Diktér jeres egen digitale suverænitet

Sådan får I både fleksibel cloud og dokumenterbar digital suverænitet på én gang.

Sovereign cloud som genvej til suverænitet og selvbestemmelse. Få et sikkert, stabilt og skalerbart IT-drifts og cloudmiljø

Indholdsfortegnelse

Bliv klogere på digital suverænitet, sovereign cloud og fordelene ved en dansk cloudplatform som sikker havn for dine data og et stabilt supplement til din digitale infrastruktur.

Derfor skal virksomheder prioritere digital suverænitet

- Og sådan kan en Sovereign Cloudplatform gøre suverænitet praktisk, sikkert og fleksibelt

Digital suverænitet kan lyde stort og statsligt. Men for en virksomhed er det i praksis et ganske jordnært spørgsmål: Hvem har kontrol over vores data, hvor befinder de sig, og hvilke regler gælder – nu og i morgen? Hvis du kan svare på de tre spørgsmål, står du stærkere i forhold til compliance, sikkerhed, kunder, og innovation.

I EU gælder der allerede regler virksomheder skal leve op til – GDPR er bare en del af dem. Men reglerne ændrer sig også hele tiden. Behovet for at beskytte virksomheders data og viden mod uønsket overvågning eller indblanding er reelt. Samtidig er data blevet din mest værdifulde råvare. Og det er svært at investere i datadrevne services, hvis du er i tvivl om ejerskab, styring og anvendelsesmuligheder. Her bliver Sovereign Cloud relevant: Det er en måde at designe cloud-arkitekturen, så den matcher lovkrav, reducerer geopolitisk risiko, og samtidig bevarer innovationskraften. Men hvorfor overhovedet suveœrnitet?

Regulatorisk sikkerhed
Alle virksomheder bliver ramt af krav. Og mellemstore virksomheder rammes ofte af de samme krav som de helt store – blot med færre ressourcer til rådighed til løsninger. Suverænitet gør compliance-kæden enkel: du ved, hvor data bor, hvem der kan tilgå dem, og hvilke kontroller og audits der dokumenterer det. Det sænker usikkerheden i dialogen med kunder, tilsyn og bestyrelse.

Geopolitisk robusthed
Lovgivning som f.eks. udenlandske "cloud acts" kan i teorien give adgang til data, hvis din infrastruktur falder ind under fremmed jurisdiktion. En suverœn tilgang handler om at minimere eksponering og indbygge jurisdictional control – fx ved at holde drift, kryptering og nøglehåndtering under bestemte nationale regler, som du anerkender.

Data som vækstmotor – uden lock-in
Når data skal binde forretningen sammen (kunderejser, produktdata, servicehistorik, AI), bliver det afgørende, at du kan flytte workloads, integrere tjenester og udvide med nye funktioner – uden at miste styring. Derfor handler suverœnitet også om din datas uafhængighed og din evne til at flytte den: At du foretager arkitekturvalg, der gør dine data og løsninger portable og fleksible.

Fra princip til praksis: **Fire suverænitetsområder du bør fokusere på**

1

Data residency & juridisk kontrol
Placering, drift og beviskæde

Det skal du overveje

Kortlægning: Begynd med en data-kortlægning: Hvilke datakategorier har I (persondata, driftsdata, IP, finans)? Hvilke lovkrav gælder? Hvor behandler og lagrer I data i dag?

Segmentering: Inddel data efter følsomhed og krav til residency. Det gør det muligt at designe en arkitektur, hvor de mest følsomme datasæt holdes inden for nationale grænser, mens mindre sensitive kan udnytte mere skalerbare platforme.

Operativ kontrol: Sikr at drift, administration og support af den del af miljøet, der bærer følsomme eller regulerede data, foregår inden for jurisdiktionen – inkl. roller, processer og eskalationsveje.

Sådan kan en certificeret Sovereign Cloud-platform hjælpe jer:

Vi har bygget en dansk cloudplatform, der er certificeret af VMware og som lever op til deres Sovereign Cloud designation.
Sovereign Cloud baseret på VMware er bygget på kravet om national kontrol og residency: miljøet leveres og drives af validerede cloud-udbydere i det pågældende land, med dokumenterede kontroller og auditerbar drift. Det gør placering og kontrol synlig og bevislig, hvilket er centralt i compliance-dialogen med kunder og myndigheder.

Forbered jer klogt:

- Etabler et data registry med ejer, type, placering og behandling – og forbind det til jeres kontrakter og SLA'er.
- Design jeres arkitekturdiagrammer med tydelig markering af suveræne zoner (lagring, compute, KMS, administration)
- Lav en bevispakke (audit-ready) med beskrivelser af residency, roller og procedurer. Det sparer tid ved kundespørgsmål og tilsyn.

2

Sikkerhed & compliance
Gå fra "vi opfylder kravene" til "vi demonstrerer dem løbende"

Det skal du overveje:

Standarder og kontroller: Vælg anerkendte sikkerhedsstandarder (fx ISO/IEC 27001) og oversæt dem til konkrete kontroller – adgang, segmentering, overvågning, hændelseshåndtering.

Kryptering og nøgleejerskab: Implementér kryptering med egen nøglekontrol (BYOK/BYO-KMS), så leverandører ikke kan tilgå indholdet.

Løbende efterlevelse: Opbyg en rytme for kontinuerlig compliance: Måling, rapportering og forbedring. Nøjes ikke kun med den årlige revision.

Sådan kan en certificeret Sovereign Cloud-platform hjælpe jer:

En VMware-certificeret Sovereign Cloud lægger vægt på auditerede sikkerhedskontroller og understøtter Bring Your Own Keys og Bring Your Own KMS, så nøglemateriale og adgang kan holdes under national kontrol.

Dertil kommer tekniske mekanismer som mikrosegmentering, Zero Trust-principper og EDR/XDR-understøttelse, som kan integreres i drift.

Forbered jer klogt:

- Definér en KMS-strategi: hvor bor nøglerne, hvem kan administrere dem, og hvordan sikrer I nøglers livscyklus (rotation, ophævning, recovery)?
- Indfør policy-as-code for sikkerhed og compliance, så kontroller kan måles og dokumenteres automatisk.
- Træn drifts- og sikkerhedsteam i hændelseshåndtering, inkl. scenarier hvor jurisdiktion og suveræne krav påvirker responsen.

3

Data uafhængighed & mobilitet: Arkitektur, der kan skifte retning uden at gå i stå

Det skal du overveje:

Portabilitet som krav: Når I vælger platforme og designs, så vurder dem på evnen til at flytte workloads, eksportere data og køre på tværs af miljøer.

Moderne applikationsmønstre: Invester i containerisering, orkestrering og API-first design. Det gør det lettere at udnytte både suveræne og offentlige cloud-tjenester – på jeres præmisser.

Exit-strategier: Skriv "exit" ind i arkitekturen: hvordan ruller vi tilbage? Hvordan migrerer vi ud? Hvilke formater og processer sikrer minimal friktion?

Sådan kan en certificeret Sovereign Cloud-platform hjælpe jer:

VMware's suveræne rammeværk understøtter moderne applikationer og multi-cloud-scenarier, så du kan kombinere lokale krav med global kapacitet. Det minimerer risikoen for vendor lock-in og skaber en pragmatisk vej til at bruge AI/ML- eller analytics-tjenester, hvor data anonymiseres/krypteres, før de forlader en suveræn zone.

Forbered jer klogt:

- Indfør referencearkitektur for portabilitet (images, artefakter, CI/CD, observability), så flytninger er rutine – ikke projekter.

- Lav dataklassificering med behandlingsregler: hvad må forlade suveræn zone (anonymiseret, tokeniseret, krypteret), og hvad må ikke.
- Etabler testmiljøer for migrationsøvelser, så organisationen har praktisk erfaring med at flytte uden nedetid.

4

Data adgang & integritet
Resiliens, redundans og ansvarlig deling

Det skal du overveje:
Redundans og tilgængelighed: Opbyg resiliens med mindst to datacenter-lokationer inden for jurisdiktionen og klare planer for failover/failback.

Privat konnektivitet og segmentering: Brug segmenterede netværk og private forbindelser til brug for kritiske systemer; kombinér med stram adgangsstyring og overvågning.

Sikker deling: Når data skal deles med partnere eller myndigheder, så gør det med klare protokoller for anonymisering/tokenisering og auditspor.

Sådan kan en certificeret Sovereign Cloud-platform hjælpe jer:

VMware-cirklen lægger vægt på resiliens i suveræne miljøer og giver byggeklodser for kontrolleret deling, hvor følsomme datasæt forbliver under national kontrol, mens mindre følsomme kan udnytte skalerbare tjenester. Det understøtter løbende integritet via certificerede kontroller og synlige driftspraksisser.

Forbered jer klogt:
- Etabler SLAer om tilgængelighed, recovery tid og data-integritet, som hænger sammen med jeres forretningskritiske processer.
- Indfør data-delingspolitikker (hvem, hvad, hvordan, hvor længe), og knyt dem til tekniske mekanismer for maskering, tokenization og logging.
- Dokumentér end-to-end-kæden: fra brugertilladelser til netværkspolicy og audit – så integritet kan demonstreres, når den udfordres.

Implementering af suverænitet

Små skridt giver jer en stor effekt

Du behøver ikke en "big bang"-transformation for at opnå digital suverænitet. En realistisk, trinvis model kunne se sådan ud:

Diagnose & design: Workshop med interessenter (IT, sikkerhed, jura, forretning). Kortlægning af data, flows og kontrakter. Suveræn referencearkitektur (zoner, residency, KMS, drift).

Pilot i suveræn zone: Udvælg et kritisk, men overskueligt datasæt. Implementér sov-modellen (residency, BYOK/BYO-KMS, audit). Mål performance, driftstid, compliance-hensyn.

Operationalisering & bevisførelse: Policy-as-code for kontroller og compliance. Automatiseret rapportering til ledelse og kunder. Træning af beredskab og migrationsøvelser. Skalering & innovation: Udvid til flere workloads. Indfør sikre data-delingsmønstre (anonymisering/tokenisering) mod analytics/AI. Forfin exit-strategier og portabilitet.

Gør suverænitet til en vane – ikke et projekt
Digital suverænitet er ikke en garanti for perfekte resultater, og den forhindrer ikke alle risici. Men det sænker sandsynligheden for ubehagelige overraskelser, den gør compliance håndgribelig, og den åbner for mere målrettet innovation med data. For en virksomhed er netop den kombination sjælden – og værd at gå efter.

Hvis du begynder med en enkel diagnose, forankrer nøgler og residency, og bygger portabilitet og dokumentation ind i daglig drift, så har du en suverænitet, der kan bevises, kan driftes, og kan udvikles.

Her kan VMware's Sovereign Cloud-ramme hjælpe dig med at gøre det hele konkret: lokal kontrol, løbende compliance, og fleksibel arkitektur – uden at love mirakler, men med en drift, du kan stå inde for.

Referencer og kilder

- VMware Sovereign Cloud – Framework & principper: VMware Sovereign Cloud Solution Overview og VMware Sovereign Cloud Initiative Guide (principper: Data Sovereignty & Jurisdictional Control, Data Access & Integrity, Data Security & Compliance, Data Independence & Mobility).
- Hvad er Sovereign Cloud? VMware's ressourceartikel og forklaring af EU-kontekst og arbejdsmåde (private clouds, kryptering, zero-trust, løbende compliance).
- Drifts- og compliancekrav i suveræn cloud: løbende audits, certificerede kontroller, redundans og private forbindelser.
- BYOK/BYO-KMS i suveræn cloud: VMware udvidelser til kundestyret nøglehåndtering, som styrker kontrol og adgangsbegrænsning.

Secure Private Cloud

Sådan leverer vi hybrid- og sovereign cloud ydelser til forretninger, der kræver fleksibilitet og stabilitet

Cyberangreb og datalæk kan have store og vidtrækkende konsekvenser – og har næsten altid signifikante negative effekter af den ene eller den anden slags, der påvirker virksomhedens økonomi, drift og kunder. I nogle tilfælde kan det endda true den ramte virksomhed eller dens kunder på livet.

Ikke desto mindre har organisationer og virksomheder lidt samme forhold til IT-sikkerhed, vi som privatpersoner har til sundhed: De færreste lever op til samtlige ekspertråd og gør ikke alt det, de egentlig godt ved, at de burde gøre for at passe på sig selv. Desuden er de færreste helt sikre på, hvilke tiltag der har den største effekt.

Men med IT-sikkerhed er der tillige den ekstra udfordring, at både risici, trusler og modforholdsregler er under konstant udvikling. Samt at langt de færreste organisationer reelt har ressourcer til at overskue, administrere og tilpasse cybersikkerhed og beredskab, så de vigtigste vinkler dækkes af.

Så når uheldet er ude, risikerer du at det er ekstremt svært, tidskrævende eller helt umuligt at gendanne data og systemer. I tilfælde af et angreb har de cyberkriminelle sandsynligvis endda slettet eller krypteret sikkerhedskopien som det første.

Det er baggrunden for, at vi har investeret i udviklingen af platforme, procesapparater og IT-managementløsninger,som dækker alle de vigtigste vinkler af i din infrastruktur.

Vi kalder ydelsen "Secure Private Cloud", og den bygger på en nøje sammensat leverance af services og vedligehold af jeres servere kombineret med en række omhyggeligt udvalgte sikkerhedselementer.

Det yder et særdeles slagkraftigt bidrag til din infrastrukturs modstandsdygtighed mod aktuelle trusler, hvilket vi kommer nærmere ind på over de følgende sider. Ligesom vi også ser på, hvad det kræver af din organisation at drage fuld nytte af mulighederne.

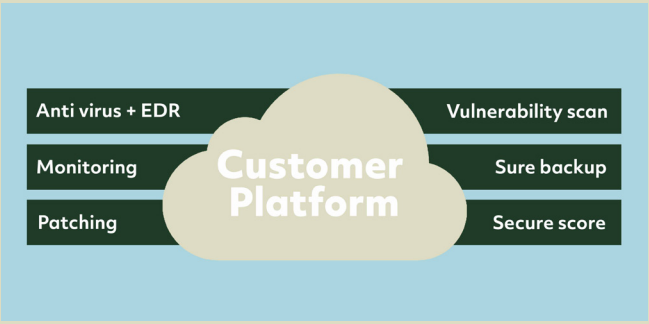
vmware CLOUD VERIFIED SOVEREIGN CLOUD

Et modsvar til konstant skiftende trusler

Langt de fleste virksomheder har implementeret værktøjer og rutiner, som dækker traditionelle IT-sikkerhedsudfordringer af.

Men løbende backup samt relativt velfungerende firewall og antivirus kan ikke længere stå alene. Cyberkriminelle tager rutinemæssigt avancerede psykologiske værktøjer og AI-services i brug for at udøve effektiv social engineer- ing med henblik på at lokke dine medarbejdere til at udlevere fortrolige informationer eller lukke skadelig kode ind ad bagdøren. Det er heller ikke usædvanligt, at IT-kriminelle trænger ind på dit netværk for derefter at bruge måned- er på at identificere svagheder, placeringen af fortrolige informationer og skaffe sig privi- legeret adgang til forretningskritiske systemer – før de eventuelt krypterer hele infrastrukturen og kræver løsepenge.

Derfor har vi designet en sammenhængende suite af Managed Services – kaldet Secure Private Cloud – som pakker både endpoints, netværk og cloudbaserede dele af din løsningsinfrastruktur ind i velfungerende, opdateret sikkerhed.



I designet af Secure Private Cloud har vi taget udgangspunkt i nogle af markedets mest velfungerende standardkomponenter med henblik på at styrke visibilitet, administration og orkestrering på tværs af den samlede sikkerhed- sinfrastruktur.

Samtidig spiller vi gerne med som betroet partner, der hjælper dig med at:

- Identificere svagheder og særlige udfordringer i din infrastruktur
- Kortlægge, hvilke komponenter og datasæt, som skal omgærdes af særlige sikkerhedsforanstaltninger
- Træffe de valg, der sikrer dig og din virksomhed bedst og mest effektivt med skarpt blik på økonomi, tids- og ressourceforbrug

Endelig spiller vi gerne med på andre felter også. For eksempel hvis der er behov for at opbygge og videreudvikle en velfunderet sikkerhedsorienteret adfærd i virksomheden, hvor samtlige medarbejdere effektivt medvirker til at mitigere risikoen for cyberangreb og kompro- mittering af fortrolighed samt kritiske data.

unit it

Sådan:
En sikker og fleksibel infrastruktur

Nogle virksomheder drifter flertallet af services og applikationer fra eget datacenter, andre satser primært på en hostingpartner og andre igen på et mix af services i public cloud.

Der er fordele og ulemper ved en hvilken som helst konfiguration og ved det sikkerhedssetup, der omgiver den.

For eksempel giver egne servere fuld kontrol over ressourceallokering – men er omvendt udfordret på svingende behov for kapacitet, hvorfor man er nødt til at overinvestere i betydelig grad. Ligeledes er det stærkt ressourcekrævende at oparbejde og vedligeholde et højt niveau af sikkerhed og redundans, ikke mindst fordi det stiller særdeles store krav til ansættelse af kostbare og svært tilgængelige ekspertkompetencer. Endelig stiller drift af egen hardware krav til løbende investering og kapitalbinding (Capex) og øger risikoen for akkumulering af teknologisk gæld.

Omvendt tilbyder Public Cloud-hosting alt den plads man kan ønske sig, men udfordringer omkring support og vedligehold af servere består.

Samtidig dikteres det ikke altid lige gennemskuelige omkostningsniveau i public cloud af globale udbydere, der de seneste år har benyttet lejligheden til at hæve priserne ganske betydeligt. Ligeledes udfordres muligheden for compliance i skyen kontinuerligt af EU's stadig skrappere krav til opbevaring og behandling af data.

Derimod giver Secure Private Cloud en lang række af de fleksible fordele, man kan opnå i public cloud – men i et dansk datacenter med mulighed for døgnsupport på dansk. Platformen er fleksibel og skalerbar og bygget af nyeste generation af hardware fra Dell, hvilket sætter os i stand til at levere en ydelse, som public cloud har svært ved at matche.

Samtidig fritager en hostingaftale med Unit IT din virksomhed for at foretage store og løbende investeringer i hardware – og her er fuld skalerbarhed med muligheden for at skrue frit op og ned for CPU- og storagekapacitet baseret på jeres aktuelle behov. Endelig kan du som nævnt drage fordel af en lang række servic- es og sikkerhedsværktøjer, udvalgt og driftet af Unit IT. Vel at mærke uden behov for at du selv skal ansætte og løbende efteruddanne ekstra IT-sikkerhedspersonale.

Totalservice med fokus på sikkerhed, stabilitet og modstandsdygtighed

Vi har specialiseret os i at levere sikre drifts-løsninger, der matcher vores kunders behov og økonomi. Secure Private Cloud ligger i tråd med denne filosofi ved at tilbyde én overskue-lig service, der kombinerer konventionel drift og support med et ekstraor- dinært højt sik-kerhedsniveau.

Secure Private Cloud leverer service og ved-ligehold af jeres servere kombineret med en række omhyggeligt udvalgte elementer, der løbende tilpasses og som øger din infrastruk-turs sikkerhedsniveau mod aktuelle og kom-mende cybertrusler.

Med egne datacentre har vi desuden mulighed for at hoste vores kunders løsninger i enten Private Cloud eller i Hybrid Cloud-konfigura-tioner. Samtidig høster du storskalafordele, da vi tilbyder at drifte din infrastruktur og dine servic- es på state-of-the art hardware kom-bineret med dyb teknisk kompetence indenfor sikkerhed og drift.

Vores backup services er brancheledende og med til at underbygge vores kunders ønsker om driftssikkerhed, redundans og adgang til hurtig og effektiv disaster recovery Service (DRaaS).

Endelig ligger vore datacentre – og dermed også vore kunders data – i Danmark, hvilket gør det nemt at sikre fuld compliance med både

EU-krav og eventuelle koncernpolitikker med krav om hosting indenfor EU's grænser. En-delig skal nævnes, at vore cloud-platforme er udsty- ret med en A+ energirating, hvilket bidrager til at minimere og dokumentere din organisations klimaaftryk.

Ekstra beskyttelse mod ransomware

I det aktuelle trusselsbillede er bekymringen for ransomwareangreb – hvor hele eller dele af IT-infrastrukturen tages som gidsel af de cyberkriminelle – med rette en af de faktorer, de fleste virksomheder er mest bekymrede for.

Derfor har vi implementeret en omfattende række af tiltag for at minimere risiko for ransomware og andre hackerangreb på vores serviceplatforme.

Vi har naturligvis stærke firewallsystemer og backupsystemer, der tager backup af vores serviceplatform-systemer og sender backup ud på geografisk adskilte lokationer.

Samtidig – og måske vigtigst – har vi "hærdet" vores serviceplatforme og management- netværk/systemer på en lang række felter, herunder:

• Minimerer risisko for "Lateral Movement" – dvs. spring fra system til system

• Brugere afkræves MFA-autentifikation ved login

• Systemadgange er tidsbegrænsede

• Her er ingen "global accounts" med altomfattende privilegier, ligesom vi har implementeret omfattende VLAN-segmenter- ing mv.

Dette er blot enkelte at de mange sikkerhed- stiltag, vi har implementeret for at minimere risikoen for angreb – samt for at minimere skadevirkningen, hvis uheldet alligevel skulle være ude. Og samlet udgør den samlede mængde af tiltag et stærkt værn mod ransom- ware og andre potentielt skadelige handlinger.

Bemærk dog, at ovenstående tiltag kun beskytter på Unit IT's serviceplatforme, hvorfor der stadig er en række tiltag, man som kunde selv skal arbejde med – og her rådgiver vi også gerne.

Fem søjler under din sikkerhed

Secure Private Cloud er fællesbetegnelsen for en model, der inkorporerer samspillet mellem en lang række elementer i vores ydelseskatalog. Den samlede ydelse bygger populært sagt på fem "søjler", nemlig:

Managed Service – nem og sikker administration ved hånden Her stiller vi services til rådighed, som gør det nemmere at optimere admin- istrere udvalgte dele af din IT- og sikkerhedsinfrastruktur. Samtidig får du mulighed for at stille IT-værktøjer og -platforme til rådighed for din organisa- tion baseret på dine eksakte krav til tilgængeligheds- og sikkerhedsniveau. Du drager desuden fordel af support og monitorering i døgndrift.

UCloud – markedsledende værktøjer, der hænger sammen Vore cloudservices bygger på tanken om "secure cloud by design" og omfatter markedsledende platforme og services indenfor bl.a. Infrastruc- ture-as-a-Service, backup og disaster-recovery driftet i A+ certificerede cloud-platform. Samtlige services er designet og skaleret med henblik på ekstraordinært højt sikkerhedsniveau, redundans og stabilitet.

End-user & Endpoint – frontlinjen i din sikkerhedsindsats Dine brugere og endpoint-enheder er frontlinjen i sikkerhedsindsatsen, hvorfor vi kan hjælpe dig med at konfigurere både laptops og mobile enheder, så de altid er sikret optimalt, er lette at overskue og administrere – samt konstant er patchet med seneste relevante sikkerhedsopdateringer på både operativsystem-, applikations- og hardwareniveau.

Public Cloud – hvor det giver størst værdi
Secure Private Cloud er en platform-agnostisk service, der benytter præcis de elementer, der kombinerer højt sikkerhedsniveau med enkel administra- tion – uanset om de så driftes i et af Unit IT's datacentre eller i Public Cloud.

Netværk – binder din virksomhed sammen
Vi forbinder alle dine services, applikationer og data i din infrastruktur – såvel indenfor og udenfor virksomhedens fire vægge – og stiller effektive net- værkssikkerhedstjenester, en moderne og effektive firewall samt værktøjertil rådighed, som sikrer din virksomhed mere effektivt mod cyberangreb, herunder mod DoS og malware.

Få hjælp til at forberede organisationen på succes

Secure Private Cloud rummer som nævnt en lang række services og værktøjer, som øger både sikkerhedsniveau, oppetid og skalerbarhed. Dertil kommer:

• Løbende scanning for og patching af sårbarheder med månedlig rapportering

• Antivirus og EDR (Endpoint Detection and Response)

• Backup med indbygget, automatisk restore-test

• Kalkulering af Secure Score, der dokumenterer sikkerhedsniveauet på jeres servere

Det er alt sammen kvaliteter, som i betydelig grad medvirker til at styrke jeres sikkerhedsniveau.

Samtidig er vi dog også åbne omkring, at et sikkerhedsorienteret samarbejde også stiller krav til din organisation før du drager fuld fordel af mulighederne. Her er således en klar gevinst forbundet ved at indgå i et samarbejde med Unit IT om jeres erfaringer, planer og udfordringer på sikkerhedsområdet – samt at arbejde målrettet for at forankre sikkerhedsindsatsen bredt i virksomheden; hele vejen fra lagergulvet til ledelsesgangen.

Her deler vi også gerne vores erfaringer for, hvordan du bedst orkestrerer indsatsen og forbereder din organisation på succes i bestræbelserne på at kombinerer styrket indsigt, modstandsdygtighed og fleksibilitet.

Vi er klar over, at mange virksomheder befinder sig i en situation, hvor de skal foretage en meget nøje overvejet afvejning af, hvilke IT-sikkerheds- mæssige tiltag de kan, bør og skal prioritere fremadrettet.

Der eksisterer en næsten uendelig række valgmuligheder ved udformningen af den fremtidige sikkerhedsplatform, og alligevel vil man sædvanligvis næsten altid vide, at der stadig er mere, man kunne gøre. Hvis blot man havde lidt flere specialistkompetencer in-house og et lidt større budget.

Her har vi på forhånd truffet en række af de sværeste valg, som gør det nemmere at øge IT-sikkerhedsniveaet markant uden samtidig at skulle øge headcount betragteligt. Ligesom vi også meget gerne rådgiver om, hvordan du prioriterer din cybersikkerhed, så du optimerer værdien af din investering.

Yderligere sikkerhedselementer

Secure Private Cloud er et af flere elementer til at beskytte jeres virksomhed og data. Vi tilbyder en række services for at øge sikkerheden, herunder:

SIEM - Identificer og reager på potentielle sikkerhedstrusler

Firewall – Next-gen funktioner som, IPS, Sandbox, Antibot, URL filter, mfl.

Microsegmentering – Opdeling af netværket i zoner/ segmenter for at begrænse muligheden for at malware kan sprede sig.

Anti-DDoS der forhindrer ødelæggende stormløb mod dine online services

Disaster Recovery Services (DRaaS) med hurtig recovery af dine beskadigede virtuelle servere på anden lokation

End-user & Device Management sikrer at dine medarbejdere sikkert og effektiv kan udføre sine IT-opgaver

Secure Hybrid Cloud Framework – Effektive værktøjer til at sikre det højeste niveau af sikkerhed og compliance for at beskytte brugeridentiteter på tværs af hybride cloud-netværk

Få mere information om Digital Suverænitet og Secure Private Cloud

+45 88 333 333

kontakt@unit-it.dk

Nærmest jër

Vi er lige så ambitiøse om jeres it, som I er om jeres forretning. Derfor insisterer vi på en ærlig snak nu – over en dårlig løsning senere. Faktisk kan vi slet ikke lade være.

For it-løsninger, der ikke virker, er ikke løsninger.

Forretningskritisk it er komplekst. Netop derfor gør vi os umage for, at samarbejdet med os er det modsatte.

Vi er specialister i it-infrastruktur lavet til virkeligheden - uanset om den infrastruktur står bedst i et dansk datacenter eller en global cloud. Eller i en kombination.

For uanset hvor infrastrukturen står, så er vi der, når det kører. Men endnu vigtigere, når det ikke gør.

Vi er 250 specialister fordelt i hele landet. Og vi hjælper danske virksomheder med at designe, bygge og drive de digitale platforme, der driver deres forretning.

Strandvejen 7 • DK-5500 Middelfart • +45 88 33 33 33 • unit-it.dk

unit it