

WHITEPAPER

Det operationelle miljø
er din genvej til **øget
sikkerhed** og digital
transformation.

Introduktion

”Den 7. maj 2021 blev Colonial Pipeline, et amerikansk olierørledningssystem som transporterer benzin og jetbrændstof til det sydøstlige USA, udsat for et ransomware-cyberangreb. Angrebet påvirkede computerstyret udstyr og stoppede alle rørledningens operationer. En regional nøderklæring for 17 stater blev efterfølgende udstedt for at holde vitale brændstofforsyningsledninger åbne ...”

Ovenstående er blot et af de seneste angreb på kritisk infrastruktur, der angiveligt kostede \$4.4 millioner i løsesum. Men endnu værre skabte angrebet panik i den amerikanske befolkning, da benzinstationerne begyndte at løbe tør for brændstof.

Det fysiske produktionsapparat - også kaldet det operationelle teknologimiljø (OT) - som fx styrer og overvåger industrirobotter, ovne i kraftvarmeværker, vandpumper på vores spildevandsanlæg eller åbne/lukke-ventiler på rørledninger har traditionelt været adskilt fra den øvrige it-infrastruktur. En række faktorer - hvoraf de sikkerhedsmæssige har karakter af brændende platforme - betyder dog, at OT og IT er i proces med at blive integreret med hinanden.

Den bevægelse medfører åbenlyse forandringer for medarbejderne i både produktionsvirksomheder og i de organisationer, der vareta-

ger vores samfundskritiske infrastruktur. Men først og fremmest betyder det tættere samarbejde mellem OT og IT, som i stor udstrækning har arbejdet uafhængigt af hinanden, at de to teams nu kan samle deres ressourcer og ekspertise. Dermed øges mulighederne for at understøtte virksomheden med bedre gennemsigtighed og automatisering i OT-miljøerne.

Dette whitepaper kommer både ind på fordelene og udfordringerne ved den accelererende sammensmeltning mellem OT og IT. Her vil især det menneskelige aspekt, de forandrede arbejdsopgaver og siloopdelinger få behørig plads. Grundpræmissen for whitepaperet er dog, at den tiltagende (og nødvendige) integration mellem OT og IT i dag er en helt uundværlig katalysator for yderligere digitalisering og transformation.

Hos Atea er vores erfaring, at mange produktionsvirksomheder gerne vil i gang med at digitalisere deres OT, men de ved ikke, hvor de skal begynde. Mange af de virksomheder, vi er i dialog med, er desuden tyngt af teknisk gæld, som besværliggør og udsætter digitaliseringen. Derfor vil dette whitepaper også adressere de vigtigste fikspunkter i en køreplan, der kan hjælpe virksomhederne i gang med den digitale transformation gennem opdateringen af OT-miljøet.



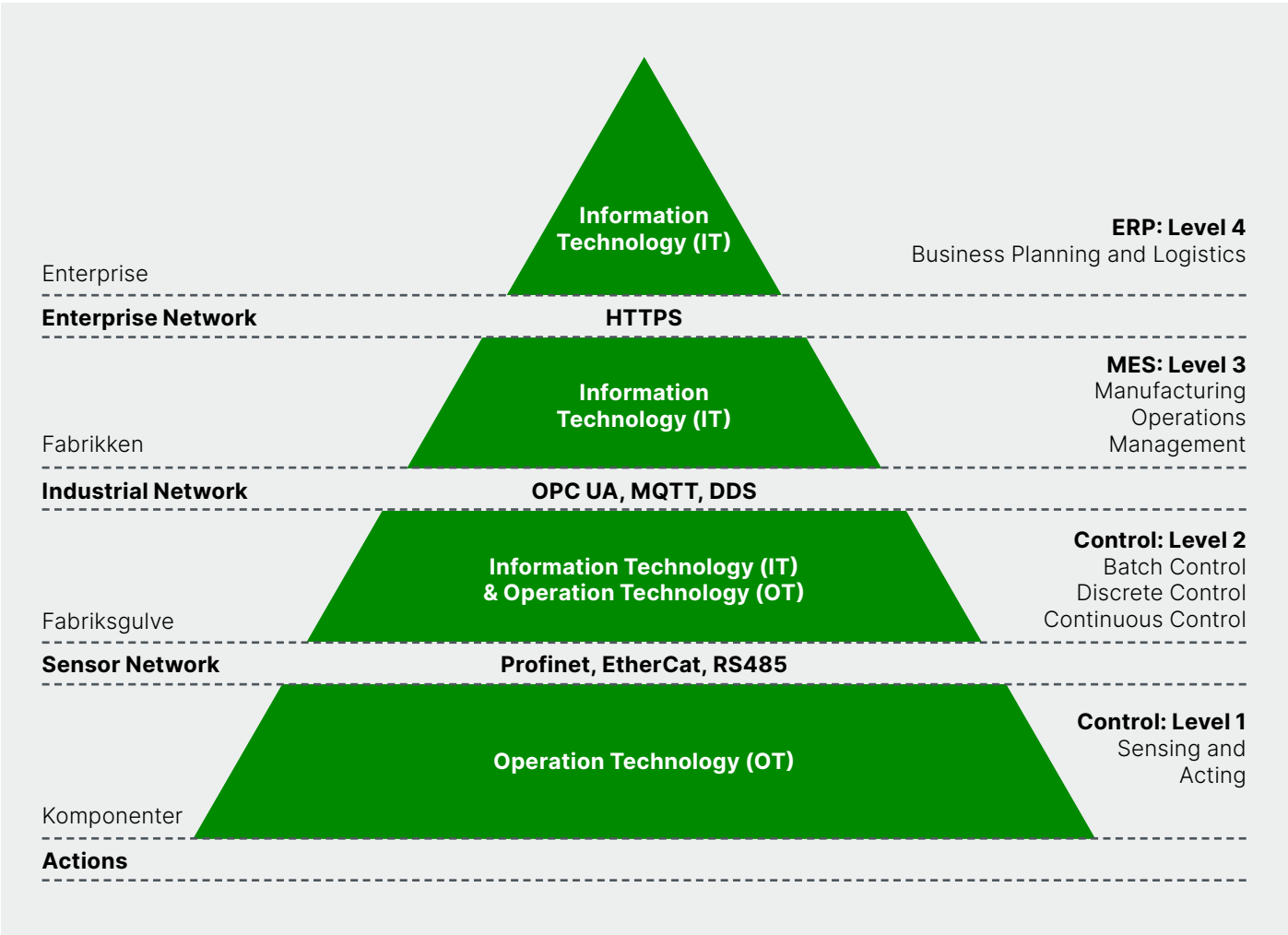
OT i opbrud

Operationel teknologi spiller en kritisk rolle inden for bl.a. produktion, fødevarer og landbrug samt for kritisk infrastruktur - blot for at nævne nogle få områder.

I en automatiseret produktionshal, på en olierig midt på havet eller i et arktisk miljø, hvor overvågning af fx olie- og gasledninger er kritiske, udfører OT-systemer ofte enkelte, men essentielle og kritiske opgaver, såsom overvågning af åbne/lukke-ventiler.

De forholdsvis simple opgaveløsninger har traditionelt resulteret i, at OT-miljøerne uforstyrret har fortsat driften uden ændringer eller opdateringer. Det betyder, at de i nogle tilfælde kører på gamle operativsystemer og forældet hardware med end-of-service lurende i horisonten.

Derudover tilgås OT-miljøet ofte på egenudviklede applikationer. Succeskriteriet for et OT-system er, kort sagt, høj driftssikkerhed. Derfor patches der ofte kun, hvis det er yderst nødvendigt eller hvis det ikke hindrer OT-systemets proces og dets kritiske funktion.



OT som konkurrenceparameter

Flere faktorer gør, at den digitale strategi med fokus på at lave egenudviklede OT-applikationer, langsomt er ved at blive udfaset, da der bl.a. begynder at være mere fokus på standardisering og automatisering.

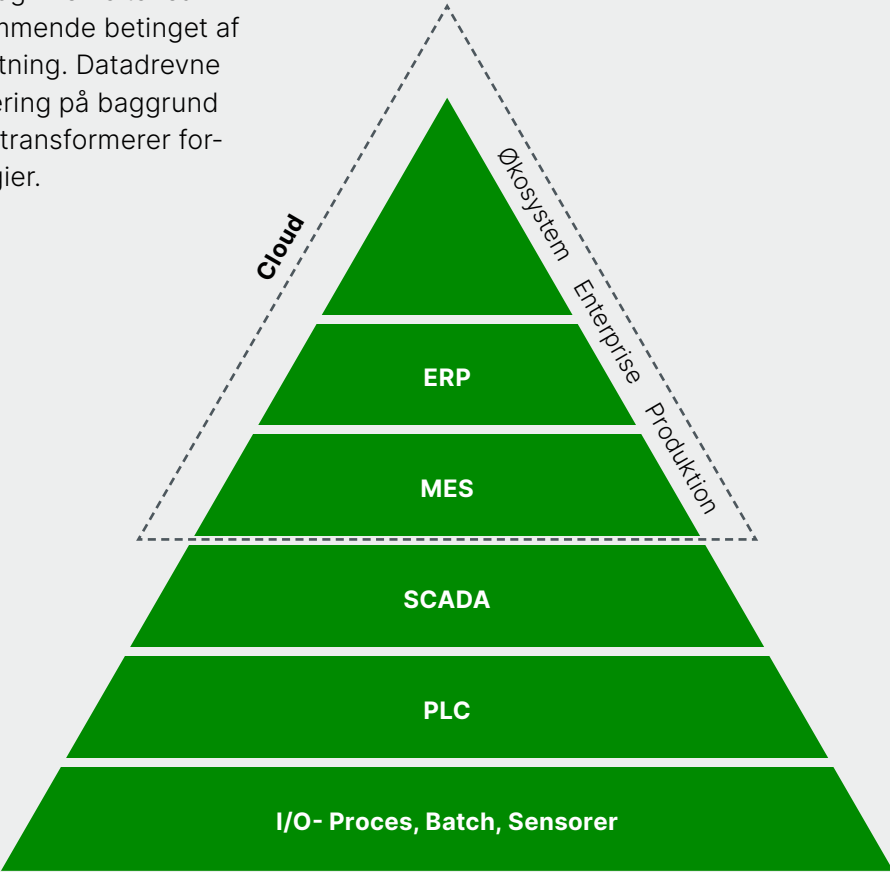
Dette er bl.a. også en af punkterne, som IDC er inde på i deres Worldwide IT/OT Convergence 2021 predictions:

”Inden 2024 vil 60 % af industrielle organisationer integrere data fra edge OT-systemer med cloud-baseret rapportering og analyser, der bevæger sig fra et single-asset view til sitewide operationel awareness”

Paradigmeskiftet, hvor OT og IT smelter sammen, er for manges vedkommende betinget af et pres fra den øvrige forretning. Datadrevne beslutninger og automatisering på baggrund af bl.a. IoT buldrer frem og transformerer forretningsområder og strategier.

Populært sagt er de fleste lavt hængende frugter, når det kommer til interne driftseffektiviseringer, blevet plukket af produktionsvirksomhedernes it-afdelinger. Nu er turen kommet til OT. Og potentialet er enormt – både for bundlinjen og for produktionsvirksomhedernes ambitioner om at sænke CO2-aftrykket.

Hos Atea viser vores erfaringer, at produktionsvirksomheder såvel som offentlige organisationer kan hente store og signifikante besparelser ved at træffe energieffektive og datadrevne beslutninger. Dermed bliver digitalisering af OT med implementering af kunstig intelligens og IIoT-sensorer et direkte konkurrenceparameter!



Intet alternativ til tårnhøj OT-sikkerhed

... Men farerne lurar lige bag hjørnet!

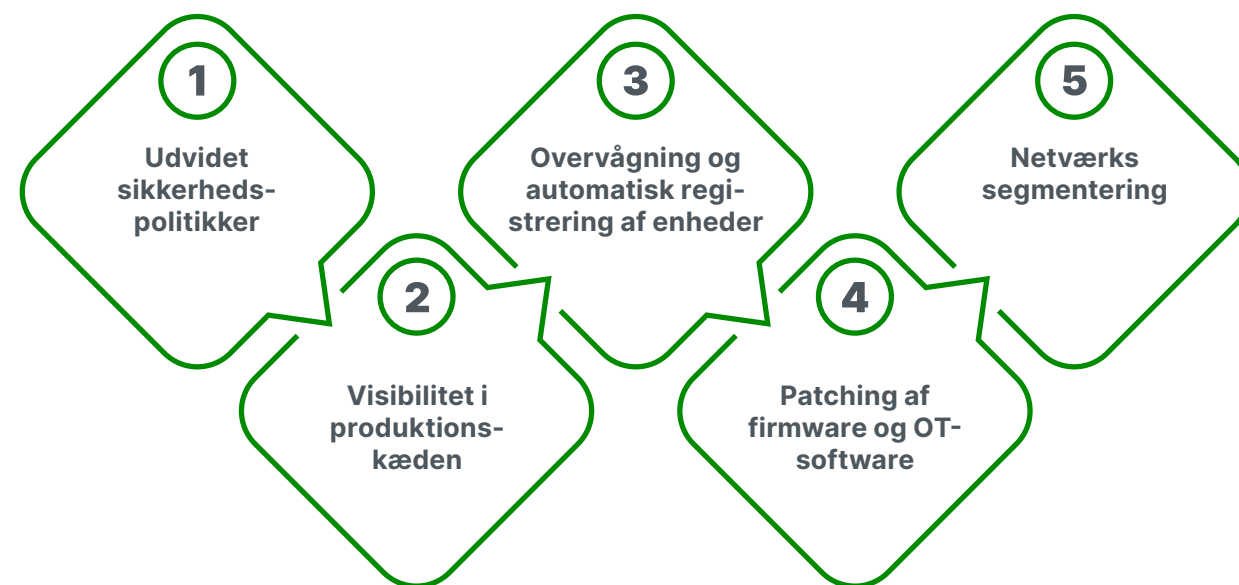
Som et resultat af en verden i hastig udvikling, en kortere time-to-market og et større pres for at digitalisere OT, bliver mange OT-systemer tilsluttet virksomhedsnetværk. Imidlertid udnytter mange af disse netværk almindelige internetprotokoller på den traditionelle it-infrastruktur, der er designet til it-brugere og ikke til OT-systemer. Desuden forbindes OT-systemerne i stigende grad via trådløs teknologi. Dette gør dem til en stor sikkerhedsrisiko og til oplagte mål for cyberkriminelle, der ønsker at stjæle data, udnytte systemerne eller simpelthen forårsage kaos.

Udover sikkerhedsrisikoen er OT-systemer notorisk sarte. Selv en systemscanning kan få disse enheder til at gå ned, hvilket – som beskrevet indledningsvist – kan have alvorlige, hvis ikke katastrofale konsekvenser.

Det er derfor altafgørende at tænke sikkerhed ind i de OT-løsninger, man planlægger at implementere eller modernisere.

5 måder til at beskytte OT-miljøer:

For at beskytte operationelle sikkerhedsmiljøer er der nogle grundlæggende beskyttelsesforanstaltninger, der skal iværksættes:



1

Udvid sikkerhedspolitikken til at omfatte OT. Truslerne mod OT-miljøernes sikkerhed er blevet tydeligere. Et kompromitteret OT-system vil ramme virksomhedens kerneforretning og skadeeffekterne vil hurtigt sprede sig som ringe i vandet, hvis der fx er tale om en gasledning eller et vandværk. Sørg derfor for at sikkerhedspolitikkerne afspejler flere typer af trusler og tag afsæt i IEC 62443.

2

Visibilitet i produktionskæden. Vær opmærksom på de hardware- og software-leverandører, der kommer ind på virksomhedens netværk og hav en klar strategi for disse, da de selv kan blive udsat for OT-sikkerhedsangreb, og dermed være en potentiel bagdør til virksomhedens produktion. Det kan medføre trusler på tværs af- og op ad produktionskæden. Derfor skal virksomheden have en struktureret tilgang til eksisterende og kommende leverandører og et framework omkring, hvilket operativt teknologimiljø de har, og hvilke sikkerhedsforanstaltninger leverandøren bruger til at beskytte deres OT/IT-systemer.

3

Brug værktøjer til overvågning og automatisk registrering af eksisterende og nye enheder, der bliver implementeret i virksomhedens netværk. Viden om, hvilke enheder virksomheden har, er et grundlæggende krav, når der skal kortlægges risikoområder og niveauer, så virksomheden kan anvende de korrekte sikkerhedsforanstaltninger.

4

Patching af firmware og OT-software kan være mere kompliceret end inden for et traditionelt IT-miljø, men det er lige så vigtigt – hvis ikke vigtigere! At have et system, der opdateres regelmæssigt, er udgangspunktet. Et end-to-end patch-styringssystem, der er specielt designet til OT-miljøer, kan være påkrævet.

5

Netværks segmentering er essentiel for at sikre OT-miljøerne, hvor første step er at etablere de korrekte netværkszoner med en klart defineret sikkerhedspolitik med granuleret netværksinspektion. For korrekt filtrering og inspektion af netværkstrafik på tværs af zoner er det nødvendigt, at løsningen samtidig forstår relevante OT-protokoller (Modbus, DNP3, OPC og andre).



OT og IT – fra silo til integration

Som tidligere nævnt har OT-systemerne traditionelt været adskilt fra virksomhedens øvrige it-netværk og ejes, administreres og drives lige så ofte af et andet team end den traditionelle it-afdeling. Det skyldes, at OT-systemer ofte har til opgave at overvåge og styre de meget følsomme industriprocesser, der er forbundet med den kritisk infrastruktur eller produktionen i en produktionsvirksomhed.

Et fundamentalt og kritisk omdrejningspunkt i enhver produktionsvirksomheds digitale transformation er derfor evnen til at samle medarbejderne fra IT og OT. Dette skal sikre sammenspil og forståelse imellem disse to verdener, så afdelingerne sammen kan skabe en sikker og stabil fremtidig infrastruktur.

Ved at forbinde on premise IIoT-enheder til cloud-baserede systemer kan der skabes en ideel digital løsningsplatform, der muliggør sammenkædning af ældre systemer og bedre styring af datakvalitet til virksomhedernes datadrevne beslutninger.

Fremdrift gennem fintunet framework

Med '8-trinsmodellen' er der skabt et holistisk framework, der med gennemprøvede metoder, giver indblik i den pågældende virksomheds udfordringer, visioner og digitale transformationsstrategi for OT-miljøet.



Frameworket bruges målrettet til at tage udgangspunkt i udfordringerne fremfor teknologien, for på den måde at finde frem til den rigtige løsning, som skaber værdi for virksomheden. Gennem rådgivning og forventningsafstemning skaber vi sammen et fundament for succes.

Atea arbejder i dag med mange kunder, som er midt i en digital transformation. Den digitale transformation medfører et behov for at ændre traditionelt meget låste systemer og processer. Transformationen introducerer samtidig nye muligheder, men også nye sikkerhedsrisici, som skal kortlægges og mitigeres.

I dag hjælper Atea en række forskellige produktions- og infrastrukturvirksomheder, som fx forsyningsselskaber, med at implementere et sikkert og stabilt framework, der imødekommer fremtidige lovkrav om gennemsigtighed og sikkerhed.

Vores opskrift på succesrig digitalisering af dit OT-miljø

Begynd processen ved at anvende Ateas digitaliseringsframework, som vil være med til at synliggøre nogle af de udfordringer og gevinster, I som medarbejdere og virksomhed står overfor.

Dette kan efterfølgende resultere i supplerende elementer, hvis dette giver værdi for jeres digitalisering:



Byg en dataplatform, der kan integrere mange forskellige teknologier, og data fra både IT- og OT-verdenen, da denne vil skabe fundamentet for en 'digital tvilling'



Gennemgå og evt. udvid sikkerhedspolitikken, så denne omhandler mennesker, processer og teknologi



Patching af firmware og OT-software, for at sikre at dette er opdateret i bedst mulige omfang



Skab medarbejder-awareness omkring sikkerhed og data



Sikre netværkssegmentering, så netværkstrafik ikke kan gå uhæmmet fra IT til OT



Opsamling

Data ændrer alt!

Den digitale transformation kan være med til at løfte industrien til nye niveauer ved at bruge moderne teknologi til at modellere, analysere eller fremvise de kæmpe datamængder, der kommer ud af produktionen og OT-miljøerne.

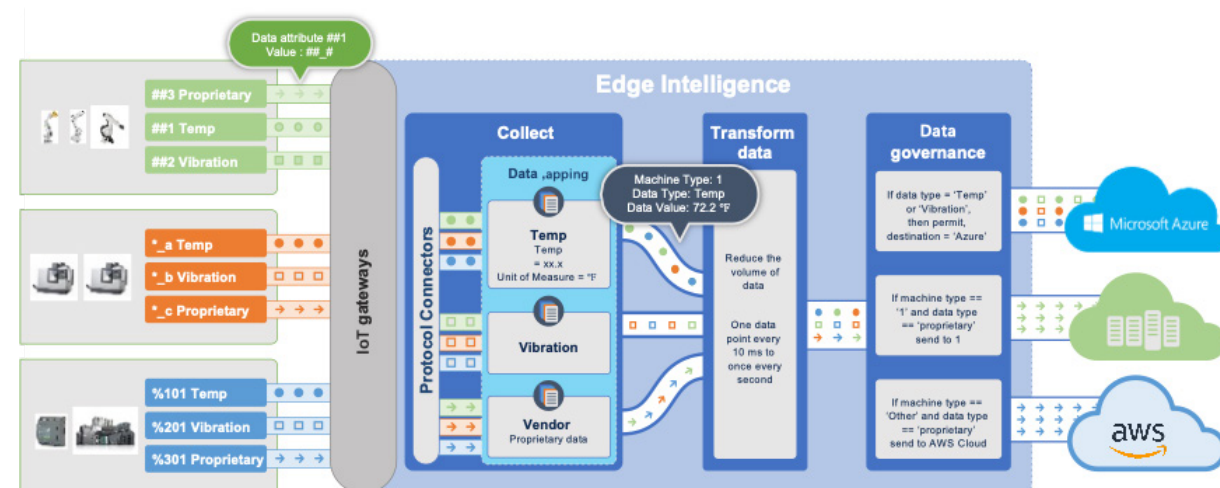
Hos Atea mener vi, at det mest fundamentale ved den digitale transformation er evnen til at træffe datadrevne beslutninger i realtid - baseret på sensorer, produktionsmaskiner, ERP-systemer og meget mere ...

En af de afgørende underliggende faktorer ved den digitale transformation ligger desuden i sikkerheden. Mange OT-miljøer er af ældre dato og bør udskiftes som en del af denne transformation.

Transformationsrejsen er hverken let eller enkel. Derfor skal den enkelte virksomhed først og fremmest udvikle en fremtidssikker digitaliseringsstrategi.

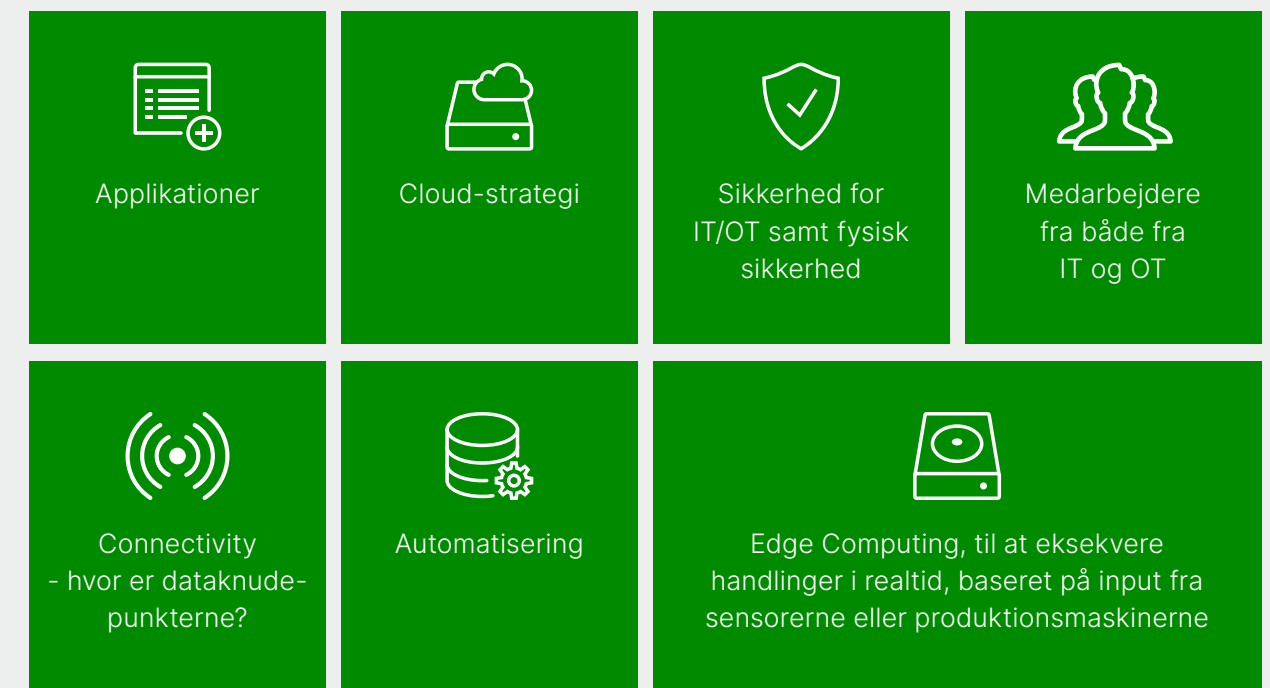
Hos Atea har vi mange års erfaring med at facilitere både strategiudvikling, hardware og de menneskelige ressourcer, der skal føre strategien ud i livet.

Atea hjælper virksomheder med at finde, designe og implementere løsninger, der vil kunne løse de udfordringer, virksomheden står overfor via '8-trinsmodellen'.



Perspektiverne ved at implementere ny teknologi, er mildest talt lovende. Som fx i ovenstående illustration, hvor implementeringen af en nyere industri-router, hjælper virksomheden med at få et bedre driftsoverblik og tilbyder Edge Computing til opsamling og databehandling ude på en understation. Meta-data bliver herefter sikkert sendt ud til et cloudmiljø, hvor en dataplatform lagre data og giver flere muligheder for analyse og visualisering. Ultimativt kan disse data bruges til at opbygge en 'digital tvilling', der kort sagt kan skabe en digital kopi af det fysiske miljø. Formålet er at forhindre kostbare fejl i fysiske enheder ved at bruge avancerede analytiske, overvågnings- og forudsigelsesmuligheds -tjenester.

Denne data-fødekæde er resultatet af en digital transformationsproces, hvor flere parametre, fra begyndelsen, er tænkt ind i den digitale strategi:



Atea har igennem mange år hjulpet Danmarks virksomheder med deres digitale transformation i IT. Den erfaring gør Atea til en oplagt partner, når medarbejderne og infrastrukturen i det operationelle miljø påbegynder selvsamme rejse.

Skal vi hjælpe dig?

Venligst kontakt,

Casper Ginderskov

Business Development Manager, Information Management Program & Sales

Casper.Ginderskov@atea.dk

+45 3078 0447

