Servicebeschreibung

Managed Detection and Response with Microsoft

Einleitung

Dell Technologies Services erbringt den „Managed Detection and Response with Microsoft Service“ (den/die „Service(s)“) gemäß dieser Servicebeschreibung („Servicebeschreibung“). Ihr Kostenvoranschlag, das Bestellformular oder eine andere vereinbarte Rechnungsform oder Auftragsbestätigung („Bestellformular“) enthält den Namen des oder der Services und verfügbare Serviceoptionen, die Sie erworben haben. Weitere Unterstützung oder eine Kopie Ihres Servicevertrags oder Ihrer Serviceverträge erhalten Sie vom technischen Support oder von Ihrem Vertriebsmitarbeiter.

Umfang des Service

Der Service stellt KundInnen die Services „Managed Detection and Response with Microsoft“ bereit.

Der Service wird remote bereitgestellt. Die Verantwortung bezüglich sämtlicher Lizenzen und Abonnements von Microsoft liegt bei den KundInnen. **Microsoft-Lizenzen sind nicht Bestandteil dieses Service.** Weitere Informationen zu den Datenvolumelimits der KundInnen im Rahmen dieses Service finden Sie im **Technischen Datenblatt**.

Kernkomponenten des Service sind in Tabelle 1 unten beschrieben:

Tabelle 1

Erworbener Service	Kernkomponenten des Service
Managed Detection and Response with Microsoft	• Services, die Technologie von Microsoft Defender XDR und Microsoft Sentinel für die Managementplattform nutzen • Betriebsstunden: 24 Stunden am Tag, 7 Tage die Woche (24x7) • Kick-off/Initiierung des Service • Ermöglichung und Vorbereitung Mandantenbetrieb • Onboarding • Erkennung • Reaktion auf Bedrohungen • Servicebezogene Sicherheitskonfiguration • Vierteljährliches Reporting • Antwort auf Incidents

	• Dies beinhaltet die obigen Komponenten und nutzt den derzeit lizenzierten XDR-Account der KundInnen. • KundInnen, die das reine Serviceangebot erwerben, müssen die Mindestanforderungen an Softwaremodulen erfüllen, um Services zu erhalten.

Hinweis: Die Funktionalität des Produkts ist von der Microsoft-Lizenzierung/dem Microsoft-Abonnement abhängig, die KundInnen zum Schutz ihrer Workloads erworben haben. Dies wirkt sich auf die für das Team von Dell Technologies Services zur Verfügung stehenden Möglichkeiten für Korrektur und Wiederherstellung aus.

Betriebsstunden

Die Dell Technologies Services Virtual Security Operations Centers (SOC) sind so konzipiert, dass sie KundInnen einen Service 24 Stunden am Tag und 7 Tage die Woche (24x7, rund um die Uhr) bereitstellen.

Der Service als eine umfassende Lösung für die IT-Umgebung der KundInnen bietet Sicherheit für Geräte, Netzwerke, Nutzeraktivitäten, Cloud-Anwendungen und Cloud-Ressourcen und nutzt Technologien von Microsoft Defender und Sentinel als Managementplattform.

Der Service umfasst die Überwachung dieser Microsoft-Komponenten über Microsoft Sentinel als Bestandteil des Basisangebots:

In Überwachung einbezogene Produkte M365 Defender:

Microsoft Defender for Office 365

Microsoft Defender for Endpoint (Service mit Mindestvoraussetzungen)

Microsoft Defender for Servers (integriert in Microsoft Defender for Endpoint)

Microsoft Defender for Identity

Microsoft Defender for Cloud Apps

Erforderliche Voraussetzungen für das Fallmanagement/Monitoring

Microsoft Sentinel (Service mit Mindestvoraussetzungen)

Hinweis: Zur Nutzung des Service sind ein dediziertes Azure-Abonnement und ein dedizierter Arbeitsbereich erforderlich.

Services für die Ermöglichung und Vorbereitung von Mandantenbetrieb werden während der normalen Geschäftszeiten erbracht. Ermöglichung und Vorbereitung von Mandantenbetrieb muss abgeschlossen sein, bevor KundInnen in ein täglich rund um die Uhr gemanagtes SOC von Dell integriert werden können.

In Tabelle 2 unten sind die Elemente der Kernkomponenten des Service aufgeführt.

Tabelle 2

Kernkomponente	Elemente
Kick-off/Initiierung des Service	• Meeting zur Initiierung des Service (Kick-off-Meeting) • Erstellen eines Kundenkontos auf der ITSM-Plattform • Von KundInnen ausgefüllte Checkliste vor dem Engagement

Ermöglichung und Vorbereitung Mandantenbetrieb	• Überprüfen der Voraussetzungen bezüglich Lizenzen und Abonnements • Planung vor der Bereitstellung • Überprüfen/Konfigurieren der Defender-Policy • Konnektoren und Datenquellen • Datenerfassung und Protokollsammlung • MDR Monitoring and Reporting
SOC-Onboarding	• Überprüfen der IT-Umgebung der KundInnen • Servicetauglichkeit
Erkennung	• 24x7-Zugriff auf Sicherheitsanalysten • Bedrohungserkennung und -ermittlungen • Bedrohungssuche von Dell initiiert
Konfiguration von Bedrohungsreaktionen und Sicherheit	• Reaktion auf Bedrohungen • Servicebezogene Sicherheitskonfiguration • Remotekorrektur im Zusammenhang mit dem Incident
Vierteljährliches Reporting	• Vierteljährlicher Report • Sicherheitsempfehlungen
Antwort auf Incidents	• Initiierung der Remote-Incident-Antwort
Projektmanagement	• Bereitstellungsmanagement für dieses Projekt

Detaillierte Beschreibung

Kick-off/Initiierung des Service:

Meeting zur Initiierung des Service
Dell Technologies Services ProjektmanagerInnen berufen ein Meeting ein, um die Erwartungen und Anforderungen mit KundInnen zu überprüfen, damit die Servicebereitstellung geplant werden kann. Ziel des Meetings zur Initiierung des Service:

- Überprüfung und Besprechung der Antworten für das Kundenprofil, um die IT-Umgebung der KundInnen, die Sicherheitskontrollen und andere relevante Kontexte zu verstehen
- Bereitstellen von Anleitungen zu den aktuellen Erkennungsmechanismen in der Umgebung der KundInnen und wie diese auf die KundInnen angewendet werden können
- Bereitstellen von Anleitungen zu Integrationen von Services in Software und Hardware anderer AnbieterInnen.

Wenn KundInnen weitere Anforderungen haben, die über den Umfang dieser Servicebeschreibung hinausgehen, wird die Unterstützung für diese Anforderungen als zusätzlicher Service gegen Aufpreis angeboten.

Von KundInnen ausgefüllte Checkliste vor dem Engagement
Vor der Überprüfung der IT-Umgebung müssen KundInnen die Pre-Engagement-Prüfliste ausfüllen. Die Pre-Engagement-Prüfliste wird von Dell Technologies Services ProjektmanagerInnen versendet und enthält eine detaillierte Prüfliste sowie technische Daten zur IT-Umgebung.

Überprüfung der IT-Umgebung
Die Überprüfung der IT-Umgebung wird durchgeführt, um Daten über die bei KundInnen vorhandene Umgebung zu erfassen, in der die Services implementiert werden.

Ermöglichung und Vorbereitung Mandantenbetrieb

Dell Technologies Services bietet Beratungen zu Kernkomponenten zur Unterstützung des Service. Die „Ermöglichung und Vorbereitung Mandantenbetrieb“ stellt sicher, dass die IT-Umgebungen der KundInnen die erforderlichen Mindestkonfigurationen für eine Überwachung 24×7 erfüllen.

Basierend auf einer ersten Überprüfung der IT-Umgebung bei KundInnen bietet Dell Technologies Services den KundInnen Anleitungen zum Konfigurieren von grundlegenden Policies zu Defender und (falls erforderlich) zum Konfigurieren des Sentinel-Arbeitsbereichs.

Weitere Informationen über den Umfang von „Ermöglichung und Vorbereitung Mandantenbetrieb“ finden Sie im **Technischen Datenblatt**.

Übersicht über „Ermöglichung und Vorbereitung Mandantenbetrieb“

1) Lizenzierung und Abonnements: Stellen Sie sicher, dass KundInnen über die erforderlichen Lizenzen und Abonnements für Microsoft 365 Defender verfügen. Ermitteln Sie den Bedarf an weiteren Kundenlizenzen basierend auf den organisatorischen Anforderungen der KundInnen.

2) Planung vor der Bereitstellung: Überprüfen Sie den Sicherheitsbedarf der KundInnen und die bereits vorhandene Infrastruktur.

3) Überprüfen/Konfigurieren von Defender-Policies Aktivieren Sie bei Bedarf Komponenten von Microsoft 365 Defender im Verwaltungsportal von Microsoft 365 der KundInnen. Helfen Sie, mit Zustimmung der KundInnen beim Konfigurieren von grundlegenden Sicherheitseinstellungen in dem/den Defender-Portal(en).

4) Datenkonnektoren, Datenerfassung und Protokollsammlung: Integrieren Sie Microsoft 365 Defender in die Sentinel-Umgebung der KundInnen, damit es einen zentralen Ort für Protokolle und Warnungen zu Ereignissen gibt. Dieser Schritt erfolgt nur sofern verfügbar und nur wie von den KundInnen vorgegeben. Stehen Sie bei der Implementierung unterstützter Datenkonnektoren zum Sammeln von Sicherheitsdaten von Microsoft Defender for Endpoint, Microsoft Defender for Office 365 und Microsoft Defender for Identity beratend zur Seite.

5) Überwachung und Berichterstattung mittels MDR: Unterstützen Sie die Umstellung auf kontinuierliche Überwachung des Sicherheitsstatus der IT-Umgebung der KundInnen mithilfe von Microsoft Defender Security Center.

SOC-Onboarding

Ermöglichung der Erbringung der Services:

- Überprüfen Sie die Voraussetzungen für die Mandantenfähigkeit für den Service
- Führen Sie KundInnen durch den Prozess der Bereitstellung des Zugriffs für das Team von Dell Technologies Services
- Führen Sie KundInnen durch die für den Zugriff von M365 Defender XDR erforderlichen Zuweisungen von RBAC (Role-Based Access Controls, rollenbasierte Zugriffssteuerung).

  Anmerkung: Die obige Aktivität wird nur ausgeführt, wenn Microsoft Sentinel / Microsoft Defender for Servers (Microsoft Defender for Cloud) im Leistungsumfang vorhanden ist.
- Führen Sie KundInnen durch das Konfigurieren von Microsoft Sentinel und Azure Lighthouse.
- Führen Sie KundInnen durch das Konfigurieren der ARM-Vorlage von Microsoft Sentinel und Azure Lighthouse für Microsoft Sentinel / Defender for Cloud für das Management von Defender für Server.
- Richten Sie eine grundlegende Automatisierungsregel/ein Playbook zur Reaktion der KundInnen auf einen Sicherheits-Incident und alle sonstigen für das SOC benötigten Automatisierungen ein.
- Die Untersuchung und das Fallmanagement werden über die Microsoft Sentinel/Defender-Instanz der KundInnen in Verbindung mit der ServiceNow/ITSM-Instanz von Dell dokumentiert. Dell Technologies Services konfiguriert diese Funktion in Zusammenarbeit mit den KundInnen. Kundenanfragen oder Fragen zu einem Incident oder zu den Services sollten über die ServiceNow-/ITSM-Plattform gestellt werden.

Erkennung

Übergang zum stabilen Zustand:

Dell Technologies Services empfiehlt, das Onboarding von Defender- und Sentinel-MandantInnen von KundInnen so schnell wie möglich durchzuführen, idealerweise innerhalb eines Monats nach Beginn der Services (von längeren Zeiten wird abgeraten), um die vom Service gebotenen Einblicke und Überwachungen zu maximieren.

Echtzeit- und Verlaufsdaten (abhängig von den Funktionen und Storage-Einstellungen der Microsoft-Produkte):

- Relevante Sicherheitsereignisse, die von Dell Technologies Services als „korrekt positiv“ eingestuft werden und Maßnahmen der KundInnen erfordern, werden im Rahmen der unten aufgeführten Servicelevels an die KundInnen eskaliert.
- Ereignisse, die als „falsch positiv“ erkannt oder automatisch korrigiert werden, sind im Quartalsbericht an die KundInnen aufgeführt.
- Von Dell Technologies Services bereitgestellte nutzerdefinierte Indikatoren für eine Kompromittierung werden analysiert, sobald sie empfangen oder erstellt werden.

24x7-Zugriff auf SicherheitsanalystInnen
Täglich rund um die Uhr stehen SicherheitsanalystInnen von Dell Technologies Services zur Verfügung, um relevante Anfragen zu beantworten.

Bedrohungserkennung und -ermittlungen
Überprüfen und Untersuchen von in der XDR-Anwendung erkannten Bedrohungen. Bedrohungen, die nach Maßgabe von Dell Technologies eine weitere Analyse erfordern, führen zur Einleitung von Ermittlungen in den Anwendungen Microsoft Defender XDR und Sentinel. Dell Technologies kontaktiert KundInnen über das XDR-Portal, per E-Mail oder über unterstützte Integrationen, wenn genügend Beweise gesammelt wurden, um eine Bedrohung als bösartig einzustufen, oder wenn Dell Technologies weitere Informationen von KundInnen benötigt, um mit den Ermittlungen fortzufahren.

Aufspüren von Bedrohungen
Dell Technologies führt eine Suche nach Bedrohungen in der IT-Umgebung der KundInnen durch, um relevante Indikatoren für die Infizierung und Taktiken zu ermitteln, die aus aktuellen Antworten auf Incidents gesammelt werden. Die Aktivitäten zum Aufspüren von Bedrohungen sind auf Daten beschränkt, die über die XDR-Plattform erfasst wurden. Dell Technologies untersucht die erfasste Kundentelemetrie, um Aktivitäten wie das Vorhandensein von Persistenzmechanismen, anomale Nutzeraktivitäten, Taktiken von BedrohungsakteurInnen, anomale Netzwerkkommunikationen und anomale Anwendungsnutzung zu erkennen. Bedrohungen, die im Rahmen des Aufspürens von Bedrohungen erkannt werden, führen zur Einleitung von Ermittlungen und zur Benachrichtigung der KundInnen über das XDR-Portal, per E-Mail oder über unterstützte Integrationen.

Reaktion auf Bedrohungen

Beim Onboarding erteilen KundInnen eine Vorabgenehmigung für ausgewählte Reaktionsmaßnahmen auf Bedrohungen, die im Rahmen des Service durchgeführt werden können. Dell Technologies Services führt Reaktionsmaßnahmen auf Bedrohungen über die XDR-Plattform durch.

Servicebezogene Sicherheitskonfiguration

Dell Technologies Services kann KundInnen während der Servicelaufzeit bis zu 40 Stunden pro Vierteljahr für die servicebezogene Sicherheitskonfiguration (remote) nach Bedarf bereitstellen. Die Sicherheitskonfiguration ist ausdrücklich auf Ermittlungen und/oder Warnmeldungen beschränkt, die sich aus der Bereitstellung des Service ergeben, und kann Folgendes umfassen:

- Troubleshooting und Best Practices für den MDR-Endpunkt-Agent
- Anleitungen für Updates der XDR-Plattform-Policies
- Anleitung zur Konfiguration und Integration von Drittanbieteranwendungen in die XDR-Plattform

Falls während der Servicelaufzeit in einem einzigen Quartal mehr als 40 Stunden für die servicebezogene Konfiguration von Bedrohungsreaktionen und Sicherheit benötigt werden, können KundInnen seine/n Dell Technologies Account-ManagerIn kontaktieren, um zusätzliche Zeit zu erwerben. Nicht genutzte Zeit am Ende eines jeden Quartals der Servicelaufzeit verfällt. Zusätzlich erworbene Zeit für ein zukünftiges Quartal innerhalb der Servicelaufzeit kann nicht vor dem Beginn des betreffenden Quartals genutzt werden.

Vierteljährliches Reporting

Dell Technologies Services berichtet vierteljährlich Trends und bemerkenswerte Aktivitäten, die über die Service-Plattform in der IT-Umgebung der KundInnen beobachtet wurden, und gibt Empfehlungen zur Abwehr von Bedrohungen. Der Quartalsbericht enthält einen Überblick über Untersuchungen und Warnmeldungstrends, Analysen und Empfehlungen zum Sicherheitsstatus.

Antwort auf Incidents

Nach Benachrichtigung durch die SicherheitsanalystInnen von Dell Technologies Services stehen die folgenden Komponenten für die Remote-Incident-Antwort zur Verfügung.

Initiierung der Remote-Incident-Antwort
Dell Technologies Services stellt den KundInnen in der Laufzeit des Service pro **Jahr** bis zu 40 Stunden Remoteunterstützung für die Antwort auf Incidents bereit, beschränkt auf die Anzahl der überwachten Endpunkte. Diese Unterstützung beinhaltet folgende Leistungen, ohne darauf beschränkt zu sein:

- Festlegen zentraler AnsprechpartnerInnen für den Service zur Antwort auf Incidents

- Initiierung einer Analyse der On-Premise- und Cloud-Infrastrukturen der KundInnen, die Folgendes umfassen kann:
    - Hostdaten
    - Netzwerkdaten
    - Bösartiger Code
    - Protokolldaten und
    - Cyber Threat Intelligence
- Erste Analyse und Koordination des Umgangs mit digitalen Medien – Anleitung und Unterstützung
- Erstes Statusreporting und Nachverfolgung von Aktionselementen
- Erste Übersicht über die erforderliche Korrektur und nächste Schritte

Wenn in einem Jahr der Servicelaufzeit mehr als 40 Stunden für Remote-Incident-Antworten benötigt werden, können KundInnen seine/n Dell Technologies Account-ManagerIn kontaktieren, um zusätzliche Zeit zu erwerben. Nicht genutzte Zeit am Ende eines jeden Jahres der Servicelaufzeit verfällt. Die Zeit für ein zukünftiges Jahr der Servicelaufzeit kann nicht vor Beginn des betreffenden Jahres genutzt werden.

Projektmanagement

Dell Technologies Services benennt für das Management der Servicebereitstellung eine/n ProjektmanagerIn (PM) als zentrale Ansprechperson („SPOC“).

- Ein/e einzige/r verantwortliche/r AnsprechpartnerIn für eine erfolgreiche Bereitstellung der Services
- Fokussierung auf Zeit, Kosten und Umfang
- Koordination und Unterstützung von Kick-off-, Status-, Leistungsüberprüfungs- und Abschlussbesprechungen
- Ausarbeitung und Management des Servicezeitplans, der Kommunikation und der Statusberichte
- Umsetzung des Changemanagements nach Bedarf
- Sicherstellung der Servicebereitstellung gemäß der Servicebeschreibung
- Einholung der Abnahme von Lieferung und Serviceabschluss von KundInnen
- Management der Kundenbeziehung
- Remoteausführung der Projektmanagementaktivitäten

Abonnementfakturierung

Der Service beinhaltet die monatliche Abonnementfakturierung, die auf dem Originalbestellformular mit dem Vermerk „Abonnement“ angegeben wird, wenn sich KundInnen dafür entschieden haben. Andernfalls gelten Standardbedingungen und -rechnungstellung. Die folgenden Bedingungen gelten für die Abonnementfakturierung:

- Das Originalbestellformular zeigt die Vertragslaufzeit und die Anzahl der vertraglich vereinbarten Endpunkte an. Die Servicelaufzeit verlängert sich danach automatisch um ein nachfolgende identische Laufzeit.
- KundInnen können die Anzahl verwalteter Endpunkte erhöhen, indem sie eine Bestellung für zusätzliche Endpunkte einreichen. Diese zusätzlichen Endpunkte werden mit den vorhandenen verwalteten Endpunkten der KundInnen kombiniert, woraus sich die neue „Gesamtzahl der Endpunkte“ ergibt.
- KundInnen wird die Gesamtzahl der verwalteten Endpunkte am Ende des Kalendermonats nachträglich in Rechnung gestellt.
- KundInnen dürfen zu keinem Zeitpunkt die Anzahl der verwalteten Endpunkte unter die Gesamtzahl der Endpunkte reduzieren, noch kann die Gesamtzahl der Endpunkte zu Abrechnungszwecken verringert werden.

- KundInnen wird ein Bericht über die Kundenendpunkte, die den Service verwenden, zur Verfügung gestellt.
- KundInnen erhalten eine einzelne Rechnung für alle Standorte (innerhalb der gleichen Region).
- KundInnen sind verpflichtet, Dell Technologies sechzig (60) Tage vor Ablauf der automatisch verlängerten Servicelaufzeit der KundInnen schriftlich über die Kündigung zu informieren.

Datenvolume und Nutzungsbeschränkungen

Der Service nutzt den Microsoft Sentinel-, Azure- und Microsoft Defender XDR-Mandanten der KundInnen sowie ein von KundInnen gehostetes, dediziertes Azure-Abonnement und einen entsprechenden Arbeitsbereich für den Service. KundInnen, die diesen Service erwerben, sind dafür verantwortlich, ihre eigenen Datenvolume- und Nutzungslimits zu kennen und zu verwalten. Dell Technologies Services lehnt alle damit verbundenen Verantwortlichkeiten oder Verpflichtungen gegenüber den KundInnen ab. KundInnen stimmen zudem zu, dass sie für alle Kosten für Daten-Storage und Computing-Kosten im Zusammenhang mit Azure-Abonnement und Sentinel-Arbeitsbereich selbst aufkommen.

Daten-Storage-Orte

KundInnen, die dieses Angebot erwerben, sind dafür verantwortlich, ihre/n Standort(e) für die Daten-Storage selbst festzulegen. Die M365-Region und die Speicherorte für Daten der konfigurierten Arbeitsbereiche werden auf Anweisung und nach Ermessen der KundInnen innerhalb der Microsoft Azure-Umgebung der KundInnen festgelegt.

Microsoft Sentinel speichert Daten von KundInnen innerhalb der Region, die in der Arbeitsbereichskonfiguration definiert ist. Microsoft speichert Daten von KundInnen in derselben geografischen Region wie den der Microsoft Sentinel-Umgebung den KundInnen zugeordneten Arbeitsbereich für die Protokollanalytik.

Microsoft Sentinel verarbeitet Daten von KundInnen an einem von zwei Speicherorten:

- Wenn sich der Log Analytics-Arbeitsbereich für die Protokollanalyse in Europa befindet, werden die Daten der KundInnen in Europa verarbeitet.
- Bei allen anderen Standorten werden die Daten der KundInnen in den USA verarbeitet.

Servicelevel

Dell misst die Leistungsfähigkeit bei der Antwort und Lösung von Bedrohungen anhand einer Reihe von Serviceleveln.

Metrik	Definition	Ziel
Durchschnittliche Reaktionszeit	Die durchschnittliche Dauer, gemessen ab dem Zeitpunkt, an dem eine Warnmeldung von hoher oder kritischer Priorität erzeugt wird, bis zu dem Zeitpunkt, an dem eine Ermittlung in der XDR-Anwendung erstellt wird.	15 Minuten
Durchschnittliche Antwortzeit	Die durchschnittliche Dauer, gemessen ab der Erstellung einer Ermittlung bis zu dem Zeitpunkt, an dem ein/e Dell Analyst/In eine erste Incident-	60 Minuten

	Analyse in der XDR-Anwendung oder eine Antwort für KundInnen bereitstellt.	
Durchschnittliche Problemlösungszeit	Die durchschnittliche Dauer, gemessen ab der Erstellung einer Ermittlung in der XDR-Anwendung bis zum Zeitpunkt der Lösung der Ermittlung.	24 bis 48 Stunden (erfordert die Zusammenarbeit mit den KundInnen)

Annahmen

Diese Servicebeschreibung wurde von Dell Technologies Services auf Grundlage der folgenden Voraussetzungen erstellt:

1. Alle von KundInnen mitgeteilten Informationen zu technischen Anforderungen und Architektur am Standort sind im Wesentlichen korrekt.
2. Dell Technologies Services implementiert nur servicebezogene Sicherheitskonfigurationsänderungen, die laut Dell Changemanagement-Prozess zulässig sind.
3. Dell Technologies Services übernimmt keine Haftung für Policy-Änderungen, die KundInnen implementieren, ohne den Dell Changemanagement-Prozess zu befolgen.
4. Alle in dieser Servicebeschreibung beschriebenen Services werden remote bereitgestellt.
5. Dell Technologies Services managt die Umgebung über Microsoft Sentinel-Dashboards.
6. Die Funktionalität des Produkts ist von der Microsoft-Lizenzierung und dem Microsoft-Abonnement abhängig, die KundInnen zum Schutz ihrer Workloads erworben haben. Dies wirkt sich auf die für das Team von Dell Technologies Services zur Verfügung stehenden Möglichkeiten für Korrektur und Wiederherstellung aus. Um beispielsweise Server zu schützen, ist Defender for Server – Plan 1 der empfohlene Mindeststandard. Server profitieren jedoch von zusätzlichen Schutzmaßnahmen von Defender for Server – Plan 2, da dieser Plan zusätzliche Funktionen von Microsoft Defender for Cloud hinzufügt.
7. Dell behält sich das Recht vor, die Lösung für Fallmanagement/ITSM zu ändern, wenn neue Funktionen veröffentlicht werden.
8. Die Anzahl der Endpunkte bei KundInnen wird basierend auf der Anzahl der in Sentinel überwachten Endpunkte berechnet.
9. Dell Technologies Services stellt KundInnen vom SOC-Onboarding auf Überwachung im stabilen Zustand um, sobald mindestens 40 % der Endpunktsensoren auf den lizenzierten Endpunkten bereitgestellt wurden.
10. Falls dieser Service innerhalb des beschriebenen Zeitraums nicht durchgeführt werden kann, behält sich Dell Technologies Services das Recht vor, die Ursache hierfür zu ermitteln. Entzieht sich die Ursache der Kontrolle von Dell Technologies Services, wird Dell Technologies Services Vorschläge zur Lösung der Verzögerung einbringen. Der Kauf zusätzlicher Services oder das Anfallen weiterer Kosten für KundInnen können Bestandteil solcher Lösungen sein, damit Dell Technologies Services diesen Service abschließen kann. Wenn KundInnen weitere Anforderungen haben, die über den Umfang dieser Servicebeschreibung hinausgehen, wird die Unterstützung für diese Anforderungen als zusätzlicher Service gegen Aufpreis angeboten.
11. Das Ökosystem von Microsoft Sentinel weist ein hohes Signal-Rausch-Verhältnis und daher nur sehr wenige Fehlalarme auf. Dell Technologies Services untersucht informative Warnmeldungen und Warnmeldungen mit niedrigem Schweregrad basierend auf der hohen Anzahl ein und desselben Warnmeldungstyps, wobei Warnmeldungen mit hoher und mittlerer Dringlichkeit priorisiert werden.

Ausschlüsse

Der Service soll KundInnen dabei helfen, Risiken zu erkennen und zu reduzieren. Es ist jedoch unmöglich, Risiken vollständig zu eliminieren. Aus diesem Grund übernimmt Dell Technologies Services keine Garantie dafür, dass in der IT-Umgebung der KundInnen nicht auch Angriffe, Kompromittierungen oder andere unbefugte Aktivitäten eintreten.

Zum Ausschluss von Zweifeln sei darauf hingewiesen, dass die folgenden Aktivitäten nicht von dieser Servicebeschreibung abgedeckt werden:

1. Alle Services, Arbeitsschritte oder Aktivitäten, die nicht ausdrücklich in dieser Servicebeschreibung aufgeführt sind
2. Der Service umfasst nicht die Entwicklung geistigen Eigentums, das exklusiv und speziell für KundInnen erstellt wird.
3. Problembehandlungen oder Behebung bereits vorhandener System-/Serverprobleme, sofern nicht anderweitig in dieser Servicebeschreibung aufgeführt, einschließlich, aber nicht beschränkt auf Defekte bei M365 Defender-Sensoren oder bei von Microsoft Sentinel unterstützten Agents
4. Tests zur Integration zwischen einem Dell Technologies Produkt und anderen Drittanbieterprodukten, darunter Verschlüsselungs- und Sicherheitsprodukte von DrittanbieterInnen.
5. Der Service umfasst weder eine Korrektur noch Abhilfe in Bezug auf die bei der Analyse der Kundenumgebung identifizierten Leistungsprobleme, sofern nicht anderweitig in dieser Servicebeschreibung beschrieben.
6. Dell Technologies Services übernimmt keine Verantwortung (einschließlich finanzieller Verantwortung) für Personal, Hardware, Software, Geräte oder Bestände der KundInnen oder von DrittanbieterInnen, die derzeit in der Betriebsumgebung der KundInnen eingesetzt werden, sofern dies nicht anderweitig in dieser Servicebeschreibung festgelegt ist.
7. Lösung von Kompatibilitäts- oder anderen Problemen, die nicht durch den Hersteller behoben werden können, oder Konfigurieren von Hardware, Software, Geräten oder Beständen auf eine Weise, die nicht den Einstellungen des Herstellers entspricht.
8. Das Monitoring von informativen Warnmeldungen und solchen mit niedrigem Schweregrad ist nicht im Umfang dieses Service enthalten.
9. Installieren und/oder Konfigurieren von Syslog-Servern oder Syslog/CEF-Kollektoren
10. Konfigurieren von Microsoft Defender for Cloud Apps-Anwendungen
11. Überwachen von Funktionen von Microsoft Defender for Cloud, die nicht in der Lizenz für Microsoft Defender for Servers – Plan 1 oder Plan 2 enthalten sind
12. Überwachen sonstiger Server, die nicht als Teil des Service integriert wurden Dell Technologies selektiert keine Warnmeldungen, die sich auf andere Entitäten als integrierte Server beziehen.
    a. Hinweis: Dies gilt nur für im Geltungsbereich enthaltene Server / Defender for Cloud.

Angebotsbezogene Pflichten der KundInnen

Die KundInnen erklären sich damit einverstanden, mit Dell Technologies Services bei der Erbringung der Services zusammenzuarbeiten, und stimmen den folgenden Pflichten zu:

1. Bei Anfragen zur Durchführung von Änderungen an der XDR-Plattform befolgen KundInnen den Changemanagement-Prozess. Zudem wird Dell Technologies Services eine Ansprechperson benannt, die solche Changemanagement-Anfragen genehmigt.
2. KundInnen ermöglichen den AnalystInnen von Dell Technologies Services während der Servicelaufzeit Zugriff auf alle erforderlichen Kundenumgebungen.
3. KundInnen benennen eine Vertretung, die bei allen Planungs- und Prüfungssitzungen anwesend und verfügbar ist.

4. KundInnen sorgen für sämtliche Berechtigungen einschließlich Autorisierungen von DrittanbieterInnen, die Dell Technologies Services für das Management der XDR-Plattform im Auftrag der KundInnen benötigt.
5. KundInnen stellen für alle von KundInnen lizenzierten Endpunkte unter Verwendung geeigneter Tools zur Anwendungsbereitstellung (z. B. Intune, SCCM usw.) Agenten bzw. Sensoren bereit.
6. KundInnen wirken in angemessener Weise an der Bereitstellung des Service mit. KundInnen ist bewusst, dass die TechnikerInnen ohne angemessene Mitwirkung der KundInnen (einschließlich Zielsetzung) möglicherweise nicht in der Lage sind, die Kundenanforderungen zu erfüllen oder den Service zu erbringen.
7. KundInnen arbeiten mit AnalystInnen von Dell Technologies Services zusammen und befolgt deren Anweisungen.
8. KundInnen überprüfen Pre-Engagement-Prüflisten und Testpläne und erklären sich damit einverstanden.
9. Sicherstellen, dass die IT-Umgebung der KundInnen über einen unterstützten Endpunkt-Agent verfügt, der auf einem Host, der für den Service lizenziert ist, installiert ist.
10. KundInnen beziehen jeglichen Support für Endpunkt-Agents von DrittanbieterInnen von diesen oder anderen autorisierten Quellen. Dell Technologies Services bietet keinen Support für Endpunkt-Agents von DrittanbieterInnen.
11. KundInnen entfernen eine Ausnahme für widersprüchliche Virenschutz- und EDR-Agents von Erst- und/oder DrittanbieterInnen oder fügen eine solche hinzu, sofern dies für die Erbringung dieses Service durch Dell Technologies Services erforderlich ist.
12. KundInnen stellen sicher, dass ausreichend Netzwerkbandbreite für die Erbringung des Service verfügbar und nutzbar ist.
13. Sicherstellen, dass alle Geräteintegrationen funktionieren und auch weiterhin ordnungsgemäß funktionieren. Wenn KundInnen dies wünschen, kann Dell Technologies Services gegen eine Gebühr dabei unterstützen.
14. KundInnen sorgen zum Zwecke der Integration(en) für einen entsprechenden Zugriff auf die XDR-Anwendungen.
15. KundInnen stellen sicher, dass eigene Sicherheitskontrollen mit den XDR-Integrationen kompatibel sind.
16. Verwalten von Zugangsdaten und Berechtigungen für Integrationen in die XDR-Anwendung.
17. Sicherstellen, dass die Liste der autorisierten Kundenkontakte aktuell bleibt, einschließlich der Berechtigungen und zugehörigen Informationen.
18. Im Rahmen von Bedrohungsermittlungen seitens Dell Technologies Services stellen KundInnen Informationen und Unterstützung (z. B. Dateien, Protokolle, IT-Umgebungskontext) unmittelbar bereit.
19. KundInnen identifizieren und authentifizieren alle NutzerInnen, die den Service verwenden.
20. Schutz vor unbefugtem Zugriff durch NutzerInnen und Wahrung der Vertraulichkeit von Nutzernamen, Kennwörtern und Kontoinformationen.
21. KundInnen sind für alle Aktivitäten der von ihnen autorisierten NutzerInnen verantwortlich und benachrichtigen Dell sofort über eine unbefugte Nutzung des Service.
22. Verwenden der Zwei-Faktor-Authentifizierung, sofern verfügbar, für den Zugriff auf den Service.
23. Akzeptieren aller Updates und Upgrades für den Endpunkt-Agent, die für die ordnungsgemäße Funktion und Sicherheit des Services erforderlich sind.
24. KundInnen stellen Dell Technologies bei Bedarf Zeitfenster für Serviceausfälle bereit.
25. KundInnen kontrollieren den Datenzugriff, um eine Client-übergreifende Kompromittierung zu verhindern sowie das Risiko von Datenverlusten oder Datenlecks in der Kundenumgebung zu begrenzen.
26. KundInnen halten eine genauen Anzahl von gemanagten Endpunkten aufrecht, die vom Service unterstützt werden.
27. KundInnen richten ein Microsoft Sentinel Azure-Abonnement ein und stellen den von Dell AnalystInnen benötigten Zugriff bereit. Dies ist eine Voraussetzung für den Service.
28. Die Bereitstellung des Zugriffs auf Microsoft 365 Defender über Microsoft Sentinel erfolgt über Microsoft Entra ID B2B-Einladungen, die von KundInnen an Dell AnalystInnen gesendet werden.

29. KundInnen sorgen für die physische und Netzwerksicherheit in der Umgebung der KundInnen.
30. KundInnen stellen die gesamte Dokumentation über Standardvorlagen von DT Services bereit, es sei denn, die Parteien vereinbaren etwas anderes.
31. KundInnen stellen mindestens zwei (2) Ebenen von Eskalationskontakten bereit, um rechtzeitig auf Dell Eskalationen reagieren zu können. Erwartet wird, dass KundInnen Eskalationskontakte bereitstellen, die auch an Feiertagen und während der Betriebsferien verfügbar sind.
32. KundInnen pflegen Integrität, Tunings und Konfiguration der Microsoft Sentinel-Dashboards.
33. KundInnen reichen Technologie-Supporttickets an Microsoft zur Lösung ein. Dell Technologies Services bietet keinen Support für Endpunkt-Agents von DrittanbieterInnen.
34. KundInnen legen fest, wie viele Sicherheitsdaten der KundInnen in Microsoft Sentinel aufgenommen werden sollen.
35. KundInnen überwachen Warnmeldungen, die für Nicht-Server-Entitäten erzeugt wurden.
36. KundInnen entfernen Erst-/Drittanbieter-AV/EDR-AgentInnen.
37. KundInnen erteilen alle für die Ausführung der Services durch DT Services erforderlichen Genehmigungen.
38. KundInnen tragen alle Kosten für Datenaufbewahrung und Computing.
39. KundInnen konfigurieren die Policy-Einstellungen auf den Bedarf der KundInnen.
40. KundInnen fügen der verwalteten MDR-Plattform Integrationen und Datenquellen hinzu.
41. KundInnen stellen ein dediziertes Azure-Abonnement bereit, das erforderlich ist, um Fall-/Incident-Management, Ermittlungen und Quartalsberichte über Microsoft Sentinel bereitzustellen.
42. Onboarding von Android- und iOS-Geräten. Beachten Sie, dass jedes überwachte Telefon als ein Endpunkt zählt, der im Rahmen dieses Services überwacht wird.

Glossar

Tabelle 3:

Begriff	Beschreibung
Warnmeldung	Dies umfasst priorisierte Vorkommen von verdächtigem oder bösartigem Verhalten, die von der MDR-Anwendung beobachtet werden.
Fallmanagement	Zentrale Plattform für die Untersuchung und Verwaltung von Sicherheits-Incidents und Warnmeldungen.
Changemanagement	Die kontrollierte Identifizierung, Implementierung und Genehmigung von erforderlichen Änderungen innerhalb einer Kundenumgebung.
Endpunkt-Agent/-Sensor	Eine Anwendung, die auf einem Endpunkt installiert und verwendet wird, um Informationen zu Aktivitäten und Betriebssystemdetails des Endpunkts zu sammeln und zur Analyse und Erkennung von Bedrohungen an die Sicherheitsanwendung zu senden.

Endpoint Detection and Response („EDR“)	Diese Sicherheitsplattform verwendet den Endpunkt-Agent des Erstanbieters, um Endnutzergeräte – wie Desktop-PCs, Laptops, Tablets und Smartphones – auf Bedrohungen zu überwachen, die von Virenschutzsoftware nicht erkannt werden.
Extended Detection and Response („XDR“)	Diese Plattform für Erkennung und Reaktion geht über den herkömmlichen Endpunkt (Cloud, OT, Netzwerk usw.) hinaus. Die XDR-Plattform verwendet Integrationen oder Connectors, um native, Drittanbieter- oder serviceorientierte Daten aufzunehmen, die im Rahmen der Sicherheitsüberwachung übergreifend korreliert werden.
Antwort auf Incidents	Diese Reaktionsmaßnahmen dienen zur Eindämmung eines identifizierten Sicherheits-Incidents.
Integration	API-Aufrufe (Application Programming Interface) oder andere Softwareskripte für die Durchführung der vereinbarten Services für die angeschlossene Technologie.
Ermittlungen	Ein zentraler Standort wird verwendet, um Nachweise, Analysen und Empfehlungen zu sammeln, die auf eine Bedrohung in der IT-Umgebung der KundInnen abzielen.
Managed Detection and Response-Anwendung („MDR“)	Diese Sicherheitsanwendung wird von der Dell MDR-Lösung unterstützt. Technische Details finden Sie im Technischen Datenblatt.
Sicherheits-Incident	Ein Fall, in dem ein Infizierung oder eine vermutete Infizierung stattgefunden hat, an der KundInnen beteiligt sind.
Sicherheits-Policy	Diese Policies der XDR-Plattform setzen die Präventions- und Erkennungseinstellungen in Kundenumgebung durch.
Sicherheitskonfiguration	Dieser in MDR enthaltene Service mit 40 Stunden pro Quartal bietet KundInnen Reaktionsaktionen mit Bezug zu Ermittlungen oder Warnmeldungen.
Ermöglichung und Vorbereitung Mandantenbetrieb	Bereitstellung von Anleitungen zu den Kernkomponenten, die für die Aktivierung der Services erforderlich sind. Die „Ermöglichung und Vorbereitung Mandantenbetrieb“ stellt sicher, dass die IT-Umgebungen der KundInnen die erforderlichen Mindestkonfigurationen für eine Überwachung 24×7 erfüllen.
Bedrohung	Dies umfasst alle von der MDR-Anwendung identifizierten Aktivitäten, die möglicherweise Schäden an einer Ressource in der IT-Umgebung der KundInnen verursachen können.
Aufspüren von Bedrohungen	Der zyklische Prozess, bei dem sowohl die Software als auch Menschen zuvor unbekannte Bedrohungen in einer IT-Umgebung suchen.

Reaktion auf Bedrohungen	Diese plattforminternen Reaktionen sind in der XDR-Anwendung verfügbar, wie z. B. Host isolieren oder Datei blockieren (Eindämmungsaktionen).

Allgemeine Pflichten der KundInnen

Befugnis zum Gewähren von Zutritt. KundInnen erklären und gewährleisten, dass sie sowohl für sich als auch für Dell Technologies Services für den Zweck der Bereitstellung dieses Service über die Berechtigung für den Zugriff auf und die Verwendung (ob remote oder persönlich) der im Kundenbesitz befindlichen oder lizenzierten Software, Hardware und Systeme, der darauf gespeicherten Daten und aller zugehörigen Hardware- und Softwarekomponenten verfügen. Wenn KundInnen noch nicht über diese Berechtigung verfügen, sind sie dafür verantwortlich, diese Berechtigung auf eigene Kosten einzuholen, bevor sie Dell Technologies Services mit der Erbringung dieser Services beauftragen.

Abwerbeverbot. KundInnen sichern zu, falls gesetzlich erlaubt, während eines Zeitraums von zwei Jahren ab dem auf dem Service-Bestellformular vermerkten Datum weder direkt noch indirekt ohne vorherige schriftliche Genehmigung seitens Dell Technologies Services MitarbeiterInnen, mit denen KundInnen im Rahmen der Serviceerbringung in Kontakt stand, zwecks Anstellung abzuwerben. Ausgenommen hiervon sind jedoch öffentliche Stellenanzeigen und sonstige, ähnlich breit angelegte Formen der Personalbeschaffung, die gemäß dieser Vereinbarung keinen direkten oder indirekten Abwerbeversuch darstellen. Zudem sind KundInnen berechtigt, ehemalige Dell Technologies Services MitarbeiterInnen, die noch vor der Aufnahme betreffender Gespräche mit KundInnen von Dell Technologies Services entlassen wurden oder selbst gekündigt haben, als potenzielle MitarbeiterInnen zu werben.

Zusammenarbeit mit KundInnen. KundInnen ist bewusst, dass Dell Technologies Services ohne eine direkte und angemessene Kooperation der KundInnen nicht in der Lage ist, den Service zu erbringen, dass der Service grundlegend verändert werden oder dass die Serviceerbringung mehr Zeit in Anspruch nehmen kann. Demzufolge ermöglichen KundInnen eine unverzügliche und angemessene Zusammenarbeit, damit Dell Technologies Services den Service ordnungsgemäß erbringen kann. Wenn KundInnen nicht auf angemessene Art und Weise im Sinne des zuvor Gesagten kooperieren, lehnt Dell Technologies Services jedwede Verantwortung für Versäumnisse bei der Durchführung des Service ab und KundInnen verlieren jedweden Erstattungsanspruch.

Pflichten vor Ort. Wenn Services vor Ort ausgeführt werden müssen, ermöglichen KundInnen (ohne Kosten für Dell Technologies Services) einen kostenlosen, sicheren und ausreichenden Zugang zu den Einrichtungen und der Umgebung des KundInnen, einschließlich eines ausreichend großen Arbeitsplatzes, einer sicheren Stromversorgung, Sicherheitsausrüstung (falls zutreffend) und eines lokalen Telefonanschlusses. Darüber hinaus müssen ein Monitor oder Display, eine Maus (oder ein anderes Zeigegerät) und eine Tastatur zur Verfügung gestellt werden (ohne Kosten für Dell Technologies Services), wenn das System nicht bereits über diese Komponenten verfügt.

Datenbackup. KundInnen sichern alle vorhandenen Daten, Software und Programme auf den betroffenen Systemen vor und während der Erbringung dieses Service. KundInnen haben als Vorsichtsmaßnahme gegen mögliche Ausfälle, Änderungen oder Verluste von Daten regelmäßig Sicherungskopien der Daten zu erstellen, die auf den betroffenen Systemen gespeichert sind. Dell Technologies Services ist nicht für die Wiederherstellung oder Neuinstallation von Programmen oder Daten verantwortlich.

Sofern nicht anderweitig durch lokale Gesetze geregelt, ÜBERNIMMT DELL TECHNOLOGIES SERVICES KEINE HAFTUNG FÜR:

- VERTRAULICHE, GESCHÜTZTE ODER PERSONENBEZOGENE DATEN

- VERLORENE ODER BESCHÄDIGTE DATEN, PROGRAMME ODER SOFTWARE
- BESCHÄDIGTE ODER VERLORENE WECHSELMEDIEN
- SYSTEM- ODER NETZWERKAUSFÄLLE UND/ODER
- ALLE HANDLUNGEN ODER UNTERLASSUNGEN, EINSCHLIESSLICH FAHRLÄSSIGKEIT DURCH DELL TECHNOLOGIES SERVICES ODER EINEN DRITTANBIETER

Services von DrittanbieterInnen. Bei der Ausführung dieser Services muss Dell Technologies Services unter Umständen auf Hardware oder Software zugreifen, die nicht von Dell Services hergestellt oder verkauft wurde. Die Gültigkeit der Gewährleistung einiger Hersteller erlischt möglicherweise, wenn Dell Technologies Services oder eine andere Partei außer dem Hersteller an der Hardware oder Software arbeitet. KundInnen müssen sicherstellen, dass die Ausführung von Services durch Dell Technologies Services keine Auswirkungen auf die Gültigkeit solcher Gewährleistungen hat bzw. dass, sollten Auswirkungen doch entstehen, diese von KundInnen akzeptiert werden. Dell Technologies Services übernimmt keine Verantwortung für Gewährleistungen Dritter oder für die Auswirkungen, die die Services auf diese Gewährleistungen haben können.

Ausgeschlossene Daten. „Ausgeschlossene Daten“ bedeutet: (i) unter Geheimschutz stehende und/oder in der US-Munitionsliste (United States Munitions List, USML) stehende Daten (einschließlich Software- und technischer Daten) oder beides; (ii) Artikel, Dienstleistungen und zugehörige technische Daten, die als Verteidigungsgüter und -dienstleistungen klassifiziert sind; (iii) veröffentlichte Daten, die unter die ITAR (International Traffic in Arms Regulations) fallen; und (iv) personenbezogene Daten, die aufgrund interner Richtlinien oder Praktiken, branchenspezifischer Standards oder gesetzlich festgelegter Sicherheitsanforderungen der KundInnen strengeren Sicherheitsanforderungen unterliegen. KundInnen erkennen an, dass der Service nicht für die Verarbeitung, Speicherung oder Verwendung von ausgeschlossenen Daten vorgesehen ist. KundInnen sind allein dafür verantwortlich, Daten zu überprüfen, die Dell Technologies Services überlassen werden oder auf die von Dell zugegriffen wird, um sicherzustellen, dass sie keine ausgeschlossenen Daten enthalten.

Servicezeiten. In Abhängigkeit von den örtlich geltenden Gesetzen und Bestimmungen in Bezug auf die wöchentlichen Arbeitsstunden werden die Services „Ermöglichung und Vorbereitung Mandantenbetrieb“, wenn nachfolgend nicht anders angegeben, während der normalen Geschäftszeiten von Dell Technologies Services von Montag bis Freitag von 8:00 bis 18:00 Uhr, Ortszeit KundInnen, erbracht.

Land	**Normale Geschäftszeiten von Dell Technologies Services**
St. Kitts, St. Lucia, St. Vincent, Trinidad, Jungferninseln, übrige englischsprachige Karibik	Montag bis Freitag von 7:00 bis 16:00 Uhr
Barbados, Bahamas, Belize, Costa Rica, Dänemark, El Salvador, Finnland, Grand Cayman, Guatemala, Honduras, Jamaika, Norwegen, Panama, Puerto Rico, Dominikanische Republik, Surinam, Schweden, Turks- und Caicosinseln	Montag bis Freitag von 8:00 bis 17:00 Uhr
Australien, Bermudas, China, Haiti, Japan, Niederländische Antillen, Neuseeland, Singapur, Thailand	Montag bis Freitag von 9:00 bis 17:00 Uhr
Argentinien, Brasilien, Ecuador, Frankreich, Indien, Indonesien, Italien, Korea, Malaysia, Mexiko, Paraguay, Peru, Taiwan, Uruguay	Montag bis Freitag von 9:00 bis 18:00 Uhr
Bolivien, Chile	Montag bis Freitag von 9:00 bis 19:00 Uhr
Naher Osten	Sonntag bis Donnerstag von 08:00 Uhr bis 18:00 Uhr
Hongkong	Montag bis Freitag von 9:00 bis 17:30 Uhr

Wenn nicht anders im Voraus schriftlich vereinbart, werden außerhalb der normalen Geschäftszeiten und an lokalen Feiertagen keine Services „Ermöglichung und Vorbereitung Mandantenbetrieb“ erbracht.

Services – Geschäftsbedingungen

Diese Servicebeschreibung stellt eine Vereinbarung zwischen Ihnen („Sie“, „Ihnen“ oder „KundInnen“) und der juristischen Person dar, die auf Ihrer Rechnung für den Service angegeben ist („Dell als juristische Person“). Dieser Service unterliegt dem von KundInnen separat unterzeichneten Rahmenvertrag mit Dell als juristischer Person, der den Verkauf des Service ausdrücklich gestattet. Gibt es keine entsprechende Vereinbarung, unterliegt dieser Service je nach Standort der KundInnen den Verkaufsbedingungen von Dell oder der in der Tabelle weiter unten erwähnten Vereinbarung (die „Vereinbarung“). In nachstehender Tabelle ist die für Ihren Kundenstandort gültige URL aufgeführt, unter der Sie die entsprechende Vereinbarung finden können. Die Vertragsparteien bestätigen, diese Onlinebedingungen gelesen zu haben und sie anzuerkennen.

Kundenstandort	**Geltende Bedingungen und Bestimmungen für Ihren Kauf der Services**	
	KundInnen, die Services direkt kaufen	**KundInnen, die Services über einen autorisierten Reseller kaufen**
Vereinigte Staaten	Dell.com/CTS	Dell.com/CTS
Kanada	Dell.ca/terms (Englisch) Dell.ca/conditions (kanadisches Französisch)	Dell.ca/terms (Englisch) Dell.ca/conditions (kanadisches Französisch)
Lateinamerika und Karibik	Lokale Verkaufsbedingungen online auf der landesspezifischen Website unter Dell.com oder Dell.com/servicedescriptions/global *	Die Servicebeschreibungen und andere Servicedokumente zu Dell als juristischer Person, die Sie von Ihrem/r VerkäuferIn erhalten, stellen keine Vereinbarung zwischen Ihnen und Dell als juristischer Person dar, sondern dienen nur als Beschreibung des Inhalts des Service, den Sie von Ihrem/r VerkäuferIn erwerben, sowie zur Klärung Ihrer Pflichten als EmpfängerInnen des Service und der Grenzen und Beschränkungen eines solchen Service. Daher ist „KundInnen“ in dieser Servicebeschreibung und in anderen Servicedokumenten zu Dell als juristische Person in diesem Kontext als Verweis auf Sie und „Dell als juristische Person“ als Verweis auf Dell als Serviceanbieter zu verstehen, der den Service im Namen Ihres/r VerkäuferIn erbringt. Aus dem hierin beschriebenen Service ergibt sich für Sie kein direktes Vertragsverhältnis mit Dell als juristischer Person. Zum Ausschluss von Zweifeln sei darauf hingewiesen, dass Zahlungsbedingungen oder andere Vertragsbedingungen, die naturgemäß nur direkt zwischen einem/r KäuferIn und einem(r VerkäuferIn relevant sind, nicht für Sie gelten und zwischen Ihnen und Ihrem/r VerkäuferIn vereinbart werden.
Asien/Pazifik/Japan	Lokale länderspezifische Dell.com-Website oder Dell.com/servicedescriptions/global *	Die Servicebeschreibung und andere Servicedokumente zu Dell als juristische Person, die Sie von Ihrem/r VerkäuferIn erhalten, stellen keine Vereinbarung zwischen Ihnen und Dell als juristischer Person dar, sondern dienen nur als Beschreibung des Inhalts des Service, den Sie von Ihrem/r VerkäuferIn erwerben, sowie zur Klärung Ihrer Pflichten als EmpfängerIn des Service und der Grenzen und Beschränkungen eines solchen Service. Daher ist „KundInnen“ in dieser Servicebeschreibung und in anderen Servicedokumenten zu Dell als juristische Person in diesem Kontext als Verweis auf Sie und „Dell als juristische Person“ als Verweis auf Dell als Serviceanbieter zu verstehen, der den Service im Namen Ihres/r VerkäuferIn erbringt. Aus dem hierin beschriebenen Service ergibt sich für Sie kein direktes

		Vertragsverhältnis mit Dell als juristischer Person. Zum Ausschluss von Zweifeln sei darauf hingewiesen, dass Zahlungsbedingungen oder andere Vertragsbedingungen, die naturgemäß nur direkt zwischen einem/r KäuferIn und einem(r VerkäuferIn relevant sind, nicht für Sie gelten und zwischen Ihnen und Ihrem/r VerkäuferIn vereinbart werden.
Asien, Pazifik, Hongkong	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	Die Servicebeschreibung und andere Servicedokumente zu Dell als juristische Person, die Sie von Ihrem/r VerkäuferIn erhalten, stellen keine Vereinbarung zwischen Ihnen und Dell als juristischer Person dar, sondern dienen nur als Beschreibung des Inhalts des Service, den Sie von Ihrem/r VerkäuferIn erwerben, sowie zur Klärung Ihrer Pflichten als EmpfängerIn des Service und der Grenzen und Beschränkungen eines solchen Service. Daher ist „KundInnen“ in dieser Servicebeschreibung und in anderen Servicedokumenten zu Dell als juristische Person in diesem Kontext als Verweis auf Sie und „Dell als juristische Person“ als Verweis auf Dell als Serviceanbieter zu verstehen, der den Service im Namen Ihres/r VerkäuferIn erbringt. Aus dem hierin beschriebenen Service ergibt sich für Sie kein direktes Vertragsverhältnis mit Dell als juristischer Person. Zum Ausschluss von Zweifeln sei darauf hingewiesen, dass Zahlungsbedingungen oder andere Vertragsbedingungen, die naturgemäß nur direkt zwischen einem/r KäuferIn und einem(r VerkäuferIn relevant sind, nicht für Sie gelten und zwischen Ihnen und Ihrem/r VerkäuferIn vereinbart werden.
Europa, Naher Osten und Afrika	Lokale landesspezifische Dell.com-Website oder Dell.com/servicedescriptions/global * KundInnen in Frankreich, Deutschland und dem Vereinigten Königreich finden zudem Informationen unter folgenden URLs: Frankreich: Dell.fr/ConditionsGeneralesdeVente Deutschland: Dell.de/Geschaeftsbedingungen Vereinigtes Königreich: Dell.co.uk/terms	Die Servicebeschreibung und andere Servicedokumente zu Dell als juristische Person, die Sie von Ihrem/r VerkäuferIn erhalten, stellen keine Vereinbarung zwischen Ihnen und Dell als juristischer Person dar, sondern dienen nur als Beschreibung des Inhalts des Service, den Sie von Ihrem/r VerkäuferIn erwerben, sowie zur Klärung Ihrer Pflichten als EmpfängerIn des Service und der Grenzen und Beschränkungen eines solchen Service. Daher ist „KundInnen“ in dieser Servicebeschreibung und in anderen Servicedokumenten zu Dell als juristische Person in diesem Kontext als Verweis auf Sie und „Dell als juristische Person“ als Verweis auf Dell als Serviceanbieter zu verstehen, der den Service im Namen Ihres/r VerkäuferIn erbringt. Aus dem hierin beschriebenen Service ergibt sich für Sie kein direktes Vertragsverhältnis mit Dell als juristischer Person. Zum Ausschluss von Zweifeln sei darauf hingewiesen, dass Zahlungsbedingungen oder andere Vertragsbedingungen, die naturgemäß nur direkt zwischen einem/r KäuferIn und einem(r VerkäuferIn relevant sind, nicht für Sie gelten und zwischen Ihnen und Ihrem/r VerkäuferIn vereinbart werden.

* KundInnen können einfach über Dell.com auf ihre lokale Dell.com-Website zugreifen, indem sie einen Computer nutzen, der an ihrem Standort mit dem Internet verbunden ist, oder indem sie auf der Dell Webseite „Choose a Region/Country“ unter Dell.com/content/public/choosecountry.aspx?c=us&l=en&s=gen eine Option auswählen.

KundInnen ist bekannt, dass eine Erneuerung, Änderung, Verlängerung oder weitere Nutzung der Services über die ursprüngliche Laufzeit hinaus der zum jeweils aktuellen Zeitpunkt geltenden Servicebeschreibung unterliegt, die unter Dell.com/servicedescriptions/global einsehbar ist.

Sollte ein Widerspruch in den Bedingungen der Dokumente vorliegen, aus denen diese Vereinbarung besteht, sind die Dokumente in der folgenden Reihenfolge anwendbar: (i) diese Servicebeschreibung, (ii) die Vereinbarung, (iii) das Bestellformular. Die vorrangigen Bedingungen werden so eng wie möglich ausgelegt, um den Widerspruch zu lösen, während so viel wie möglich von den widerspruchsfreien Bedingungen erhalten bleibt, einschließlich der widerspruchsfreien Bedingungen innerhalb desselben Paragrafen, Abschnitts oder Unterabschnitts.

Durch die Bestellung der Services, den Erhalt der Services, die Verwendung der Services oder der zugehörigen Software bzw. durch Klicken auf die Schaltfläche/Aktivieren des Felds „I agree“ (Ich stimme zu) oder Ähnliches auf der Dell.com- oder DellEMC.com-Website im Zuge des Kaufvorgangs oder in einer Dell Technologies Software oder Internetoberfläche verpflichten Sie sich zur Einhaltung dieser Servicebeschreibung und der durch Verweis in dieser enthaltenen Vereinbarungen. Wenn Sie diese Servicebeschreibung im Namen eines Unternehmens oder einer anderen juristischen Person unterzeichnen, bestätigen Sie, dass Sie über die entsprechende Befugnis zum Eingehen dieser Servicebeschreibung verfügen. In diesem Fall bezieht sich „Sie“, „Ihnen“ oder „KundInnen“ auf jene juristische Person. In manchen Ländern muss neben dem Erhalt der Servicebeschreibung u. U. auch ein Bestellformular unterzeichnet werden.

Mitteilung zu Datenerhebung und -nutzung

In dieser Mitteilung („Hinweis“) wird erläutert, wie Dell Technologies und seine Unternehmensgruppe im eigenen Namen oder für einen Drittanbieter oder für seine unmittelbaren und mittelbaren Tochtergesellschaften („Dell“) Ihre Daten erfasst, verwendet und weitergibt, wenn Sie Dell Software verwenden. Wir erfassen und verwenden bestimmte Datentypen, die nachfolgend beschrieben sind, um Ihre Erfahrung in Bezug auf Dell Produkte zu personalisieren sowie um unseren Support und unsere Produkte, Lösungen und Services zu verbessern („Dell Lösungen“).

Informationen, die wir bereits erfassen. Wir erfassen möglicherweise automatisch Verhaltens- und Nutzungsinformationen zur Verwendung von, zum Zugriff auf oder zur Interaktion mit den Dell Lösungen. Diese Informationen geben nicht unbedingt direkt Aufschluss über Ihre Identität, können aber eine eindeutige Kennung und andere Informationen über das von Ihnen verwendete Gerät enthalten, wie z. B. Ihr Service-Tag, das Hardwaremodell, die Betriebssystemversion, Hardwareeinstellungen und Systemabstürze, installierte Anwendungen, deren Einstellungen und Nutzung und/oder (MAC-)Adresse und andere Daten, die Ihr Gerät oder System eindeutig identifizieren können.

Wir erfassen möglicherweise außerdem Informationen darüber, wie Ihr System oder Gerät mit den Dell Lösungen interagiert hat, z. B. statistische Informationen, Netzwerkverbindungsindikatoren und Routing oder im Fall von Dell Service, Informationen im Zusammenhang mit Sicherheitsereignissen. In einigen Fällen können die erfassten Informationen direkt oder indirekt EndnutzerInnen identifizieren und eine Person mit bestimmten Onlineverhalten verknüpfen, sofern dies für die in diesem Hinweis angegebenen Zwecke erforderlich ist.

Zum Unterstützen dieser Aktivitäten erklären Sie sich damit einverstanden, Dell eine eingeschränkte, nicht exklusive Lizenz zur Nutzung Ihrer Daten zur Bereitstellung des Service zu gewähren. Sie erklären sich außerdem damit einverstanden, Dell eine eingeschränkte, nicht exklusive, unbefristete, weltweite, unwiderrufliche Lizenz zur Nutzung und anderweitigen Verarbeitung von Daten im Zusammenhang mit Sicherheitsereignissen während und nach der Laufzeit des Service zur Entwicklung und/oder Verbesserung des Service und der Dell Lösungen zu gewähren, die wir anbieten und unseren KundInnen bereitstellen. Dell ist nicht verpflichtet, Daten im Zusammenhang mit Sicherheitsereignissen nach Beendigung des Service aus irgendeinem Grund zurückzugeben oder zu löschen.

[Dell Software kann alle oder einen Teil der oben genannten Informationen in Datenprotokollen konsolidieren, die an Dell übertragen werden, wenn eine Internetverbindung hergestellt wird.]

Die von Dell verwendeten Technologietypen können sich im Laufe der Zeit ändern, da sich die Technologie weiterentwickelt. Weitere Informationen zur Verwendung von Cookies und ähnlichen Tracking-Technologien finden Sie unter Cookies und ähnliche Technologien im online verfügbaren Datenschutzhinweis von Dell.

Datenübertragungen. Die in diesem Hinweis beschriebenen Daten werden möglicherweise außerhalb Ihres Landes an andere Standorte wie z. B. in den USA, der EU und Japan oder an Hosting-Standorte von DrittanbieterInnen übertragen. Wir werden alle geeigneten technischen und organisatorischen Maßnahmen treffen, um die von uns übertragenen Daten zu schützen.

Aufbewahrung Ihrer Daten. Ihre personenbezogenen Daten werden in Übereinstimmung mit den in diesem Hinweis beschriebenen Zwecken und gemäß den Aufbewahrungsrichtlinien von Dell und geltendem Recht aufbewahrt. Die von Dell wie in diesem Hinweis beschrieben erfassten Daten werden gemäß den Aufbewahrungsrichtlinien von Dell und geltendem Recht aufbewahrt.

Personenbezogene Daten und Datenschutz. Die Erfassung, Verwendung und Verarbeitung der von Ihnen bereitgestellten personenbezogenen Daten durch Dell werden im Datenschutzhinweis von Dell beschrieben. Wenn Sie uns aus irgendeinem Grund in Bezug auf unsere Datenschutzpraktiken kontaktieren möchten, senden Sie eine E-Mail an privacy@dell.com oder lesen Sie unseren vollständigen Datenschutzhinweis unter https://www.dell.com/learn/us/en/uscorp1/policies-privacy-country-specific-privacy-policy

Ergänzende Geschäftsbedingungen

1. Laufzeit des Service. Diese Servicebeschreibung tritt an dem auf Ihrem Bestellformular aufgeführten Datum in Kraft und gilt für die auf dem Bestellformular angegebene Laufzeit („**Laufzeit**“). Die Anzahl der Systeme, Lizenzen, Installationen, Bereitstellungen, verwalteten Endpunkte oder EndnutzerInnen, für die KundInnen einen oder mehrere Services erwerben, der Tarif oder Preis sowie die jeweilige Laufzeit des Service sind im jeweiligen Bestellformular angegeben. Sofern nicht anderweitig mit Dell Technologies Services schriftlich vereinbart, werden die in dieser Servicebeschreibung beschriebenen Services den KundInnen nur zur internen Nutzung bereitgestellt. Den KundInnen ist nicht gestattet, die Services an Dritte weiterzuverkaufen oder für die Zwecke eines Servicebüros zu verwenden.

2. Wichtige Zusatzinformationen

A. Terminänderung. Wurde für den Service ein Termin vereinbart, sind Terminänderungen mindestens acht (8) Kalendertage vor dem ursprünglich vereinbarten Termin anzukündigen. Wenn KundInnen den Servicetermin innerhalb von 7 Tagen oder weniger vor dem ursprünglich vereinbarten Termin ändern, fällt eine Änderungsgebühr an, die jedoch höchstens 25 % des Preises für den Service beträgt. KundInnen stimmen zu, dass jegliche Terminänderungen mindestens acht (8) Tage vor dem Beginn des Service bestätigt werden müssen.

B. Zahlung für mit den Services gekaufte Hardware. Sofern nicht anderweitig schriftlich vereinbart, ist die Zahlung für Hardware in keinem Fall an die Ausführung oder Erbringung von zusammen mit der Hardware erworbenen Services gebunden.

C. Wirtschaftlich angemessene Einschränkungen der Serviceerbringung. Dell Technologies Services behält sich das Recht vor, die Erbringung des Service abzulehnen, wenn Dell Technologies Services der begründeten Meinung ist, dass dadurch ein unangemessenes Risiko für Dell Technologies Services oder die von Dell Technologies Services beauftragten ServiceanbieterInnen entsteht oder dass die Erbringung einer verlangten Leistung über den Serviceumfang hinausgeht. Dell Technologies Services übernimmt keine Haftung für Ausfälle oder nicht termingerecht erbrachte Leistungen aufgrund von Umständen, die Dell nicht zu vertreten hat, einschließlich der Nichteinhaltung der Verpflichtungen der KundInnen gemäß dieser Servicebeschreibung.

D. Optionale Services. Unter Umständen sind optionale Services (einschließlich Support vor Ort, Installation, Beratung, Managed und Professional Services oder Schulungsservices) von Dell Technologies Services erhältlich, die je nach Kundenstandort variieren. Für optionale Services ist unter Umständen eine separate Vereinbarung mit Dell Technologies Services erforderlich. Ist eine solche Vereinbarung nicht vorhanden, werden optionale Services in Übereinstimmung mit der vorliegenden Servicebeschreibung erbracht.

E. Abtretung und Unterverträge. Dell Technologies Services kann diesen Service im Rahmen eines Untervertrags von DrittanbieterInnen ausführen lassen und/oder diese Servicebeschreibung auf externe ServiceanbieterInnen übertragen, die den Service im Auftrag von Dell Technologies Services ausführen.

F. Kündigung. Dell Technologies Services ist berechtigt, diesen Service jederzeit während der Servicelaufzeit aus folgenden Gründen zu kündigen:

- KundInnen kommen der Zahlungsverpflichtung für diesen Service gemäß den Zahlungsbedingungen nicht oder nicht in vollem Umfang nach.
- KundInnen machen beleidigende oder drohende Bemerkungen oder verweigern die Zusammenarbeit mit den unterstützenden AnalystInnen oder Vor-Ort-TechnikerInnen.
- KundInnen halten die Geschäftsbedingungen dieser Servicebeschreibung nicht ein.

Im Falle einer Kündigung durch Dell Technologies Services schickt Dell Technologies Services eine schriftliche Kündigung an die Rechnungsadresse der KundInnen. Das Schreiben enthält den Grund für die Kündigung sowie das Datum, an dem diese wirksam wird. Zwischen dem Datum des Versendens der Kündigung durch Dell Technologies Services an KundInnen und dem Vertragsende müssen mindestens zehn (10) Tage liegen, sofern nicht vom Gesetzgeber zwingend ein anderer Zeitraum vorgeschrieben ist. Beendet Dell Technologies Services diesen Service auf Grundlage dieses Absatzes, haben KundInnen keinen Anspruch auf Erstattung von an Dell Technologies Services geleisteten Zahlungen.

G. Geografische Einschränkungen und Standortänderung. Dieser Service ist nicht überall verfügbar. Serviceoptionen, inklusive Servicelevel, Geschäftszeiten des technischen Supports und Vor-Ort-Antwortzeiten, hängen von der jeweiligen Region ab, und manche Optionen sind möglicherweise am Kundenstandort nicht verfügbar; die entsprechenden Details erfahren Sie von unseren VertriebsmitarbeiterInnen.