

Indsigt i Windows Endpoint- beskyttelse mod målrettede cyberangreb

Hænderne på rattet!!

Palle Hedegaard

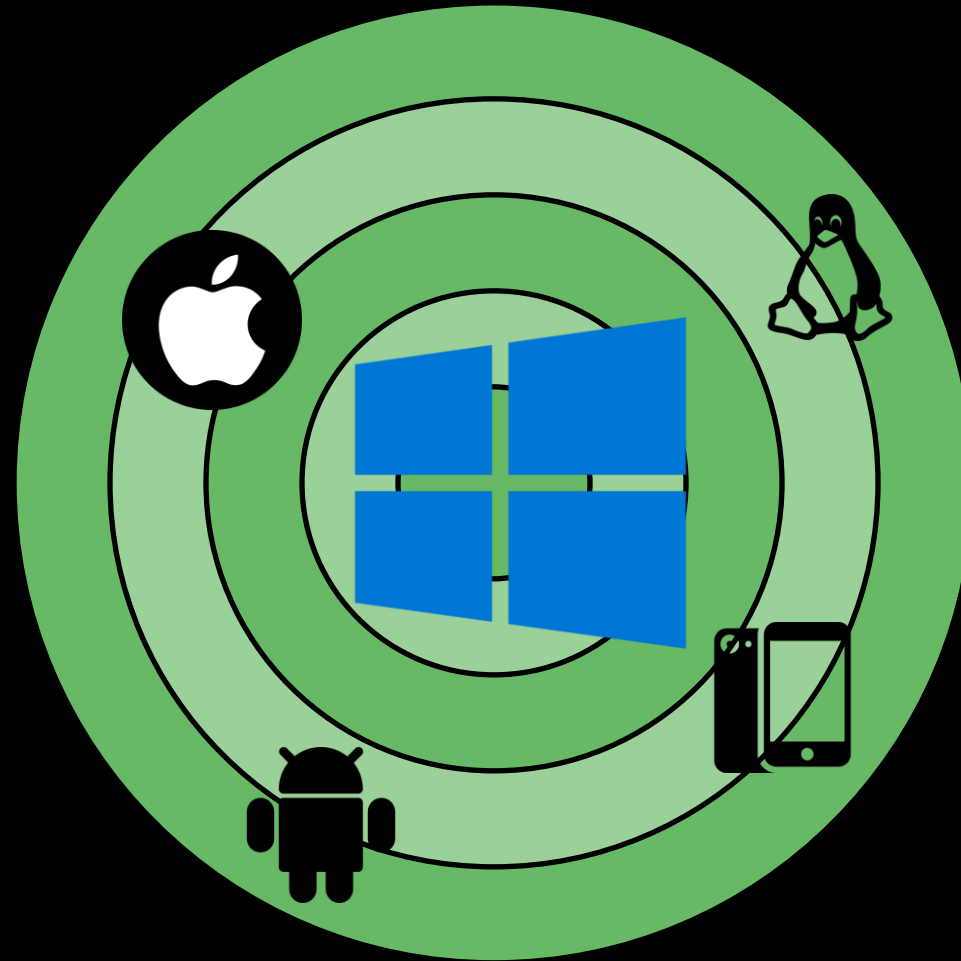
Lead Architect – Secure Workplace

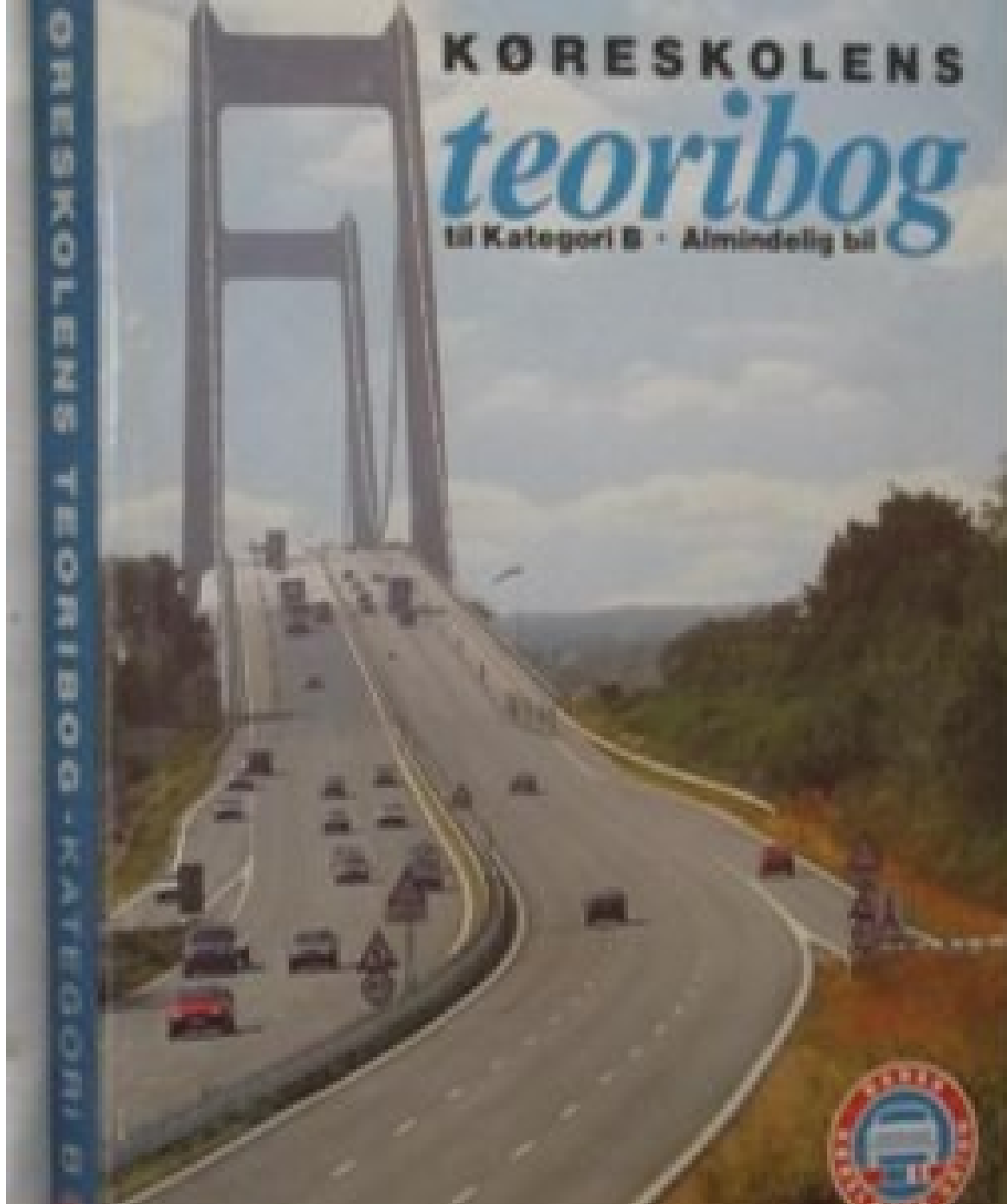


Jesper Lindholdt

Technology Architect – Secure Workplace







Jo jo..... i teorien Men de andre

- Glemmer selen
- Glemmer Spejl Spejl skulder
- Er uopmærksomme
- Kører for stærkt



Bilens systemer hjælper bilisten

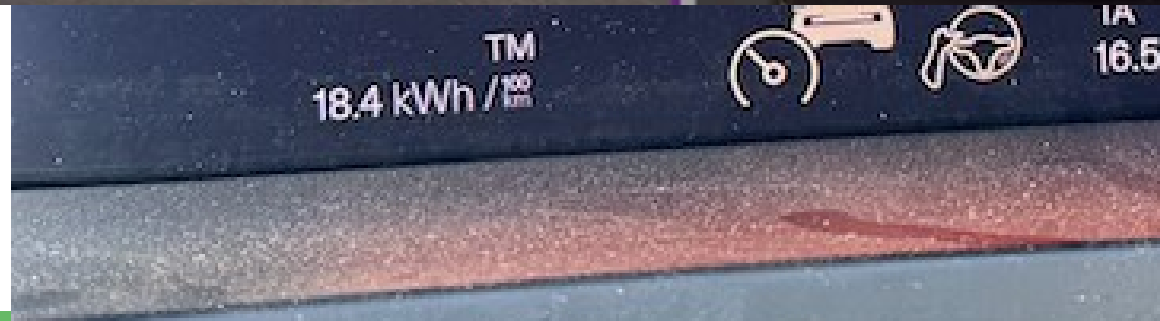
Selealarm

Hastighedsalarm

Trætheds assistent

Lane Assist

Laveste trafikdrabte



Hjælp brugeren til at blive en mere sikker Endpoint "bilist" - Aktiv sikkerhed

Bil	Windows Endpoint
Selealarm	AppLocker
Hastighedsalarm	Windows SmartScreen
Trætheds assistent	Attack Surface Reduction
Lane assist	Edge SmartScreen

Hærd dit Windows Endpoint – Passiv sikkerhed



Bil	Windows Endpoint
Låst motorhjelme	Fysisk adgang
Deformeringszoner	Disable RDP, C\$, Printspooler, SMB1
Selestrammere	Deaktiver Admin, Guest, LAPS
Airbag	Firewall regler

Baseline politikker

Microsoft Security Baselines

CIS Level 1 & 2

Atea Policy Framework (Balanceret)

- Attack Surface Reduction
- User Rights Management
- Kryptering og Antimalware
- Windows Hello for Business
- Og meget andet...

from creating child processes ⓘ

ASR Only Per Rule Exclusions ⓘ

Block all Office applications from creating child processes ⓘ Block

ASR Only Per Rule Exclusions ⓘ

Block Adobe Reader from creating child processes ⓘ Warn

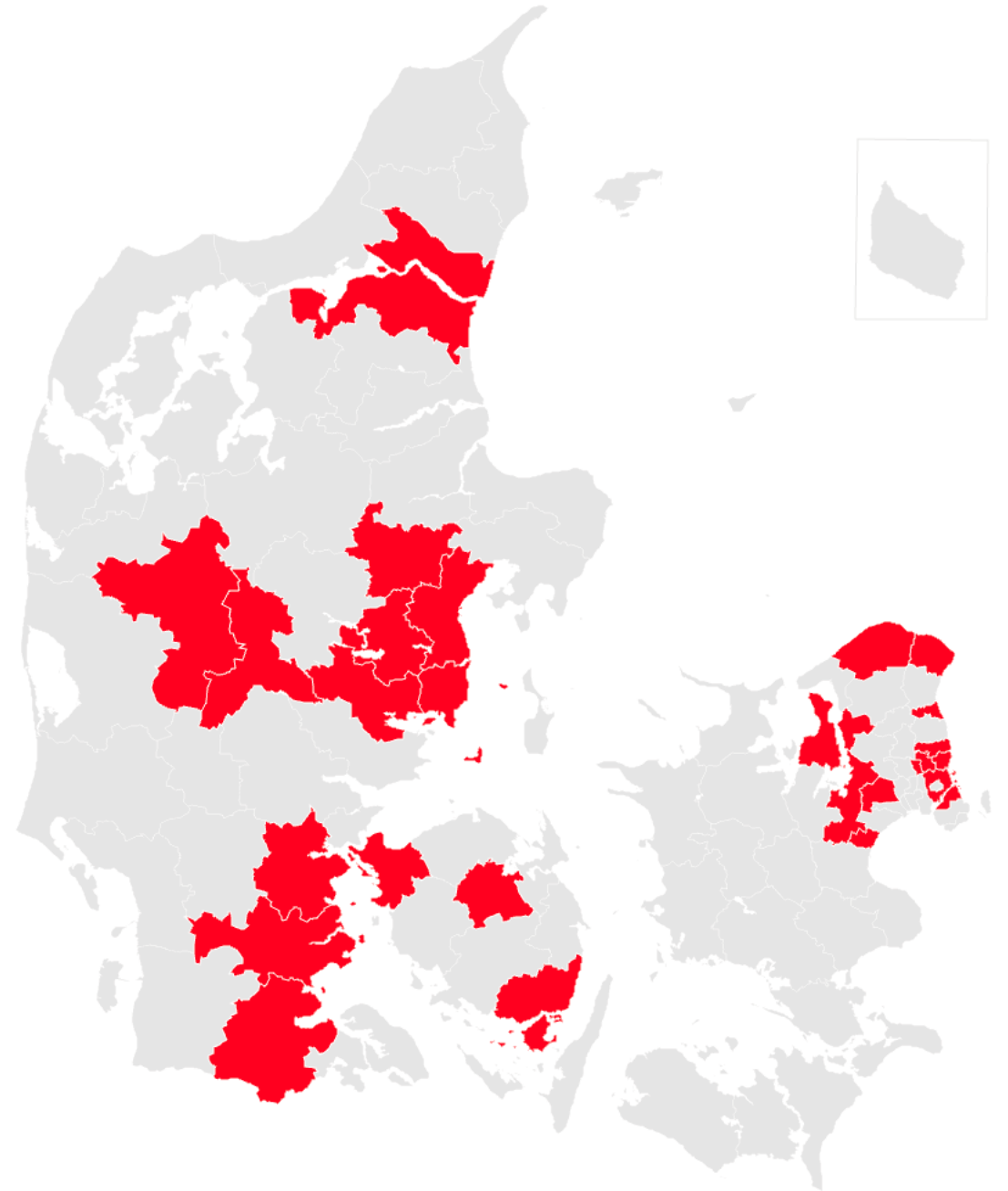
ASR Only Per Rule Exclusions ⓘ

Block credential stealing from the Windows local security authority subsystem ⓘ Block

Hardware sikkerhed

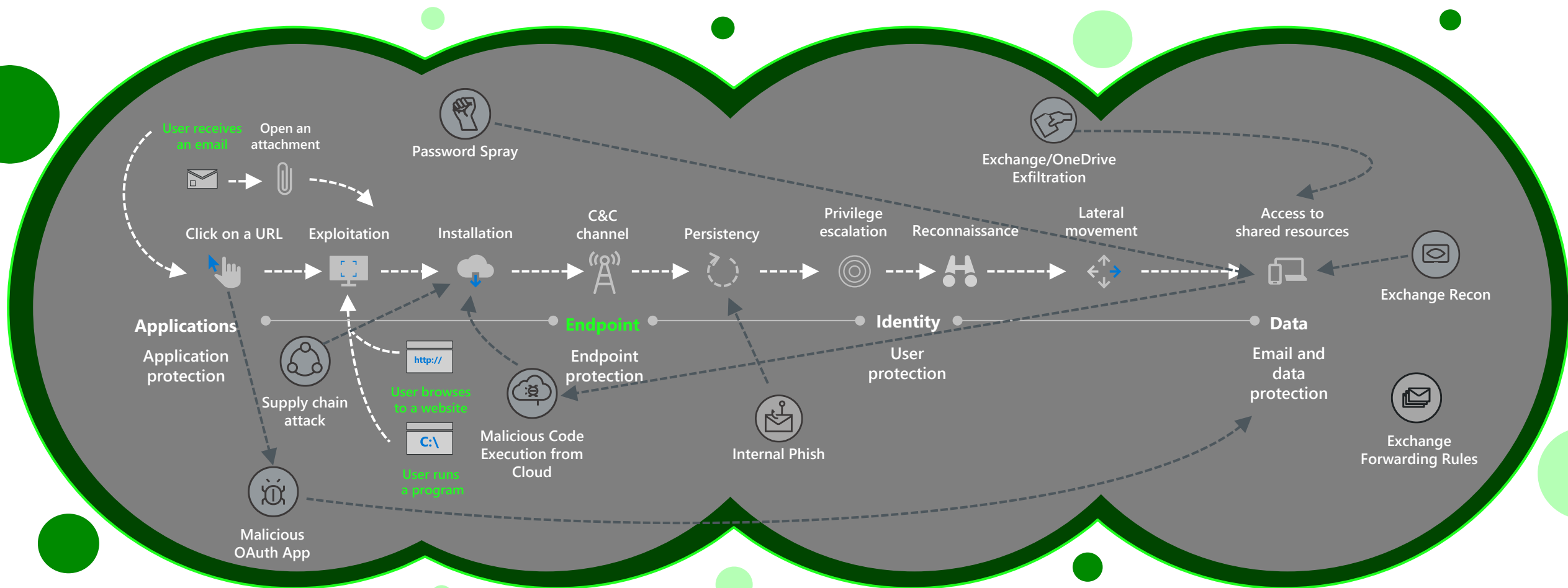


- BIOS konfigureret og låst
- UEFI Secure boot, bitlocker
- Firmware er sikkerhedsopdateret
- Fysisk adgang i det offentlige rum (borgervendte PC'ere. Varehus PC'ere)



Application control/whitelisting

- Applocker
- Application Control for Business (ACfB / WDAC)
- Implementering....

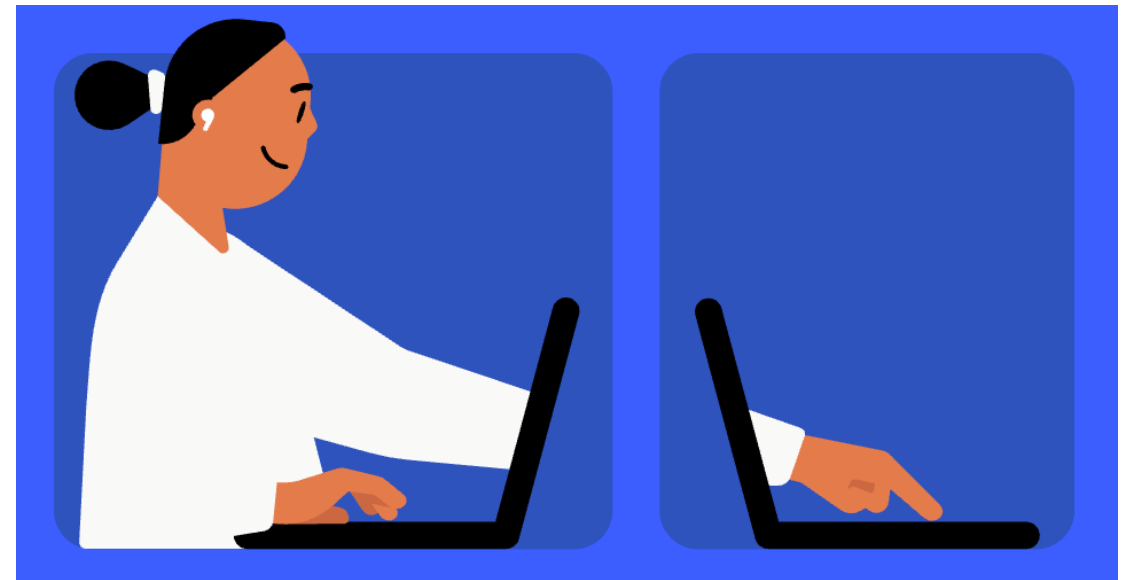


Remote Adgang på en sikker måde

Virtual Private Network - VPN

Global Secure Access - GSA

Virtual Desktop Infrastruktur - VDI



Konklusion

Sikkerhed er tilgængeligt, men er ofte ikke slået til.

Implementer en Baseline

En vigtig brik i det store sikkerhedspuslespil

Det er forbundet med omkostninger at implementere/administrere

Stil krav til leverandører - Modenhed



igen og

igen og....

Spørgsmål?

**Kør forsigtigt.Og
Husk.....**

Spejl spejl skulder !

**Næste indlæg:
Gendan hurtigt og sikkert
efter cyberangreb**

citrix®

intel®