



Servicebeschrijving

Managed Detection and Response with Microsoft

Inleiding

Dell Technologies Services levert graag de service Managed Detection and Response met Microsoft (de 'Service(s)') conform deze servicebeschrijving ('Servicebeschrijving'). Uw offerte, bestelformulier of ander wederzijds overeengekomen type factuur of bestellingsbevestiging (waar van toepassing, het 'bestelformulier') moet de naam bevatten van de service(s) en beschikbare serviceopties die u hebt aangeschaft. Neem voor extra hulp of voor het aanvragen van een exemplaar van uw servicecontract(en) contact op met de technische support of met uw verkoopvertegenwoordiger.

Het toepassingsgebied van deze service

De service is erop gericht de klant te voorzien van Managed Detection and Response met Microsoft services op het gebied van cyberbeveiliging.

De service wordt op afstand geleverd. De klant is verantwoordelijk voor alle Microsoft-licenties en -abonnementen; **Microsoft-licenties zijn niet inbegrepen als onderdeel van deze service**. Raadpleeg het [technische gegevensblad](#) voor meer informatie over de datavolumelimieten van de klant in het kader van deze service.

De cruciale onderdelen van de service worden beschreven in tabel 1:

Tabel 1

Aangeschafte service	Cruciale onderdelen van de service
Managed Detection and Response met Microsoft	<ul style="list-style-type: none"> • Services die gebruikmaken van technologie van Microsoft Defender XDR en Microsoft Sentinel voor het beheerplatform. • Openingsuren: 24 uur per dag, 7 dagen per week (24x7) • Aftrap/initiatie service • Tenant Enablement & Readiness • Onboarding • Detectie • De Threat Response-service • Servicegerelateerde beveiligingsconfiguratie • Driemaandelijks rapportage

	<ul style="list-style-type: none"> • Incident Response-service • Omvat de bovenstaande onderdelen en maakt gebruik van het XDR-account waarvoor de klant momenteel een licentie heeft. • Klanten die alleen het serviceaanbod aanschaffen, moeten voldoen aan de minimale vereisten voor softwaremodules om Services te kunnen ontvangen.
--	--

Opmerking: De productcapaciteit is afhankelijk van de Microsoft-licentie/het Microsoft-abonnement dat de klant heeft aangeschaft om de workloads van de klant te beschermen; Dit zal gevolgen hebben voor de beschikbare herstelopties van het Dell Technologies Services team.

Openingsuren

De virtuele beveiligingsoperatiecentra (SOC) van Dell Technologies Services zijn ontworpen om de klant een 24 uur per dag, 7 dagen per week (24x7) service te bieden.

De Service biedt een complete oplossing voor de IT-omgeving van een klant en biedt beveiliging voor apparaten, netwerken, gebruikersactiviteiten, cloudtoepassingen en cloudresources, waarbij technologie van Microsoft Defender en Sentinel wordt gebruikt als beheerplatform.

De Service omvat controle van deze Microsoft-onderdelen via Microsoft Sentinel als onderdeel van het basisaanbod:

M365 Defender producten binnen het bereik voor bewaking:

- Microsoft Defender for Office 365
- Microsoft Defender for Endpoint (minimaal vereiste service)
- Microsoft Defender for Servers (onboarded naar Microsoft Defender for Endpoint)
- Microsoft Defender for Identity
- Microsoft Defender for Cloud Apps

Vereisten die nodig zijn voor casebeheer/monitoring

- Microsoft Sentinel (minimaal vereiste service)

Opmerking: Voor de Service is een toegewezen Azure-abonnement en --werkruimte vereist.

Tenant Enablement & Readiness Services worden aangeboden tijdens normale kantooruren. Tenant Enablement & Readiness moeten worden voltooid voordat een klant wordt opgenomen in het 24/7 beheerde SOC van Dell.

Tabel 2 hieronder bevat een lijst met alle elementen van de cruciale onderdelen van de service.

Tabel: 2

Cruciaal onderdeel	Elementen
Aftrap/initiatie service	<ul style="list-style-type: none"> • Service-initiatievergadering (eerste vergadering) • Maak een klantaccount aan in het ITSM-platform • Door de klant ingevulde pre-engagement-controlelijst
Tenant Enablement & Readiness	<ul style="list-style-type: none"> • Controle van vereisten voor licentie en abonnement • Planning voorafgaand aan de implementatie • Defender-beleid controleren/configureren

	<ul style="list-style-type: none"> • Connectoren en databronnen • Data-opname en logboekverzameling • MDR-bewaking en -rapportage
SOC-onboarding	<ul style="list-style-type: none"> • Beoordeling van de IT-omgeving van de klant • Activering van de service
Detectie	<ul style="list-style-type: none"> • 24x7 toegang tot beveiligingsanalisten • Detectie en onderzoeken van bedreigingen • Door Dell gestarte opsporing van bedreigingen
Threat Response en beveiligingsconfiguratie	<ul style="list-style-type: none"> • Threat Response • Servicegerelateerde beveiligingsconfiguratie • Herstel op afstand met betrekking tot het incident
Driemaandelijke rapportage	<ul style="list-style-type: none"> • Driemaandelijke rapportage • Beveiligingsaanbevelingen
Incident Response	<ul style="list-style-type: none"> • De Incident Response-service op afstand starten
Projectbeheer	<ul style="list-style-type: none"> • Leveringsbeheer van deze opdracht

Gedetailleerde beschrijving

Aftrap/initiatie van de service:

Service-initiatievergadering

De projectmanager van Dell Technologies Services belegt een vergadering om de verwachtingen en vereisten van de service te bespreken met de klant om de levering van de service te kunnen plannen. Hieronder vindt u het doel van de service-initiatievergadering:

- De reacties op het klantprofiel evalueren en bespreken om inzicht te krijgen in de IT-omgeving van de klant, beveiligingscontroles en andere relevante context.
- Richtlijnen bieden bij de huidige detectiemechanismen in de klantomgeving en hoe deze op de klant kunnen worden toegepast.
- Begeleiding bieden bij service-integraties met software en hardware van derden.

Mocht de klant nog aanvullende vereisten hebben die buiten het toepassingsgebied van deze servicebeschrijving vallen, dan kan support voor deze vereisten als extra service worden voorgesteld tegen een extra kost.

Door de klant ingevulde pre-engagement-controlelijst

Het is de verantwoordelijkheid van de klant om te voldoen aan de pre-engagement-controlelijst voordat de evaluatie van de IT-omgeving van start gaat. De pre-engagement-controlelijst wordt door de projectmanager van Dell Technologies Services verzonden en bevat een gedetailleerde controlelijst en specificatie van de IT-omgeving.

Evaluatie van de IT-omgeving

De beoordeling van de IT-omgeving is een activiteit die wordt uitgevoerd om data te verzamelen over de bestaande IT-omgeving van de klant waarin de Service zal worden geïmplementeerd.

Tenant Enablement & Readiness

Dell Technologies Services biedt advies over de kernonderdelen ter ondersteuning van de Service. Tenant Enablement & Readiness is ontworpen om ervoor te zorgen dat de IT-omgeving van de klant voldoet aan de minimaal vereiste configuraties om 24/7 bewaking te bieden.

Op basis van de initiële beoordeling van de IT-omgeving van de klant biedt Dell Technologies Services de klant begeleiding bij de configuratie van het basisbeleid van Defender en de configuratie van de (indien nodig) Sentinel-werkruimte.

Raadpleeg het [technische gegevensblad](#) voor meer informatie over de beperkingen van Tenant Enablement & Readiness onder deze Service.

Overzicht van Tenant Enablement & Readiness

- 1) Licenties en abonnementen: controleer of de klant over de benodigde licenties en abonnementen voor Microsoft 365 Defender beschikt. Identificeer of er aanvullende klantenlicenties nodig zijn op basis van de organisatorische behoeften van de klant.
- 2) Planning voorafgaand aan de implementatie: beoordeel de beveiligingsbehoeften van de klant en de bestaande infrastructuur.
- 3) Defender-beleid controleren/configureren: activeer Microsoft 365 Defender-onderdelen in de Microsoft 365-beheerportal van de klant, indien nodig. Assisteer, met goedkeuring van de klant, bij de configuratie van basisbeveiligingsinstellingen binnen de Defender portal(s).
- 4) Dataconnectoren, data-opname en logboekverzameling: integreer Microsoft 365 Defender met de Sentinel-omgeving van de klant om logboeken en waarschuwingen voor beveiligingsgebeurtenissen te centraliseren, indien beschikbaar en alleen zoals aangegeven door de klant. Advies over de implementatie van ondersteunde dataconnectoren voor het verzamelen van beveiligingsdata van Microsoft Defender for Endpoint, Microsoft Defender for Office 365 en Microsoft Defender for Identity.
- 5) MDR-bewaking en -rapportage: maak de overgang naar continue bewaking van de beveiligingsstatus van de IT-omgeving van de klant mogelijk met behulp van het Microsoft Defender Security Center.

SOC-onboarding

Activering van de Service:

- Controleer of aan de huurvoorwaarden voor de Service is voldaan
 - Begeleid de klant door het proces van provisioningtoegang tot het Dell Technologies Services team
 - Begeleid de klant door de toewijzingen van de op rollen gebaseerde toegangscontroles (RBAC) die vereist zijn voor M365 Defender XDR-toegang
- Opmerking:** De bovenstaande activiteit is alleen van toepassing als Microsoft Sentinel / Microsoft Defender for Servers (Microsoft Defender for Cloud) binnen het bereik valt.
- Begeleid de klant door de configuratie van Microsoft Sentinel en Azure Lighthouse
 - Begeleid de klant door de configuratie van Microsoft Sentinel en Azure Lighthouse voor Microsoft Sentinel/Defender voor Cloud ARM-sjabloon voor beheer van Defender for Servers

- Stel een basisautomatiseringsregel of playbook in voor klantrespons op een beveiligingsincident en eventuele SOC vereiste automatisering
- Onderzoek en casemanagement worden gedocumenteerd via de Microsoft Sentinel/Defender-instantie van de klant in combinatie met de ServiceNow/ITSM-instantie van Dell. Dell Technologies Services werkt samen met de klant om deze mogelijkheid te configureren. Alle verzoeken of vragen van klanten met betrekking tot een incident of de Services moeten worden gemeld via het ServiceNow/ITSM-platform.

Detectie

Overgang naar steady state:

De aanbeveling van Dell Technologies Services is om de Defender- en Sentinel-tenant van de klant zo snel mogelijk aan boord te krijgen, idealiter binnen een maand na aanvang van de Services (daarna niet aanbevolen), waardoor de inzichten en bewaking die de Service biedt, worden gemaximaliseerd.

Realtimedata en historische data (afhankelijk van de productopties en storage-instellingen van Microsoft):

- Relevante beveiligingsgebeurtenissen die door Dell Technologies Services als "true positives" zijn aangemerkt en actie van de klant vereisen, worden geëscaleerd naar de klant binnen de hieronder beschreven serviceniveaus
- Gebeurtenissen waarvan is vastgesteld dat ze fout-positief zijn of automatisch worden hersteld, worden vermeld in het kwartaalrapport van de klant
- Aangepaste indicatoren van compromittering die door Dell Technologies Services worden geleverd, worden geanalyseerd zodra ze worden ontvangen of gemaakt

24x7 toegang tot beveiligingsanalisten

De beveiligingsanalisten van Dell Technologies Services zijn 24 uur per dag, 7 dagen per week beschikbaar om u te helpen met relevante vragen.

Detectie en onderzoeken van bedreigingen

Controleer en onderzoek bedreigingen die in de XDR-applicatie zijn gedetecteerd. Bedreigingen die volgens Dell Technologies nadere analyse vereisen, resulteren in het starten van een onderzoek binnen de Microsoft Defender XDR- en Sentinel-applicaties. Dell Technologies neemt via het XDR-portal, e-mail of ondersteunde integraties contact op met de klant als er voldoende bewijs is verzameld om een bedreiging als schadelijk te beschouwen, of als Dell Technologies verdere input van de klant nodig heeft om door te kunnen gaan met het onderzoek.

Opsporing van bedreigingen

Dell Technologies spoort bedreigingen op in de IT-omgeving van de klant voor relevante inbreukindicatoren en tactieken die zijn verzameld in het kader van lopende Incident Response-verbintenissen. Activiteiten op het vlak van opsporing van bedreigingen zijn beperkt tot data die via het XDR-platform zijn verzameld. Dell Technologies controleert de verzamelde telemetrie van de klant voor de detectie van activiteiten, zoals de aanwezigheid van persistentiemechanismen, afwijkende gebruikersactiviteiten, tactieken van bedreigingsactoren, afwijkende netwerkcommunicatie en afwijkend toepassingsgebruik. Bedreigingen die tijdens het opsporen ervan worden gedetecteerd, leiden tot het instellen van een onderzoek en tot kennisgeving aan de klant via de XDR-portal, e-mail of ondersteunde integraties.

Threat Response

Tijdens onboarding keurt de klant vooraf bepaalde Threat Response-acties goed die kunnen worden ondernomen als onderdeel van de service. Dell Technologies Services voert Threat Response-acties uit met behulp van het XDR-platform.

Servicegerelateerde beveiligingsconfiguratie

Dell Technologies Services kan gedurende elk kwartaal in de servicetermijn indien nodig maximaal 40 uur aan servicegerelateerde beveiligingsconfiguratie op afstand goedkeuren om de klant te ondersteunen. De beveiligingsconfiguratie is specifiek beperkt tot onderzoeken en/of waarschuwingen die voortvloeien uit het verlenen van de Service en kan het volgende omvatten:

- Probleemoplossing bij MDR-eindpuntagenten en richtlijnen voor best practices.
- Richtlijnen met updates voor XDR-platformbeleidsregels.
- Richtlijnen voor het configureren en integreren van applicaties van derden in het XDR-platform.

Als er in een enkel kwartaal tijdens de serviceperiode meer dan 40 uur nodig is voor servicegerelateerde hulp bij de Threat Response-service en de beveiligingsconfiguratie, dan kan de klant samen met zijn accountmanager van Dell Technologies extra tijd kopen. Ongebruikte tijd vervalt aan het einde van elke drie maanden van de serviceperiode komt te vervallen. Extra tijd die is aangeschaft voor een toekomstig kwartaal binnen de serviceperiode kan niet vóór het begin van dat kwartaal worden gebruikt.

Driemaandelijkse rapportage

Dell Technologies Services zal elk kwartaal verslag uitbrengen over trends en opvallende activiteiten die zijn waargenomen binnen de IT-omgeving van de klant via het Serviceplatform, en aanbevelingen doen over hoe u zich kunt verdedigen tegen bedreigingen. Het kwartaalrapport bevat een overzicht van onderzoeken en waarschuwingstrends, analyses en richtlijnen voor de beveiligingshouding.

Incident Response

Na melding door de beveiligingsanalist van Dell Technologies Services zijn de volgende onderdelen van Incident Response-service op afstand beschikbaar.

De Incident Response-service op afstand starten

Dell Technologies Services biedt de klant tot 40 uur hulp op afstand bij respons op incidenten voor elk **jaar** gedurende de serviceperiode, beperkt tot het aantal bewaakte eindpunten. Hulp omvat onder andere, maar is niet beperkt tot het volgende:

- Implementatie van het centrale contactpunt voor de Incident Response-service
- Initiëren van een analyse van de on-premise en cloud-infrastructuren van de klant, die het volgende kunnen bevatten:
 - hostdata
 - netwerkdata
 - schadelijke code
 - logboekdata en
 - informatie over cyberbedreigingen
- Voorlopige analyse en coördinatie voor begeleiding en support bij het behandelen van digitale media
- Voorlopige statusrapportering en tracking van actie-items
- Voorlopig overzicht van het vereiste herstel en de volgende stappen

Als er een jaar van de serviceperiode meer dan 40 uur nodig is voor hulp bij de Incident Response-service, dan kan de klant samen met zijn accountmanager van Dell Technologies extra tijd kopen. Ongebruikte tijd aan het einde van elk jaar van de serviceperiode komt te vervallen. Tijd voor een toekomstig jaar binnen de serviceperiode kan niet worden gebruikt voor het begin van dat jaar.

Projectbeheer

Dell Technologies Services wijst een projectmanager (PM) toe als een centraal aanspreekpunt (SPOC) toe om de levering van de service te beheren.

- Centraal aanspreekpunt en verantwoordelijkheid voor succesvolle levering van de services.
- Focus houden op tijd, kosten en bereik.
- Coördineren en faciliteren van vergaderingen bij kick-off, status, leveringscontrole en afsluiting.
- Opstellen en beheren van de serviceplanning, communicatie en statusrapportage.
- Faciliteren van wijzigingsbeheer indien nodig.
- Bevestigen dat de geleverde services in overeenstemming zijn met de servicebeschrijving.
- Acceptatie van het te leveren product en voltooiing van de services van de klant.
- Beheer van de klantrelatie.
- Projectbeheeractiviteiten worden op afstand uitgevoerd.

Abonnementsfacturering

De serviceprovider voorziet in maandelijkse facturering van abonnementen. Deze wordt op het oorspronkelijke bestelformulier aangegeven met de vermelding 'Abonnement' indien de klant voor een dergelijk abonnement heeft gekozen. Anders zijn de standaardvoorwaarden en -facturering van toepassing. De volgende voorwaarden zijn van toepassing op de facturering van abonnementen:

- Op het oorspronkelijke bestelformulier wordt de termijn van de overeenkomst en het aantal gecontracteerde eindpunten vermeld. De serviceperiode wordt daarna automatisch verlengd voor opeenvolgende identieke termijnen.
- De klant kan het aantal beheerde eindpunten verhogen door een bestelling voor extra eindpunten te doen. Deze extra eindpunten zullen worden gecombineerd met de bestaande beheerde eindpunten van de klant om het nieuwe 'totaal aantal eindpunten' te worden.
- De klant wordt maandelijks achteraf gefactureerd, voor het totale aantal eindpunten dat aan het eind van de kalendermaand wordt beheerd.
- Op geen enkel punt kan de klant het aantal beheerde eindpunten verlagen tot een aantal onder het totale aantal eindpunten, en kan het totale aantal eindpunten niet worden verkleind voor factureringdoeleinden.
- Een rapport van de eindpunten van de klant die de service gebruiken wordt aan de klant ter beschikking gesteld.
- De klant ontvangt één factuur voor alle locaties (binnen dezelfde regio).
- De klant is verplicht Dell Technologies zestig (60) dagen van tevoren schriftelijk in kennis te stellen van de beëindiging van de automatisch verlengde serviceperiode van de klant.

Datavolumes en gebruiksbepalingen

De Service maakt gebruik van de Microsoft Sentinel-, Azure- en Microsoft Defender XDR-tenant van de klant en een door de klant gehost, toegewezen Azure-abonnement en -werkruimte voor de Service. Klanten die deze Service aanschaffen, zijn zelf verantwoordelijk voor het begrijpen en beheren van hun eigen datavolume en gebruiksbepalingen. Dell Technologies Services doet afstand van alle dergelijke gerelateerde verantwoordelijkheden of verplichtingen jegens de klant. De klant erkent bovendien dat hij verantwoordelijk is voor alle kosten voor datastorage en berekening in verband met hun Azure-abonnement en Sentinel-werkruimte.

Locaties voor datastorage

Klanten die dit aanbod aanschaffen, zijn zelf verantwoordelijk voor het bepalen van de storagelocatie(s) van hun data. De M365-regio en de datalocaties van de geconfigureerde werkruimte worden ingesteld binnen de Microsoft Azure-omgeving van de klant, op instructie van en zoals bepaald door de klant.

Microsoft Sentinel slaat klantdata op binnen de regio die is gedefinieerd in hun werkruimteconfiguratie. Microsoft slaat klantdata op in dezelfde geografie als de Log Analytics-werkruimte die is gekoppeld aan de Microsoft Sentinel-omgeving van de klant.

Microsoft Sentinel verwerkt klantdata op een van de volgende twee locaties:

- Als de Log Analytics-werkruimte zich in Europa bevindt, worden klantdata in Europa verwerkt.
- Voor alle andere locaties worden klantdata verwerkt in de Verenigde Staten.

Serviceniveaus

Dell meet zijn prestaties voor respons op bedreigingen en oplossingen aan de hand van een aantal serviceniveaus.

Metrisch	Definitie	Doelstelling
Gemiddelde responstijd	De gemiddelde tijd die verstrijkt tussen het tijdstip waarop een hoge of kritische waarschuwing wordt gegenereerd en het tijdstip waarop een onderzoek wordt ingesteld in de XDR-applicatie.	15 minuten
Gemiddelde responstijd	De gemiddelde tijd gemeten vanaf het moment dat een onderzoek wordt ingesteld tot het moment dat een Dell analist een eerste incidentanalyse uitvoert in de XDR-applicatie of een antwoord geeft aan de klant.	60 minuten
Gemiddelde tijd om het probleem op te lossen	De gemiddelde tijd gemeten vanaf het moment dat een onderzoek in de XDR-applicatie wordt ingesteld tot het moment dat het onderzoek is opgelost.	24-48 uur (samenwerking met de klant is vereist)

Veronderstellingen

Dell Technologies Services heeft de volgende veronderstellingen gedaan bij het documenteren van de service die in deze servicebeschrijving worden vermeld:

1. Alle informatie die door de klant wordt aangeleverd met betrekking tot de technische eisen en architectuur on-site is materieel gesproken correct.
2. Dell Technologies Services implementeert alleen servicegerelateerde wijzigingen in de beveiligingsconfiguratie die zijn toegestaan door het Dell Change Management-proces.
3. Dell Technologies Services is niet aansprakelijk voor beleidswijzigingen die de klant doorvoert zonder het wijzigingsbeheerproces te volgen.
4. De services die worden beschreven in deze servicebeschrijving worden op afstand uitgevoerd.
5. Dell Technologies Services beheert de omgeving via Microsoft Sentinel-dashboards.

6. De productmogelijkheden zijn afhankelijk van de Microsoft-licentie en het abonnement dat de klant heeft aangeschaft om de workloads van de klant te beschermen; dit zal gevolgen hebben voor de beschikbare herstelopties van het Dell Technologies Services team. Om bijvoorbeeld servers te beschermen, is Defender for Server Plan 1 de aanbevolen minimale basislijn. Servers profiteren echter van extra bescherming van Defender for Server Plan 2, waarmee extra Microsoft Defender for Cloud-mogelijkheden worden toegevoegd.
7. Dell behoudt zich het recht voor om de Case Management/ITSM-oplossing te wijzigen wanneer er nieuwe mogelijkheden worden uitgebracht.
8. Het aantal eindpunten van de klant wordt berekend op basis van het aantal eindpunten dat wordt bewaakt in Sentinel.
9. Dell Technologies Services verplaatst een klant van SOC-onboarding naar steady state monitoring zodra minimaal 40% van de eindpuntsensoren is geïmplementeerd op de gelicentieerde eindpunten.
10. Indien deze service niet binnen de beschreven tijdsperiode is voltooid, behoudt Dell Technologies Services zich het recht voor de onderliggende oorzaak te onderzoeken. Indien de onderliggende oorzaak buiten de controle van Dell Technologies Services ligt, zal Dell Technologies Services voorstellen doen voor stappen om de vertraging op te lossen. Deze stappen vereisen mogelijk dat de klant aanvullende services aanschaf of aanvullende onkosten maakt om Dell Technologies Services in staat te stellen deze service te voltooien. Mocht de klant nog aanvullende vereisten hebben die buiten het toepassingsgebied van deze servicebeschrijving vallen, dan kan support voor deze vereisten als extra service worden voorgesteld tegen een extra kost.
11. Het Microsoft Sentinel-ecosysteem heeft een hoge signaal-ruisverhouding en dus lage valse positieven; Dell Technologies Services onderzoekt informatieve waarschuwingen en waarschuwingen met een lage prioriteit op basis van een hoog volume van hetzelfde type waarschuwing, geprioriteerd na het onderzoeken van hoge en gemiddelde waarschuwingen.

Uitsluitingen

Hoewel de Service is bedoeld om de klant te helpen bij het identificeren en beperken van risico's, is het onmogelijk om risico's volledig uit te sluiten. Daarom garandeert Dell Technologies Services niet dat er geen ongeoorloofde toegang, inbreuken of andere ongeoorloofde activiteiten kunnen plaatsvinden in de IT-omgeving van de klant.

Voor alle duidelijkheid maken de volgende activiteiten geen deel uit van deze servicebeschrijving:

1. Services, taken of activiteiten die niet uitdrukkelijk in deze servicebeschrijving worden vermeld.
2. De service is exclusief de ontwikkeling van enige intellectuele eigendommen die uitsluitend en specifiek voor de klant worden ontwikkeld.
3. Het oplossen van problemen of het oplossen van bestaande systeem-/serverproblemen tenzij anderszins beschreven in deze Servicebeschrijving, inclusief maar niet beperkt tot M365 Defender-sensoren of defecten van door Microsoft Sentinel ondersteunde agents.
4. Het testen van de integratie tussen een product van Dell Technologies en andere producten van derden, zoals onder andere, maar niet uitsluitend, versleutelings- of beveiligingsproducten van derden.
5. De service omvat geen herstel of beperking van prestatieproblemen die naar voren zijn gekomen uit de analyse van de omgeving van de klant tenzij anderszins beschreven in deze servicebeschrijving.
6. Tenzij in deze servicebeschrijving anderszins is vermeld, neemt Dell Technologies Services geen enkele verantwoordelijkheid (ook geen financiële verantwoordelijkheid) voor medewerkers, hardware, software, apparatuur of andere middelen van de klant of van derden waarvan momenteel gebruik wordt gemaakt in de besturingsomgeving van de klant.

7. Oplossing van compatibiliteitsproblemen of andere problemen die niet kunnen worden opgelost door de fabrikant of voor het configureren van hardware, software, apparatuur of middelen die tegengesteld zijn met de instellingen die de fabrikant ondersteunt.
8. Controle van informatieve waarschuwingen en waarschuwingen met een lage prioriteit vallen buiten de reikwijdte van deze service.
9. Installatie van; of configuratie van, syslog-servers of syslog/CEF-collectors.
10. Configuratie van Microsoft Defender for Cloud Apps-toepassingen.
11. Bewaking van Microsoft Defender for Cloud-functies die niet zijn opgenomen in de Microsoft Defender voor Servers Plan 1- of Plan 2-licentie.
12. Bewaking van servers die niet zijn toegevoegd als onderdeel van de Service. Dell Technologies zal geen waarschuwingen sorteren die betrekking hebben op andere entiteiten dan de aangesloten servers.
 - a. Opmerking: Dit is alleen van toepassing op servers in scope / Defender for Cloud.

Aanbodspecifieke verplichtingen van de klant

De klant stemt ermee akkoord samen te werken met Dell Technologies Services bij de levering van de services, en gaat akkoord met de volgende verantwoordelijkheden:

1. Volgen van het Change Management-proces bij verzoeken om wijzigingen aan te brengen in het XDR-platform en Dell Technologies Services voorzien van een contactpersoon voor de klant die verzoeken voor wijzigingsbeheer goedkeurt.
2. De Dell Technologies Services analist toegang bieden tot alle vereiste klantomgevingen gedurende de termijn van de service.
3. Ervoor zorgen dat een door de klant aangestelde vertegenwoordiger aanwezig en beschikbaar is gedurende alle plannings- en beoordelingssessies.
4. Alle autorisaties verstrekken, inclusief autorisaties van derden, die nodig zijn om Dell Technologies Services toe te staan het XDR-platform namens de klant te beheren.
5. Implementeer agent(s)/sensor(en) op alle gelicentieerde eindpunten van de klant met behulp van de juiste implementatietools voor applicaties (zoals Intune, SCCM, enz.).
6. Indien geschikt, deelnemen aan de levering van de service. De klant begrijpt dat de technicus zonder de juiste medewerking (inclusief doelstelling) niet kan voldoen aan de klantbehoeften of aan de uitvoering van de service.
7. Medewerking verlenen en instructies volgen die door analisten van Dell Technologies Services worden gegeven.
8. Controleer en ga akkoord met de Pre-Engagement-controlelijsten en testplannen.
9. Controleer of de IT-omgeving van de klant een ondersteunde eindpuntagent heeft die is geïnstalleerd op een host met een licentie voor service.
10. Alle support verkrijgen voor eindpuntagents van derden of andere erkende bronnen. Dell Technologies Services biedt geen support voor eindpuntagents van derden.
11. Verwijder of voeg een uitzondering toe voor conflicterende antivirus- en EDR-agents van eerste en/of derde partijen, indien nodig zodat Dell Technologies Services deze service kan leveren.
12. Zorgen voor de beschikbaarheid van en toegang tot voldoende netwerkbandbreedte om de service uit te voeren.
13. Zorg ervoor dat alle apparaatinterregaties goed werken en naar behoren functioneren. Indien de klant dit wenst, kan Dell Technologies Services hierbij helpen tegen een vergoeding.
14. Passende toegang bieden tot XDR-applicaties voor integratie(s).
15. Ervoor zorgen dat de beveiligingsfuncties van de klant compatibel zijn met XDR-integraties.
16. Beheer referenties en machtigingen voor integraties met de XDR-applicatie.
17. Zorg ervoor dat de lijst met erkende contactpersonen van de klant actueel blijft, inclusief machtigingen en bijbehorende informatie.
18. Directe informatie en assistentie bieden (bijv. bestanden, logboeken, IT-omgevingscontext) tijdens bedreigingsonderzoeken door Dell Technologies Services.

19. Identificatie en autorisatie van alle gebruikers waarvan de klant toestaat dat ze de service gebruiken.
20. Controle tegen ongeoorloofde toegang door gebruikers en behoud de vertrouwelijkheid van gebruikersnamen, wachtwoorden en accountgegevens.
21. De klant is verantwoordelijk voor alle activiteiten van door de klant geautoriseerde gebruikers. Dell wordt onmiddellijk op de hoogte gesteld van elk ongeoorloofd gebruik van de Service.
22. Gebruik de tweeledige verificatiemethode, indien beschikbaar, om toegang te krijgen tot de-service.
23. Accepteer alle updates en upgrades van de Endpoint Agent die nodig zijn voor de juiste werking en beveiliging van de service.
24. Geef Dell Technologies indien nodig informatie over de periodes waarin de service uitvalt.
25. De toegang tot data beheren of infecties tussen clients te voorkomen en om dataverlies of risico's op datalekken in de omgeving van de klant te beperken.
26. Zorg voor een nauwkeurig aantal beheerde eindpunten dat door de Service wordt ondersteund.
27. Installatie van Microsoft Sentinel Azure-abonnement en provisioning van toegang die nodig is voor Dell analisten. Dit is een vereiste voor de Service.
28. Toegang tot Microsoft 365 Defender via Microsoft Sentinel wordt verstrekt via Microsoft Entra ID B2B-uitnodigingen die door de klant naar Dell analisten worden verzonden.
29. De fysieke en netwerkbeveiliging van de klantomgeving.
30. Alle documentatie over standaardsjablonen van DT Services aanleveren, tenzij beide partijen anders overeenkomen.
31. Zorg voor ten minste twee (2) niveaus van escalatiecontactpersonen om tijdig te kunnen reageren op escalaties van Dell. Van de klant wordt verwacht dat escalatiecontactpersonen beschikbaar zijn tijdens vakanties en bedrijfssluitingen.
32. Onderhoud van de status, afstemming en configuratie van de Microsoft Sentinel-dashboards.
33. Versturen van tickets voor technologische ondersteuning naar Microsoft voor oplossing. Dell Technologies Services biedt geen ondersteuning voor externe agents van eindpunten.
34. Bepaal hoeveel van de beveiligingsdata van de klant moeten worden opgenomen in Microsoft Sentinel.
35. Bewaak waarschuwingen die worden gegenereerd voor niet-serverentiteiten.
36. Verwijdering van een eerste- of externe AV/EDR-agent.
37. Voorzie DT Services van alle vereiste toestemmingen die nodig zijn om de Service uit te voeren
38. Alle kosten voor dataretentie en berekening.
39. Configureer de beleidsinstellingen om te voldoen aan de behoeften van de klant.
40. Voeg integraties en databronnen toe aan het beheerde MDR-platform.
41. Een speciaal Azure-abonnement is nodig voor het leveren van casus-/incidentbeheer, onderzoeken en kwartaalrapporten via Microsoft Sentinel.
42. Onboarding van Android- en iOS-apparaten. Houd er rekening mee dat elke telefoon die wordt bewaakt, telt als een eindpunt dat wordt bewaakt als onderdeel van deze Service.

Woordenlijst

Tabel: 3

Term	Beschrijving
Waarschuwing	Geprioriteerde gevallen van verdacht of schadelijk gedrag die door de MDR-applicatie zijn waargenomen.
Casebeheer	Gecentraliseerd platform dat wordt gebruikt voor het onderzoeken en beheren van beveiligingsincidenten en waarschuwingen.
Wijzigingsbeheer	Het gecontroleerd identificeren, implementeren en goedkeuren van vereiste wijzigingen binnen een klantomgeving.
Eindpuntagent/sensor	Een applicatie die op een eindpunt is geïnstalleerd en wordt gebruikt om informatie over activiteiten en details van het besturingssysteem van het eindpunt te verzamelen en naar de beveiligingsapplicatie te sturen voor analyse en detectie van bedreigingen.
Managed Detection and Response (EDR)	Een beveiligingsplatform dat gebruikmaakt van de 'first-party' eindpuntagent om apparaten van eindgebruikers, desktops, laptops, tablets en telefoons, te controleren op bedreigingen die antivirussoftware niet kan detecteren.
Managed Detection and Response (XDR)	Een detectie- en responsplatform dat verder gaat dan alleen het traditionele eindpunt (cloud, OT, netwerk, enz.). Het XDR-platform maakt gebruik van integraties of connectors om native data, data van derden, of servicegerichte data op te nemen die kruislings worden gecorreleerd voor beveiligingsbewaking.
Incident Response	Responsacties die worden ondernomen om een geïdentificeerd beveiligingsincident te beperken.
Integratie	API-oproepen (Application Programming Interface) of andere softwarescripts voor het uitvoeren van de overeengekomen services voor de verbonden technologie.
Onderzoek	Een centrale locatie die wordt gebruikt om bewijsmateriaal, analyses en aanbevelingen te verzamelen met betrekking tot een bedreiging die mogelijk gericht is op een asset in de IT-omgeving van de klant.
Managed Detection and Response-applicatie (MDR)	Beveiligingsapplicatie die wordt ondersteund door de Dell MDR-aanbieding. Voor technische details raadpleegt u het technische gegevensblad .
Beveiligingsincident	Een omstandigheid waarbij een inbreuk of vermoedelijke inbreuk op de klant heeft plaatsgevonden.

Beveiligingsbeleid	Beleidsregels van het XDR-platform waarmee de instellingen voor preventie en detectie binnen de klantomgeving worden afgedwongen.
Beveiligingsconfiguratie	Service van 40 uur per kwartaal inbegrepen in MDR die klanten voorziet van responsacties voor onderzoek of waarschuwingen.
Tenant Enablement & Readiness	Geef richtlijnen over de kerncomponenten die nodig zijn om de Services mogelijk te maken. Tenant Enablement & Readiness is ontworpen om ervoor te zorgen dat de IT-omgeving van de klant voldoet aan de minimaal vereiste configuraties om 24/7 bewaking te bieden.
Bedreiging	Elke activiteit die door de MDR-applicatie wordt geïdentificeerd en schade kan toebrengen aan een asset in de IT-omgeving van de klant.
Opsporing van bedreigingen	Het cyclische proces waarin zowel de software als personen op zoek gaan naar nog niet eerder geïdentificeerde bedreigingen binnen een IT-omgeving.
Threat Response	Antwoorden op het platform die beschikbaar zijn in de XDR-applicatie, zoals het isoleren van de host of block-bestanden (actie van het type insluiting).

Algemene verantwoordelijkheden van de klant

Bevoegdheid om toegang te verlenen. De klant verklaart en garandeert dat hij of zij toestemming heeft verkregen voor zowel de klant als Dell Technologies Services voor zowel externe als directe toegang tot en gebruik van alle software, hardware, systemen, daarop opgeslagen data en daarin opgenomen hardware- en softwarecomponenten waarvan de klant eigenaar of licentiehouder is, teneinde deze services te kunnen leveren. Als de klant nog niet over deze toestemming beschikt, is de klant ervoor verantwoordelijk dat deze toestemming op eigen kosten wordt verkregen, voordat de klant Dell Technologies Services verzoekt deze services uit te voeren.

Niet-wervingsclausule. Waar toegestaan door de wet, zal de klant gedurende een periode van twee jaar vanaf de datum op uw bestelformulier zonder voorafgaande schriftelijke goedkeuring van Dell Technologies Services niet, direct of indirect, proberen een werknemer van Dell Technologies Services met wie u contact hebt gehad tijdens het uitvoeren van de service door Dell Technologies Services, te werven; algemene advertenties en andere gelijksoortige brede vormen van werving vallen niet direct of indirect onder werving en het is toegestaan werknemers te werven die zijn ontslagen of die ontslag hebben genomen bij Dell Technologies Services voorafgaand aan sollicitatiegesprekken met u.

Medewerking van de klant. De klant begrijpt dat Dell Technologies Services zonder directe en adequate medewerking de service niet kan uitvoeren of, indien uitgevoerd, de service materieel gewijzigd of vertraagd kan worden. Dienovereenkomstig zal de klant Dell Technologies Services snel en voor zover dat redelijk mag worden geacht, alle medewerking verlenen die Dell Technologies Services nodig heeft om de service uit te voeren. Als de klant overeenkomstig het bovenstaande geen voldoende medewerking verleent, kan Dell Technologies Services niet verantwoordelijk worden gehouden voor het eventueel niet kunnen uitvoeren van de service. De klant komt in dat geval niet in aanmerking voor een vergoeding.

Verplichtingen onsite. Wanneer een medewerker van Dell Technologies Services voor het uitvoeren van de services onsite bij de klant aanwezig dient te zijn, moet de klant (zonder extra kosten voor Dell Technologies Services) gratis, veilige en voldoende toegang tot zijn of haar faciliteiten en de omgeving bieden, inclusief voldoende werkruimte, elektriciteit, veiligheidsuitrusting (waar van toepassing) en een lokale telefoonlijn. Verder dienen een monitor of beeldscherm, een muis (of ander aanwijsapparaat) en een toetsenbord voorhanden te zijn (zonder bijkomende kosten voor Dell Technologies Services), voor zover het systeem niet al met deze apparaten is uitgerust.

Databack-up. De klant dient een volledige back-up te maken van alle aanwezige data, software en programma's op alle betrokken systemen voordat deze service wordt geleverd en tijdens het uitvoeren van deze service. De klant dient een regelmatige back-up te maken van de data die op alle betreffende systemen staan opgeslagen als voorzorgsmaatregel voor mogelijke storingen, wijzigingen of dataverlies. Dell Technologies Services is niet verantwoordelijk voor het herstel of de herinstallatie van programma's of data.

Tenzij anders bepaald door de toepasselijke lokale wetgeving, IS DELL TECHNOLOGIES SERVICES NIET AANSPRAKELIJK VOOR:

- AL UW EVENTUEEL VERTROUWELIJKE, EXCLUSIEVE OF PERSOONLIJKE INFORMATIE;
- VERLIES OF BESCHADIGING VAN DATA, PROGRAMMA'S OF SOFTWARE;
- BESCHADIGING OF VERLIES VAN VERWISSELBARE MEDIA;
- VERLIES VAN HET GEBRUIK VAN EEN SYSTEEM OF NETWERK; EN/OF
- VOOR ALLE EVENTUELE HANDELINGEN OF WEGLATINGEN, INCLUSIEF NALATIGHEID, VAN DELL TECHNOLOGIES SERVICES OF EEN EXTERNE SERVICEPROVIDER.

Garanties van derden. Voor deze services kan het nodig zijn dat Dell Technologies Services hardware- of software moet gebruiken die niet door Dell Technologies Services is vervaardigd of verkocht. De garantie van sommige fabrikanten kan komen te vervallen, indien Dell Technologies Services of iemand anders dan de fabrikant aan de hardware of software werken. De klant moet ervoor zorgen dat de services van Dell Technologies Services deze garanties niet zullen beïnvloeden of, indien dit wel gebeurt, dat de gevolgen aanvaardbaar zijn voor de klant. Dell Technologies Services neemt niet de verantwoordelijkheid voor garanties van derden of voor de gevolgen die de services kunnen hebben op deze garanties.

Uitgesloten gegevens. Onder 'uitgesloten gegevens' wordt verstaan: (i) gegevens die geclassificeerd zijn, gebruikt worden op de United States Munitions List munitielijst (inclusief software en technische gegevens); of beide; (ii) artikelen, services en gerelateerde technische gegevens die worden aangemerkt als defensieartikelen en defensiediensten; (iii) ITAR (International Traffic in Arms Regulations) vrijgegeven gegevens; en (iv) persoonlijk identificeerbare informatie die onderhevig is aan verhoogde beveiligingseisen als gevolg van het interne beleid of de interne praktijken van de klant, industriespecifieke normen of bij wet. De klant erkent dat de service niet is ontworpen om uitgesloten gegevens te verwerken, op te slaan of in verband daarmee te gebruiken. De klant is als enige verantwoordelijk voor het controleren van gegevens die worden verstrekt aan of geraadpleegd door Dell Technologies Services om er zeker van te zijn dat deze geen uitgesloten gegevens bevatten.

Service tijden. Tenzij hieronder anders vermeld, worden Tenant Enablement & Readiness Services uitgevoerd volgens de lokale wetgeving met betrekking tot wekelijkse werkuren van maandag tot en met vrijdag tijdens de normale kantooruren van Dell Technologies Services, dat wil zeggen van 08:00 tot 18:00 uur lokale tijd van de klant:

Land	Normale kantooruren van Dell Technologies Services
St. Kitts, St. Lucia, St. Vincent, Trinidad, Maagdeneilanden, de rest van het Engelstalig Caribisch gebied	Maandag t/m vrijdag van 7:00 tot 16:00
Barbados, Bahama's, Belize, Costa Rica, Denemarken, El Salvador, Finland, Grand Cayman, Guatemala, Honduras, Jamaica, Noorwegen, Panama, Puerto Rico, Dominicaanse Republiek, Suriname, Zweden, Turks- en Caicoseilanden	Maandag t/m vrijdag van 08:00 tot 17:00
Australië, Bermuda, China, Haïti, Japan, Nederlandse Antillen, Nieuw-Zeeland, Singapore, Thailand	Maandag t/m vrijdag van 09:00 tot 17:00
Argentinië, Brazilië, Ecuador, Frankrijk, India, Indonesië, Italië, Korea, Maleisië, Paraguay, Peru, Taiwan, Uruguay	Maandag t/m vrijdag van 09:00 tot 18:00
Bolivia, Chili	Maandag t/m vrijdag van 09:00 tot 19:00
Midden-Oosten	Zondag t/m donderdag van 8:00 tot 18:00
Hongkong	Maandag t/m vrijdag van 09:00 tot 17:30

Buiten de normale kantooruren of tijdens lokale feestdagen vinden er geen Tenant Enablement & Readiness Services-activiteiten plaats, tenzij vooraf schriftelijk andere afspraken zijn gemaakt.

Algemene servicevoorwaarden

Deze servicebeschrijving is een overeenkomst die is aangegaan door de klant ('u' of de 'klant') en de rechtspersoon die staat vermeld op uw bestelformulier voor de aankoop van deze service (de 'rechtspersoon van Dell'). Deze service wordt aangeboden op grond van en onder de afzonderlijk ondertekende hoofdserviceovereenkomst tussen de klant en de rechtspersoon van Dell die de verkoop van deze service nadrukkelijk heeft geautoriseerd. Bij het ontbreken van een dergelijke overeenkomst wordt de service, afhankelijk van de locatie van de klant, geleverd onder de commerciële verkoopvoorwaarden van Dell of onder de overeenkomst die wordt vermeld in onderstaande tabel (zoals van toepassing, de 'overeenkomst'). Zie de onderstaande tabel met de URL die van toepassing is op uw klantlocatie waar uw overeenkomst zich kan bevinden. De partijen bevestigen hierbij dat zij de overeenkomst hebben gelezen en zich hebben verbonden aan de online bepalingen.

Locatie klant	Voorwaarden en bepalingen die van toepassing zijn op uw aanschaf van de services	
	Klanten die rechtstreeks services aanschaffen	Klanten die services aanschaffen via een geautoriseerde reseller
Verenigde Staten	Dell.com/CTS	Dell.com/CTS
Canada	Dell.ca/terms (Engels) Dell.ca/conditions (Frans-Canadees)	Dell.ca/terms (Engels) Dell.ca/conditions (Frans-Canadees)
Latijns-Amerika en Caribisch gebied	U kunt de lokale online commerciële verkoopvoorwaarden vinden op de landspecifieke website op Dell.com of Dell.com/servicedescriptions/global .*	Servicebeschrijvingen en andere servicedocumenten van de rechtspersoon van Dell die u mogelijk ontvangt van uw wederverkoper vormen geen overeenkomst tussen u en de rechtspersoon van Dell, maar fungeren louter als beschrijving van de inhoud van de service die u bij uw wederverkoper aanschaf, uw verplichtingen als ontvanger van de service en de grenzen en limieten van dergelijke services. Als gevolg hiervan moet elke referentie aan de 'klant' in deze servicebeschrijving en in alle andere servicedocumenten van de rechtspersoon van Dell in deze context worden beschouwd als een verwijzing naar u en zal elke verwijzing naar de rechtspersoon van Dell alleen worden uitgelegd als een verwijzing naar de rechtspersoon van Dell als serviceprovider die de service namens uw wederverkoper aanbiedt. U heeft geen directe contractuele relatie met de rechtspersoon van Dell met betrekking tot de hierin beschreven service. Om twijfel te voorkomen is hier vermeld dat alle eventuele betalingsvoorwaarden of andere contractuele voorwaarden die door hun aard uitsluitend relevant zijn voor de directe relatie tussen een koper en een verkoper, niet op u van toepassing zijn. Deze voorwaarden zullen zijn zoals overeengekomen tussen u en uw verkoper.
Azië, Oceanië en Japan	Landspecifieke website van Dell.com of Dell.com/servicedescriptions/global .*	Servicebeschrijvingen en andere servicedocumenten van de rechtspersoon van Dell die u mogelijk ontvangt van uw wederverkoper vormen geen overeenkomst tussen u en de rechtspersoon van Dell, maar fungeren louter als beschrijving van de inhoud van de service die u bij uw wederverkoper aanschaf, uw verplichtingen als ontvanger van de service en de grenzen en limieten van dergelijke services. Als gevolg hiervan moet elke referentie aan de 'klant' in deze servicebeschrijving en in alle andere servicedocumenten van de rechtspersoon van Dell in deze context worden beschouwd als een verwijzing naar u en zal elke verwijzing naar de rechtspersoon van Dell alleen worden uitgelegd als een verwijzing naar de rechtspersoon van Dell als serviceprovider die de service namens uw wederverkoper aanbiedt. U heeft geen directe contractuele relatie met de rechtspersoon van

		Dell met betrekking tot de hierin beschreven service. Om twijfel te voorkomen is hier vermeld dat alle eventuele betalingsvoorwaarden of andere contractuele voorwaarden die door hun aard uitsluitend relevant zijn voor de directe relatie tussen een koper en een verkoper, niet op u van toepassing zijn. Deze voorwaarden zullen zijn zoals overeengekomen tussen u en uw verkoper.
Azië, Pacifisch gebied en Hongkong	https://www.dell.com/learn/hk/zh/hkcorp1/legal_terms-conditions_dellgarmwebpage/commercial-terms-of-sale-hk-en-zh?c=hk&l=zh&s=corp&cs=hkcorp1	Servicebeschrijvingen en andere servicedocumenten van de rechtspersoon van Dell die u mogelijk ontvangt van uw wederverkoper vormen geen overeenkomst tussen u en de rechtspersoon van Dell, maar fungeren louter als beschrijving van de inhoud van de service die u bij uw wederverkoper aanschaft, uw verplichtingen als ontvanger van de service en de grenzen en limieten van dergelijke services. Als gevolg hiervan moet elke referentie aan de 'klant' in deze servicebeschrijving en in alle andere servicedocumenten van de rechtspersoon van Dell in deze context worden beschouwd als een verwijzing naar u en zal elke verwijzing naar de rechtspersoon van Dell alleen worden uitgelegd als een verwijzing naar de rechtspersoon van Dell als serviceprovider die de service namens uw wederverkoper aanbiedt. U heeft geen directe contractuele relatie met de rechtspersoon van Dell met betrekking tot de hierin beschreven service. Om twijfel te voorkomen is hier vermeld dat alle eventuele betalingsvoorwaarden of andere contractuele voorwaarden die door hun aard uitsluitend relevant zijn voor de directe relatie tussen een koper en een verkoper, niet op u van toepassing zijn. Deze voorwaarden zullen zijn zoals overeengekomen tussen u en uw verkoper.
Europa, Midden- Oosten en Afrika	Lokale landspecifieke website van Dell.com of Dell.com/services/global . Daarnaast kunnen klanten in Frankrijk, Duitsland en het Verenigd Koninkrijk de hieronder genoemde toepasselijke URL selecteren: Frankrijk: Dell.fr/ConditionsGeneralesdeVente Duitsland: Dell.de/Geschaeftsbedingungen VK: Dell.co.uk/terms	Servicebeschrijvingen en andere servicedocumenten van de rechtspersoon van Dell die u mogelijk ontvangt van uw wederverkoper vormen geen overeenkomst tussen u en de rechtspersoon van Dell, maar fungeren louter als beschrijving van de inhoud van de service die u bij uw wederverkoper aanschaft, uw verplichtingen als ontvanger van de service en de grenzen en limieten van dergelijke services. Als gevolg hiervan moet elke referentie aan de 'klant' in deze servicebeschrijving en in alle andere servicedocumenten van de rechtspersoon van Dell in deze context worden beschouwd als een verwijzing naar u en zal elke verwijzing naar de rechtspersoon van Dell alleen worden uitgelegd als een verwijzing naar de rechtspersoon van Dell als serviceprovider die de service namens uw wederverkoper aanbiedt. U heeft geen directe contractuele relatie met de rechtspersoon van Dell met betrekking tot de hierin beschreven service. Om twijfel te voorkomen is hier vermeld dat alle eventuele betalingsvoorwaarden of andere contractuele voorwaarden die door hun aard uitsluitend relevant zijn voor de directe relatie tussen een koper en een verkoper, niet op u van toepassing zijn. Deze voorwaarden zullen zijn zoals overeengekomen tussen u en uw verkoper.

* Klanten kunnen naar hun lokale website van [Dell.com](https://www.dell.com) gaan door vanaf een computer met internetverbinding naar [Dell.com](https://www.dell.com) te gaan, of te kiezen uit de opties voor 'Een regio/land selecteren' op de Dell website: [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).

De klant gaat er verder mee akkoord dat het vernieuwen, aanpassen, verlengen of voortzetten van de service na de oorspronkelijke termijn resulteert in uitvoering van de service krachtens de op dat moment geldende servicebeschrijving die voor naslag beschikbaar is op [Dell.com/services/global](https://www.dell.com/services/global).

Als er sprake is van een conflict tussen de bepalingen van de documenten die deze overeenkomst vormen, zullen de documenten in de onderstaande volgorde voorrang hebben: (i) deze servicebeschrijving; (ii) de overeenkomst; (iii) het bestelformulier. De term 'heersende voorwaarden' wordt zo eng mogelijk opgevat om het conflict te kunnen oplossen met behoud van zoveel mogelijk van de niet-strijdige voorwaarden, waaronder het behoud van niet-conflicterende bepalingen in dezelfde alinea, paragraaf of subparagraaf.

Door uw order voor de services te plaatsen, de services te ontvangen, de services of verwante software te gebruiken of door in verband met uw aanschaf te klikken op de knop/het vakje 'Ik ga akkoord' op de website Dell.com of DellEMC.com of binnen een Dell Technologies-software- of internetinterface, verbindt u zich aan deze servicebeschrijving en aan de overeenkomsten die ter referentie in dit document zijn opgenomen. Als u deze servicebeschrijving aangaat uit naam van een bedrijf of andere juridische entiteit dat/die u vertegenwoordigt, verklaart u dat u bevoegd bent deze entiteit aan deze servicebeschrijving te binden, in welk geval 'u' of 'klant' naar deze entiteit verwijst. In sommige landen moeten klanten niet alleen deze servicebeschrijving in ontvangst nemen maar ook een bestelformulier ondertekenen.

Kennisgeving over verzameling en gebruik van gegevens

In deze mededeling ('mededeling') wordt uitgelegd hoe [Dell Technologies en haar bedrijvengroep](#), namens zichzelf of voor een derde partij of voor haar directe en indirecte dochterondernemingen ('Dell'), uw gegevens verzamelt, gebruikt en deelt wanneer u Dell software gebruikt. We verzamelen en gebruiken bepaalde soorten gegevens, die hieronder worden beschreven, om uw ervaring met Dell producten te personaliseren, onze support te verbeteren en onze producten, oplossingen en services ('Dell oplossingen') te verbeteren.

Gegevens die we al hebben verzameld. We kunnen automatisch gedrags- en gebruiksgegevens verzamelen over de manier waarop u de Dell oplossingen gebruikt, er toegang toe krijgt of ermee werkt. Deze gegevens maken niet noodzakelijkerwijs rechtstreeks uw identiteit openbaar, maar kunnen een unieke identifier en andere gegevens bevatten over het specifieke apparaat dat u gebruikt, zoals uw servicetag, het hardwaremodel, de versie van het besturingssysteem, hardware-instellingen en systeemcrashes, geïnstalleerde applicaties, hun instellingen en gebruik, en/of (MAC-)adres, en andere gegevens die uw apparaat of systeem op unieke wijze kunnen identificeren.

Wij kunnen ook data verzamelen over de manier waarop uw systeem of apparaat heeft samengewerkt met Dell oplossingen, zoals statistische data, netwerkaansluitingsindicatoren en routing, of in het geval van de Dell Vulnerability Management Service, data met betrekking tot beveiligingsgebeurtenissen. In sommige gevallen kunnen de verzamelde gegevens rechtstreeks of onrechtstreeks een eindgebruiker identificeren en een persoon aan bepaalde online gedragingen koppelen in de mate die nodig is voor de doeleinden van deze kennisgeving.

Om deze activiteiten te ondersteunen, gaat u ermee akkoord dat u Dell een beperkte, niet-exclusieve licentie verleent om uw data te gebruiken voor het uitvoeren van de Service. U gaat er tevens mee akkoord om Dell een beperkte, niet-exclusieve, permanente, wereldwijde, onherroepelijke licentie te verlenen voor het gebruik van en anderszins verwerken van data met betrekking tot beveiligingsgebeurtenissen tijdens en na de Servicetermijn om de Service en de Dell Oplossingen die wij aanbieden aan onze klanten te ontwikkelen, uit te breiden en/of te verbeteren. Dell is niet verplicht om om welke reden dan ook data met betrekking tot beveiligingsproblemen te retourneren of te verwijderen na beëindiging van de Service.

[Dell Software kan alle of een deel van de bovengenoemde gegevens consolideren in gegevenslogboeken die naar Dell worden verzonden wanneer een internetverbinding tot stand wordt gebracht.]

De soorten technologie die Dell gebruikt, kunnen in de loop der tijd veranderen naarmate de technologie evolueert. Voor meer informatie over ons gebruik van cookies en andere soortgelijke traceertechnologieën kunt u onze [Cookies en soortgelijke technologieën](#) lezen in de online [privacyverklaring](#) van Dell.

Dataoverdracht. Gegevens die in deze kennisgeving worden beschreven, kunnen buiten uw land worden overgedragen naar andere locaties, zoals de Verenigde Staten, de Europese Unie, Japan, met inbegrip van hostingsites van derden. We nemen alle passende technische en organisatorische maatregelen om de gegevens die wij doorgeven te beschermen.

Opslag van uw gegeven. Wij slaan uw persoonsgegevens op voor zover dit nodig is in verband met de doeleinden die in deze kennisgeving worden beschreven, en in overeenstemming met het Dell beleid inzake datastorage en de toepasselijke wetgeving. De gegevens die door Dell worden verzameld die worden beschreven in deze kennisgeving, worden opgeslagen in overeenstemming met het Dell beleid inzake het opslaan van gegevens en de toepasselijke wetgeving.

Persoonlijke gegevens en privacy. Het verzamelen, gebruiken en verwerken van door u verstrekte persoonlijke gegevens door Dell wordt beschreven in de privacyverklaring van Dell. Als u om welke reden dan ook contact met ons wilt opnemen in verband met onze privacypraktijken, kunt u een e-mail sturen naar privacy@dell.com of onze volledige privacyverklaring online bekijken op <https://www.dell.com/learn/us/en/uscorp1/policies-privacy-country-specific-privacy-policy>

Aanvullende bepalingen en voorwaarden

1. **Service termijn.** Deze servicebeschrijving begint op de datum die vermeld staat op uw bestelformulier en loopt door voor de termijn ('**Termijn**') die op het bestelformulier staat. Het aantal systemen, licenties, installaties, implementaties, beheerde eindpunten waarvoor en het aantal eindgebruikers voor wie de Klant een of meer services heeft gekocht, het tarief of de prijs, en de toepasselijke Termijn voor elk worden aangegeven op het Bestelformulier van de Klant. Tenzij schriftelijk anders overeengekomen tussen Dell Technologies Services en de klant, zijn de aankopen van services in het kader van deze servicebeschrijving uitsluitend bestemd voor eigen, intern gebruik door de klant en niet bestemd voor wederverkoop-of servicebureaudoeleinden.
2. **Belangrijke aanvullende informatie**
 - A. **Opnieuw plannen.** Als deze service eenmaal is gepland, dienen wijzigingen in de planning minimaal 8 kalenderdagen voor de geplande datum te worden aangebracht. Als de klant de planning voor deze service binnen 7 dagen voor de geplande datum wijzigt, wordt een vergoeding voor het opnieuw plannen berekend van maximaal 25% van de prijs voor de service. De klant stemt ermee in dat elke herplanning van de service minimaal 8 dagen voor aanvang van de service wordt bevestigd.
 - B. **Betaling van hardware die bij services wordt aangeschaft.** Tenzij anders schriftelijk is overeengekomen, zal betaling voor apparatuur in geen geval afhankelijk zijn van het uitvoeren of het leveren van services die bij dergelijke apparatuur zijn aangeschaft.
 - C. **Commercieel redelijke beperkingen aan de omvang van de service.** Dell Technologies Services mag weigeren de service te verlenen indien Dell Technologies Services of diens serviceproviders, naar eigen redelijke mening, door het leveren van de dienst onredelijk risico lopen of als de gevraagde service niet binnen het kader van de dienst valt. Dell Technologies Services is niet aansprakelijk voor eventuele fouten of vertragingen van de prestaties als gevolg van oorzaken die buiten diens controle liggen, inclusief wanneer de klant niet aan zijn verplichtingen onder deze servicebeschrijving voldoet.
 - D. **Optionele services.** Optionele services (inclusief point-of-need support, installatie, advies, beheerde en professionele support- en trainingsdiensten) kunnen beschikbaar zijn voor aankoop bij Dell Technologies Services en verschillen per locatie van de klant. Optionele services kunnen een aparte overeenkomst met Dell Technologies Services vereisen. Bij het ontbreken van een dergelijke overeenkomst worden optionele services geleverd op grond van deze servicebeschrijving.
 - E. **Toewijzing en uitbesteding.** Dell Technologies Services kan deze service uitbesteden en/of deze servicebeschrijving toewijzen aan gekwalificeerde externe serviceproviders die de service zullen verlenen namens Dell Technologies Services.
 - F. **Annulering.** Dell Technologies Services kan deze service op elk gewenst moment tijdens de termijn annuleren op grond van een van de volgende redenen:
 - De Klant is niet in staat om de totale prijs voor deze Service te betalen in overeenstemming met de factuurvoorwaarden;
 - De klant beledigt, bedreigt of weigert medewerking te verlenen aan de technicus of de analist die de klant op locatie helpt; of
 - De klant houdt zich niet aan alle voorwaarden die in deze servicebeschrijving staan vermeld.

Als Dell Technologies Services deze service annuleert, stuurt Dell Technologies Services een schriftelijke opzegging naar de klant op het adres dat wordt vermeld op de factuur van de klant. De mededeling bevat de reden voor de annulering en de effectieve datum van opzegging, die niet minder mag zijn dan tien (10) dagen vanaf de verzenddatum van de opzegging door Dell Technologies Services aan de klant, tenzij de lokale wetgeving andere annuleringsbepalingen vereist die niet door de overeenkomst kunnen worden gewijzigd. Indien Dell Technologies Services deze service op grond van

deze paragraaf annuleert, heeft de klant geen recht op enige terugbetaling van kosten die de klant aan Dell Technologies Services heeft betaald of verschuldigd is.

G. Geografische beperkingen en verhuizing. Deze service is niet op alle locaties beschikbaar. Serviceopties, inclusief serviceniveaus, tijden voor technische support, servicekenmerken en -functionaliteit, en reactietijden onsite, verschillen op basis van geografische locatie, en bepaalde opties zijn onsite bij de klant mogelijk niet verkrijgbaar. Neem voor meer informatie hierover contact op met uw verkoopvertegenwoordiger.

© 2024 Dell Inc. Alle rechten voorbehouden. De handelsmerken en handelsnamen die in dit document worden gebruikt, verwijzen naar de rechtspersonen die aanspraak maken op de merken en namen of naar de producten ervan. Op aanvraag is ook een gedrukt exemplaar van de verkoopvoorwaarden en-bepalingen van Dell beschikbaar.