

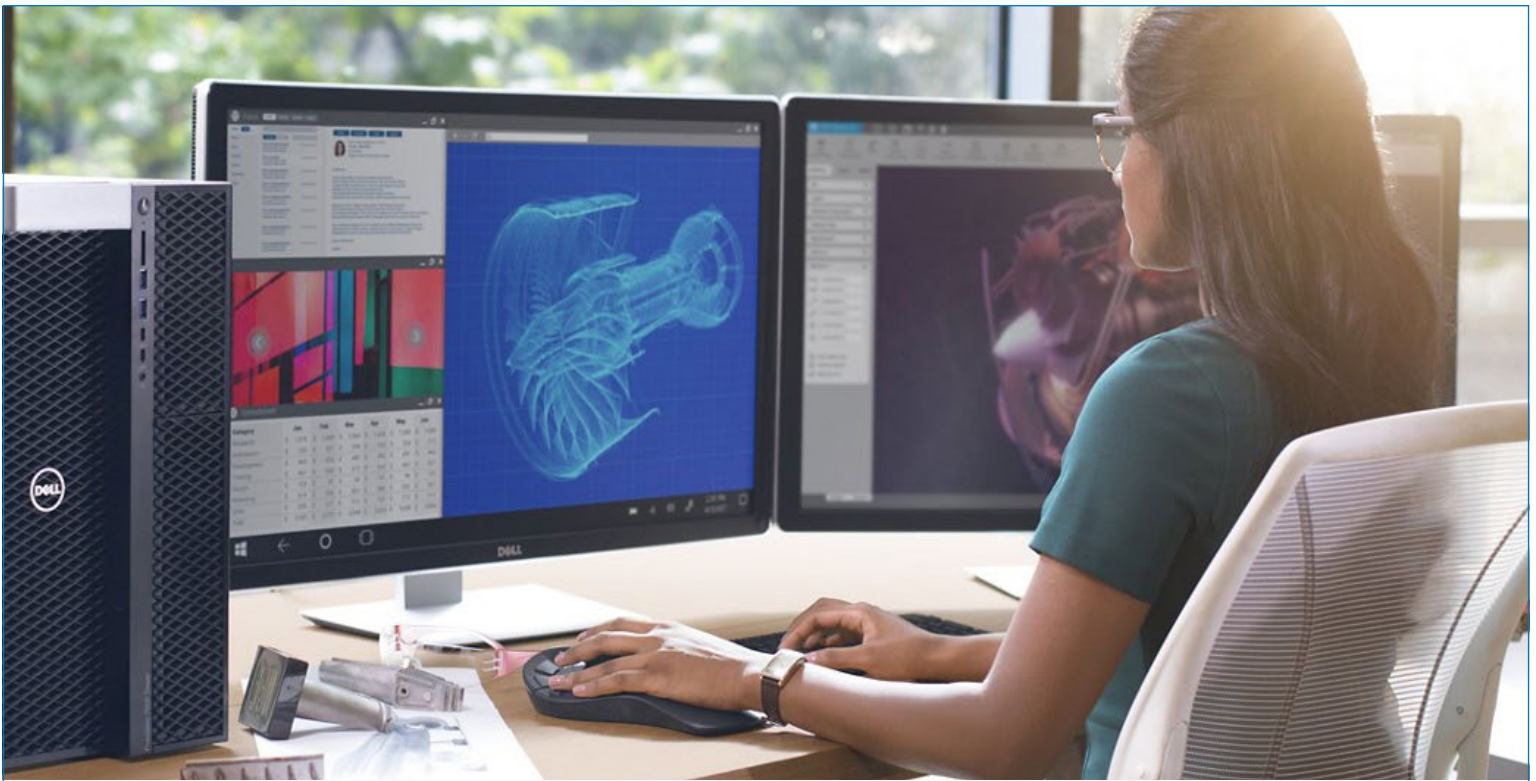


SupportAssist for Business PCs: Sicherheit – Übersicht

Fünf wichtige Fragen, die Sie möglicherweise zum Thema Sicherheit bei SupportAssist haben – und ihre Antworten

Mit SupportAssist können Sie den Support von Dell Technologies automatisieren, da Hardware- und Softwareprobleme in Ihrer gesamten PC-Flotte erkannt werden. SupportAssist behebt Probleme mit der Systemleistung und -stabilisierung, reduziert Sicherheitsbedrohungen, überwacht und erkennt Hardwarefehler und automatisiert den Prozess der Einbindung des technischen Supports von Dell.

SupportAssist erfasst zudem proaktiv Telemetriedaten von Ihren PCs und bietet Einblicke in die PC-Auslastung und Korrekturen basierend auf Ihrem Serviceplan.



Inhalt

- I. Einführung 3**
- II. Informationen zu SupportAssist 4**
 - a. Merkmale 4
- III. SupportAssist-Architektur 5**
 - a. Zentrales Management von SupportAssist mithilfe von TechDirect..... 5
- IV. Sicherheit bei SupportAssist 6**
 - a. Welche Daten werden von SupportAssist gesammelt?.....7
 - b. Wie werden Daten von SupportAssist sicher übertragen?..... 8
 - c. Wie werden die Daten von SupportAssist behandelt? 9
 - d. Wie werden Daten von SupportAssist sicher gespeichert? 9
 - e. Welche Sicherheitsverfahren und -richtlinien nutzt Dell Technologies? 12
- V. Fazit 14**

I: Einführung

Der Ausfall eines Laptops kann sowohl zu Unterbrechungen führen als auch frustrierend sein. Derartige Probleme können die Mitarbeiterproduktivität stark beeinträchtigen – und das oft zum ungünstigsten Zeitpunkt. Aus diesem Grund machen sich CIOs in Unternehmen zunehmend Gedanken über die Qualität und Verfügbarkeit ihrer Computerflotten.

Viele CIOs setzen auf die neueste und fortschrittlichste Technologie, die Data-Science-Erkenntnisse nutzt, um Milliarden von Datenpunkten zu verarbeiten und IT-AdministratorInnen dabei zu unterstützen, effizienter zu arbeiten. Dazu werden Systemstatusinformationen von Endnutzersystemen an die IT-Abteilung des Unternehmens oder an einen Hardware- oder Softwareanbieter gesendet, um Probleme so schnell wie möglich zu beheben oder gar nicht erst auftreten zu lassen. Dell ProSupport Plus mit SupportAssist-Konnektivitätstechnologie warnt Sie vor einer defekten Festplatte über eine zentrale Ansicht Ihrer gesamten PC-Flotte im TechDirect-Portal.

Für Verfügbarkeit und Effizienz ist diese Technologie unverzichtbar. CIOs haben jedoch manchmal Fragen zu den dabei gesammelten Informationen und deren Handhabung.

Die folgenden Fragen werden als kritisch betrachtet:

- Welche Daten werden von SupportAssist gesammelt?
- Wie werden diese Daten bei der Übermittlung an die IT-Abteilung des Unternehmens oder an den Computeranbieter geschützt?
- Werden die Daten nach Erreichen des Ziels so gespeichert, dass sie privat und sicher bleiben?

In diesem Whitepaper werden diese und andere verwandte Fragen verwendet, um Data-Science-unterstützte Technologien zu bewerten. Es bietet einen kurzen Überblick darüber, wie SupportAssist mit der differenzierenden ProSupport Suite for PCs einen kompletten Supportservice bereitstellt, der Probleme vorhersehen und beheben kann, bevor sie sich auf Ihr Unternehmen auswirken. Außerdem wird detailliert beschrieben, wie Dell Technologies Services sensible Daten in seinen Prozessen sowie beim Transport und Speichern von Daten schützt.



II: Informationen zu SupportAssist

SupportAssist ist unsere intelligente Konnektivitätstechnologie¹, mit der Unternehmen einen automatisierten technischen Support für ihre gesamte PC-Flotte erhalten können. Die Lösung überwacht Endnutzengeräte, erkennt proaktiv Hardware- und Softwareprobleme und bietet Einblicke in die Systemnutzung.

Wenn ein Problem erkannt wird, öffnet SupportAssist automatisch eine Supportanfrage an den technischen Support. Je nach Art des Problems kann die Warnmeldung eine technische Supportanfrage oder einen automatischen Ersatzteilversand auslösen. SupportAssist sammelt sowohl Hardware- als auch Softwaredaten, die vom technischen Support für das Troubleshooting und die Problemlösung verwendet werden.



Dell ProSupport Suite for PCs bietet die umfassendsten Supportfunktionen in einer einzigen Lösung – ohne die Notwendigkeit, Services kombinieren zu müssen.²
[Erfahren Sie mehr.](#)

Hauptmerkmale

- Flottenweite proaktive und vorausschauende Erkennung für eine schnellere Problembekämpfung
- Schnelle Analyse der Bewertungen für Integrität, Anwendungserfahrung und Sicherheit auf einem einzigen Bildschirm
- Kundenspezifische Regeln zur Definition von Korrekturworkflows
- Automatisierte Erstellung und Bereitstellung von kundenspezifischen Updatekatalogen für Dell BIOS, Treiber, Firmware und Anwendungen
- Flexibilität bei der Anpassung Ihrer Ansichten und Dashboards in TechDirect

Verfügbare Funktionen sind je nach dem für einen PC erworbenen Supportplan unterschiedlich

- Mit ProSupport Plus erhalten EndnutzerInnen sämtliche Funktionen von SupportAssist, einschließlich vorausschauender Problemerkennung und Fehlerprävention.

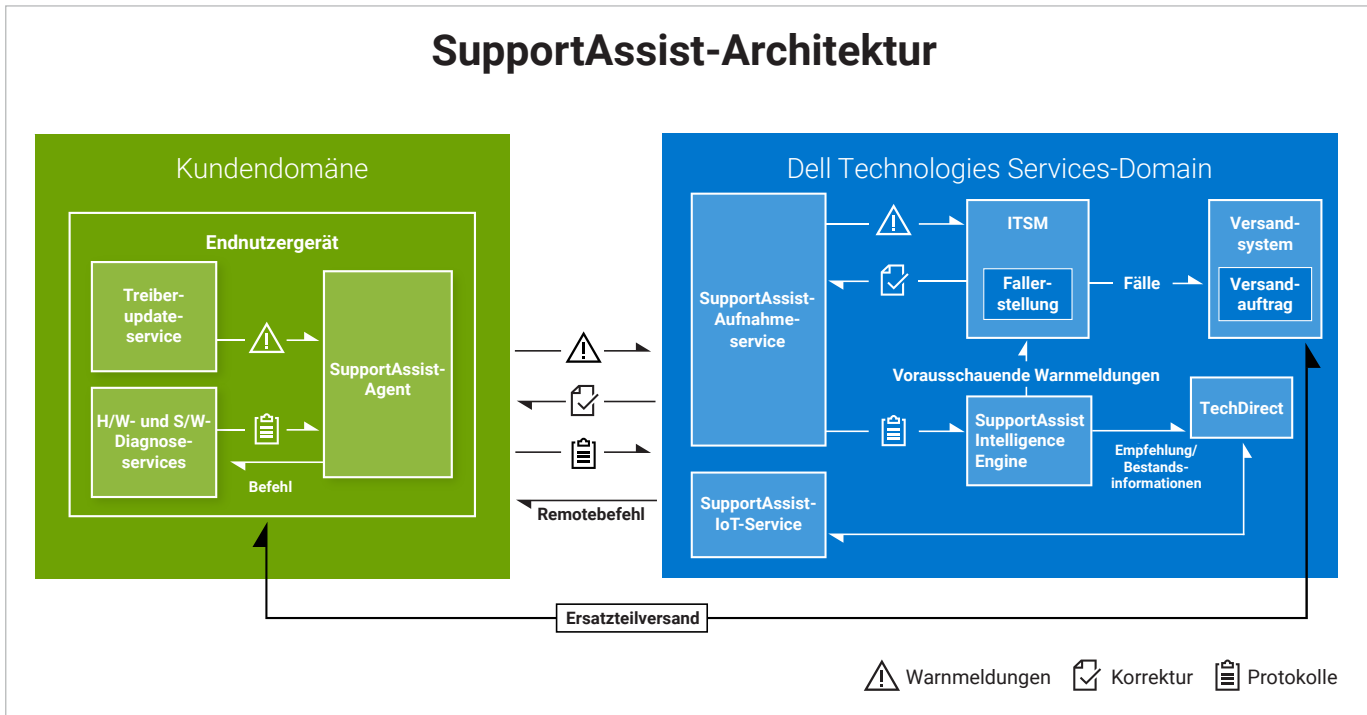
Eine vollständige Liste der Funktionen und Merkmale finden Sie in unserem [Administratorhandbuch](#).



III. SupportAssist-Architektur

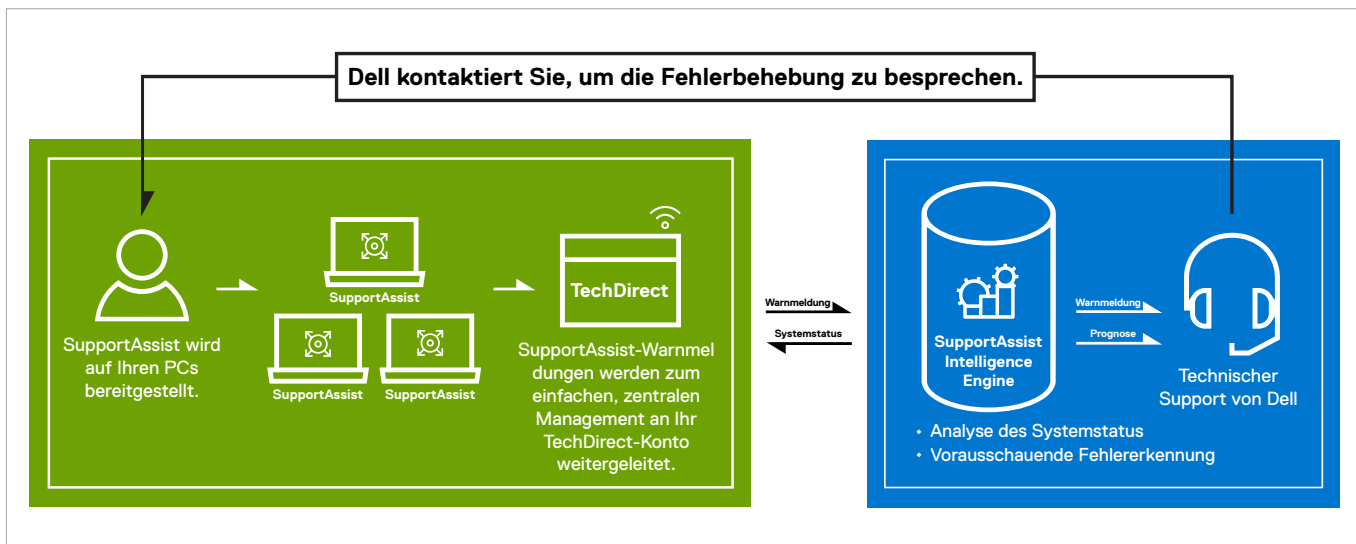
SupportAssist umfasst eine Reihe von Services, die Systeme kontinuierlich überwachen und zeitplanbasierte Integritätsprüfungen auf einem Gerät durchführen. Diese Informationen werden zurück an Dell Technologies Server übertragen, um die Daten zu analysieren und Empfehlungen bereitzustellen.

Eine vollständige Liste der Netzwerk-, Endpunkt-, Port-, Firewall- oder Gatewayanforderungen für die SupportAssist-Bereitstellung und -Korrektur finden Sie in unserem [Bereitstellungshandbuch](#). Unsere Korrekturskripte werden von Dell entwickelt, getestet und signiert und dann vor der Ausführung bestätigt.



Zentrales Management von SupportAssist mit TechDirect

SupportAssist-Warnmeldungen werden für ein komfortables, zentrales Management in das TechDirect-Konto eines Unternehmens übertragen. Unternehmen mit einem ProSupport- oder ProSupport Plus-Serviceplan können Warnmeldungen außerdem automatisch an Dell Technologies Services weiterleiten lassen.



Zentrales Management von SupportAssist mit TechDirect (Fortsetzung):

SupportAssist Insights, eine sehr nützliche Analysekomponente, erfasst Daten zur Systemauslastung, die in der TechDirect-Konsole angezeigt werden können. Dazu gehören die CPU-Auslastung, freier Speicherplatz, die maximale Akkukapazität, die Akkulaufzeit und viele weitere nützliche Einblicke. In TechDirect können diese Informationen für alle Systeme, für Systeme in einer bestimmten Gerätegruppe oder für ein einzelnes System angezeigt werden. Kunden können Leistungsprobleme identifizieren und bessere Geschäftsentscheidungen treffen (z. B. ob ein Upgrade oder ein Austausch von Hardware durchgeführt werden muss oder nicht).

IV. Sicherheit bei SupportAssist

CIOs oder CSOs von Unternehmen haben möglicherweise die nachfolgend aufgeführten Fragen zu den von SupportAssist for Business PCs gesammelten Datentypen und deren Handhabung. In diesem Abschnitt werden diese Fragen beantwortet. Wir erläutern, dass SupportAssist nur die zur Behebung von Kundenproblemen benötigten Daten sammelt und diese Daten dann mit optimaler Sicherheit verarbeitet.



Welche Daten werden von SupportAssist gesammelt?



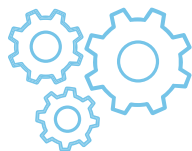
Wie werden Daten von SupportAssist sicher übertragen?



Wie werden die Daten von SupportAssist behandelt?



Wie werden Daten von SupportAssist sicher gespeichert?



Welche Sicherheitsverfahren und -richtlinien nutzt Dell Technologies?



Welche Daten werden von SupportAssist gesammelt?

SupportAssist erfasst automatisch die Daten, die für das Troubleshooting erforderlich sind, und sendet sie sicher an den technischen Support. Mit diesen Daten können wir eine adaptive, intelligente und beschleunigte Supporterfahrung bereitstellen.

Das Service-Tag, das zur Identifizierung des spezifischen, zu bearbeitenden Endnutzergeräts benötigt wird, ist die einzige Information über das Unternehmen, die von Geräten erfasst wird. Wenn SupportAssist feststellt, dass ein Teil proaktiv versandt werden sollte, verwenden wir vorhandene Kontaktinformationen, die sicher auf Dell Technologies Servern gespeichert sind.

Die folgenden Systeminformationen werden im Rahmen des routinemäßigen Systemmonitorings alle 24 Stunden erfasst und gesendet:

- **Schemaversion:** Version des Schemas, das für das routinemäßige Systemmonitoring verwendet wird
- **Agent-Version:** Auf dem System bereitgestellte Version von SupportAssist
- **Service-Tag:** Eindeutige Kennung des Systems
- **Systemmodell:** Modellname des Systems
- **Registrierungsinformationen:** Registrierungsstatus von SupportAssist
- **BS-Version:** Version des auf dem Gerät ausgeführten Betriebssystems
- **SP-Version:** Service Pack des Betriebssystems
- **UTC-Datum:** Datum und Uhrzeit des Versands der Informationen aus dem routinemäßigen Systemmonitoring an Dell Technologies Services
- **BIOS-Version:** Auf dem System installierte BIOS-Version
- **Status:** Status der Warnmeldung je nach Schweregrad, z. B. Warnung
- **Beschreibung:** Informationen über den Systemausfall, z. B. hohe CPU-Auslastung
- **Freier Speicherplatz auf der Festplatte:** Freier Speicherplatz, der auf der Systemfestplatte vorhanden ist
- **Arbeitsspeicherauslastung:** Menge des verwendeten Systemspeichers
- **CPU-Auslastung:** Menge der verwendeten CPU

- **Lokales Datum:** Datum und Uhrzeit des Systems
- **Datum des letzten Startvorgangs:** Datum und Uhrzeit, als das System zuletzt neu gestartet wurde
- **Ausführungsdatum des Windows-Updates:** Datum und Uhrzeit des letzten Windows-Updates auf dem System
- **BSOD-Anzahl in 24 Stunden:** Anzahl der Bluescreenvorkommen in den letzten 24 Stunden
- **Warnmeldungsinformationen:** Eindeutige Kennung der Warnmeldung



Weitere Informationen zu Systemmonitoringdaten, die von einem aktiven System gesammelt werden, finden Sie [hier](#) auf unserer Dell.com-Seite.



Alle Informationen werden über gesicherte Kanäle übertragen.



Wie werden Daten von SupportAssist sicher übertragen?

Die von SupportAssist an Dell Technologies Services übermittelten Daten werden mit 256 Bit verschlüsselt und über das TLS-Protokoll (Transport Layer Security) sicher übertragen.

Während der Installation des Pakets wird zur Laufzeit auf jedem Computer ein Verschlüsselungsschlüssel erzeugt. Der Verschlüsselungsschlüssel wird zusammen mit dem Salt verwendet, um installierte Informationen zu verschlüsseln. Zur Verschlüsselung von ruhenden Daten wird ein Algorithmus nach Branchenstandard verwendet.

In der Kryptografie handelt es sich bei einem Salt um zufällige Daten, die als Eingabe für eine unidirektionale Funktion verwendet werden, die Daten, ein Kennwort oder eine Passphrase „hasht“. Die Hauptfunktion von Salts besteht darin, Wörterbuchangriffe oder ihr gehashtes Gegenstück, einen vorberechneten Rainbow-Table-Angriff, abzuwehren.

Alle Verschlüsselungsschlüssel werden mit sicheren Zufallszahlengeneratoren generiert. Daten während der Übertragung werden mit TLS über HTTPS (Hypertext Transfer Protocol Secure) gesichert. Alle Verschlüsselungsalgorithmen entsprechen dem Branchenstandard und ruhende Daten werden ebenfalls verschlüsselt.

HTTPS wird in der Off-Box-Kommunikation für die Übertragung von Nutzerfeedback, Diagnosetelemetrieereignissen und API-Abfragen auf Dell.com oder Microsoft Azure IoT Hub für die im Wiederherstellungsprozess verwendeten Systeminformationen genutzt. Für den Pub-Sub-Ansatz wird ein sicheres MQTT-Protokoll verwendet.

Standard-HTTPS wird verwendet, um die Kommunikation zwischen dem Client und der Backend-Infrastruktur beim Übertragen oder Herunterladen von Inhalten an das Endnutzengerät zu sichern. HTTPS oder ein sicheres MQTT-Protokoll wird verwendet, um die Übermittlung von Telemetriedaten, die Kommunikation mit einer Backend-API auf Dell.com oder Microsoft Azure IoT Hub und das Herunterladen von Inhalten, die von Dell.com abgerufen wurden, zu sichern.

Alle Netzwerkkomponenten befinden sich hinter einer Firewall und werden von einem Netzwerksicherheitsteam verwaltet. Der Netzwerkverkehr wird streng kontrolliert. Der gesamte eingehende Datenverkehr wird über bestimmte Ports übertragen und nur an die entsprechenden Zielnetzwerkadressen gesendet. SupportAssist nutzt die Netzwerkbandbreite für verschiedene Ereignisse, die eine Verbindung mit der Infrastruktur von Dell Technologies Services erfordern. Die verwendete Bandbreite kann je nach Anzahl der Zielsysteme, die von SupportAssist überwacht werden, variieren. Tabelle 1 enthält die durchschnittliche Netzwerkbandbreite, die SupportAssist für das Monitoring eines einzelnen PCs verwendet.

Tabelle 1: Durchschnittlicher Datenverbrauch

| Ereignis | Häufigkeit des Ereignisses | Datenverbrauch pro PC |
|---|---|-----------------------|
| Registrieren von SupportAssist | Einmal nach der Bereitstellung | 15 KB |
| Senden von PC-Informationen oder minimalen Telemetriedaten | Einmal alle 6 bis 24 Stunden | 4 KB |
| Hochladen von PC-Informationen während geplanter Scans | Wöchentlich oder monatlich gemäß Konfiguration in den SupportAssist-Einstellungen in TechDirect | 120 KB |
| Senden regelmäßiger PC-Monitoringinformationen | Alle 30 bis 45 Tage nach der Bereitstellung | 135 KB |
| Senden von Warnmeldungen und Systemstatusinformationen | Wenn eine Warnmeldung erkannt oder ein Fehler beobachtet wird | 145 KB |
| Erstellen von Supportanfragen | Wenn eine Warnmeldung für die Erstellung einer Supportanfrage qualifiziert ist | 160–350 KB |
| Überprüfen auf SupportAssist-Versionsupdates | Einmal pro Woche | 16 KB |
| Upgrade auf die neueste SupportAssist-Version | Wenn die neueste Version verfügbar ist | 318 MB |
| Überprüfen auf Dell Empfehlungen für PC-Updates | Zweimal pro Woche | 1–2 MB* |
| Prüfen auf intelligente PC-Updateempfehlungen | Zweimal pro Woche | 65 KB |
| Senden von PC-Einblicken (Informationen zur Integrität und Anwendungserfahrung) | Einmal pro Stunde | 2.320 KB |

Hinweis: Die bereitgestellten Daten basieren auf SupportAssist for Business PCs Version 3.5.0.

* Die Daten variieren je nach Update.



Physische und logische Sicherheitsmaßnahmen zum Schutz der gespeicherten Daten



Wie werden die Daten von SupportAssist behandelt?

SupportAssist verwendet die gesammelten Daten, um Kunden einen automatisierten, proaktiven und vorausschauenden Support bereitzustellen. Wenn ein Problem mit einem System vorliegt, erzeugt SupportAssist eine Warnmeldung, damit ein/e MitarbeiterIn des technischen Supports das Problem beheben kann.

SupportAssist nutzt die gesammelten Daten auch, um vorherzusagen, wann eine Komponente kurz vor dem Ausfall steht. Dabei wird eine KI-Software (künstliche Intelligenz) eingesetzt, die auf Daten basiert, die von mehreren zehn Millionen Dell Systemen im Einsatz gesammelt wurden. Diese vorausschauende Warnung kann verwendet werden, um ein Teil zu versenden, bevor es ausfällt, wodurch Systemverfügbarkeit und Data Protection optimiert werden.

Schließlich verwendet SupportAssist die Daten, um Viren und Malware auf Nutzersystemen zu erkennen und zu entfernen, die Betriebssystemleistung zu optimieren und Empfehlungen zu BIOS-, Treiber- und Firmwareupdates bereitzustellen.

Die Systemanwendungsnutzung stellt Einblicke in die Systemnutzung mit der Insights-Komponente bereit.

Physische Sicherheit

Dell Technologies Services hostet SupportAssist-Daten – einschließlich der Anwendungs-, System-, Netzwerk- und Sicherheitskomponenten – in einem Rechenzentrum in den USA, das höchste Verfügbarkeit und Sicherheit bietet. SupportAssist-Daten werden durch eine Vielzahl von Maßnahmen geschützt.

Zu den Rechenzentren, in denen sich die Infrastruktur befindet, haben nur autorisierte MitarbeiterInnen Zugang. Dies wird mit Smartcards kontrolliert.



Logische Sicherheit

Die von SupportAssist generierten Daten werden gemäß [Dell Datenschutzerklärung](#) gespeichert.

Der logische Zugriff auf die Dell Technologies Services-Infrastruktur (Server, Lastenausgleich, Netzwerkfreigaben usw.) wird durch interne Tools eingeschränkt, die gemäß den Dell Digital-IT-Richtlinien geprüft und bewertet werden.

- **Auditing:** Überwachte Geräteprotokolle werden verwaltet und sind nur für die Infrastruktur und/oder Anwendungen von Dell Technologies Services zugänglich. In diesen Protokollen werden alle Versuche aufgezeichnet, sich beim Betriebssystem oder der SupportAssist-Webserverkonsole anzumelden oder darauf zuzugreifen.

Von der IT gemanagte Builds werden mithilfe der von CIS (Center for Internet Security) empfohlenen Kontrollen durch Sicherheits-Best-Practices verstärkt.

Schließlich nutzt das SupportAssist-Ökosystem sowohl lokale Hochverfügbarkeit innerhalb des Rechenzentrums als auch eine identische Infrastruktur in einem separaten Rechenzentrum. Die einzigen Ausnahmen sind Technologien, die eine intrinsisch hohe Verfügbarkeit bieten, z. B. Big Data-Cluster und Private Clouds.

Für Datenanalysen nutzt Dell Technologies Services Cloud-Umgebungen, die wir vollständig kontrollieren und managen, einschließlich Private, Hybrid und Public Clouds. Relationale Datenbanken, einfache Storage-Services und Data Warehouses sind alle verschlüsselt und verwenden die geringsten Berechtigungen. Keine der relationalen Datenbanken ist öffentlich zugänglich. Data Warehouses werden über HTTPS gesichert.



Welche Sicherheitsverfahren und -richtlinien nutzt Dell Technologies?

Entwicklung

Unser interner SDL-Standard (Secure Development Lifecycle) dient als grundlegende Referenz für Dell Technologies Produktabteilungen und bietet wesentliche Benchmarks für die sichere Produkt- und Anwendungsentwicklung. Dell stellt einen definierten SDL-Kontrollkatalog bereit, der auf ISO/IEC 27034 und einem auf dem NIST Secure Software Development Framework (SSDF) aufbauenden Standard basiert. Mit diesen Tools können Dell Teams sichere Produkte für Kunden entwickeln und verhindern, dass Sicherheitslücken und Schwachstellen in die von Dell entwickelte/unterstützte Software und Hardware eingeführt werden. Diese Kontrollen müssen von Engineeringteams während der Entwicklung neuer Merkmale und Funktionen übernommen werden. Sie umfassen Analyseaktivitäten sowie normative proaktive Maßnahmen, die sich auf wichtige Risikobereiche konzentrieren.

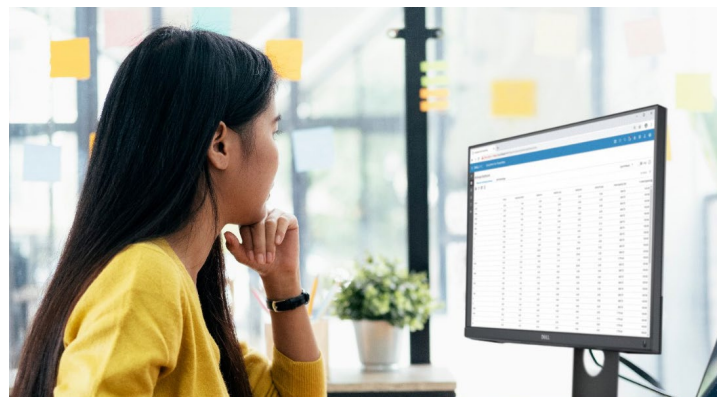
Analyseaktivitäten, darunter Bedrohungsmodellierung, statische Codeanalyse, Scanning und Sicherheitstests, sind wesentliche Komponenten, die darauf abzielen, Sicherheitsmängel während des gesamten Entwicklungslebenszyklus zu identifizieren und zu beheben. Darüber hinaus enthält der SDL normative Kontrollen, um sicherzustellen, dass Entwicklungsteams bestimmte Sicherheitsprobleme proaktiv angehen, einschließlich derjenigen, die in Branchenstandards wie den Open Web Application Security Project (OWASP) Top 10 und SANS Top 25 beschrieben sind.

SupportAssist for Business PCs ist an diesem robusten SDL-Framework ausgerichtet und nutzt das Dell SDL-Reifegradmodell, um Sicherheitskontrollen gemäß Branchenstandards zu implementieren. Das DevSecOps-Programm sichert die modernen Softwareentwicklungs- und -bereitstellungsprozesse bei Dell durch die Automatisierung von SDL-Kontrollen und die Durchsetzung von Sicherheitsrichtlinien in einer CI-/CD-Umgebung (Continuous Integration/Continuous Deployment). Diese CI-/CD-Tools automatisieren die Build-, Test- und Bereitstellungsprozesse und sorgen dafür, dass Codeänderungen integriert und kontinuierlich als Teil des Entwicklungsworkflows getestet werden.

SDL-TechnikerInnen führen SDL-Sicherheitsbewertungen durch, um Sicherheitsprobleme und -lücken in Software zu identifizieren und den Entwicklungsteams Empfehlungen zur Behebung dieser Sicherheitsergebnisse bereitzustellen. Diese Vergewisserung bietet Einblicke in den Reifegrad unserer Sicherheitspraktiken und den Sicherheitsstatus unserer Software und Hardware.

Die Bewertung umfasst Folgendes:

- Bewertung von Sicherheitslücken durch Penetrationstests
- Sicherheitstests von Drittanbietern, die von angesehenen Anbietern wie SecureWorks durchgeführt werden
- Bewertung von Authentifizierungs-, Autorisierungs- und Identitätsmanagementlösungen
- Gründliches Scannen aller Bibliotheken und Komponenten von Drittanbietern mit branchenführenden Tools zur Analyse der Softwarezusammensetzung
- Weitergabe von Dell Sicherheitsratgebern für spezifische Sicherheitsverbesserungen
- Rigorose Datenklassifizierung in Zusammenarbeit mit unserer Global Security-Abteilung, Abstimmung von Datenschutz- und Sicherheitsbemühungen für den Schutz elektronischer Daten
- Durchführung von Sicherheitsaudits und Governance-Verfahren für Anwendungen



Sichere Prozesse und bewährte Branchenpraktiken zur Wahrung der Sicherheit von SupportAssist



Sicherheitsvalidierungstests

Drittanbieter-Sicherheitsbewertungen werden regelmäßig für die SupportAssist-Anwendung und die zugehörige Infrastruktur durchgeführt.

Die Anwendungsbewertungen decken die Sicherheit bei Datenübertragung und API, statische und dynamische Quellcodeanalysen, OWASP-Gegenproben (Open Web Application Security Project) und Bibliotheken von Drittanbietern ab.

Bei den Infrastrukturbewertungen werden interne und externe Netzwerkgeräte, Server und Serviceanbieter berücksichtigt.

Changemanagement

Der Changemanagementprozess von Dell Technologies folgt den Best Practices der ITIL Foundation, wie von unserem Corporate Change Management Board vorgegeben. Alle Änderungen werden über Änderungsanforderungstickets verwaltet. Alle, die auf unser System zugreifen, um Änderungen zu initiieren, müssen eine ITIL-Schulung absolvieren und sich mit dem SDL vertraut machen. Alle Updates und Upgrades, die auf die Backend-Infrastruktur angewendet werden, unterliegen einer Versionskontrolle, um eine ordnungsgemäße Nachverfolgung und Rückverfolgbarkeit zu gewährleisten. Das Team verwendet einen automatisierten Build-Prozess, um neue Builds anzuwenden oder bereitgestellte Builds oder Hotfixes zu widerrufen.

Jede Version, die auf Dell.com/support bereitgestellt wird, enthält Informationen zu den eingeführten Änderungen und bekannten Einschränkungen.

Alle neuen Funktionen und Änderungen werden von unserem Produktmanagementteam gepflegt und mithilfe von Plan-of-Record- und Changemanagementprozessen priorisiert.

Authentifizierung

SupportAssist verwendet Dell MyAccount für die Authentifizierung bei der Dell Technologies Services-Infrastruktur, einen zufälligen symmetrischen Schlüssel für Anwendungen, JWT und BS-Anmeldegruppen für die Authentifizierung beim Gerät.

Gruppen wie das Datenbankadministrationsteam und das operative Supportteam, die Zugriff auf SupportAssist-Komponenten haben, werden separate Aufgaben und Zugriffsrechte zugewiesen. Alle Updates der Produktionsumgebung durchlaufen ein festgelegtes Änderungskontrollverfahren, das auch Prüfungen und Ausgleichsverfahren umfasst.

Sicherheitsbewusste Community

Wir bieten einen rollenbasierten Sicherheitsschulungslehrplan, um neue und vorhandene MitarbeiterInnen über die jobspezifischen Sicherheits-Best-Practices und die Verwendung relevanter Ressourcen zu informieren. Dell Technologies ist bestrebt, eine sicherheitsbewusste Unternehmenskultur in der gesamten Community zu schaffen. Darüber hinaus ist unsere Entwicklercommunity Teil des Security Champion-Programms von Dell, das darauf ausgelegt ist, das „Shift Security Left“-Konzept in den Softwareentwicklungspraktiken zu fördern.

Incident-Reporting

Bei Dell Technologies sind alle MitarbeiterInnen verpflichtet, verdächtige Aktivitäten, Cybersicherheitsprobleme oder Bedrohungen umgehend per E-Mail an das Computer Security Incident Response Team (CSIRT) unter security@dell.com zu melden.

Reaktion auf Sicherheitslücken

Dell Technologies ist bestrebt, Risiken im Zusammenhang mit Sicherheitslücken in unseren Produkten, Anwendungen und Cloud-Services zu minimieren. Um eine zeitnahe Reaktion auf Sicherheitslücken zu ermöglichen, halten wir uns an die Richtlinien des Dell Technologies Vulnerability Response Standard (VRT). Dell beteiligt sich aktiv an verschiedenen Communityinitiativen, darunter das [Forum of Incident Response and Response Teams \(FIRST\)](#) und das [Software Assurance Forum for Excellence in Code \(SAFECode\)](#). Unsere Prozesse und Verfahren entsprechen dem [FIRST PSIRT Services Framework](#) sowie anderen Standards wie [ISO/IEC 29147:2018](#) und [ISO/IEC 30111:2019](#).

Dell Technologies ist bestrebt, Sicherheitslücken in unseren Produkten, Anwendungen und Cloud-Services in der kürzesten wirtschaftlich vertretbaren Zeit zu schließen. Die genauen Zeitpläne können je nach der spezifischen Sicherheitslücke und ihren Auswirkungen variieren, z. B. wie komplex der Aufwand/die Auswirkung der Behebung der Sicherheitslücke ist. Unser Product Security Incident Response Team (PSIRT) koordiniert die Reaktion und Offenlegung aller uns gemeldeten Produktsicherheitslücken. Alle Offenlegungen zu Sicherheitslücken in Produkten von Dell Technologies werden online auf der Seite [Dell Sicherheitsratgeber, Mitteilungen und Ressourcen](#) zur Verfügung gestellt. Weitere Informationen zu den Verfahren von Dell für die Reaktion auf Sicherheitslücken finden Sie in der [Dell Richtlinie für die Reaktion auf Sicherheitslücken](#).

Branchenmitgliedschaften

Dell Technologies ist Mitglied in mehreren branchenweiten Gruppen für die Zusammenarbeit mit anderen führenden Anbietern. Gemeinsam definieren, optimieren und teilen wir Best Practices für die Produktsicherheit und treiben die sichere Entwicklung weiter voran. Beispiele für die Zusammenarbeit in der Branche:

- Dell Technologies ist Mitbegründer und derzeit Vorsitzender des Vorstands von SAFECode (Software Assurance Forum for Excellence in Code). Zu den weiteren Vorstandsmitgliedern gehören VertreterInnen von Microsoft, Adobe, SAP, Intel, Siemens, CA und Symantec. SAFECode-Mitglieder teilen und veröffentlichen Softwaresicherheitspraktiken und -schulungen.



Branchenführend
bei der Definition
von Best Practices für
die Produktsicherheit
und bei der Förderung
einer sicheren
Entwicklung

Branchenmitgliedschaften (Fortsetzung)

- Dell Technologies ist ein aktives Mitglied im Forum of Incident Response and Security Teams ([FIRST](#)). FIRST ist eine führende Organisation und anerkannter weltweiter Marktführer in der Reaktion auf Incidents und Sicherheitslücken.
- Wir beteiligen uns aktiv am Open Group Trusted Technology Forum ([OTTF](#)). OTTF leitet die Entwicklung eines globalen Programms und Frameworks für die Integrität der Lieferkette.
- Dell MitarbeiterInnen waren Gründungsmitglieder des IEEE Center for Secure Design, das im Rahmen der IEEE-Cybersicherheitsinitiative eingeführt wurde, um SoftwarearchitektInnen zu helfen, gängige Mängel beim Sicherheitsdesign zu verstehen und zu beheben.

Branchenspezifische Sicherheitsstandards

- Dell MitarbeiterInnen sind aktiv an Normungsgremien und Branchenkonsortien beteiligt, die sich auf die Entwicklung von Sicherheitsstandards und auf die Definition branchenweiter Sicherheitsverfahren konzentrieren. Hierzu zählen:
- CSA (Cloud Security Alliance)
- FIRST (Forum of Incident Response and Security Teams)
- The Open Group
- SAFECODE (Software Assurance Forum for Excellence in Code)
- SNIA (Storage Networking Industry Association)

Dell Technologies ist nach ISO 9001 zertifiziert. Unser Unternehmen führt regelmäßige vierteljährliche Audits und Complianceüberprüfungen für alle Entwicklungs- und Fertigungszentren durch.

V. Fazit

Die SupportAssist-Konnektivitätstechnologie bietet intelligente Automatisierungs- und Korrekturfunktionen, um eine maximale Verfügbarkeit für die Dell Desktop-PC- und Laptopflotte eines Unternehmens zu ermöglichen. Dell Technologies Services kann diese hochmoderne Technologie mit optimaler Sicherheit durch die Fokussierung auf sichere Prozesse, eine sichere Datenübertragung und einen sicheren Daten-Storage bereitstellen.

Wenn Sie Fragen haben oder weitere Informationen benötigen, besuchen Sie Dell.com/SupportAssist.

¹ Informationen zu unterstützten Systemen und Anforderungen finden Sie in unserem [Administratorhandbuch](#) unter „Unterstützte Systeme“. Proaktive und vorausschauende Funktionen hängen von Ihrem aktiven Serviceplan und den Geschäftsregeln von Dell Technologies ab. Informationen zu den Funktionen der ProSupport Suite for PCs finden Sie in unserem [Administratorhandbuch](#) unter „Funktionen für das Verbinden und Verwalten und Dell Servicepläne“.

² Basierend auf einer Analyse von Dell, Dezember 2023.