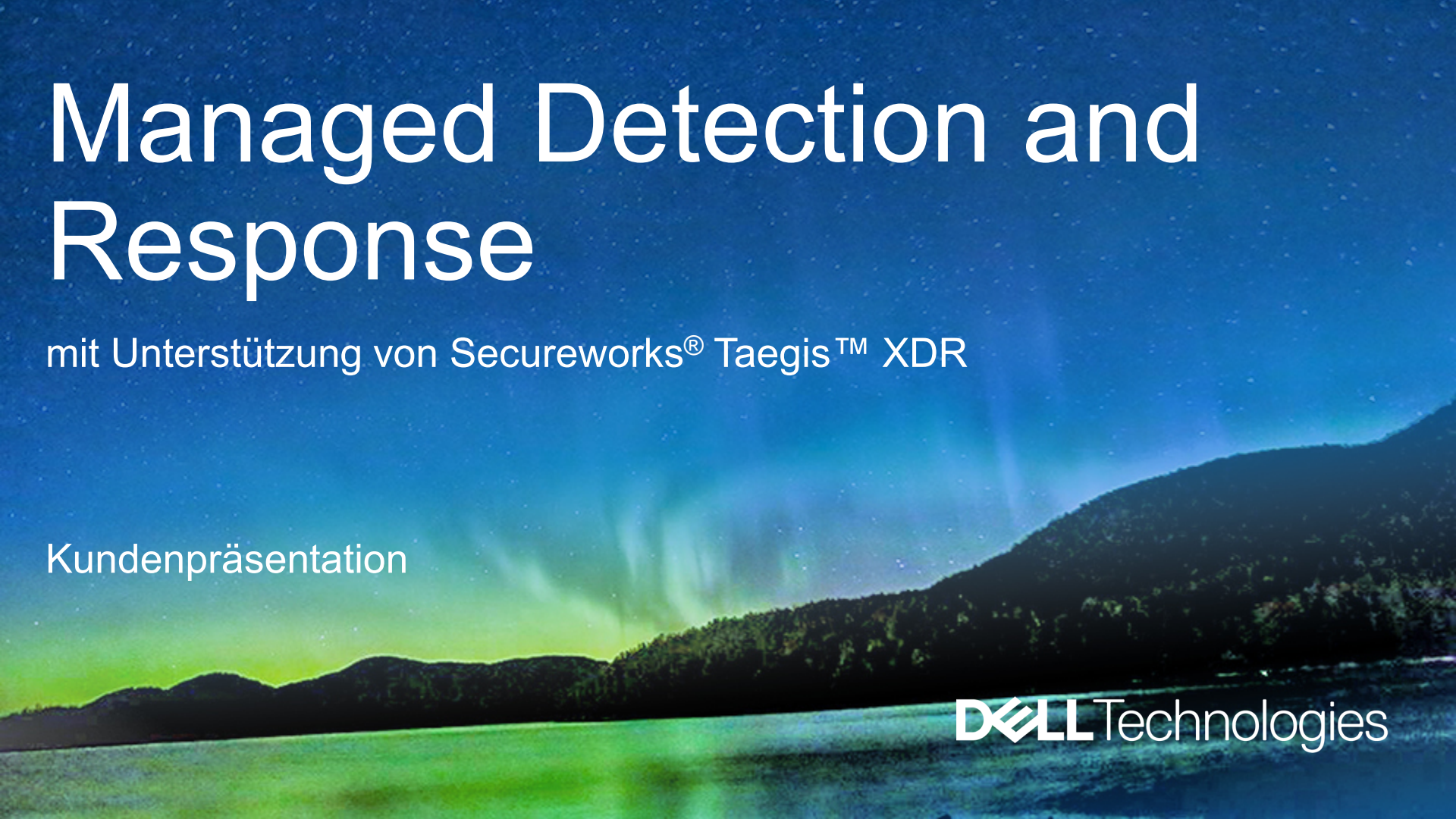
Managed Detection and Response

mit Unterstützung von Secureworks® Taegis™ XDR

Kundenpräsentation



Unternehmen haben Mühe, mit Sicherheitsbedrohungen Schritt zu halten

84 %
der Kunden sind loyaler gegenüber Unternehmen mit starken Sicherheitskontrollen[1]

63 % der Unternehmen erlebten bereits, dass eine Sicherheitslücke ausgenutzt und Daten infiziert wurden[2]

13 Mio. USD kostet im Durchschnitt eine Datenschutzverletzung[3]

3,5 Mrd. persönliche Datensätze wurden allein bei den zwei wichtigsten Datenschutzverletzungen des letzten Jahrzehnts gestohlen[4]

6 Bill. USD betragen die geschätzten Kosten der globalen Schäden durch Cyberkriminalität im Jahr 2021[5]

1 Quelle: State of the Connected Customer. Salesforce, 2019.
2 Quelle: Von Dell in Auftrag gegebenes Forrester Consulting Thought Leadership Paper, BIOS Security – The Next Frontier for Endpoint Protection, Juni 2019
3 Quelle: Accenture, Ninth Annual Cost of Cybercrime Study, März 2019.
4 Quelle: CSO, The 15 biggest data breaches of the 21st century, April 2020.
5 Quelle: Ransomware Attacks Predicted to Occur... The National Law Review, 2020.

Die Lösung

Ganz gleich, ob Sie Ihre Sicherheitsvorkehrungen verbessern möchten oder eine Sicherheitsverletzung erlebt haben und Unterstützung bei der Wiederherstellung benötigen, Dell Technologies Managed Detection and Response mit Unterstützung von Secureworks® Taegis™ XDR kann Ihnen helfen.

Mit unserem Fachwissen in Sachen Sicherheit und der Taegis XDR Security Analytics-Plattform können wir Ihre Umgebung über die Endpunkte, das Netzwerk und die Cloud hinweg schützen.

Wenn Sie einen Cyber-Vorfall erlebt haben, ist unser Team von Incident Response Experten mit jahrelanger Erfahrung bei der erfolgreichen Wiederherstellung von Kundenumgebungen jeder Größe bereit, Ihnen zu helfen.

MDR ist mit Sicherheitskameras zur Überwachung eines Hauses vergleichbar

NIST

Ermitteln	Schützen	Erkennen	Reagieren	Wiederherstellen
		Dell Technologies Managed Detection and Response		
Schritte	Einen Plan schmieden	Schlösser an Türen und Fenstern	Sicherheitskameras, Bewegungsmelder und ein Sicherheitsunternehmen, das 24x7 überwacht		Schnelle Reaktion auf Incidents

Informationen zum Angebot Managed Detection and Response

Dell Technologies Managed Detection & Response

mit Unterstützung von Secureworks Taegis XDR

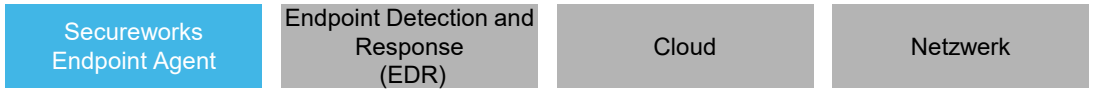
Dell Technologies bietet ein virtuelles, global verteiltes Security Operations Center (SOC), das Folgendes umfasst:

- Von Dell geschulte Ressourcen
- Unterstützung beim Agent-Rollout
- Erkennung und Ermittlung von Bedrohungen (24x7)
- Reaktion und aktive Korrektur (bis zu 40 Std./Quartal)
- Einleitung von Maßnahmen gegen Cyber-Incidents[1] (bis zu 40 Std./Jahr)
- Vierteljährliche Überprüfung mit dem Kunden

Der Service wird mithilfe von Secureworks Taegis XDR bereitgestellt
für Erkennung, Ermittlung und Reaktion auf fortgeschrittene Angriffe

- KI-basierte Erkennungen
- Integrierte Threat Intelligence (Deep Learning)
- Secureworks-Netzwerkeffekt (Einblicke von mehr als 4.200 Kunden)
- Ask An Expert Chat Box – von zertifizierten Dell Sicherheitsanalysten verwaltet
- APIs für Umgebungsintegrationen (Open-Source (GraphQL))

API-Integrationen zur Bereitstellung von Telemetrie zu XDR



[1]Wird nur im Fall eines tatsächlichen Incident bereitgestellt

Funktionen und Merkmale von Managed Detection and Response

mit Unterstützung von Taegis XDR

Unterstützung beim Agent-Rollout 1

Erkennung und Ermittlung von Bedrohungen 2

Antwort und aktive Korrektur 3

Einleiten von Maßnahmen gegen Cyber-Incidents 4

Wir analysieren gemeinsam mit Ihnen die Umgebung und unterstützen Sie bei der Bereitstellung des Software-Agents auf den entsprechenden Endpunkten – ohne zusätzliche Kosten.

- Unterstützung beim Agent-Rollout auf den Endpunkten
- Die Unterstützung beim Agenten-Rollout wird von erfahrenen Bereitstellungsexperten geleistet
- Bei Bedarf können wir auch zusätzliche Sicherheitslösungen hinzufügen, wenn Sie sich dafür entscheiden

Der Großteil Ihrer Umgebung ist ohne zusätzliche Kosten bereit für stationäres Monitoring

DELL Technologies

Funktionen und Merkmale von Managed Detection and Response

mit Unterstützung von Taegis XDR

Unterstützung beim Agent-Rollout 1

Erkennung und Ermittlung von Bedrohungen 2

Antwort und aktive Korrektur 3

Einleiten von Maßnahmen gegen Cyber-Incidents 4

Wir nutzen die marktführende Secureworks-Technologie, um fortgeschrittene Bedrohungen zu erkennen

- Überprüfen und Untersuchen von erkannten Bedrohungen[1]
- Nutzen von Secureworks-Angriffsdaten aus mehr als 1.400 Incident-Response-Projekten im letzten Jahr
- Von Secureworks zertifizierte Dell Sicherheitsanalysten sind rund um die Uhr für Sie verfügbar
- Vierteljährliche Überprüfungen und Anleitung zur Verbesserung der Sicherheitslage

Rund um die Uhr End-to-End-Monitoring

[1] Zusätzliche Gebühren für erfasste Daten, die mehr als 4 GB/vertraglich abgedecktem Endpunkt/Monat überschreiten. Kunden, die diese Grenze überschreiten, werden benachrichtigt und es werden Optionen vorgeschlagen.

DELL Technologies

Funktionen und Merkmale von Managed Detection and Response

mit Unterstützung von Taegis XDR

Unterstützung beim Agent-Rollout 1

Erkennung und Ermittlung von Bedrohungen 2

Antwort und aktive Korrektur 3

Einleiten von Maßnahmen gegen Cyber-Incidents 4

Wir sind die einsatzbereiten Sicherheitsexperten, die Sie rund um die Uhr unterstützen können, wenn XDR eine Bedrohung erkennt.

- Bereitstellen von empfohlenen Maßnahmen zur Behebung der erkannten Bedrohung
- Schritt-für-Schritt-Anweisungen zur Eindämmung der Bedrohung selbst in komplexesten Situationen
- Bis zu 40 Stunden Anleitung zur Remote-Korrektur pro Quartal[1].

Schnelle Reaktion auf Bedrohungen und Schutz der Umgebung Ihrer Kunden

[1] Zusätzliche Gebühren fallen an, wenn das 40-Stunden-Limit überschritten wurde

DELL Technologies

Funktionen und Merkmale von Managed Detection and Response

mit Unterstützung von Taegis XDR

Unterstützung beim Agent-Rollout 1

Erkennung und Ermittlung von Bedrohungen 2

Antwort und aktive Korrektur 3

Einleiten von Maßnahmen gegen Cyber-Incidents 4

Wenn bei Ihnen eine Sicherheitsverletzung aufgetreten ist, haben wir einen Prozess eingerichtet, um schnell einzugreifen

- Bis zu 40 Stunden zur Remote-Einleitung von Maßnahmen gegen Incidents pro Jahr zur Beschleunigung der aktiven Ermittlungen
- Anleitung durch unsere zertifizierten Sicherheitsexperten, die Unternehmen jeder Größe geholfen haben, schwerwiegende Sicherheitsvorfälle in wenigen Wochen zu beheben[1]
- Bei Bedarf sind zusätzliche Services für die Reaktion auf Incidents verfügbar

Wir initiieren den Prozess, um eine schnelle Wiederaufnahme des Betriebs zu ermöglichen.

[1] Zusätzliche Gebühren fallen an, wenn das 40-Stunden-Limit überschritten wurde

DELL Technologies

Gründe für Dell Technologies Managed Detection and Response

Eine einzigartige Kombination aus fundiertem IT-Fachwissen und der branchenführenden Secureworks Security Analytics-Plattform

Unsere Experten verfügen zusammen über mehr als 150 Jahre Cyber-Erfahrung mit mehreren Plattformen

Sie sind versiert in Ermittlungen von Bedrohungen, dem Aufspüren von Bedrohungen, Endpoint Security, Incident-Management und Beratung.

Verfügbar für Kunden mit nur 50 Endpunkten

Unterstützung beim Agent-Rollout, um Sie kostenlos bei der Bereitstellung von Agents zu unterstützen

Flexible Fakturierungsoptionen: kalkulierbare monatliche Zahlungen oder Jahresverträge

Alle Analysten sind XDR-zertifiziert und verfügen über verschiedene Zertifizierungen, einschließlich GIAC Sans, CEH, CISSP, CompTia usw.

Korrigieren von Indikatoren für eine Infizierung mit schrittweiser Anleitung, um sicherzustellen, dass Ihre Umgebung sicher bleibt

Secureworks Taegis XDR

vormals Red Cloaking TDR

Dell Technologies Managed Detection and Response

mit Unterstützung von Taegis XDR

- Rund-um-die-Uhr-Bedrohungserkennung und -ermittlungen zum Schutz Ihrer Umgebung und Unterstützung bei der Korrektur, falls erforderlich.

- Verbesserte Sicherheit durch Unterstützung bei der XDR-Bereitstellung und 24x7-Überwachung von Warnmeldungen
- Ein sicheres Gefühl durch Unterstützung bei der Reaktion auf Incidents
- Schnelle Wiederaufnahme des Betriebs durch unsere End-to-End-Antwort- und Korrekturlösungen

- Aus mehr als 21 Jahren Daten zu Angriffs- und Bedrohungsakteuren
- Über 80 Forscher in der Secureworks Counter Threat Unit ™
- Über 135 Bedrohungsgruppen, die aktiv überwacht werden
- Täglich mehr als 52.000 Aktualisierungen eindeutiger Bedrohungsindikatoren

Was leistet XDR?

- **Korreliert** sicherheitsrelevante Daten von Endpunkt-, Netzwerk-, Cloud- und Geschäftssystemen
- **Erkennt** bekannte und unbekannte Bedrohungen
- **Reichert Daten an mit** relevantem Nutzer- und Asset-Kontext für schnellere Einsichten
- **Ordnet** Sicherheitshinweise dem MITRE ATT&CK-Framework zu
- **Unterstützt** kooperative Ermittlungen
- **Automatisiert** Maßnahmen zur Eindämmung und Prävention
- **Beinhaltet** den marktführenden Threat Intelligence- und Endpunkt-Agent von Secureworks

XDR-Datenquellenintegrationen

Netzwerk

- Secureworks iSensor[2]
- Aruba ClearPass
- Barracuda NGFW und WAF
- Check Point
- Cisco ASA, FTD, Meraki, Ironport, IOS, NX-OS
- Citrix ADC
- F5 LTM und ASM WAF
- Fortinet Fortigate und FortiWeb
- Imperva-WAF
- Infoblox
- Juniper Pulse Secure und SRX
- Lastline
- McAfee Web Gateway
- Palo Alto-Firewall
- SonicWall Firewall
- Suricata
- Symantec ProxySG (Blue Coat)
- WatchGuard Firewall
- zScaler Firewall

Endpunkt

- Red Cloak Endpoint Agent[1, 2]
- CrowdStrike Falcon Insight[1]
- VMware Carbon Black Cloud Endpoint Standard[1]
- VMware Carbon Black Cloud Enterprise EDR
- VMware Carbon Black Hosted EDR
- Microsoft Windows-Ereignisprotokolle
- Microsoft DNS
- Microsoft Defender for Endpoint[3]
- Linux Server

Cloud

- Microsoft Office 365
- Microsoft Azure AD[2]
- Microsoft Azure
- AWS-GuardDuty
- AWS CloudTrail

1 Eine EDR-Technologie, die für den MDR-Service erforderlich ist, CrowdStrike Falcon Insight (TDR/MDR)
2 Verfügbare Antwortmaßnahmen
3 Microsoft Defender for Endpoint (nur TDR) – vormals **Microsoft Defender ATP**
- CrowdStrike Falcon Prevent (nur TDR)

Threat Intelligence

Bedrohungslandschaft vom Secureworks Counter Threat Unit™ Research Team

- KUNDENEREIGNISSE
- BEZIEHUNGEN
- MALWARE-ANALYSE
- BOTNET-MONITORING
- SICHERHEITSBLOGS
- MAILING-LISTE
- WEBSITE-SCRAPING
- GEOPOLITISCHE ANALYSE
- ERMITTLUNGEN
- UNTERSTÜTZUNG FÜR THREAT INTELLIGENCE
- ANTWORT AUF INCIDENTS
- UNTERGRUND
- ÜBERWACHUNG
- SOCIAL MEDIA

Secureworks® Mitgliedschaften und Akkreditierung

- Secureworks ist seit 2005 aktives Mitglied im Forum of Incident Response and Security Teams (FIRST).
- Akkreditierung vom nationalen Cyber Security Centre (NCSC) als Anbieter von Cyber-Incident-Reaktionen (CIR) in Großbritannien.
- Akkreditierung von der National Security Agency Central Security Serviced NSA|CSS als National Security Cyber Support Program (NSCAP) Cyber Incident Response Support (CIRA)-Anbieter in den USA.
- Zusätzliche Verbindungen zu US Department of Homeland Security, FBI, NH-ISAC, FS-ISAC, National Cyber Forensics Training Alliance (NCFTA), United States Secret Service, National Institute of Standards and Technology (NIST) sowie European Union Agency for Network and Information Security (ENISA). Langjährige Beziehungen zu Strafverfolgungsbehörden, Nachrichtendiensten und Regierungsbehörden ermöglichen Secureworks die Zusammenarbeit bei Ermittlungen.

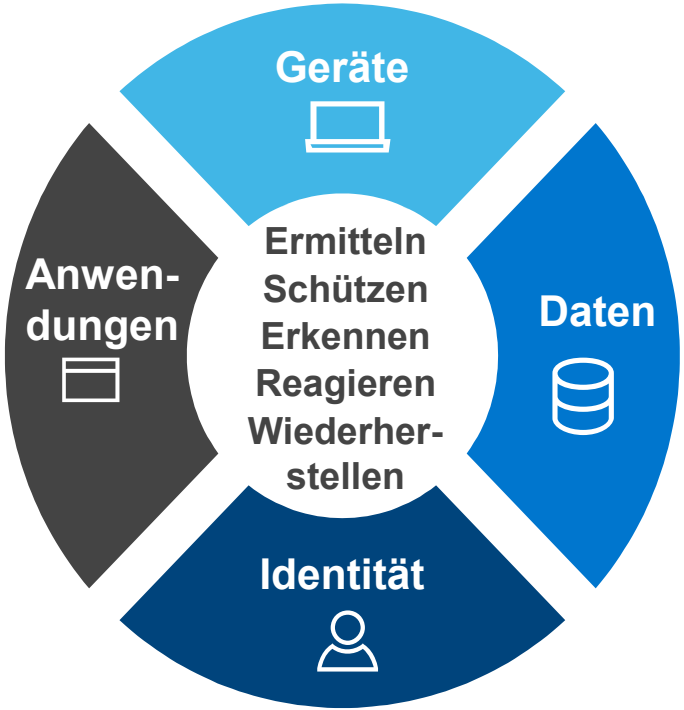
Incident-Antwort von Dell Technologies

Wenn Sie mehr benötigen, sehen Sie sich unsere Angebote an.

Verfügbare kundenspezifische Sicherheitsfunktionen

Proaktiv

- Workshops
- Assessments
- Management
- Compliance
- Managed Services
- Vor-Ort-Service



Reaktive

- Antwort auf Incidents
- Digitale Forensik
- Sicherheitstransformation
- Infrastrukturtransformation
- Vorschussleistungen

Gründe für Dell Technologies Incident Recovery

Zentrale Anlaufstelle für IT- und Cyber-Antwort mit Fachwissen in den Bereichen Recht, Versicherungen, Hardware, Software, Services, Incident-Antwort und mehr.

Wir können die Cyber-Recovery-Bemühungen schnell an Ihre Anforderungen anpassen – unabhängig von ihrer Größe oder Recovery-Anforderungen.

100 %

Erfolgsrate bei der Wiederherstellung von Kunden, die einen Cyber-Vorfall erlebt haben. [1]

Engagiertes Team von Experten für die Antwort auf Cyber-Incidents, dessen meisten Mitglieder über **mehr als 10 Jahre Erfahrung in Cybersicherheit verfügen.**

Schnelle Antwortzeit – wir können innerhalb von Minuten/Stunden telefonisch eingreifen, sodass ein **Incident Response Team in weniger als 48 Stunden vor Ort ist**.

[1] Ab Januar 2021.

Häufig gestellte Fragen

Häufig gestellte Fragen

Frage	Antwort
Wie kann ich diesen Service kaufen?	Wir empfehlen wegen der kalkulierbaren monatlichen Zahlungen den Kauf eines Abonnements. Falls erforderlich, sind auch 1-, 3- oder 4-Jahresverträge verfügbar. Weitere Unterstützung erhalten Sie von Ihrem Dell Sales oder Services Specialist.
Muss ich Software für MDR kaufen?	Wenn Sie MDR erwerben, verwendet unser Team Taegis XDR, um Bedrohungen in Ihrer Umgebung zu erkennen. Sie müssen keine XDR-Lizenzen erwerben. Es wird dringend empfohlen, dass Sie zusätzlich zum MDR-Service über eine Virenschutzsoftware verfügen.
Benötige ich noch eine Virenschutzsoftware, wenn ich MDR kaufe?	Ja, es wird dringend empfohlen, eine Virenschutzsoftware zu haben. MDR ist eine umfassende Lösung für die Überwachung, Erkennung und Reaktion auf Sicherheitsbedrohungen. Wir empfehlen jedoch, dass Sie auch über eine Virenschutzsoftware verfügen. Wenn Sie keine haben, wenden Sie sich an Ihren Vertriebsmitarbeiter, um eine zu erwerben.
Spielt es eine Rolle, welche Virenschutzsoftware ich habe?	Sie können ein beliebiges Virenschutzprogramm Ihrer Wahl verwenden. Die folgenden Optionen ermöglichen es unserem MDR-Service, die Telemetriedaten der Virenschutzsoftware zu nutzen: • VMware Carbon Black • Microsoft Defender • Crowdstrike
Mein Unternehmen ist weltweit tätig. Sind Mitteilungen auch in anderen Sprachen als Englisch verfügbar?	Derzeit erfolgt die gesamte Kommunikation nur in englischer Sprache. Wichtige Sprachen werden so bald wie möglich zur Verfügung gestellt.

Häufig gestellte Fragen

Frage	Antwort
Was bedeutet das Daten-Storage-Limit?	Je nach der Nutzung ihrer Endpunkte generieren einige Kunden mehr zu überwachende Daten als andere Kunden. Um die Kosten für den Großteil der Kunden niedrig zu halten, begrenzen wir die Menge der zu überwachenden erfassten Daten auf 4 GB pro vertraglich abgedecktem Endpunkt pro Monat. Wenn Sie diese Grenze überschreiten, werden wir Sie benachrichtigen und Ihnen Optionen anbieten.
Wird MDR vor Ort oder remote bereitgestellt?	MDR wird remote bereitgestellt.
Wo finde ich die Servicebeschreibung?	Die Beschreibung des Dell Technologies Managed Detection and Response Service finden Sie hier.
Was wird als Endpunkt betrachtet?	Ein Endpunkt kann fast jedes Gerät sein, das eine Netzwerkverbindung herstellen kann. Beispiele hierfür sind Laptops, Desktop-PCs, Firewalls und (virtuelle) Server.

Häufig gestellte Fragen

Frage	Antwort
Welche Betriebssysteme können mit MDR überwacht werden?	Die Betriebssysteme Windows und Linux können überwacht werden. In Kürze werden wir auch MacOS überwachen können. Wir sind nicht in der Lage, ChromeOS zu überwachen.
Wird zum Überwachen von Geräten eine werkseitig installierte Option benötigt?	Nein. Die Überwachung erfolgt über Cloud Console.
Wann genau beginnt der Vertrag?	Der Vertrag beginnt an dem Tag, an dem die Bestellung aufgegeben wurde.
Muss ich ProManage erwerben, um MDR zu erhalten?	Nein. Managed Detection and Response ist als ProManage-Modul (nur Nordamerika) verfügbar. Der Service ist aber auch in 32 Ländern (einschließlich Nordamerika) als eigenständiger Service erhältlich.
Ist MDR dasselbe wie das Gerätemanagement beim Microsoft Endpoint Manager ProManage-Modul?	Nein. Das Gerätemanagement bei Microsoft Endpoint Manager ist ein anderes Angebot und verwendet unterschiedliche Technologien.

Verfügbarkeit

Managed Detection and Response

Länderverfügbarkeit

ABU

1. USA
2. Kanada
3. Brasilien
4. Chile
5. Mexiko

EMEA

1. Österreich
2. Belgien
3. Tschechische Republik
4. Dänemark
5. Finnland
6. Frankreich
7. Deutschland
8. Griechenland
9. Irland
10. Italien
11. Luxemburg
12. Niederlande
13. Norwegen
14. Polen
15. Portugal
16. Slowakei
17. Südafrika
18. Spanien
19. Schweden
20. Schweiz
21. Vereinigtes Königreich

APJ

1. Australien
2. Hongkong und Macau
3. Indien
4. Japan[1]
5. Neuseeland
6. Singapur

[1]Eingeschränkter Funktionsumfang

Glossar

Glossar

Laufzeit	Beschreibung
Warnmeldung	Priorisierte Vorkommen von verdächtigem oder bösartigem Verhalten, die von einer TDR-Anwendung beobachtet werden.
Endpunkt-Agent	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 XDR-Anwendung zu senden. Link zum Zugriff auf die Liste der Endpunkt-Agents, die mit der XDR-Anwendung von Secureworks kompatibel sind: **https://docs.ctpx.secureworks.com/at_a_glance/#endpoints**
Integration	Application Programming Interface (API)-Aufrufe oder andere Softwareskripte, die Drittanbieterprodukten und Sicherheitstools die Einspeisung von Telemetrie in Secureworks Taegis XDR erlauben.
Bedrohung	Jede von der XDR-Anwendung identifizierte Aktivität, die auf eine mögliche Infizierung der oder Cyber-Bedrohung für die Umgebung des Kunden hinweist.

Glossar

Laufzeit	Beschreibung
Ermittlungen	Ein zentraler Standort in der XDR-Anwendung, der verwendet wird, um Nachweise, Analysen und Empfehlungen zu sammeln, die auf eine Bedrohung in der IT-Umgebung des Kunden abzielen.
Sicherheits-Incident	Ein XDR-generierter Umstand, wobei eine Infizierung oder eine vermutete Infizierung stattgefunden hat, an der der Kunde beteiligt ist.
Aufspüren von Bedrohungen	Der zyklische Prozess, bei dem sowohl die Software als auch Menschen zuvor unbekannte Bedrohungen in einer IT-Umgebung suchen. Wenn Bedrohungen identifiziert werden, werden sie im System aufgezeichnet, um sicherzustellen, dass sie später erkannt werden können.


DELL Technologies

Kunden-Workflow

Kunden

Managed Detection and Response

mit Unterstützung von Secureworks Taegis XDR

DELL Technologies

Service initialisieren

Mandanten konfigurieren

Services verbinden*

* siehe Integrationen

Onboarding und Agenten-Rollout

Monitoring beginnen

DELL Technologies