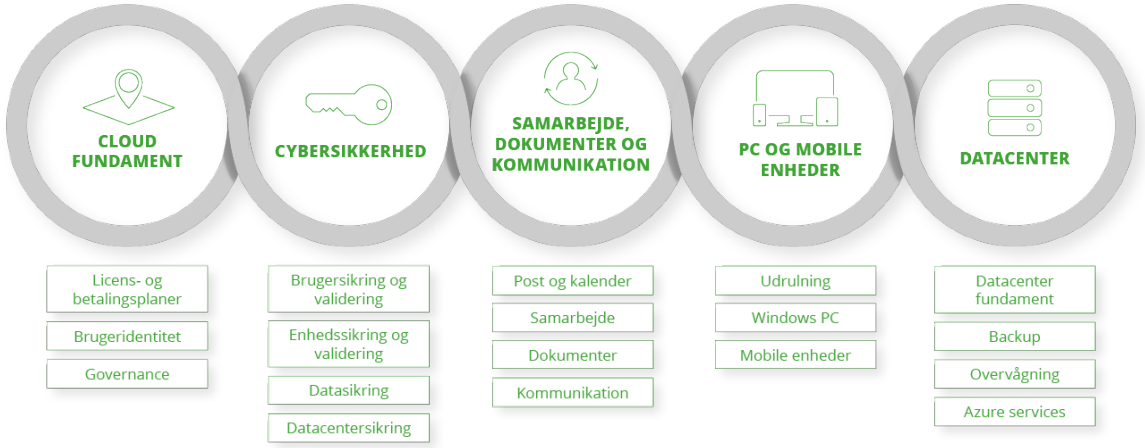
timengo's mission er at levere én samlet Cloud Platform, der effektivt og økonomisk realiserer den fulde værdi af Microsoft cloud hos vores kunder.

timengo.
enter the cloud

timengo's tilgang til cloud

Mere end 40.000 timers implementering, udvikling og metoder, puttet på flaske, så vores kunder kan komme på den samlede Microsoft Cloud Platform sikkert og effektivt

- Sæt de 3000 flueben rigtigt
- Sikkerhed & sammenhæng
- Effektiv implementering
- Integreret med Jeres IT platform
- Fundament for Cloud Innovation



timengo.
enter the cloud

Udnyt MS cloud sikkerhed – og hold den løbende opdateret

CYBERSECURITY PLATFORM

Cyber Security Roadmap
- It-sikkerhedsbehov kortlægges
- Opsummerende rapport
- Prioriteter og anbefalinger

Konfiguration og implementering
- Brugersikring og validering
- Enhedssikring og validering
- Datasikring
- Datacentersikring
- Implementering og konfig. af Secure Score

CYBERSECURITY ADVISOR

Løbende sikkerhedsbulletiner
- I skal ikke følge med i alt hvad der kommer fra Microsoft
- Dækker: Windows 10, EMS, Office365 og Azure

Anbefalinger
- Hvad skal I konkret gøre for at holde platformen opdateret
  - Brugersikring og validering
  - Enhedssikring og validering
  - Datasikring
  - Datacentersikring

Færdiglavede opdateringer til Jeres M365/Azure platform
- Konfigurationer der kan importeres direkte i Jeres cloud platform

timengo.
enter the cloud

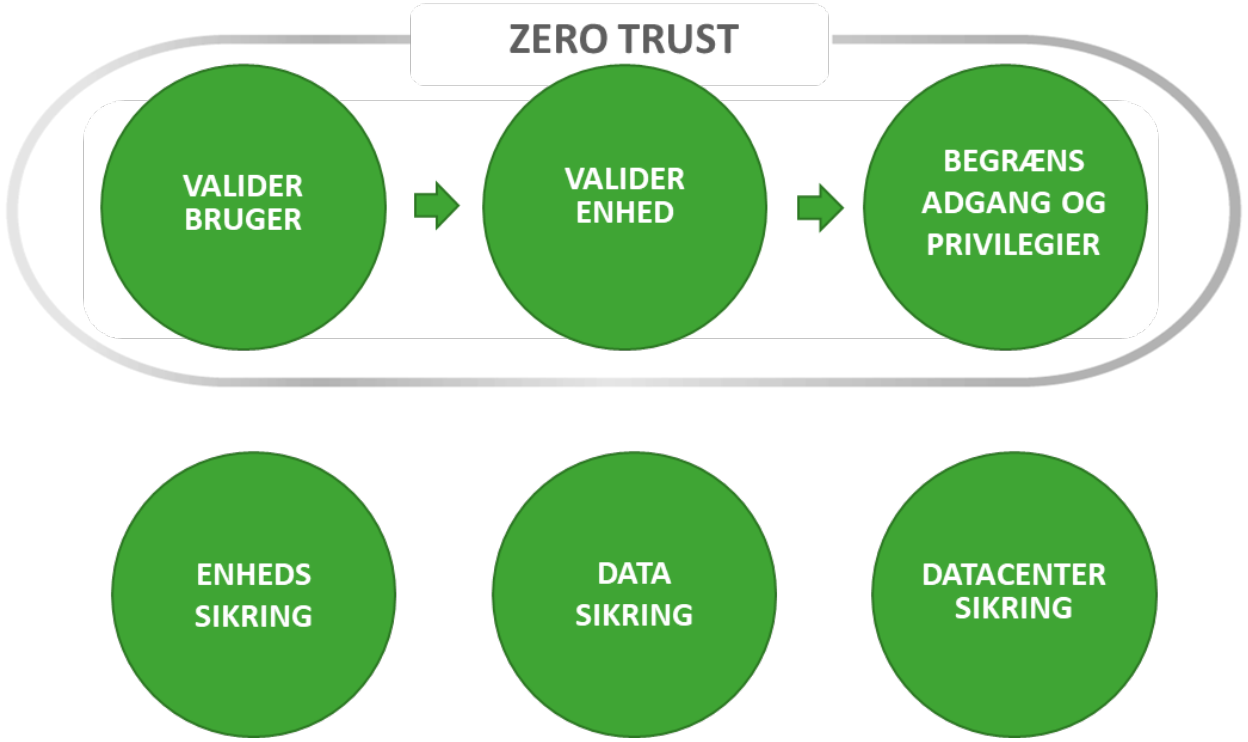
Cybersikkerhed ud fra et zero-trust princip

Kristian Berggren,
Principal Cloud Konsulent i timengo

timengo.
enter the cloud

Cloud Cybersikkerhed

Baseret på zero trust



Phishing

- Hvorfor er det et problem
- Hvordan gør angriberen
- Hvordan kan det se ud for brugeren
- Hvad er slut resultatet?
- Hvordan kan timengo Cloud Platform være med til at beskytte jeres brugere

Hvor stort er Phishing i 2019 – 2020?

Its big business – 2019 tab er estimeret til 26.2 Milliarder €

2 ud af 3 phishing sites bruger nu HTTPS

Flere PaaS sites derude

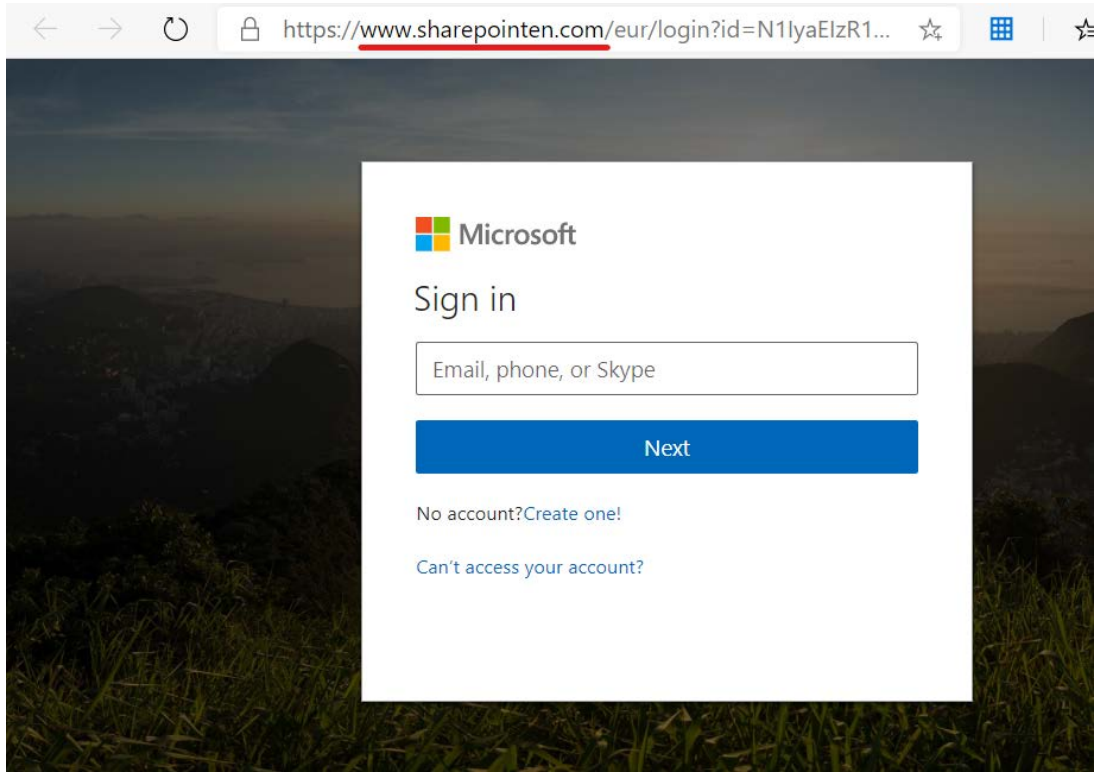
667% flere phishing kampagner under Covid19 på bare en måned

https://www.enisa.europa.eu/publications/phishing

Phishing - Angriber

Identitets eksempel: Credential harvest

- Opretter side til login der afspejler Microsoft 365 login page
- Sender mails til slutbrugeren med link til siden

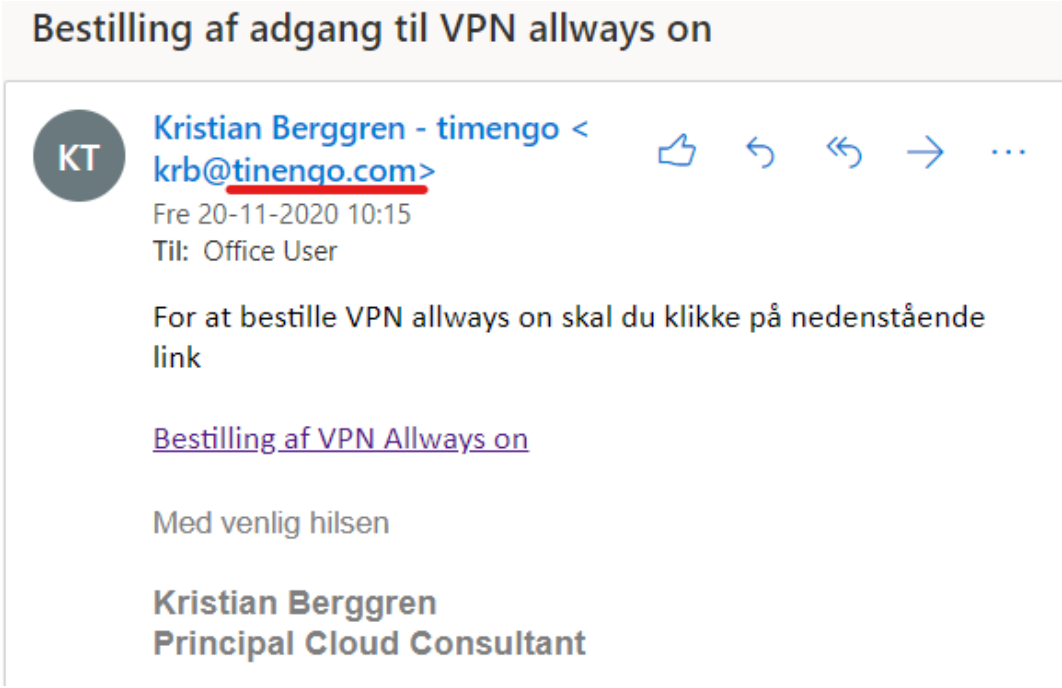


timengo.
enter the cloud

Phishing - Slutbrugeren

Identitets eksempel: Credential harvest

- Modtager klikker på link
- Taster brugernavn og kode i login feltet



timengo.
enter the cloud

Phishing – Hvad så nu?

Credential harvest - Endgame

- Adgang til data som brugeren har adgang til
  - Kontakter
  - Filer
  - Sites
  - Systemer
    - VPN ? Med tilhørende adgang til onprem

Phishing – Hvordan stopper vi det?

Conditional Access	• Block Legacy Authentication • Enable MFA • Block Downloads sammen med Cloud App Security
Identity Protection	• Risk based Remidiations • Forced Password change
Defender for Office 365	• Safe Links • Safe Attachments • AntiPhishing
Defender for Endpoint	• SmartScreen filter • Endpoint detection and response (EDR) in block mode

Conditional Access

Block Legacy Authenticaton

- Blokerer IMAP, POP3 og SMTP adgang
- Tvinger MFA igennem

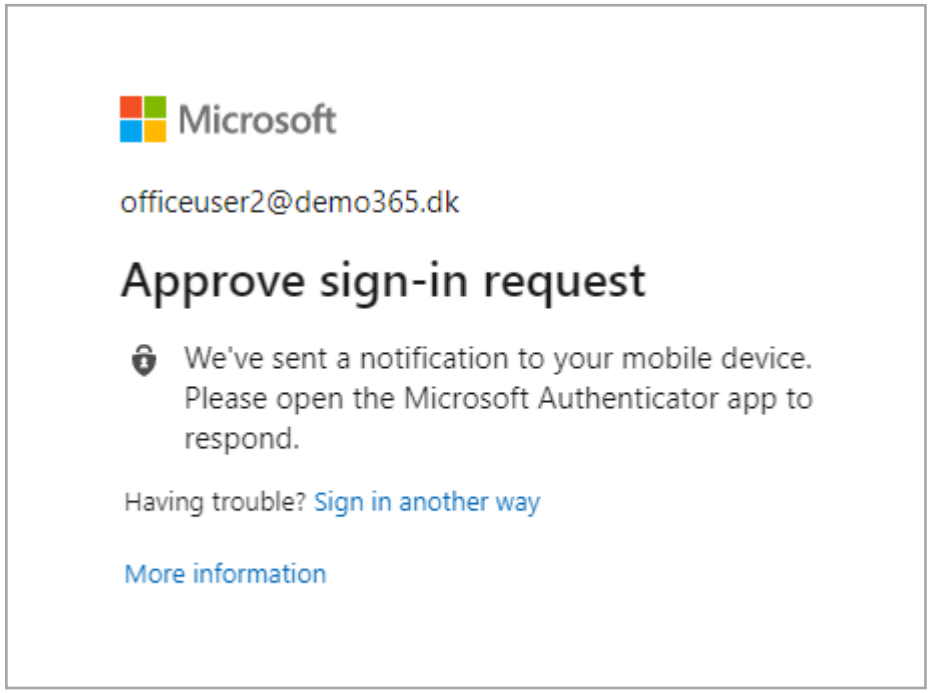
MFA logon prompt

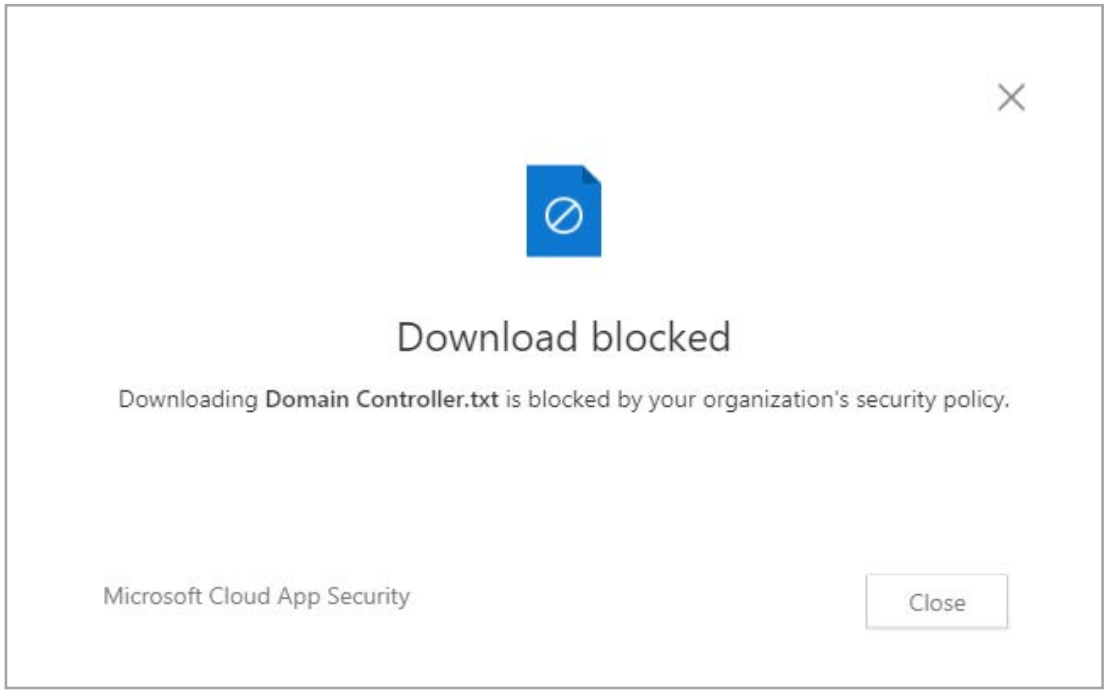
- Sikrer en ekstra validering af brugeren

Block Downloads

- Kombineres med logins fra ukendte enheder

Conditional Access & Cloud App Security
MFA og Block Downloads





timengo.
enter the cloud

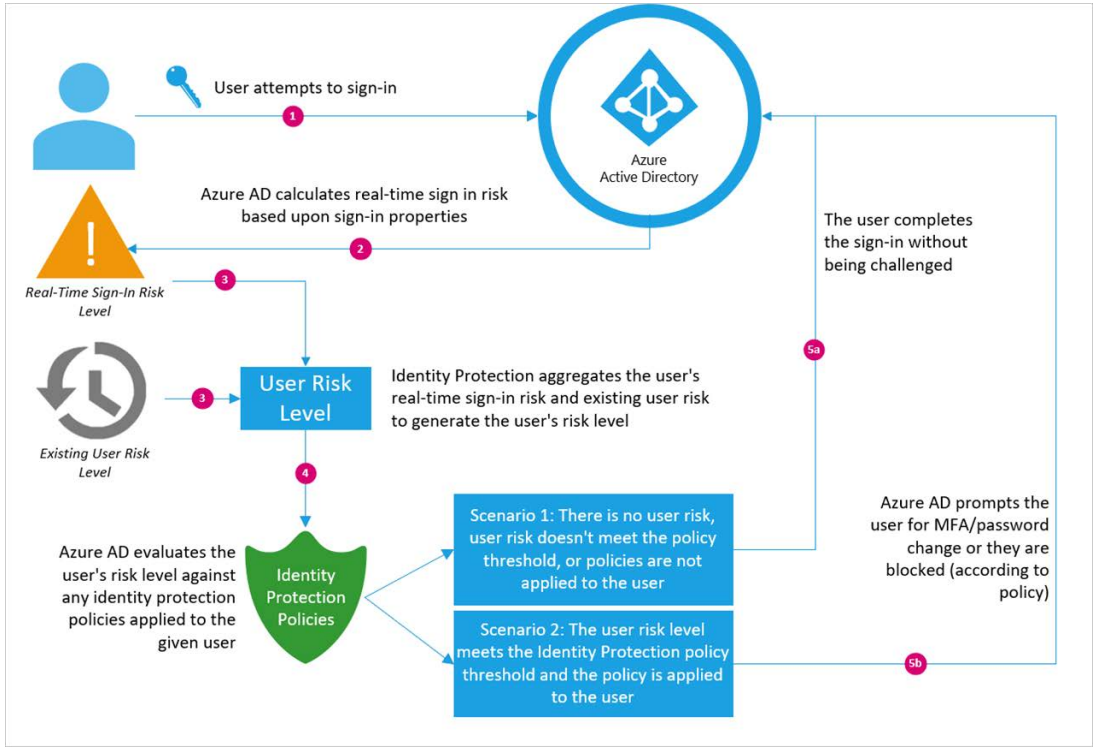
Azure Identity Protection

Real Time Sign in risk

- Travel time
- Unfamiliar locations
- Low reputation locations

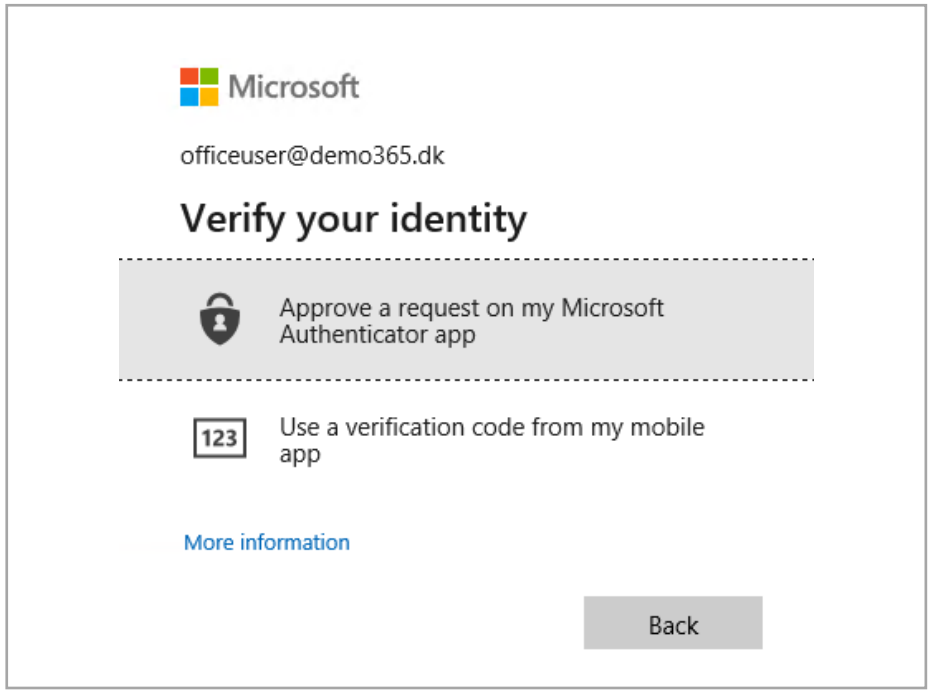
Risk Policies

- Medium Risk - Require MFA
- High Risk (Credential Theft)
  - Require MFA
  - And Require Password Change
  - Or
  - Block user



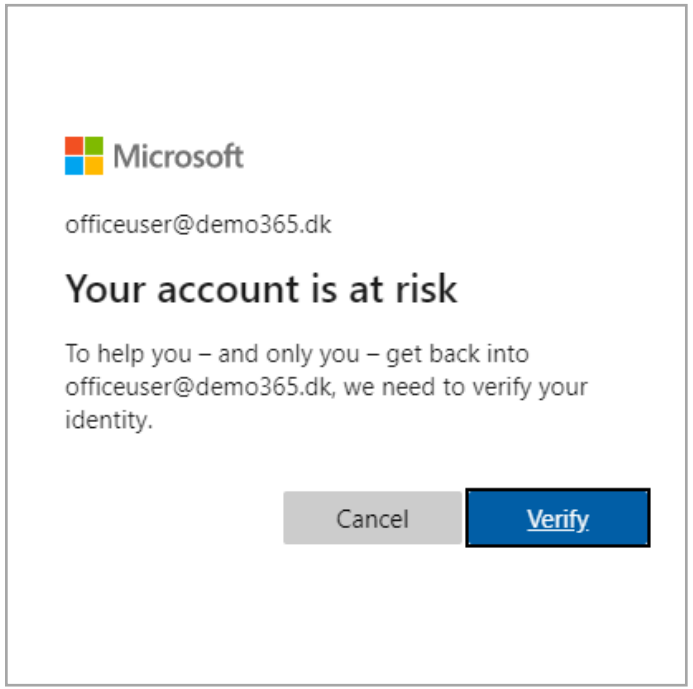
timengo.
enter the cloud

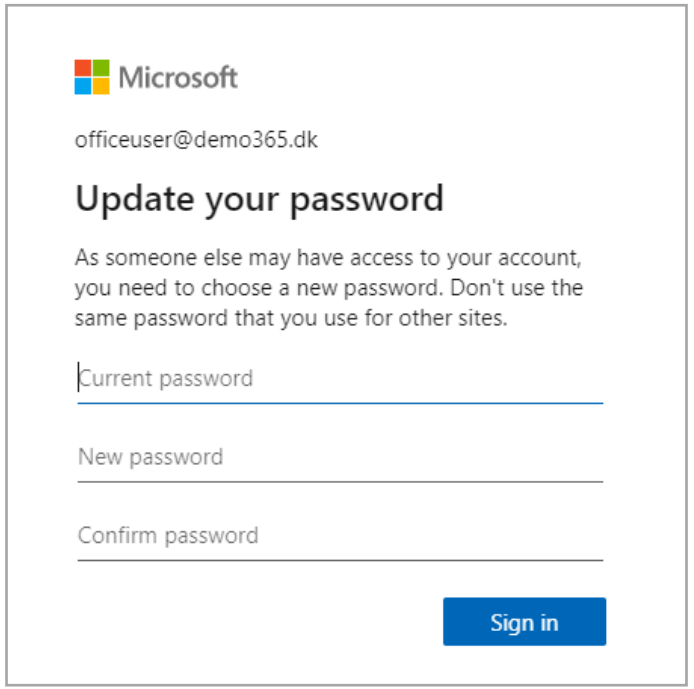
Azure Identity Protection – User experience Low to Medium Risk



timengo.
enter the cloud

Azure Identity Protection – User experience High Risk – Autoremidiation

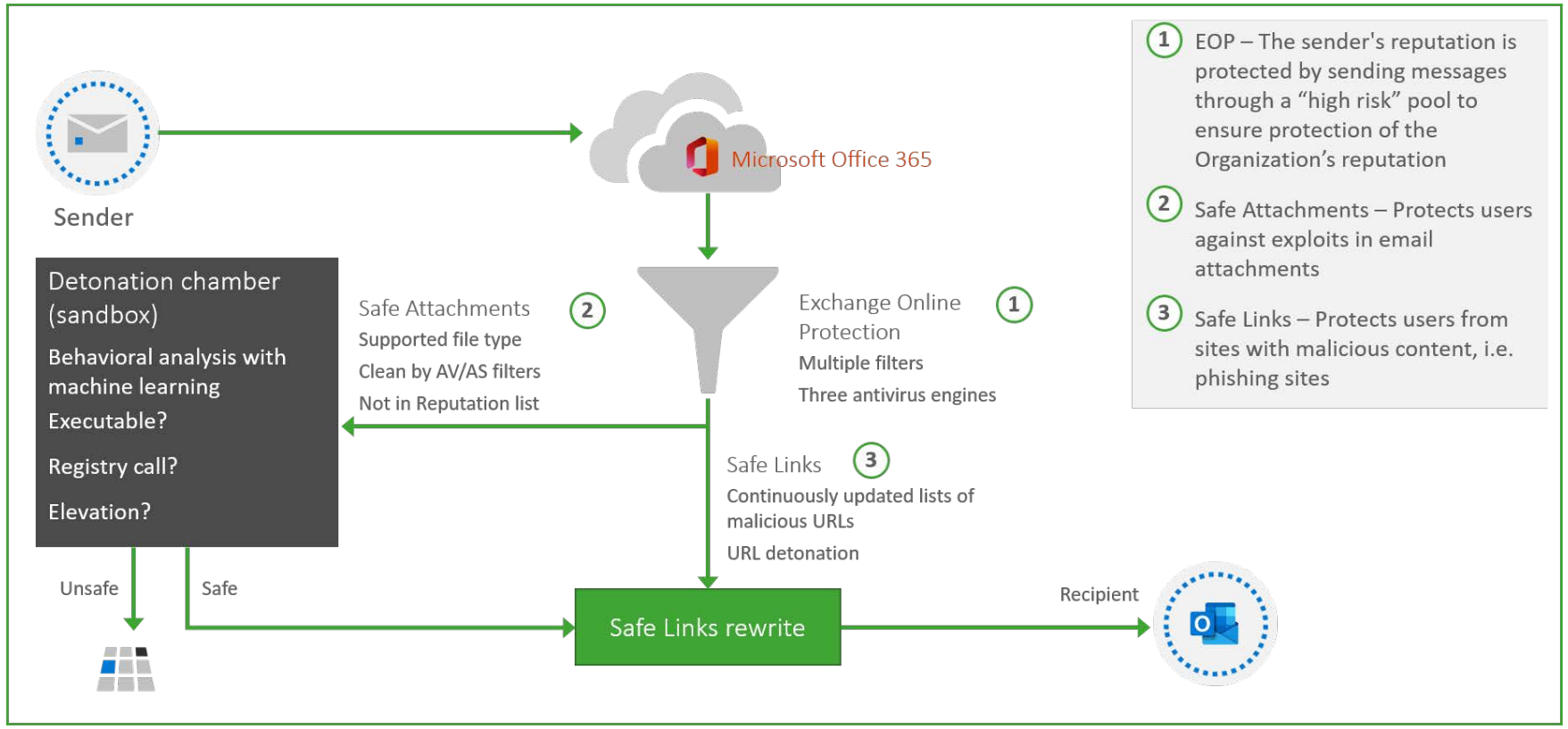




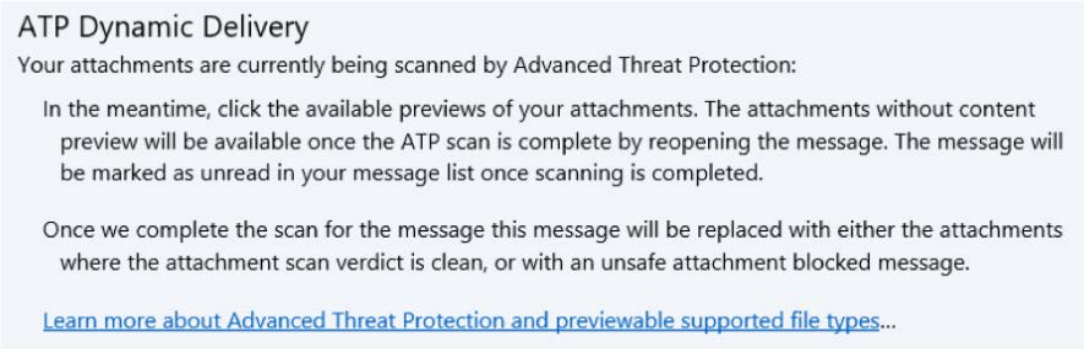
timengo.
enter the cloud

Azure Identity Protection – User experience
High Risk – Block User

Defender for Office 365
Safe Links og Safe Attachments



Safe Attachments & Safe Links



Safe link

https://techcommunity.microsoft.com/t5/microsoft-defender-for-endpoint/bg-p/MicrosoftDefenderATPBlog

https://eur01.safelinks.protection.outlook.com/?url=https%3A%2F%2Ftechcommunity.microsoft.com%2Ft5%2Fmicrosoft-defender-for-endpoint%2Fbg-p%2FMicrosoftDefenderATPBlog&data=04%7C01%7Ckrb%40timengo.com%7C6431aa6d3aa14c99b48f08d88d5e971c%7C3f55c8ce644d4062afc9998ae72a282a%7C1%7C0%7C637414784889703926%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=FWlslGzuL%2F9LF3tzaJndV3iYTriCQH0H4WyoajfqXIM%3D&reserved=0

timengo.
enter the cloud

Anti Phishing

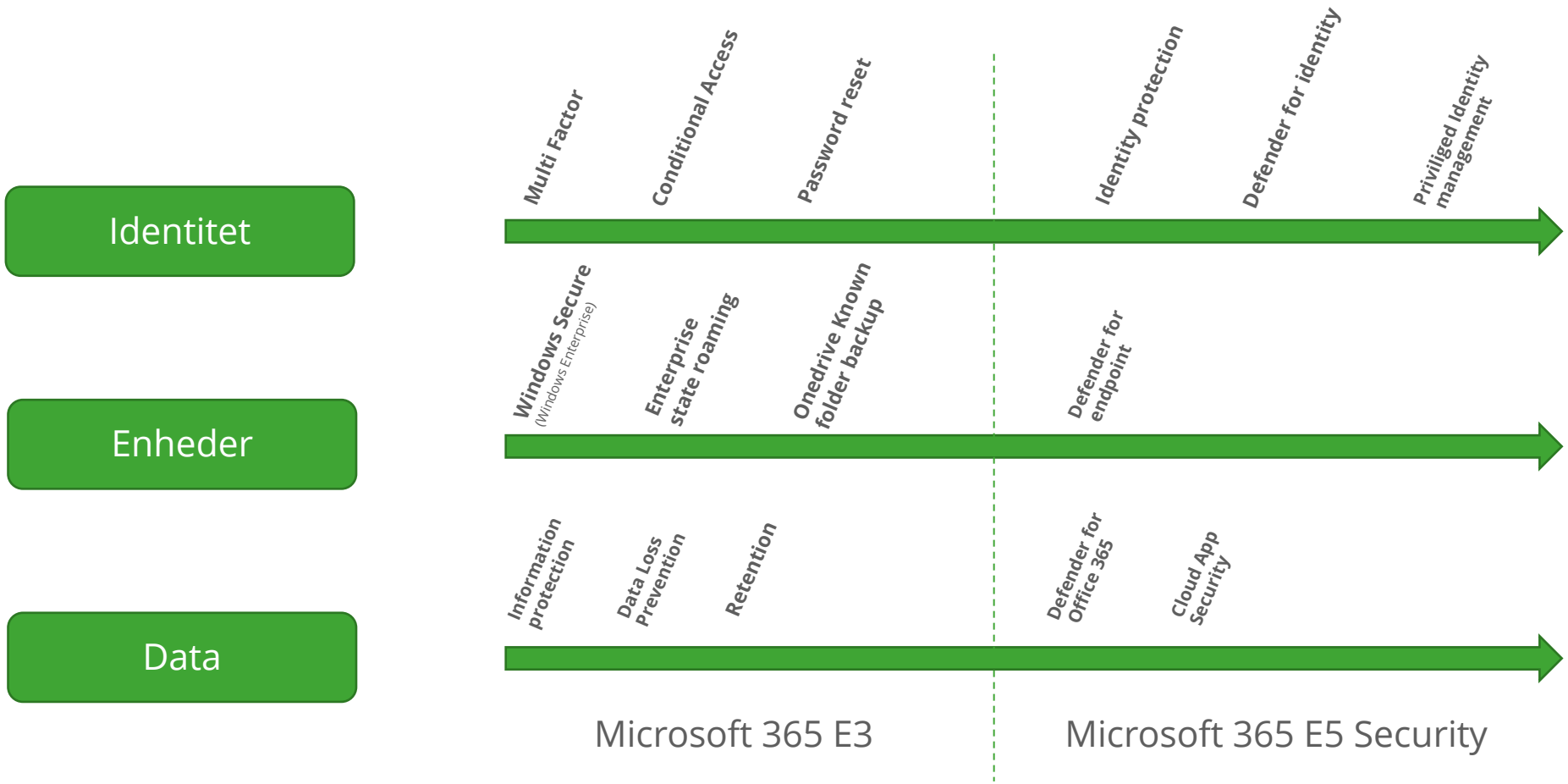
Beskytter mod

- Impersonated users / domains
- Ekstra beskyttede brugere
    - CEO = Glenn Nørgaard – timengo
    - CEO Email = gn@timengo.com
- User Recieves mail
    - From = gn@bingo.com
    - Navn = Glenn Nørgaard
    - Action = Quarentine e-mail

Er det svært?

Demo

Attack and Defence vectors



timengo.
enter the cloud

Konstant opdateret cyberforsvar – som en service

Morten Grundtvig, Principal Cloud Advisor i timengo

timengo.
enter the cloud

timengo cyber-sikkerheds advisory service

Industri anbefalinger

timengo erfaringer

timengo WindowsSecure

Microsoft 365 SecureScore

Defender for Endpoint

Security Baseline

timengo cyber-sikkerheds advisory service

Formålet med timengo cyber-sikkerheds advisory service er at sætter virksomheden i stand til at løbende opretholde et højt sikkerhedsniveau baseret på timengo reference arkitektur. Der vil løbende komme advisories for at vedligeholde sikkerhedsniveauet og udnytte timengo og Microsofts sikkerheds anbefalinger optimalt.

timengo cyber-sikkerheds anbefalinger

Anbefalinger til Microsoft 365 SecureScore og Defender for Endpoints

Sikkerheds advisories

Anbefalinger til konfigurations indstillinger og automatiseringer med, Endpoint Manager og powershell

timengo cyber-sikkerhed

Overordnet anbefalinger

Brugersikring og validering

Multi-Factor, Conditional access. For hjælp til at beskytte, sikkerhedsovervåge og rapportere baseret på brugerens login til platformen med en ekstra validering (App, SMS eller opringning). Med Conditional Access kan det gøre betinget af det scenarie brugeren befinder sig i (Placering, enhed, compliance etc.)

Selfservice Password Reset. For nemt og sikkert brugerdrevet skift af password, samt integration med Identity protection.

Identity protection og Defender for Identity. For Avanceret AI bruger sikkerhed og identificering af mistænkelig brugeradfærd på AD og AAD.

Enhedssikring og validering

WindowsSecure. For sikring af arbejdspladser ud fra tre niveauer. Følger desuden vigtige anbefalinger fra SecureScore og Defender for Endpoint

Enterprise State Roaming. For sikker synkronisering af bruger og program indstillinger. Gælder indstillinger såsom, temaer, browser, passwords og sprog etc.

OneDrive known folder backup. For at sikre der tages backup af dokumenter, billeder og desktop fra den lokale PC

Defender for Endpoint. For avanceret beskyttelse af arbejdspladser inklusiv web beskyttelse (voksent indhold etc).

Datasikring

Information Protection. For sikring af data uanset hvor data befinder sig

Data Loss Prevention. Forbygger utilsigtet handlinger, der tages ved arbejde med følsomme data og forhindre utilsigtet, tab, brug og offentliggørelse af dem.

Retention. Sikre virksomhedens livscyklus for e-mail og dokumenter ved at opbevare indhold og fjerne indhold når det ikke længere er nødvendigt eller kræves slettet.

Cloud App Security. For omfattende synlighed, kontrol og forbedret beskyttelse af virksomhedens data i cloud applikationer. Identificere over 13.000 apps fra alle enheder - og få risikovurderinger og løbende analyser.

Defender for Office 365. For at beskytte e-mail og dokumenter mod malware-angreb og forhindrer brugerne i at få adgang til skadelige vedhæftede filer eller farlige websteder via links.

Cloud fundament

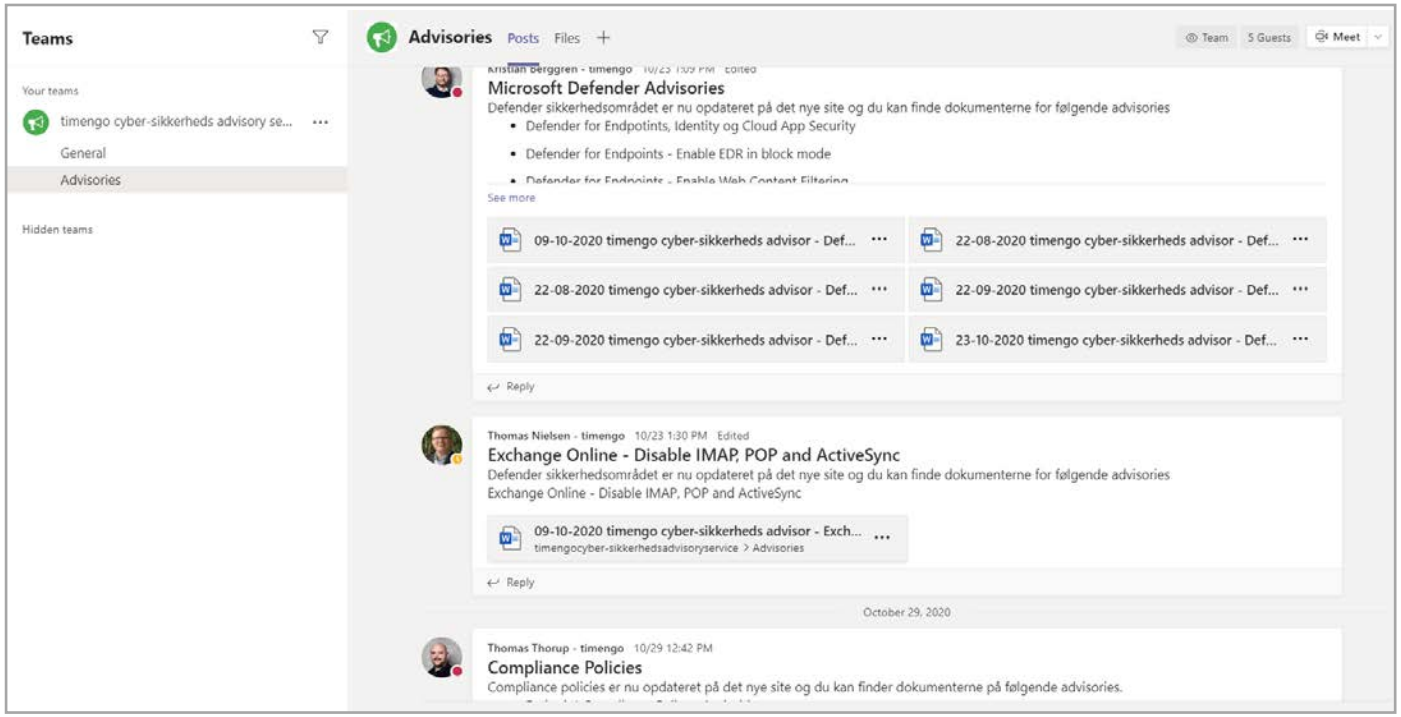
Licens. Microsoft 365 E3 / E5 security

Identitet. ADConnect med synkronisering af passwords og enheder for anvendelse på tværs af platformen, såsom password reset, enheds konfigurationer etc.

Privilegerede konti. Priviliged Identity Management for håndtering af privilegerede kontis. En konto skal aktiveres før rettigheder tildeles, og er typisk tidsbetinget.

Indhold via Teams

- Adgang til advisories og andet indhold via Teams
- Alle advisories vil indeholde anbefaling og konfiguration
- En række anbefalinger vil desuden blive leveret som automatiseringer
- Mulighed for chat og dialog med timengo og andre virksomheder på services



timengo.
enter the cloud

Opsamling & næste skridt

Våbenkapløbet…	• MS Cloud sikkerhed = 360 graders model for zero trust cybersikkerhed • Hvis I har en MS baseret infrastruktur er det vejen at gå
Udnyt potentialet	• Udnyt det I betaler for: M365 E3/E5 og Azure sikkerhed • Det er komplekst at få MS cloud sikkerhed optimalt konfigureret • **Få et cybersecurity roadmap/projekt I gang**
Vedligehold det	• Følg med i trusselsbilledet • Følg med I ændringer fra Microsoft • Eller **outsource det: Få en cybersecurity advisor service**

Europæisk status rapport på phishing angreb: https://www.enisa.europa.eu/publications/phishing

Evaluér eventet ved at følge det link vi ligger ud i chatten.

Tak. Det betyder meget for os.

Tak for i dag!

Vi glæder os til at se dig til næste event...

OPNÅ MERE MED CLOUD – KOM RIGTIGT I AZURE

7. december kl. 09.00!

Jeg vil gerne deltage

timengo.
enter the cloud