IT-sikkerhet
i digitaliserte bygg

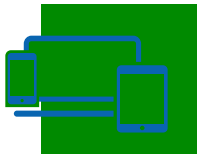
ATEA

Endringer i IT-landskapet

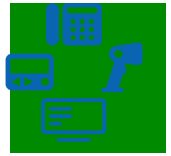
Brukere, enheter og apper er overalt

Eksterne brukere, entreprenører & tredjeparter

Personlige og mobile enheter



IoT-enheter



Omfang i sterk utvikling

Cloud applikasjoner

Hybrid Infrastruktur

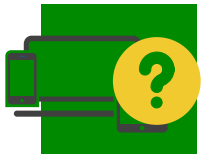
Cloud Infrastruktur

Forretningsmessige utfordringer

Økt tilgang, angrepsflate & manglende synlighet

Hvordan vet man at brukerne er den de utgir seg for?

Er brukernes klienter sikre og oppdaterte?



Hva finnes på nettverket? Hvordan henger det sammen?

Overdreven tillit

Hvilke data lagres i skyen? Hvem og hva har tilgang til den?

Hvordan kan vi se og sikre alle tilkoblinger?

Hva finnes i skyen? Hvordan henger det sammen?

Sikre hvordan noen eller noe får tilgang til work assets

NOEN

Ansatte

Entreprenører

Partnere

Forhandlere

Revisjon

Kunder

Etc…

NOE

IoT

API´er

Script

Printere

Kamera

Containere

Mikrotjenester

Operasjonelt utstyr

Virtuelle maskiner

Medisinsk utstyr

Maskiner på salgssted

WORK ASSETS

Virtuelle private skyer

Portaler

API´er

Nettverk

Servere

Databaser

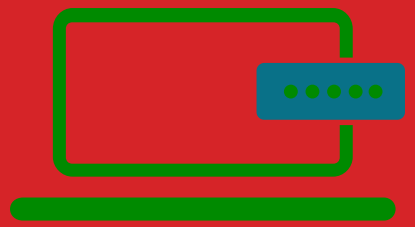
Containere

Applikasjoner

Nettverkssegmenter

Mikrotjenester

Trusselbildet i dag, som et resultat



Angrep på identitet

81% av sikkerhetsbruddene involverte kompromittert påloggingsinformasjon

Angrep på applikasjoner

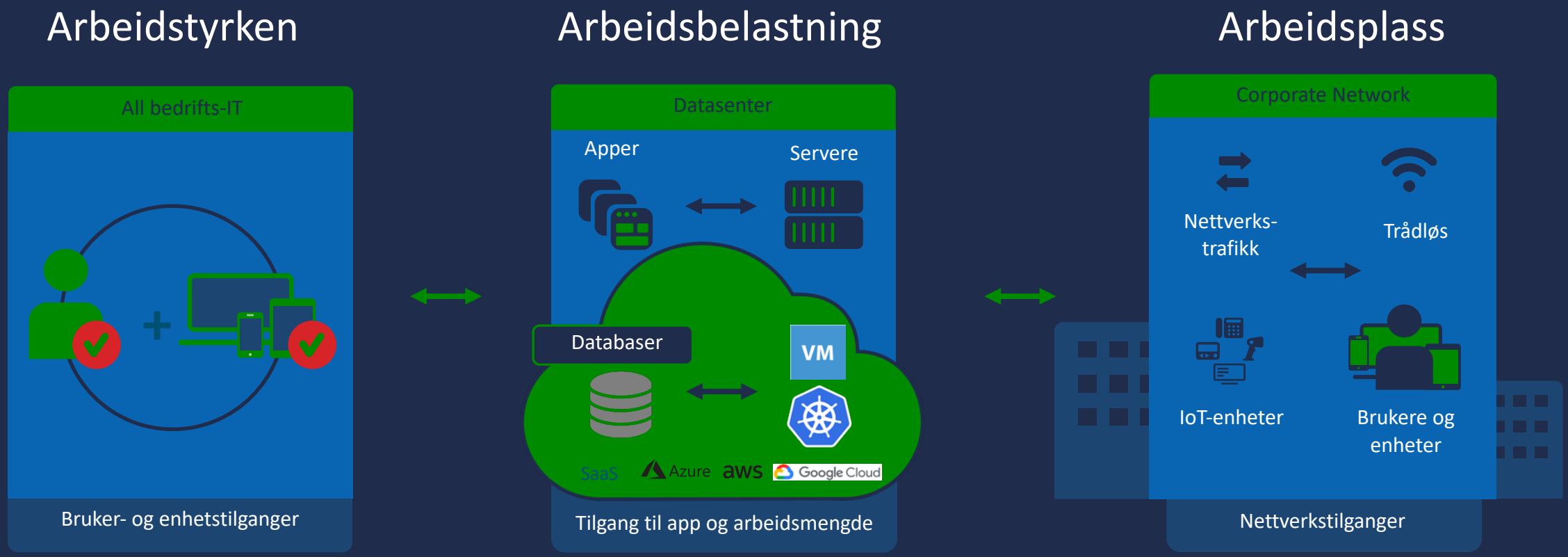
54% av sårbarhetene i nettapplikasjonene hadde en mulighet for offentlig utnyttelse

Angrep på enheter

300% økning i skadelig programvare for IoT (malware)

Sikre tilganger

Tilgang skjer overalt – hvordan får du synlighet og sørger for sikre tilganger?

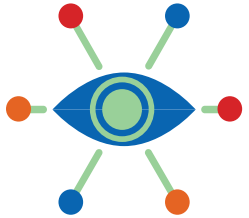


Aktivere sikker tilgang – Zero Trust

Nulltillitstilnærming til sikkerhet for å sikre tilganger til hele IT-miljøet ditt

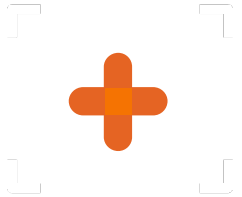
Forhindre risiko

Reduser risikoen for inntrengning før det skjer



Få oversikt og synlighet

Identifiser risikoer og indikatorer for tillitsbrudd



Reduser angrepsflaten

Begrens inntrengningen og stopp angripers mulighet for lateral bevegelse i nettverket

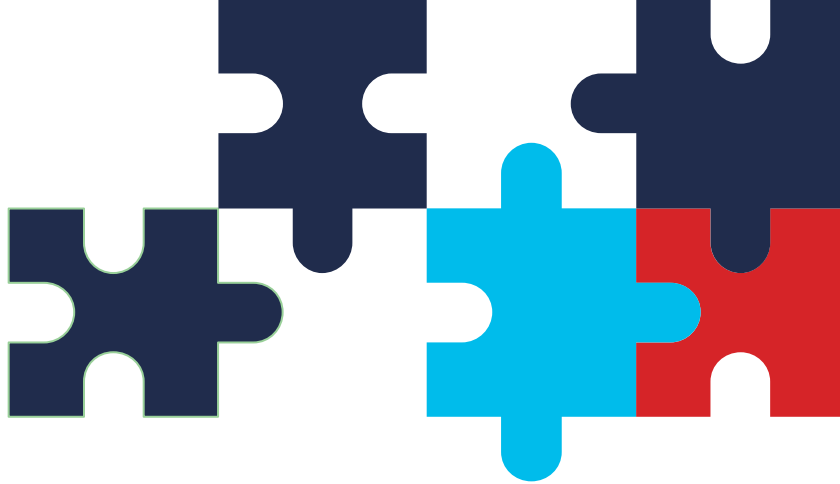
Zero Trust tilnærmingen:

Aktiver policy-baserte kontroller for hver tilgangsforespørsel i et bedriftsmiljø

Kontroller hvem og hva som får tilgang til applikasjoner, arbeidsmengder og nettverket

Segmenter nettverket og “workload´ene” dine ved å håndheve detaljerte kontroller

Hva er annerledes ved en Zero-Trust tilnærming?



Tradisjonell tilnærming

Tillit er basert på nettverksplasseringen en tilgangsforespørsel kommer fra.

Gjør det mulig for angripere å bevege seg lateralt i et nettverk for å komme til "kronjuvelene".

Utvider ikke sikkerheten til den nye omkretsen.

Zero Trust tilnærmingen:

Tillit er etablert for hver eneste tilgangsforespørsel, uavhengig av hvor forespørselen kommer fra.

→

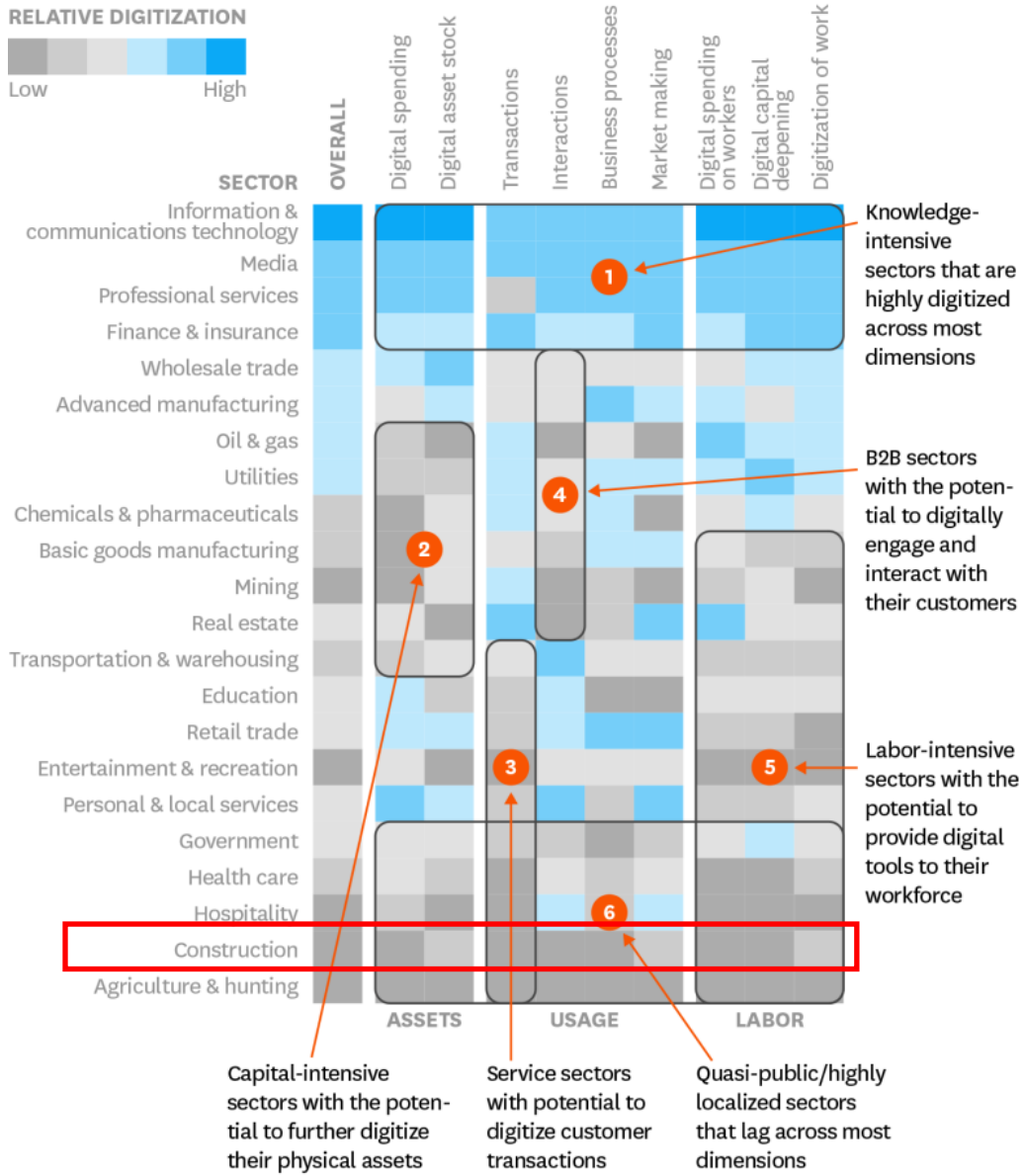
Sikrer tilgang på tvers av applikasjonene og nettverket. Sikrer at bare riktige brukere og enheter har tilgang.

Utvider tilliten til å støtte en moderne bedrift med BYOD, skyapper, hybridmiljøer m.m.

ATEA

How Digitally Advanced Is Your Sector?

An analysis of digital assets, usage, and labor.



SOURCE DATA ANALYSIS AND EXPERT INTERVIEWS CONDUCTED BY THE MCKINSEY GLOBAL INSTITUTE

Brukertjenester

- WiFi
- AV og møterom
- Mobilnett
- Booking/navigasjon
- Videosamhandling

Byggtjenester

- Belysning
- Heis
- HVAC
- Brannvarsling
- 24/7 overvåking
- Adgang og sikkerhet
- Energistyring

ATEA