



Servicebeskrivelse

Managed Detection and Response with Microsoft

Indledning

Dell Technologies Services er glade for at kunne levere Managed Detection and Response med Microsoft Service ("servicen") i overensstemmelse med denne servicebeskrivelse ("servicebeskrivelsen"). Dit tilbud, din ordreformular eller en anden gensidigt aftalt form for faktura eller ordrebekræftelse (den, der gælder, "Ordreformularen") indeholder navnet på de(n) service(s) og de tilgængelige servicemuligheder, som du har købt. Hvis du vil have yderligere assistance eller anmode om en kopi af servicekontrakterne, skal du kontakte teknisk support eller din salgsrepræsentant.

Omfanget af denne service

Servicen søger at tilbyde kunden Managed Detection and Response med Microsoft Services.

Servicen fjernleveres. Kunden er ansvarlig for alle Microsoft-licenser og -abonnementer. **Microsoft-licenser er ikke inkluderet som en del af denne service.** Se det [tekniske datablad](#) for oplysninger vedrørende mængdebegrænsninger for kundedata under denne service.

Nøglekomponenterne i servicen er beskrevet i tabel 1 nedenfor:

Tabel 1

Service købt	Servicens nøglekomponenter
Managed Detection and Response med Microsoft	<ul style="list-style-type: none"> • Service, der udnytter teknologi fra Microsoft Defender XDR og Microsoft Sentinel til administrationsplatformen. • Driftstimer: 24 timer i døgnet, 7 dage om ugen (24x7) • Service-kickoff/-opstart • Tenant Enablement & Readiness • Onboarding • Detektion • Trusselsreaktion • Servicerelateret sikkerhedskonfiguration • Kvartalsvis rapportering • Hændelsesreaktion • Omfatter ovenstående komponenter, der udnytter kundens aktuelt licenserede XDR-konto.

- Kunder, der kun køber servicetilbuddet, skal opfylde minimumskravene til softwaremodulet for at modtage servicen.

Bemærk: Produktfunktionen afhænger af den Microsoft-licens/det Microsoft-abonnement, som kunden har købt til at beskytte kundens workloads, og det har betydning for, hvilke afhjælpningsmuligheder der er tilgængelige for Dell Technologies Services-teamet.

Åbningstider

Dell Technologies Services' virtuelle sikkerhedsdriftscentre (SOC) er designet til at give kunden service 24 timer i døgnet, 7 dage om ugen (24x7).

Servicen leverer en komplet løsning til kundens IT-miljø og giver sikkerhed til enheder, netværk, brugeraktivitet, cloud-applikationer og cloud-ressourcer, der udnytter teknologi fra Microsoft Defender og Sentinel som administrationsplatform.

Servicen omfatter overvågning af disse Microsoft-komponenter med Microsoft Sentinel som en del af basistilbuddet:

M365 Defender-produkter, der er omfattet til overvågning af:

- Microsoft Defender til Office 365
- Microsoft Defender til slutpunkt (**minimum required service**)
- Microsoft Defender til servere (indbygget i Microsoft Defender til slutpunkt)
- Microsoft Defender til identitet
- Microsoft Defender til cloud-apps

Nødvendige forudsætninger for sagsadministration/-overvågning

- Microsoft Sentinel (**minimum required service**)

Bemærk: Der kræves et dedikeret Azure-abonnement og -arbejdsområde til servicen.

Service til Tenant Enablement & Readiness leveres inden for normal åbningstid. Tenant Enablement & Readiness skal være fuldført, før kunden kan introduceres til Dells sikkerhedsdriftscenter (SOC), der er åbent 24/7.

Tabel 2 nedenfor viser hvert af elementerne i servicens nøglekomponenter.

Tabel 2

Nøglekomponent	Elementer
Service-kickoff/-opstart	<ul style="list-style-type: none"> • Serviceopstartsmøde (kickoffmøde) • Opret kundekonto på ITSM-platformen • Tjekliste før engagement udfyldt af Kunden
Tenant Enablement & Readiness	<ul style="list-style-type: none"> • Gennemgang af forudsætninger for licens og abonnement • Planlægning forud for implementering • Gennemgang/konfiguration af Defender-politikken • Connectorer og datakilder • Dataoverførsel og logindsamling • MDR-overvågning og -rapportering

SOC-onboarding	<ul style="list-style-type: none"> • Gennemgå kundens IT-miljø • Aktivering af service
Detektion	<ul style="list-style-type: none"> • 24x7-adgang til sikkerhedsanalytikere • Trusselsdetektion og -undersøgelser • Dell-indledt trusselsjagt
Trusselsreaktion og sikkerhedskonfiguration	<ul style="list-style-type: none"> • Trusselsreaktion • Servicerelateret sikkerhedskonfiguration • Fjernafhjælpning relateret til hændelsen
Kvartalsvis rapportering	<ul style="list-style-type: none"> • Kvartalsvis rapport • Sikkerhedsanbefalinger
Hændelsesreaktion	<ul style="list-style-type: none"> • Fjerninitiering af hændelsesreaktion
Projektstyring	<ul style="list-style-type: none"> • Administration af disse processer

Detaljeret beskrivelse

Servicekickoff/-opstart:

Serviceopstartsmøde

En Dell Technologies Services-projektleder vil indkalde til et møde for at gennemgå serviceforventninger og -krav med kunden, så der kan foretages planlægning af serviceleveringen. Formålet med serviceinitieringsmødet er at:

- Gennemgå og diskutere kundeprofilreaktioner for at forstå kundens IT-miljø, sikkerhedskontroller og enhver anden relevant kontekst.
- Give vejledning om de eksisterende detektionsmekanismer i kundens miljø, og hvordan de kan anvendes hos kunden.
- Give vejledning om serviceintegrationer med tredjepartssoftware og -hardware.

Såfremt Kunden har yderligere krav, der ikke er omfattet af denne Servicebeskrivelse, vil hjælp i forbindelse med disse krav blive foreslået som en ekstra service mod et yderligere gebyr.

Tjekliste før engagement udfyldt af Kunden

Kunden er ansvarlig for at udfylde tjekliste før engagement, forud for gennemgangen af IT-miljøet. Tjeklisten før engagement, fremsendes af Dell Technologies Services-projektlederen og indeholder en detaljeret tjekliste og IT-miljøspecifikationer.

Gennemgang af IT-miljø

Gennemgangen af IT-miljøet udføres for at indsamle data om kundens eksisterende IT-miljø, hvor servicen skal implementeres.

Tenant Enablement & Readiness

Dell Technologies Services giver vejledning i kernekomponenter til understøttelse af servicen. Tenant Enablement & Readiness er designet til at sikre, at kundens IT-miljø opfylder minimumskravene til konfigurationer, for at kunne levere overvågning 24/7.

Baseret på den indledende gennemgang af kundens IT-miljø vil Dell Technologies Services vejlede kunden i konfiguration af Defenders basislinjepolitikker og konfigurationen af (om nødvendigt) Sentinel-arbejdsområdet.

Se det [tekniske datablad](#) for flere oplysninger vedrørende begrænsningerne for Tenant Enablement & Readiness under denne service.

Oversigt over Tenant Enablement & Readiness

- 1) Licens og abonnement: Sørg for, at kunden har de nødvendige licenser og abonnementer til Microsoft 365 Defender. Identificer behovet for yderligere kundelicenser baseret på kundens organisatoriske behov.
- 2) Planlægning forud for implementering: Gennemgå kundens sikkerhedsbehov og eksisterende infrastruktur.
- 3) Gennemgang/konfiguration af Defender-politik: Aktivér Microsoft 365 Defender-komponenter i kundens Microsoft 365-administrationsportal efter behov. Hjælp efter kundens godkendelse med konfiguration af grundlæggende sikkerhedsindstillinger på Defender-portalene/-portalerne.
- 4) Dataconnectorer, dataoverførsel og logindsamling: Integrer Microsoft 365 Defender i kundens Sentinel-miljø for at centralisere hændelseslogfiler og advarsler om sikkerhed, når de er tilgængelige og kun som anvist af kunden. Rådgiv om implementering af understøttede dataconnectorer til indsamling af sikkerhedsdata fra Microsoft Defender til slutpunkt, Microsoft Defender til Office 365 og Microsoft Defender til identitet.
- 5) MDR-overvågning og -rapportering: Gør overgangen til kontinuerlig overvågning af sikkerhedsstatus for kundens IT-miljø mulig ved hjælp af Microsoft Defender-sikkerhedscenteret.

SOC-onboarding

Aktivering af service:

- Verificer lejerforudsætninger for servicen
 - Guide kunden igennem processen med at sørge for adgang til Dell Technologies Services-teamet
 - Guide kunden igennem tildelinger via Role-Based Access Controls (RBAC), der kræves for at få adgang til M365 Defender XDR
- Bemærk:** Ovenstående aktivitet gælder kun, hvis Microsoft Sentinel/Microsoft Defender til servere (Microsoft Defender til cloud) er omfattet.
- Guide kunden igennem konfiguration af Microsoft Sentinel og Azure Lighthouse
 - Guide kunden igennem konfiguration af Microsoft Sentinel og Azure Lighthouse for Microsoft Sentinel/Defender til cloud iht. ARM-skabelonen til administration af Defender til server
 - Konfigurer grundlæggende automatiseringsregel/vejledning for kundereaktion på en sikkerhedshændelse og enhver påkrævet SOC-automatisering
 - Undersøgelse og sagsadministration dokumenteres via kundens Microsoft Sentinel/Defender-forekomst sammen med Dells ServiceNow/ITSM-forekomst. Dell Technologies Services arbejder sammen med kunden om at konfigurere denne funktion. Enhver kudeanmodning eller forespørgsler relateret til en hændelse eller servicen skal indsendes via ServiceNow/ITSM-plattformen.

Detektion

Overgang til Steady State:

Dell Technologies Services' anbefaling er at indbygge kundens Defender- og Sentinel-lejer så hurtigt som muligt, ideelt set inden for en måned efter servicestart (anbefales ikke derefter), hvilket maksimerer den indsigt og overvågning, som servicen leverer.

Realtidsbaserede og historiske data (underlagt Microsofts produktfunktioner og lagerindstillinger):

- Relevante sikkerhedshændelser, som Dell Technologies Services vurderer som "sande positive", og som kræver kundehandling, eskaleres til kunden inden for de serviceniveauer, der er beskrevet nedenfor
- Hændelser, der vurderes som "falske positive" eller automatisk afhjælpes, noteres i kundens kvartalsvise rapport
- Tilpassede indikatorer for kompromitteringer, der leveres af Dell Technologies Services, analyseres, efterhånden som de modtages eller oprettes

24x7-adgang til sikkerhedsanalytikere

Dell Technologies Services-sikkerhedsanalytikere er tilgængelige 24x7 for at hjælpe med relevante undersøgelser.

Trusselsdetektion og -undersøgelser

Gennemgang og undersøgelse af trusler, der er opdaget i XDR-programmet. Trusler, der kræver yderligere analyse efter Dell Technologies' skøn, resulterer i oprettelsen af en undersøgelse i Microsoft Defender XDR- og Sentinel-programmerne. Dell Technologies kontakter kunden via XDR-portal, e-mail eller understøttede integrationer, hvis der indsamles tilstrækkelige beviser til at vurdere en trussel som skadelig, eller hvis Dell Technologies kræver yderligere input fra kunden for at fortsætte undersøgelsen.

Trusselsjagt

Dell Technologies udfører trusselsjagt på tværs af kundens IT-miljø for at finde relevante indikatorer for kompromisser og taktikker, der er indsamlet fra aktuelle hændelsesreaktionsaftaler. Trusselsjagtaktiviteter er begrænset til data indsamlet via XDR-plattformen. Dell Technologies vil inspicere indsamlet kundeteleometri for at detektere aktivitet, såsom tilstedeværelse af vedholdende mekanismer, unormal brugeraktivitet, trusselsaktørtaktik, unormal netværkskommunikation og unormal programanvendelse. Trusler, der registreres som en del af trusselsjagtprocessen, vil resultere i oprettelse af en undersøgelse og underretning af kunden via XDR-portal, e-mail eller understøttede integrationer.

Trusselsreaktion

Under introduktionen skal kunden forhåndsgodkende udvalgte trusselsreaktionshandlinger, der kan udføres som en del af servicen. Dell Technologies Services udfører trusselsreaktionshandlinger ved at bruge XDR-plattformen.

Servicerelateret sikkerhedskonfiguration

Dell Technologies Services kan godkende op til 40 timers servicereleateret fjernsikkerhedskonfiguration efter behov for at hjælpe kunden for hvert kvartal i serviceperioden. Sikkerhedskonfigurationen er specifikt begrænset til undersøgelser og/eller advarsler som følge af levering af servicen og kan omfatte:

- Vejledning i Fejlfinding af MDR-slutpunktsagent og bedste praksis.
- Vejledning i opdateringer af XDR-platforms politikker.
- Vejledning i konfiguration og integration af tredjepartsprogrammer i XDR-plattformen.

Hvis der er behov for mere end 40 timers servicereleateret hjælp til trusselsreaktion og sikkerhedskonfiguration i et enkelt kvartal i løbet af serviceperioden, kan kunden kontakte sin Dell Technologies-kontoadministrator for at købe ekstra tid. Al uudnyttet tid ved udgangen af hvert kvartal af Serviceperioden går tabt. Yderligere tid, der er købt til et fremtidigt kvartal inden for serviceperioden, kan ikke anvendes før starten af det kvartal, for hvilket den blev købt.

Kvartalsvis rapportering

Dell Technologies Services udarbejder en kvartalsvis rapport om tendenser og unormal aktivitet observeret inden for kundens IT-miljø gennem serviceplatformen og kommer med anbefalinger til, hvordan man forsvarer sig mod trusler. Den kvartalsvise rapport indeholder en gennemgang af tendenserne for undersøgelser og advarsler, analyser og en vejledning i sikkerhedsforhold.

Hændelsesreaktion

Efter underretning fra Dell Technologies Services' sikkerhedsanalytiker er følgende eksterne hændelsesreaktionskomponenter tilgængelige.

Fjerninitiering af hændelsesreaktion

Dell Technologies Services leverer op til 40 timers fjernsupport for hændelsesreaktion til kunden for hvert år i løbet af serviceperioden, begrænset i omfang til antallet af overvågede slutpunkter. Assistancen kan omfatte, men er ikke begrænset til følgende:

- Oprettelsen af det enkle kontaktpunkt for hændelsesreaktions servicen
- Påbegyndelse af analyse af kundens lokale infrastrukturer og cloudinfrastrukturer, som kan indeholde:
 - hostdata
 - netværksdata
 - skadelig kode
 - logdata, og
 - efterretninger om cybertrusler
- Indledende analyse og koordinering af vejledning og support omkring digital medie håndtering
- Indledende statusrapportering og sporing af handlingselementer
- Indledende overblik over den nødvendige afhjælpning og de næste skridt

Hvis der er behov for mere end 40 timers fjernsupport til hændelsesreaktion i et hvilket som helst år af serviceperioden, kan kunden kontakte sin Dell Technologies-kontoadministrator for at købe ekstra tid. Eventuelt uudnyttet tid ved udgangen af hvert år af Serviceperioden vil gå tabt. Tid for et kommende år inden for serviceperioden kan ikke anvendes før starten af det år, for hvilket det blev købt.

Projektstyring

Dell Technologies Services vil tildele en projektleder (PM) som den primære kontakt ("SPOC", Single Point of Contact) til at administrere leveringen af denne opgave.

- Primær kontakt og ansvar for vellykket levering af servicerne.
- Bevaring af fokus på tid, omkostninger og omfang.
- Koordinering og facilitering af opstarts-, status-, projektgennemgangs- og afslutningsmøder.
- Etablering og administration af serviceplanen, kommunikationen og statusrapporteringen.
- Facilitering af administration af ændringer efter behov.
- Bekræftelse på, at de leverede services er i overensstemmelse med servicebeskrivelsen.
- Indhentning af accept af levering og servicefuldførelse fra kunden.

- Administration af kundeforholdet.
- Projektledelsesaktiviteter fjernudføres.

Abonnementsfakturering

Servicen giver mulighed for månedlig abonnementsfakturering, som vil være angivet på den oprindelige ordreformular med påtegningen "Abonnement", hvis kunden har tilvalgt det. Alternativt gælder standardvilkårene og -faktureringen. Følgende vilkår gælder for abonnementsfakturering:

- Den oprindelige ordreformular angiver kontraktperioden og antallet af kontraktmæssige slutpunkter. Serviceperioden fornyes derefter automatisk med de samme løbende perioder.
- Kunden kan øge antallet af administrerede slutpunkter ved at indsende en ordre på yderligere slutpunkter. Disse yderligere slutpunkter vil blive kombineret med Kundens eksisterende administrerede slutpunkter, og bliver det nye "Samlede antal slutpunkter."
- Kunden vil blive bagudfaktureret månedligt for det samlede antal slutpunkter, der er administreret ved udgangen af kalendermåneden.
- Kunden må på intet tidspunkt reducere antallet af administrerede slutpunkter til en mængde under det samlede antal slutpunkter, og det samlede antal slutpunkter må heller ikke reduceres med henblik på fakturering
- En rapport over Kundens slutpunkter, der bruger Servicen, vil blive stillet til rådighed for Kunden.
- Kunden modtager en enkelt faktura for alle lokationer (inden for samme region.)
- Kunden er forpligtet til at give Dell Technologies skriftlig varsel tres (60) dage før opsigelse af Kundens automatisk fornyede Serviceperiode.

Begrænsninger af datavolumen og -brug

Servicen anvender kundens Microsoft Sentinel-, Azure- og Microsoft Defender XDR-lejer samt et kundeforholdet, dedikeret Azure-abonnement og -arbejdsområde til servicen. Kunder, der køber denne service, er ansvarlige for at forstå og administrere deres egne datamængde- og brugsbegrænsninger, og Dell Technologies Services fraskriver sig ethvert sådant relateret ansvar eller forpligtelser over for kunden. Kunden anerkender desuden at være ansvarlig for alle datastorage- og databehandlingsomkostninger, der er forbundet med Azure-abonnementet og Sentinel-arbejdsområdet.

Datastorageplaceringer

Kunder, der køber dette tilbud, er ansvarlige for uafhængigt at bestemme deres datastorageplacering(er). M365-området og de konfigurerede arbejdsområder for dataplaceringer indstilles i kundens Microsoft Azure-miljø efter kundens instruktion og ønske.

Microsoft Sentinel gemmer kundedata inden for det område, der er defineret i arbejdsområdekonfigurationen. Microsoft gemmer kundedata i samme geografiske område som arbejdsområdet for loganalyse, der er knyttet til kundens Microsoft Sentinel-miljø.

Microsoft Sentinel behandler kundedata på én af to placeringer:

- Hvis arbejdsområdet til loganalyse er placeret i Europa, behandles kundedata i Europa.
- For alle andre placeringer behandles kundedata i USA.

Serviceniveauer

Dell måler sin trusselsreaktion og sin afviklingspræstation i forhold til en række serviceniveauer.

Måling	Definition	Mål
Gennemsnitlig reaktionstid	Den gennemsnitlige tid målt fra det tidspunkt, hvor en høj eller kritisk alarm genereres, til det tidspunkt, hvor en undersøgelse oprettes i XDR-applikationen.	15 minutter
Gennemsnitlig svartid	Den gennemsnitlige tid målt fra det tidspunkt, hvor en undersøgelse oprettes, til det tidspunkt, hvor en Dell-analytiker leverer en indledende hændelsesanalyse i XDR-applikationen eller giver et svar til kunden.	60 minutter
Gennemsnitlig løsnings tid	Den gennemsnitlige tid målt fra det tidspunkt, hvor en undersøgelse oprettes i XDR-applikationen, til det tidspunkt, hvor undersøgelsen er løst.	24-48 timer (kræver kundesamarbejde)

Forudsætninger

Dell Technologies Services har specifikt antaget følgende forudsætninger under dokumentation af den service, der er angivet i denne servicebeskrivelse:

1. Alle oplysninger leveret af kunden vedrørende stedets tekniske krav og arkitektur skal i det væsentlige være rigtige.
2. Dell Technologies Services implementerer kun servicerelaterede ændringer i sikkerhedskonfigurationen, som er tilladt i henhold til Dell Change Management-processen.
3. Dell Technologies Services er ikke ansvarlig for eventuelle politikændringer, som kunden implementerer uden at følge Change Management-processen.
4. De services, der er beskrevet i denne servicebeskrivelse, vil blive udført eksternt.
5. Dell Technologies Services administrerer miljøet via Microsoft Sentinel-dashboards.
6. Produktfunktionen afhænger af den Microsoft-licens og det Microsoft-abonnement, som kunden har købt til at beskytte kundens workloads, og det har betydning for, hvilke afhjælpningsmuligheder der er tilgængelige for Dell Technologies Services-teamet. Til beskyttelse af servere anbefales Defender til servere Plan 1 som minimumsbasislinje. Servere vil dog drage fordel af yderligere beskyttelse fra Defender til servere Plan 2, som tilføjer yderligere Microsoft Defender til cloud-funktioner.
7. Dell forbeholder sig ret til at ændre sagsadministrations-/ITSM-løsningen, efterhånden som nye funktioner frigives.
8. Antallet af kundeslutpunkter beregnes ud fra antallet af slutpunkter, der overvåges i Sentinel.
9. Dell Technologies Services flytter en kunde fra SOC-onboarding til Steady State-overvågning, når mindst 40 % af slutpunktssensorerne er blevet implementeret på de licenserede slutpunkter.

10. Hvis denne service ikke fuldføres inden for det beskrevne tidsrum, forbeholder Dell Technologies Services sig ret til at vurdere årsagen. Hvis årsagen er uden for Dell Technologies Services' kontrol, vil Dell EMC Services foreslå nogle trin til at håndtere forsinkelsen. Disse trin kan gøre det nødvendigt for kunden at købe yderligere services eller påtage sig ekstra omkostninger for at gøre Dell Technologies Services i stand til at gennemføre denne service. Såfremt Kunden har yderligere krav, der ikke er omfattet af denne Servicebeskrivelse, vil hjælp i forbindelse med disse krav blive foreslået som en ekstra service mod et yderligere gebyr.
11. Microsoft Sentinel-økosystemet har et højt signal-støj-forhold og derfor et lavt antal falske positive. Dell Technologies Services undersøger informative advarsler og advarsler med lav alvorsgrad baseret på en stor mængde af samme type advarsel, som prioriteres efter undersøgelse af advarsler med høj og middel alvorsgrad.

Udelukkelse

Selvom servicen har til formål at hjælpe kunden med at identificere og reducere risikoen, er det umuligt helt at eliminere risikoen. Derfor giver Dell Technologies Services ingen garanti for, at indtrænging, kompromitteringer eller anden uautoriseret aktivitet ikke vil forekomme i kundens IT-miljø.

For at undgå tvivl er følgende aktiviteter ikke omfattet af denne servicebeskrivelse:

1. Enhver service, opgave eller aktivitet, som ikke udtrykkeligt er angivet i denne servicebeskrivelse.
2. Servicen omfatter ikke udviklingen af nogen intellektuel ejendom, som kun er skabt specifikt til kunden.
3. Fejlfinding eller løsning af eksisterende system-/serverproblemer, medmindre andet er beskrevet i denne servicebeskrivelse, herunder, men ikke begrænset til, fejl ved M365 Defender-sensorer eller ved Microsoft Sentinel-understøttede agenter
4. Test af integration mellem Dell Technologies-produkter og andre tredjepartsprodukter, såsom, men ikke begrænset til, krypterings- eller sikkerhedsprodukter fra tredjepart.
5. Afhjælpning af de performance-relaterede problemer, som blev identificeret ved analyse af kundens miljø, medmindre andet er beskrevet i denne servicebeskrivelse.
6. Dell Technologies Services' ansvar (herunder økonomisk ansvar) for kundens og/eller tredjeparters personale, hardware, software, udstyr eller andre aktiver, der i øjeblikket anvendes i operativsystemets miljø til kunden, medmindre andet er beskrevet i denne servicebeskrivelse.
7. Løsning i forbindelse med kompatibilitetsproblemer eller andre forhold, der ikke kan løses af producenten, eller for at konfigurere hardware, software, udstyr eller aktiver, i strid med de indstillinger, der understøttes af producenten.
8. Overvågning af informative advarsler og advarsler med lav alvorsgrad er ikke omfattet af denne service.
9. Installation af eller konfiguration af syslog-servere eller syslog/CEF-indsamlere
10. Konfiguration af appprogrammer til Microsoft Defender til cloud.
11. Overvågning af Microsoft Defender til cloud-funktioner, der ikke er inkluderet i Microsoft Defender til servere Plan 1- eller Plan 2-licensen.
12. Overvågning af eventuelle servere, der ikke er blevet onboardet som en del af servicen. Dell Technologies prioriterer ikke advarsler relateret til andre enheder end de onboardede servere.
 - a. Bemærk: Dette gælder kun for omfattede servere/Defender til cloud.

Tilbudsspecifikke kundeansvarsområder

Kunden accepterer at samarbejde med Dell Technologies Services i forbindelse med leveringen af de aftalte Services og accepterer følgende ansvar:

1. At følge processen til administration af ændringer for anmodninger om at foretage ændringer på XDR-plattformen og sende Dell Technologies Services den kundekontakt, der godkender anmodninger om administration af ændringer.
2. At give Dell Technologies Services-analytikeren adgang til alle påkrævede kundemiljøer i serviceperioden.
3. At stille en kundenomineret repræsentant til rådighed, der vil være til stede og tilgængelig for alle planlægnings- og gennemgangssessioner.
4. At give alle tilladelser, herunder tredjepartsgodkendelser, der kræves for at tillade Dell Technologies Services at administrere XDR-plattformen på kundens vegne.
5. At implementere agent/sensor(er) på alle kundens licenserede slutpunkter ved hjælp af passende programimplementeringsværktøjer (f.eks. Intune, SCCM osv.).
6. At deltage i leveringen af servicen på passende vis. Kunden forstår, at uden korrekt deltagelse, herunder målsætning, kan teknikeren ikke opfylde kundens behov eller udføre servicen.
7. At samarbejde med og imødekomme instruktionerne fra Dell Technologies Services-analytikere.
8. At gennemgå og acceptere tjeklister og testplaner før engagement.
9. Sørge for, at kundens IT-miljø har en understøttet slutpunktsagent, der er installeret på en host, der er licenseret til Servicen.
10. At indhente al support til tredjepartsslutpunktsagenter fra tredjeparter eller andre autoriserede kilder; Dell Technologies Services yder ikke support for tredjepartsslutpunktsagenter.
11. At fjerne eller tilføje en undtagelse for modstridende første- og/eller tredjepartsantivirus- og EDR-agenter efter behov, så Dell Technologies Services kan levere denne service.
12. At sikre tilgængelighed af og adgang til tilstrækkelig netværksbåndbredde til at udføre servicen.
13. Sørge for, at alle enhedsintegrationer fungerer korrekt, og fortsætter med at fungere korrekt. Hvis kunden kræver det, kan Dell Technologies Services hjælpe med dette mod et gebyr.
14. At give passende adgang til XDR-programmer for integration(er).
15. At sørge for, at kundesikkerhedskontroller er compatible med XDR-integrationer.
16. Administrere legitimationsoplysninger og tilladelser til integrationer med XDR-programmet.
17. Sørge for, at listen over kundeautoriserede kontakter forbliver aktuel, herunder tilladelser og tilknyttede oplysninger.
18. At give omgående oplysninger og assistance (f.eks. filer, logfiler, IT-miljøkontekst) under Dell Technologies Services' trusselsundersøgelser.
19. At identificere og godkende alle kundeautoriserede brugere af tjenesten.
20. Kontrollere mod uautoriseret adgang for brugere, og opretholde fortroligheden af brugernavne, adgangskoder og kontooplysninger.
21. Ansvar for alle aktiviteter, der udføres af kundeautoriserede brugere, og øjeblikkelig underretning af Dell om enhver uautoriseret brug af servicen.
22. Bruge tofaktorautentifikation, hvor det er muligt, for at tilgå Servicen.
23. Acceptere alle opdateringer og opgraderinger til og af slutpunktsagenten, der er nødvendige for servicens korrekte funktion og sikkerhed.
24. At sørge for Dell Technologies serviceafbrydelsesvinduer efter behov.
25. At kontrollere dataadgang for at forhindre bestøvning af data på tværs af klienter og for at begrænse risikoen for datatab eller datalækage i kundens miljø.
26. At opretholde et nøjagtigt antal administrerede slutpunkter, der understøttes af servicen.
27. At konfigurere Microsoft Sentinel Azure-abonnementet og give den adgang, som en Dell-analytiker har brug for. Dette er en forudsætning for servicen.
28. At give adgang til Microsoft 365 Defender via Microsoft Sentinel. Adgangen gives via Microsoft Entra ID B2B-invitationer, der sendes af kunden til Dell-analytikere.

29. Den fysiske sikkerhed og netværkssikkerheden i kundens miljø.
30. At levere dokumentation af standardskabeloner for DT-servicen, medmindre begge parter aftaler andet.
31. At stille kontaktoplysninger til mindst to (2) eskaleringsniveauer til rådighed, så du kan reagere rettidigt på Dell-eskalationer. Kunden forventes at stille kontaktoplysninger til brug ved eskalering på personer, der er tilgængelige under helligdage og ved forretningslukning.
32. Bevar tilstanden, justeringen og konfigurationen af Microsoft Sentinel-dashboards.
33. At indsende anmodninger om teknologisupport til Microsoft med henblik på afhjælpning. Dell Technologies Services yder ikke support til tredjepartsslutpunkttagenter.
34. At bestemme, hvor mange af kundens sikkerhedsdata der skal overføres til Microsoft Sentinel.
35. At overvåge advarsler, der genereres for enheder, som ikke er servere.
36. At fjerne enhver AV/EDR-agent fra første-/tredjeparter.
37. At indhente de nødvendige samtykker for DT-servicen til udførelse af servicen
38. Alle omkostninger til dataopbevaring og databehandling.
39. At konfigurere politikindstillingerne, så de opfylder kundens behov.
40. At tilføje integrationer og datakilder til den administrerede MDR-platform.
41. At tilbyde et dedikeret Azure-abonnement, som er nødvendigt for at levere sags-/hændelsesadministration, undersøgelser og kvartalsvise rapporter via Microsoft Sentinel.
42. Onboarding af Android- og iOS-enheder. Bemærk, at enhver telefon, der overvåges, tæller som et slutpunkt, der overvåges som en del af denne service.

Ordliste

Tabel 3

Løbetid	Beskrivelse
Advarsel	Prioriterede forekomster af mistænkelig eller skadelig adfærd observeret af MDR-programmet.
Sagsadministration	Centraliseret platform, der bruges til at undersøge og administrere sikkerhedshændelser og -alarmer.
Administration af ændringer	Den kontrollerede identifikation, implementering og godkendelse af nødvendige ændringer i et kundemiljø.
Slutpunktsagenter/-sensorer	Et program installeret på et slutpunkt, der bruges til at indsamle og sende oplysninger om aktiviteter og operativsystemoplysninger for slutpunktet til sikkerhedsprogrammet til analyse og detektion af trusler.
Endpoint Detection and Response ("EDR")	En sikkerhedsplatform, der bruger førstepartsslutpunktsagenten til at overvåge slutbrugerenheder – stationære computere, bærbare computere, tablets og telefoner – for trusler, som antivirussoftware ikke kan registrere.

Extended Detection and Response ("XDR")	En registrerings- og reaktionsplatform, der strækker sig ud over blot det traditionelle slutpunkt (cloud, OT, netværk osv.). XDR-plattformen bruger integrationer eller connectors til at indtage selv-vejede, tredjeparts- eller serviceorienterede data, der krydskorreleres til sikkerhedsovervågningskontekst.
Hændelsesreaktion	Reaktionshandlinger, der er truffet for at afbøde en identificeret sikkerhedshændelse.
Integrering	API (Application Programming Interface) eller andre softwarescripts til udførelse af de aftalte Services for den tilsluttede teknologi.
Undersøgelse	En central placering, der bruges til at indsamle beviser, analyser og anbefalinger relateret til en trussel, der kan være rettet mod et aktiv i kundens IT-miljø.
Managed Detection and Response Application ("MDR")	Sikkerhedsprogram, der er understøttet af Dell MDR-tilbuddet. For tekniske detaljer henvises til det tekniske datablad .
Sikkerhedshændelse	En omstændighed, hvor der er opstået en kompromittering eller hvor der er mistanke om kompromittering, der involverer kunden.
Sikkerhedspolitik	XDR-plattformens politikker, der håndhæver forebyggelses- og registreringsindstillingerne i kundens miljø.
Sikkerhedskonfiguration	40 timers service pr. kvartal inkluderet i MDR, der giver kunderne undersøgelses- eller advarselsrelaterede reaktionshandlinger.
Tenant Enablement & Readiness	At give vejledning om de kernekomponenter, der er nødvendige for at muliggøre servicen. Tenant Enablement & Readiness er designet til at sikre, at kundens IT-miljø opfylder minimumskravene til konfigurationer, for at kunne levere overvågning 24/7.
Trussel	Enhver aktivitet identificeret af MDR-programmet, der kan forårsage skade på et aktiv i kundens IT-miljø.
Trusselsjagt	Den cykliske proces, hvor både softwaren og mennesker søger efter tidligere uidentificerede trusler i et IT-miljø.
Trusselsreaktion	Tilgængelige reaktioner på platformen i XDR-programmet, f.eks. "isoler host" eller "bloker fil" (indeslutningstypehandling).

Kundens generelle ansvarsområder

Myndighed til at tildele adgang. Kunden erklærer og garanterer, at der er indhentet tilladelse fra både kunden og Dell Technologies Services til at få adgang til og anvende, enten via fjernadgang eller personligt, software ejet af eller givet i licens til kunden samt hardware, systemer og data placeret derpå og alle hardware- og softwarekomponenter omfattet deri med det formål at levere disse services. Hvis kunden ikke allerede er i besiddelse af denne tilladelse, er kunden forpligtet til, for egen regning, at indhente en sådan tilladelse, inden kunden anmoder Dell Technologies Services om at udføre disse services.

Kundeklausul. Hvor loven tillader det, kan kunden i en periode på to år fra den anførte dato på ordreformularen, uden Dell Technologies Services, ikke direkte eller indirekte anmode om ansættelse af en Dell Technologies Services-medarbejder, som han/hun har været i kontakt med i forbindelse med Dells udførelse af servicen uden et skriftligt samtykke fra Dell Technologies Services. Forudsat, at generelle annoncer og andre lignende, almene henvendelser i bred form ikke vil udgøre direkte eller indirekte henvendelse herunder, og at kunden har tilladelse til at opfordre til ansættelse af en medarbejder, som har afsluttet sin ansættelse eller har fratrukket sin stilling hos Dell Technologies Services, inden han/hun indleder drøftelser om ansættelse med dig.

Samarbejde med kunden. Kunden forstår, at uden et omgående og tilstrækkeligt samarbejde kan Dell Technologies Services ikke udføre servicen, eller hvis den udføres kan servicen være væsentligt ændret eller forsinket. Derfor skal kunden straks og på rimelig måde samarbejde med Dell Technologies Services om alt nødvendigt for at Dell Technologies Services kan yde servicen. Hvis kunden ikke samarbejder på et rimeligt niveau i henhold til det foregående, vil Dell Technologies Services ikke være ansvarlig for manglende opfyldelse af servicen og kunden vil ikke være berettiget til en refundering.

Onsite-forpligtelser. Hvor det er nødvendigt at udføre services onsite, skal kunden sikre gratis (uden at det koster noget for Dell Technologies Services), sikker og tilstrækkelig adgang til kundens faciliteter og miljø, herunder god plads til udførelse af arbejdet, elektricitet, sikkerhedsudstyr (hvis nødvendigt) og en lokal telefonlinje. Der skal ligeledes være adgang til en skærm, en mus (eller et pegeredskab) og et tastatur (uden omkostninger for Dell Technologies Services), hvis systemet ikke allerede omfatter disse elementer.

Sikkerhedskopiering af data. Kunden skal foretage en sikkerhedskopiering af alle eksisterende data, software og programmer på alle påvirkede systemer forud for og i løbet af leveringen af denne service. Kunden skal udføre regelmæssige sikkerhedskopieringer af de gemte data på alle berørte systemer som en sikkerhedsforanstaltning mod eventuelle fejl, ændringer eller tab af data. Dell Technologies Services er ikke ansvarlig for gendannelse eller geninstallation af programmer eller data.

Medmindre det er påkrævet ifølge relevant lokal lovgivning, VIL DELL TECHNOLOGIES SERVICES IKKE HAVE NOGET ANSVAR FOR:

- ALLE DINE FORTROLIGE, OPHAVSRETTLIGT BESKYTTEDE ELLER PERSONLIGE OPLYSNINGER
- TABTE ELLER BESKADIGEDE DATA, PROGRAMMER ELLER SOFTWARE
- BESKADIGEDE ELLER TABTE UDTAGELIGE MEDIER
- NEDETID FOR ET SYSTEM ELLER NETVÆRK, OG/ELLER
- NOGEN HANDLINGER ELLER UDELADELSER, HERUNDER FORSØMMELIGHED, AF DELL TECHNOLOGIES SERVICES ELLER EN TREDJEPARTSSERVICEUDBYDER.

Tredjepartsgarantier. Disse services kan indebære, at Dell Technologies Services skal have adgang til hardware eller software fra andre producenter end Dell Technologies Services. Visse producenters garantier bortfalder muligvis, hvis Dell Technologies Services eller andre end producenten selv udfører arbejde på hardwaren eller softwaren. Kunden skal sikre, at Dell Technologies Services' udførelse af services ikke vil påvirke sådanne garantier, eller hvis de gør, at påvirkningen vil være acceptabel for kunden. Dell Technologies Services fraskriver sig ethvert ansvar for tredjepartsgarantier eller eventuelle virkninger, som service kan have på disse garantier.

Ekskluderede data. Ekskluderede data" betyder: (i) data, der er fortrolige, og som anvendes i USA. krigsmaterielliste (herunder software og tekniske data); eller begge dele; (ii) artikler, services og relaterede tekniske data, der er udpeget som forsvarsartikler og forsvarsservices; (iii) frigivne ITAR-data (International Traffic in Arms Regulations); og (iv) personligt identificerbare oplysninger, der er underlagt skærpede sikkerhedskrav som resultat af kundens interne politikker eller praksis, branchespecifikke standarder eller ved lov. Kunden anerkender, at servicen ikke er designet til at behandle, gemme eller blive brugt i forbindelse med ekskluderede data. Kunden er eneansvarlig for at gennemse data, der leveres til eller tilgås af Dell Technologies Services, for at sikre, at de ikke indeholder ekskluderede data.

Åbningstider. Underlagt lokal lovgivning vedrørende ugentlig arbejdstid, medmindre andet er angivet nedenfor, leveres Tenant Enablement & Readiness fra mandag til fredag inden for Dell Technologies Services' normale åbningstid, som er fra kl. 08.00 til 18.00 i kundens lokaltid:

Land	Normal åbningstid for Dell Technologies Services
St. Kitts, St. Lucia, St. Vincent, Trinidad, Jomfruøerne, resten af det engelsktalende Caribien	Mandag til og med fredag fra kl. 07.00 til 16.00
Barbados, Bahamas, Belize, Costa Rica, Danmark, El Salvador, Finland, Grand Cayman, Guatemala, Honduras, Jamaica, Norge, Panama, Puerto Rico, Den Dominikanske Republik, Surinam, Sverige, Turks- og Caicosøerne	Mandag til og med fredag fra kl. 08.00 til 17.00
Australien, Bermuda, Haiti, Japan, Kina, de Nederlandske Antiller, New Zealand, Singapore, Thailand	Mandag til og med fredag fra kl. 09.00 til 17.00
Argentina, Brasilien, Ecuador, Frankrig, Indien, Indonesien, Italien, Korea, Malaysia, Mexico, Paraguay, Peru, Taiwan, Uruguay	Mandag til og med fredag fra kl. 09.00 til 18.00
Bolivia, Chile	Mandag til og med fredag fra kl. 09.00 til 19.00
Mellemøsten	Søndag til og med torsdag fra kl. 8.00 til 18.00
Hongkong	Mandag til og med fredag fra kl. 9.00 til 17.30

Ingen aktiviteter for Tenant Enablement & Readiness foregår uden for normal åbningstid eller på lokale helligdage, medmindre andet er aftalt skriftligt på forhånd.

Vilkår og betingelser for services

Denne servicebeskrivelse er indgået mellem dig som kunde ("dig" eller "Kunden") og den juridiske enhed, der fremgår af din ordreformular for købet af denne service ("Dells juridiske enhed"). Denne service leveres underlagt og styret af kundens separat underskrevne hovedserviceaftale med Dells juridiske person, som specifikt tillader salg af denne service. I mangel af en sådan aftale, leveres denne service afhængigt af kundens geografiske placering i henhold til og underlagt enten Dells kommercielle salgsvilkår eller aftalen, som der henvises til i tabellen herunder (som relevant "Aftalen"). Se nedenstående tabel, som viser den URL, der gælder for din kundelokation, hvor din aftale kan findes. Parterne erkender, at de har læst og accepterer at være bundet af sådanne onlinevilkår.

Kundelokation	Vilkår og betingelser, som gælder for dit køb af disse services	
	Kunder, som køber disse services direkte	Kunder, som køber services via en autoriseret forhandler
USA	Dell.com/CTS	Dell.com/CTS
Canada	Dell.ca/terms (Engelsk) Dell.ca/conditions (Fransk-canadisk)	Dell.ca/terms (Engelsk) Dell.ca/conditions (Fransk-canadisk)
Latinamerika og Caribien	Lokale online kommercielle salgsbetingelser placeret på Dell.com landespecifik website eller Dell.com/servicesdescriptions/global .*	Servicebeskrivelser og andre af Dells juridiske persons servicedokumenter, som du måtte modtage fra sælgeren, vil ikke udgøre en aftale mellem dig og Dells juridiske person, men skal kun tjene til at beskrive indholdet af servicen, som du køber fra sælgeren, dine forpligtelser som modtager af servicen og grænser og begrænsninger for en sådan service. Som en konsekvens heraf skal enhver henvisning til "kunden" i denne servicebeskrivelse og i alle andre servicedokumenter fra Dells juridiske person i denne kontekst forstås som en henvisning til dig, mens enhver henvisning til Dells juridiske person kun skal forstås som en henvisning til Dells juridiske person som en serviceudbyder, der leverer servicen på vegne af sælgeren. Du vil ikke have et direkte kontraktforhold med Dells juridiske person vedrørende den service, der er beskrevet heri. For at undgå tvivl om betalingsbetingelser eller andre kontraktvilkår, som i sagens natur kun er relevante direkte mellem en køber og en sælger, finder disse ikke anvendelse for dig og vil være som aftalt mellem dig og sælgeren.
Asien, Stillehavsområdet og Japan	Lokalt Dell.com landespecifikt website eller Dell.com/servicesdescriptions/global .*	Servicebeskrivelser og andre af Dells juridiske persons servicedokumenter, som du måtte modtage fra sælgeren, vil ikke udgøre en aftale mellem dig og Dells juridiske person, men skal kun tjene til at beskrive indholdet af servicen, som du køber fra sælgeren, dine forpligtelser som modtager af servicen og grænser og begrænsninger for en sådan service. Som en konsekvens heraf skal enhver henvisning til "kunden" i denne servicebeskrivelse og i alle andre servicedokumenter fra Dells juridiske person i denne kontekst forstås som en henvisning til dig, mens enhver henvisning til Dells juridiske person kun skal forstås som en henvisning til Dells juridiske person som en serviceudbyder, der leverer servicen på vegne af sælgeren. Du vil ikke have et direkte kontraktforhold med Dells juridiske person vedrørende den service, der er beskrevet heri. For at undgå tvivl om betalingsbetingelser eller andre

		kontraktvilkår, som i sagens natur kun er relevante direkte mellem en køber og en sælger, finder disse ikke anvendelse for dig og vil være som aftalt mellem dig og sælgeren.
Asien- Stillaahavsregionen- Hong Kong	https://www.dell.com/learn/hk/zh/hkcorp1/legal_terms_conditions_dellgrmwebpage/commercial-terms-of-sale-hk-en-zh?c=hk&l=zh&s=corp&cs=hkcorp1	Servicebeskrivelser og andre af Dells juridiske persons servicedokumenter, som du måtte modtage fra sælgeren, vil ikke udgøre en aftale mellem dig og Dells juridiske person, men skal kun tjene til at beskrive indholdet af servicen, som du køber fra sælgeren, dine forpligtelser som modtager af servicen og grænser og begrænsninger for en sådan service. Som en konsekvens heraf skal enhver henvisning til "kunden" i denne servicebeskrivelse og i alle andre servicedokumenter fra Dells juridiske person i denne kontekst forstås som en henvisning til dig, mens enhver henvisning til Dells juridiske person kun skal forstås som en henvisning til Dells juridiske person som en serviceudbyder, der leverer servicen på vegne af sælgeren. Du vil ikke have et direkte kontraktforhold med Dells juridiske person vedrørende den service, der er beskrevet heri. For at undgå tvivl om betalingsbetingelser eller andre kontraktvilkår, som i sagens natur kun er relevante direkte mellem en køber og en sælger, finder disse ikke anvendelse for dig og vil være som aftalt mellem dig og sælgeren.
Europa, Mellemøsten og Afrika	Lokalt Dell.com landespecifikt website eller Dell.com/service-descriptions/global . Desuden kan kunder i Frankrig, Tyskland og Storbritannien vælge den relevante URL nedenfor: Frankrig: Dell.fr/ConditionsGeneralesdeVente Tyskland: Dell.de/Geschaeftsbedingungen Storbritannien: Dell.co.uk/terms	Servicebeskrivelser og andre af Dells juridiske persons servicedokumenter, som du måtte modtage fra sælgeren, vil ikke udgøre en aftale mellem dig og Dells juridiske person, men skal kun tjene til at beskrive indholdet af servicen, som du køber fra sælgeren, dine forpligtelser som modtager af servicen og grænser og begrænsninger for en sådan service. Som en konsekvens heraf skal enhver henvisning til "kunden" i denne servicebeskrivelse og i alle andre servicedokumenter fra Dells juridiske person i denne kontekst forstås som en henvisning til dig, mens enhver henvisning til Dells juridiske person kun skal forstås som en henvisning til Dells juridiske person som en serviceudbyder, der leverer servicen på vegne af sælgeren. Du vil ikke have et direkte kontraktforhold med Dells juridiske person vedrørende den service, der er beskrevet heri. For at undgå tvivl om betalingsbetingelser eller andre kontraktvilkår, som i sagens natur kun er relevante direkte mellem en køber og en sælger, finder disse ikke anvendelse for dig og vil være som aftalt mellem dig og sælgeren.

* Kunder kan få adgang til deres lokale [Dell.com](https://www.dell.com)-website ved blot at gå til [Dell.com](https://www.dell.com) fra en computer med forbindelse til internettet på deres sted eller ved at vælge blandt mulighederne på Dells website "Vælg en region/et land", som er tilgængeligt på [Dell.com/content/public/choosecountry.aspx?c=us&l=en&s=gen](https://www.dell.com/content/public/choosecountry.aspx?c=us&l=en&s=gen).

Kunden accepterer, at ved fornyelse, ændring, udvidelse eller fortsat brug af denne Service, ud over den oprindelige periode, vil denne Service blive underlagt den Servicebeskrivelse, som er gældende på det pågældende tidspunkt, og som er tilgængelig på [Dell.com/service-descriptions/global](https://www.dell.com/service-descriptions/global).

Hvis der er en konflikt mellem vilkårene for et hvilket som helst af de dokumenter, som indgår i denne aftale, vil dokumenterne være gældende i følgende rækkefølge: (i) denne servicebeskrivelse, (ii) aftalen, (iii) ordreformulareren. Gældende vilkår vil blive fortolket så snævert som muligt for at løse konflikten, samtidig med at så mange af de ikke-modstridende vilkår som muligt bibeholdes, herunder bevarelse af ikke-modstridende bestemmelser i samme punkt, afsnit eller underafsnit.

Når du afgiver din ordre på serviceydelser, modtager levering af serviceydelser, benytter serviceydelser eller den tilhørende software, eller når du klikker på knappen eller feltet "Jeg accepterer" på websitet Dell.com eller DellEMC.com i forbindelse med dit køb eller i en Dell Technologies-software eller internetgrænseflade, accepterer du, at du er forpligtet af denne servicebeskrivelse og de aftaler, der som reference er inkorporeret heri. Hvis du indgår denne servicebeskrivelse på vegne af en virksomhed eller anden juridisk person, erklærer du, at du har myndighed til at indgå denne servicebeskrivelse på vegne af den pågældende juridiske enhed. I dette tilfælde henviser "du" eller "kunden" til enheden. Udover at modtage denne servicebeskrivelse kan kunder i visse lande være nødt til at udstede en underskrevet ordreformular.

Erklæring om dataindsamling og -brug

Denne erklæring ("Erklæring") forklarer, hvordan [Dell Technologies og koncernen](#), på vegne af sig selv eller for en tredjepart eller for sine direkte og indirekte datterselskaber ("Dell") indsamler, bruger og deler dine data, når du bruger Dell-software. Vi indsamler og bruger visse typer data, der er beskrevet nedenfor, for at tilpasse din oplevelse med Dell-produkter, for at forbedre vores support og for at forbedre vores produkter, løsninger og services ("Dell-løsninger").

Oplysninger, vi allerede indsamler. Vi kan automatisk indsamle adfærds- og brugsoplysninger om, hvordan du bruger, tilgår eller interagerer med Dell-løsningerne. Disse oplysninger kan måske ikke afsløre din identitet direkte, men kan omfatte unikke identifikatorer og andre oplysninger om den specifikke enhed, du bruger, såsom din servicekode, hardwaremodellen, operativsystemsversion, hardwareindstillinger og systemnedbrud, installerede programmer, indstillinger og brug og/eller (MAC)-adresse og andre data, der entydigt kan identificere din enhed eller dit system.

Vi kan også indsamle oplysninger om, hvordan dit system eller din enhed har interageret med Dell-løsningerne, såsom statistiske oplysninger, netværksforbindelsesindikatorer og -routing, eller i tilfælde af Dell-service, oplysninger relateret til sikkerhedshændelser. I nogle tilfælde kan de indsamlede oplysninger direkte eller indirekte identificere en slutbruger og knytte en person til en bestemt onlineadfærd i det omfang, det er nødvendigt for de formål, der er angivet i denne erklæring.

For at kunne understøtte disse aktiviteter, accepterer du at give Dell en begrænset, ikke-eksklusiv licens til at bruge dine data, så virksomheden kan udføre servicen. Du accepterer også at give Dell en begrænset, ikke-eksklusiv, evig, global, uigenkaldelig licens til at bruge og på anden måde behandle data relateret til sikkerhedsbegivenheder under og efter serviceperioden for at udvikle, forbedre og/eller forbedre den service og de Dell-løsninger, vi tilbyder og leverer til vores kunder. Dell er ikke forpligtet til at returnere eller slette data relateret til sikkerhedshændelser ved ophør af servicen, uanset årsag.

[Dell-software kan samle alle eller dele af ovennævnte oplysninger i datalogfiler, der overføres til Dell, når en internetforbindelse oprettes.]

De typer teknologi, der anvendes af Dell, kan ændre sig med tiden, efterhånden som teknologien udvikler sig. For yderligere oplysninger om vores brug af cookies og andre lignende sporingsteknologier bedes du læse vores [Cookies og lignende teknologier](#) i Dells online [Fortrolighedserklæring](#).

Dataoverførsler. Data, der er beskrevet i denne erklæring, kan overføres uden for dit land til andre steder såsom i USA, EU og Japan, herunder til hostingsider fra tredjeparter. Vi vil træffe alle relevante tekniske og organisatoriske foranstaltninger for at beskytte de data, vi overfører.

Opbevaring af dine data. Vi opbevarer dine personoplysninger efter behov i forbindelse med de formål, der er beskrevet i denne erklæring, og i overensstemmelse med Dells opbevaringspolitikker og gældende lovgivning. De data, der indsamles af Dell som beskrevet i denne erklæring, vil blive opbevaret i overensstemmelse med Dells opbevaringspolitikker og gældende lovgivning.

Personoplysninger og fortrolighed. Dells indsamling, brug og behandling af personoplysninger, som du oplyser, er beskrevet i Dells Fortrolighedserklæring. Hvis du ønsker at kontakte os af vedrørende vores databeskyttelsespraksis, bedes du sende os en e-mail på privacy@dell.com eller se vores fulde fortrolighedserklæring online på <https://www.dell.com/learn/us/en/uscorp1/policies-privacy-country-specific-privacy-policy>

Vigtige supplerende betingelser

1. **Servicebetingelser.** Denne servicebeskrivelse begynder på datoen, som er anført på ordreformularen og fortsætter i hele løbetiden ("**løbetid**"), som angivet på ordreformularen. Som gældende for det antal systemer, licenser, installationer, implementeringer, administrerede slutpunkter eller slutbrugere, hvortil kunden har købt en eller flere services, vil rater eller priser og den relevante løbetid for hver service være angivet på kundens ordreformular. Medmindre andet er skriftligt aftalt mellem Dell Technologies Services og kunden, er services, der købes under denne servicebeskrivelse, kun til kundens egen Internal Use og må ikke anvendes til videresalg eller i forbindelse med et servicebureau.

2. Andre vigtige oplysninger

- A. **Omlægning af plan.** Når denne service er blevet planlagt, skal enhver ændring af planen ske mindst otte kalenderdage forud for den planlagte dato. Hvis kunden omlægger planen for denne service inden for syv dage eller mindre før tidsplandatoen, er der et omlægningsgebyr, der ikke må overstige 25 % af kundens pris for disse services. Enhver omlægning af planen for servicen skal bekræftes af kunden mindst otte dage, før denne service begynder.
- B. **Betaling for hardware, der købes med services.** Medmindre andet er skriftligt aftalt, er betaling for hardware under ingen omstændigheder betinget af ydeevne eller levering af services, der købes sammen med sådan hardware.
- C. **Kommercielt rimelige begrænsninger for servicens omfang.** Dell Technologies Services kan nægte at levere en service, hvis Dell Technologies Services med kommerciel rimelighed anser det for at være sandsynligt, at servicen skaber en urimelig risiko for Dell Technologies Services eller Dell Technologies Services-serviceudbydere eller hvis en sådan anmodet service ligger uden for servicens omfang. Dell Technologies Services er ikke ansvarlig for nogen fejl eller forsinkelse i en ydelse som følge af omstændigheder, der ligger udenfor Dell Technologies Services' kontrol, herunder kundens manglende overholdelse af sine forpligtelser i henhold til denne servicebeskrivelse.
- D. **Services som tilvalg.** Services som tilvalg (herunder point-of-need-support, installation, konsulentbistand, administreret professionel support eller uddannelse) kan muligvis købes af Dell Technologies Services og varierer efter kundelokationen. Services som tilvalg kræver muligvis en separat aftale med Dell Technologies Services. I fravær af en sådan aftale leveres servicen i overensstemmelse med denne servicebeskrivelse.
- E. **Overdragelse og udlicitering.** Dell Technologies Services kan udlicitere denne service og/eller tildele denne service til kvalificerede tredjepartsserviceudbydere, der vil udføre serviceydelsen på Dell Technologies Services vegne.
- F. **Annulering.** Dell Technologies Services kan opsige denne service når som helst i løbet af gyldighedsperioden af følgende grunde:
- Kunden betaler ikke den fulde pris for denne service, som nærmere angivet i faktureringsvilkårene.
 - Kunden er grov, truende eller nægter at samarbejde med den assisterende analytiker eller onsite-tekniker.
 - Kunden overholder ikke de vilkår og betingelser, der er beskrevet i denne servicebeskrivelse.

Hvis Dell Technologies Services opsiger denne service, sender Dell Technologies Services en skriftlig meddelelse om opsigelsen til den adresse, der er angivet på kundens faktura. Varslingen herom vil omfatte opsigelsesårsagen og ikrafttrædelsesdatoen, der ikke vil være mindre end ti (10) dage fra den dato, hvor Dell Technologies Services sender varslingen om opsigelsen til kunden, medmindre lokal lovgivning kræver andre forholdsregler ved opsigelse, der ikke kan fraviges efter aftale. Hvis Dell Technologies Services opsiger denne service i henhold til dette punkt, er kunden ikke berettiget til at få refunderet gebyrer, der er indbetalt til eller er forfaldne hos Dell Technologies Services.

G. Geografiske begrænsninger og flytning. Denne service er ikke tilgængelig overalt. Servicemulighederne, herunder serviceniveauer, åbningstider for teknisk support, servicefunktioner og onsite-svartider varierer efter geografisk område. Visse services kan muligvis ikke købes i kundens område, så kontakt en salgsrepræsentant for at få disse oplysninger.

© 2024 Dell Inc. Alle rettigheder forbeholdes. Varemærker og handelsnavne kan bruges i dette dokument til at henvise til enten de enheder, der gør krav på mærkerne og navnene eller deres produkter. En trykt papirkopi af Dells vilkår og betingelser for salg er også tilgængelig på anmodning.