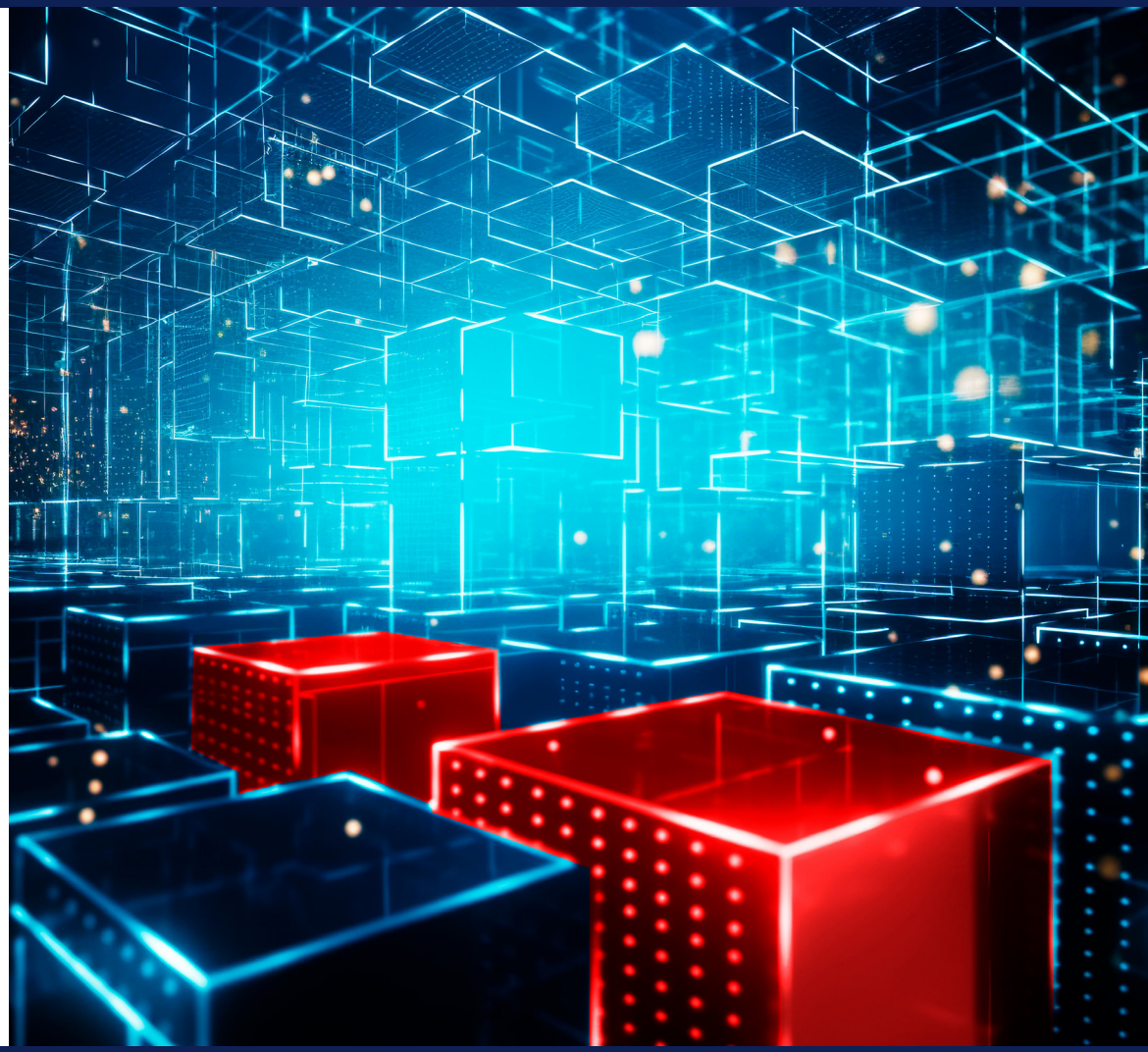
So sichern Sie die Nutzung von KI am Endpunkt

Schützen Sie KI-Workloads auf dem Gerät mit sicheren, modernen Geräten und der Denkweise von Cyberkriminellen.



Zusammenfassung

On-Device-KI bietet enorme Vorteile, birgt aber auch Cyberrisiken. In diesem E-Book erfahren Sie, wie Sie Ihr Unternehmen so aufstellen können, dass Sie KI-Innovationen am Endpunkt sicher nutzen können.

Inhaltsverzeichnis

Die Angriffsfläche von On-Device-KI

Was unterliegt einem Angriffsrisiko?

Alle neuen Technologien bergen aus einem Grund Cybersicherheitsrisiken: Sie sind Neuland – das große Unbekannte. Das war schon so bei Cloud-Computing, bei Blockchain und bei zahlreichen anderen Technologien. Dasselbe gilt nun für die On-Device-KI. Der Schlüssel zur Minderung dieses Risikos besteht wie immer darin, Licht ins Dunkel zu bringen.

Bevor wir darüber sprechen können, welche Sicherheitsmaßnahmen zur Minimierung der Angriffsfläche erforderlich sind, ist es sinnvoll, zu klären, was wir schützen wollen und warum. Stellen Sie sich ein Rohrsystem in einem Geschäftsgebäude vor, in dem mehrere Unternehmen untergebracht sind. Diese Rohre transportieren Wasser, Gas usw. im gesamten Gebäude für eine Vielzahl von Anwendungsfällen. Wenn die Materie, die durch die Rohre fließt, kontaminiert oder unterbrochen ist, kann sie ihre Aufgabe nicht erfüllen. Wenn die Rohre, die die Materie transportieren, beschädigt oder verunreinigt sind, können sie ihre Funktion nicht erfüllen. Sowohl die Rohre als auch ihr Inhalt müssen in einem guten Betriebszustand sein, um die Anforderungen ihrer jeweiligen Anwendungsfälle zu erfüllen.►

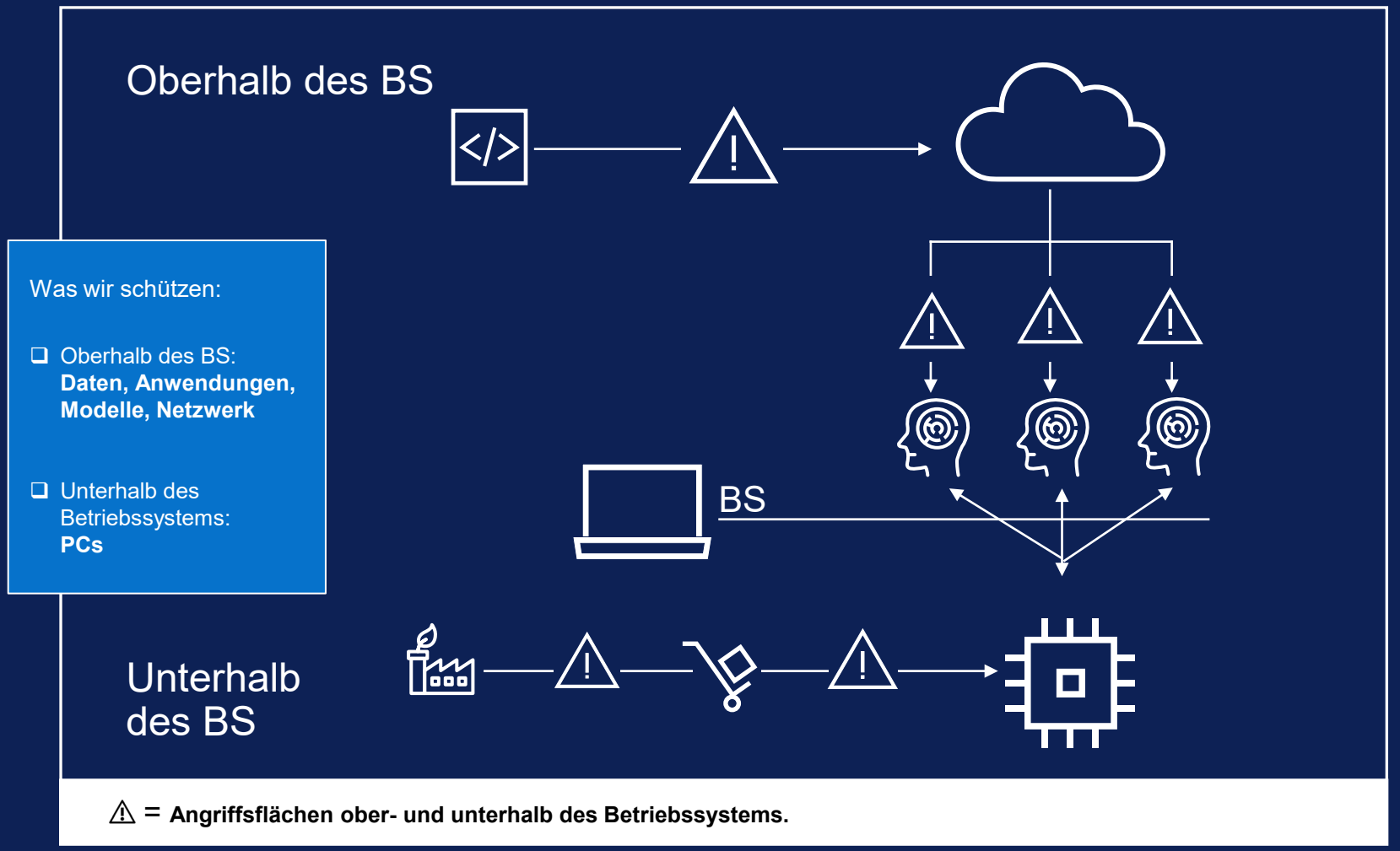
Die Angriffsfläche von On-Device-KI, Fortsetzung

Was unterliegt einem Angriffsrisiko, Fortsetzung

Was uns zur KI am Endpunkt bringt:

- Die Rohre sind Ihre Infrastruktur – Ihre PCs, Ihre Unternehmensnetzwerke. Das „Wie“ und „Wo“ Sie arbeiten.
- Die Inhalte, die durch die Rohre fließen, sind die Daten, Anwendungen und Modelle, die verschiedene KI-Anwendungsfälle unterstützen. Die Assets und Ressourcen, die Sie für Ihre Arbeit benötigen.

Und Sie haben es bestimmt schon erraten: Cyberkriminelle haben es auf beides abgesehen. Sie können geistiges Eigentum stehlen, um Lösegeld zu erpressen, oder Daten oder Modelle manipulieren, um den operativen Betrieb zu stören. In jedem Fall können die Folgen schwerwiegend sein und zu finanziellen Einbußen und Reputationsschäden führen bzw. behördliche Überprüfungen nach sich ziehen.▶



Sicherheitsrisiken am Endpunkt

Taktiken, die AngreiferInnen nutzen, um sich Zugang zu verschaffen

Sprechen wir jetzt über die Methoden, mit denen AngreiferInnen sich Zugang zu beiden Zielen verschaffen können.

Gefährdung von Geräten. Wie wir in Endpoint Security Market Insights, Forrester Research, Inc., März 2025 lesen können, gehören PCs zu den Hauptzielen moderner Cyberbedrohungen. Diese Art von Angriff kann weit vor Beginn der KI-Arbeit auf dem Gerät stattfinden, also ein **Angriff auf die Hardware- oder Softwarelieferkette** sein. Es gibt Dutzende, wenn nicht Hunderte von Punkten in der Lieferkette, an denen eine böswillige Partei Komponenten wie Schaltkreise oder Firmware manipulieren kann, um Schwachstellen einzubauen, die später ausgenutzt werden können. Stellen Sie sich die drohende Katastrophe vor, wenn ein Investmentunternehmen eine brandneue Lieferung von PCs mit gefälschten Komponenten erhält.

Gefährdung von Identitäten. Sicherheitsverletzungen im Zusammenhang mit gestohlenen oder kompromittierten Zugangsdaten sind einer der am schnellsten wachsenden Angriffsvektoren. Kein Wunder. AngreiferInnen können sich mit gültigen Zugangsdaten bei einem PC anmelden, sich frei innerhalb des Unternehmensnetzwerks bewegen und über einen längeren Zeitraum unbemerkt bleiben. Laut dem neuesten Bericht zu Kosten einer Datenschutzverletzung von IBM nahm die Identifizierung und Eindämmung dieser Sicherheitsverletzungen durchschnittlich 292 Tage in Anspruch – länger als bei jedem anderen untersuchten Angriffsvektor. Diese Zugriffsebene ist für BedrohungsakteurInnen zu wertvoll, um sie zu ignorieren. Tatsächlich zeigen Untersuchungen von Zscaler, dass böswillige Akteure ihre Methoden zum Diebstahl von Anmeldedaten verbessern und Phishing-Angriffe mithilfe von GenAI ausweiten. Dieser unbefugte Zugriff auf sensible Trainings- oder Inferenzdaten oder direkt auf Modelle wird als **Angriff auf die Modell-Lieferkette** kategorisiert.

Insiderbedrohung. Aktuelle Studien zeigen, dass **bösartige Insiderangriffe** im Vergleich zu anderen Angriffsvektoren mit durchschnittlich 4,99 Mio. USD die höchsten Kosten verursachten. Bedenken Sie, dass Insiderangriffe in der gesamten Hardware-, Software- und Modell-Lieferkette auftreten können.▶

Durchschnittliche Zeit, bis ein/e EndnutzerIn auf eine **Phishing**-E-Mail hereinfällt: <60 Sekunden*

Durchschnittlich 292 Tage, bis eine **Kompromittierung von Zugangsdaten** entdeckt und eingedämmt wird**

Bösartige Insiderangriffe kosten im Durchschnitt 4,99 Mio. USD**

** Quelle: Verizon DBIR, 2024.*
***Quelle: IBM Cost of a Data Breach, 2024.*

Zu ergreifende Gegenmaßnahmen

Was Risiken mindert

Keines dieser Angriffsziele ist grundlegend neu. Auch die Endziele der AngreiferInnen sind nicht neu. Wie immer möchten wir uns darauf konzentrieren, dass Ihre Flotte sicher und ausfallsicher bleibt. **Durch die Kombination von Gegenmaßnahmen** können Sie die Angriffsfläche reduzieren und verdächtiges Verhalten sofort erkennen.

Eine **Zero-Trust-Mentalität** mindert Risiken in Ihrer gesamten Flotte. Mit diesen Prinzipien – niemals vertrauen, immer überprüfen und kontinuierlich überwachen – können Sie AngreiferInnen immer einen Schritt voraus sein. Es ist unmöglich, 100 % der Angriffe zu blockieren. Für einen starken Sicherheitsstatus benötigen Sie **Transparenz und Kontrolle** in Ihrer gesamten IT-Umgebung.

Überprüfen Sie vor diesem Hintergrund Ihre Infrastruktur, insbesondere die Systeme und Prozesse, die mit KI interagieren. Welche Gegenmaßnahmen minimieren das Gefährdungsrisiko von Geräten, Identitäten und Bedrohungen durch Insider?►

Zero-Trust-Prinzipien tragen zur Minderung von Risiken bei und reduzieren den Wirkungsradius von Cyberaktivitäten

Zu ergreifende Gegenmaßnahmen, Fortsetzung

Was Risiken mindert, Fortsetzung

Es gibt insgesamt zwei Kategorien von Gegenmaßnahmen.

Die Sicherheit „unterhalb des Betriebssystems“ schützt die KI-Geräte, an denen Sie arbeiten. Wir können dies in zwei Teile unterteilen:

- Schützen Sie Ihre Flotte mit Geräten mit **integrierter Sicherheit**. Das bedeutet, dass Sie AI PCs verwenden, die von Grund auf sicher sind, also nach sicheren Designprinzipien und in einer sicheren Lieferkette entwickelt wurden.
- Schützen Sie Ihre Flotte mit Geräten, die **integrierte Sicherheitsfunktionen** haben. Sichere AI PCs verfügen über mehrere integrierte Schutzebenen, die sofort nach dem Auspacken Transparenz bieten – bis hinunter zur BIOS- und Chipebene.

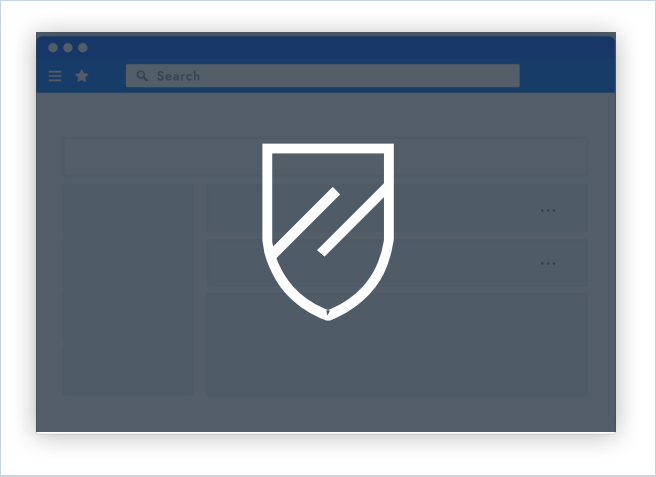
Sicherheit „oberhalb des Betriebssystems“ schützt den Zugriff auf KI-Modelle. Schützen Sie die Daten und Modelle, *mit* denen Sie arbeiten, sowie die Unternehmensnetzwerke, *in* denen Sie arbeiten, mit **Softwaresicherheit**. Es ist unerlässlich, die Sicherheitsvorgänge für maschinelles Lernen zu schützen und den Netzwerkverkehr bereitgestellter KI-Workloads zu überwachen.►

Sicherheit unterhalb der Betriebssystemebene

Sichere AI PCs

Hardware- und Firmwaresicherheit, Lieferkettensicherheit, Core-Chip

Sicherheit oberhalb der Betriebssystemebene



Softwaresicherheit

Zusätzliche Sicherheitsebene für Endpunkte, Netzwerke und Cloud-Umgebungen

Sicherheitsservices und Fachwissen sind verfügbar, um alles miteinander zu verbinden.

Best Practices für Ihre Flotte

Wie Dell AI PCs grundlegende Sicherheit für Ihre Flotte bieten

Hier kommt Dell Trusted Workspace in Spiel. Unsere TechnikerInnen entwickeln und konzipieren die Sicherheit unserer AI PCs mit einem profunden Verständnis für die Denkweise der Cyberkriminellen.

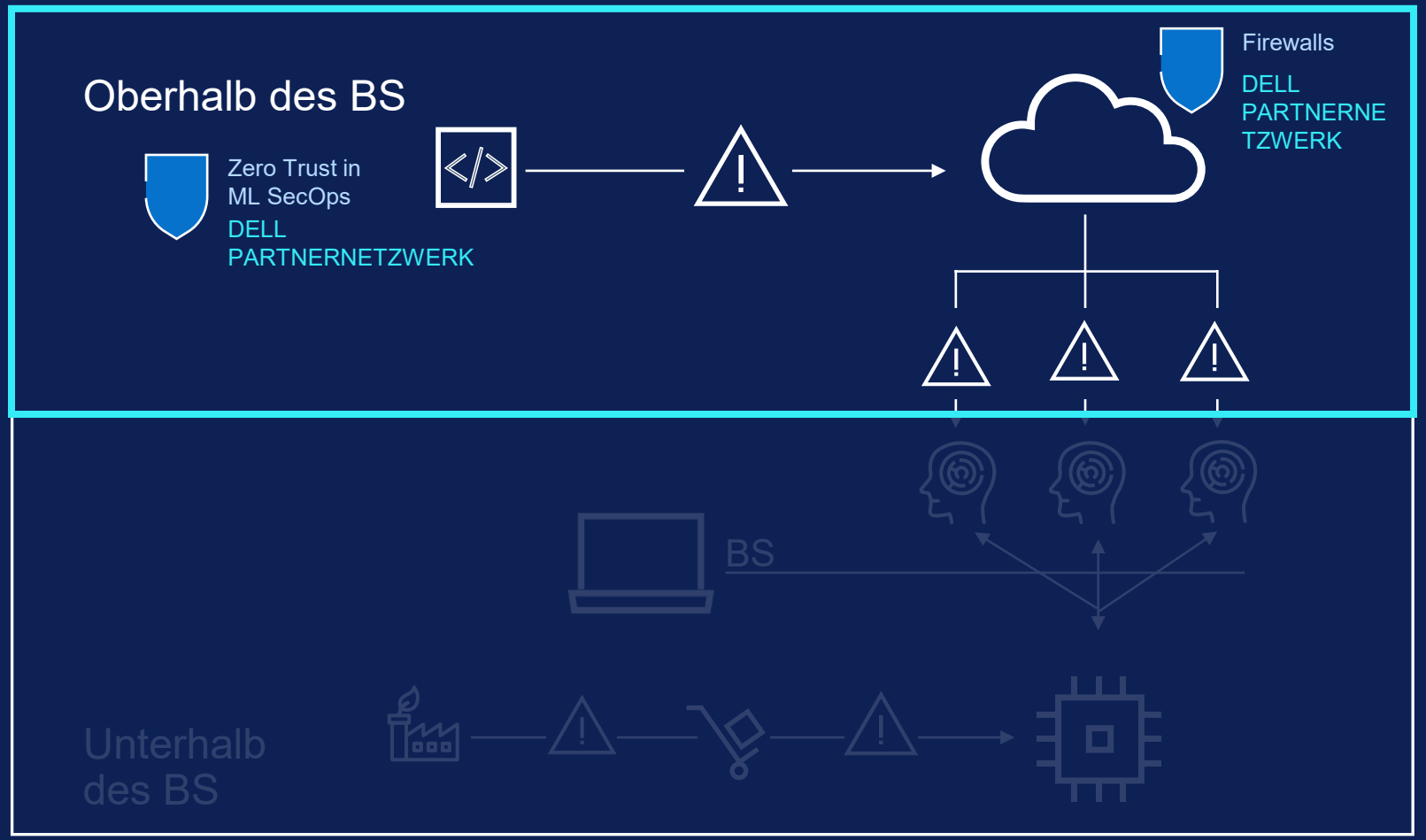
Unterhalb des Betriebssystems tragen sicheres Design, robuste Lieferkettenkontrollen und optionale Lieferkettensicherheit dazu bei, dass PCs ab dem ersten Start sicher sind. Integrierte Hardware- und Firmware-Sicherheitsfunktionen schützen den PC während der Nutzung, z. B. die Dell-exklusive* Manipulationserkennung auf BIOS-Ebene (Dell SafeBIOS) und die passwortlose Sicherheitsfunktion für Zugangsdaten (Dell SafeID) zum Schutz vor unbefugtem Zugriff. Darüber hinaus bieten Intel® Chiptechnologien eine Grundlage für den Schutz verschiedener Aspekte der KI, wie sie von AI PC-Clients verwendet wird. Beispielsweise trägt Intel zur Sicherung von KI-Data at Rest auf dem Client bei, indem es die Verschlüsselung von Modellen auf der Festplatte beschleunigt.►

Best Practices für Ihre Flotte, Fortsetzung

Wie Dell AI PCs grundlegende Sicherheit für Ihre Flotte bieten, Fortsetzung

Als Ergänzung zu dieser Sicherheit unterhalb des Betriebssystems kann die Persistence-Technologie unseres Partners Absolute werkseitig integriert werden, um noch mehr Transparenz und Kontrolle über den gesamten Lebenszyklus des PCs zu erreichen. So lassen sich beispielsweise Geräte unterwegs geolokalisieren und wichtige Anwendungen im schlimmsten Fall automatisch reparieren.

Tatsächlich hat Dell ein Ökosystem von Software-Partnerlösungen kuratiert, darunter CrowdStrike Falcon XDR und Absolute Secure Access, die Zero-Trust-Prinzipien aktivieren, um Ihre Modell-Lieferkette vor unbefugtem Zugriff **oberhalb des Betriebssystems** zu schützen. Mit diesen Lösungen können Sie Policies mit granularen Zugriffskontrollen (z. B. rollenbasierte Zugriffskontrolle oder RBAC) erstellen und durchsetzen, um das Risiko zu minimieren, dass böswillige Insider auf Ihre KI-Modelle zugreifen oder diese manipulieren.►



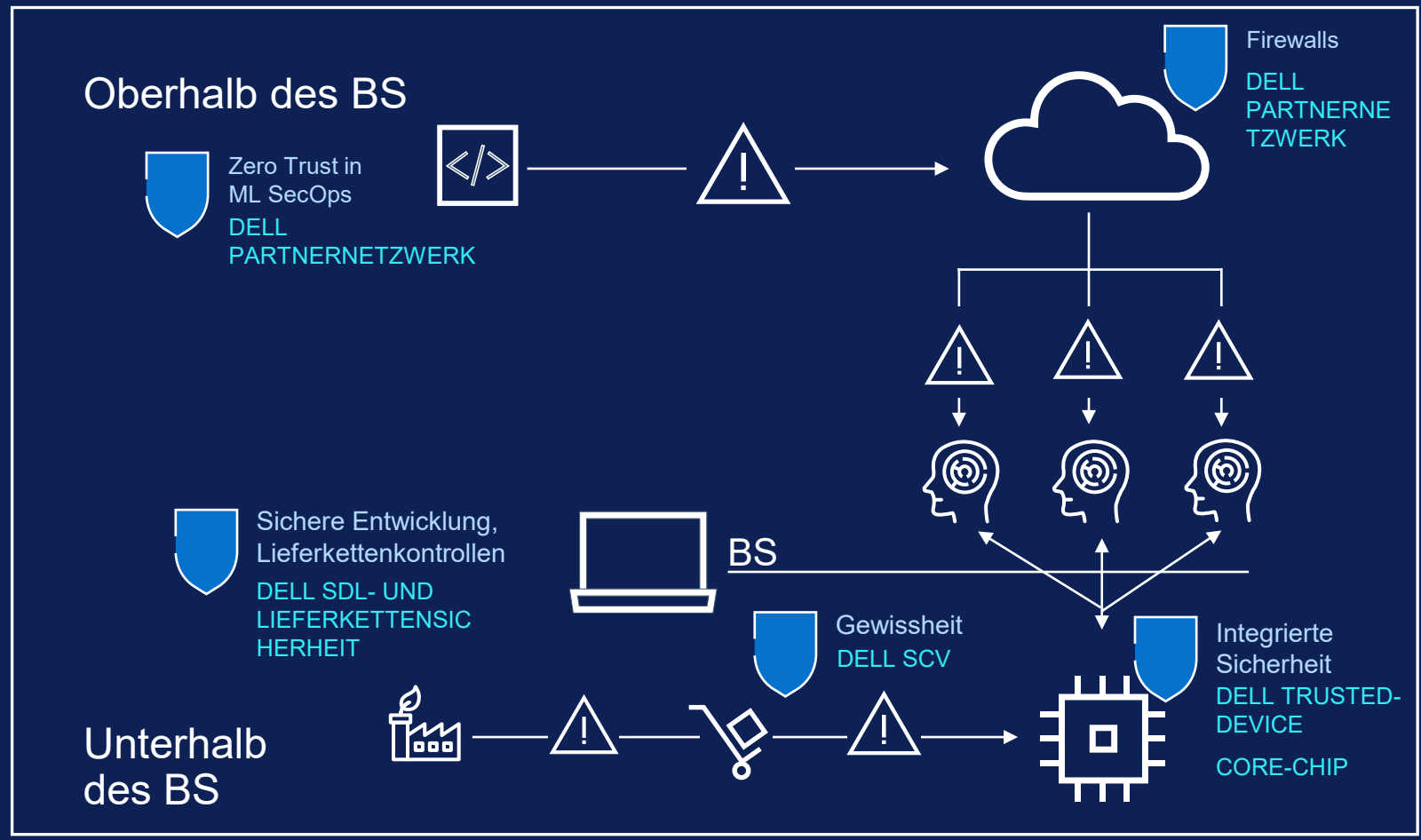
Best Practices für Ihre Flotte, Fortsetzung

Wie Dell AI PCs grundlegende Sicherheit für Ihre Flotte bieten, Fortsetzung

All dies zusammen ergibt die ***Sicherheit für KI.*** Diese Funktionen schützen KI-Workloads auf dem Gerät vor Cyberangriffen, sodass Sie sich auf Innovationen und den Erfolg Ihres Unternehmens konzentrieren können.►

Stoppen Sie erweiterte Endpunktangriffe mit koordinierten Hardware- und Softwareabwehrmaßnahme

Dell arbeitet mit Intel und CrowdStrike zusammen, um die Ebenen unterhalb und oberhalb des Betriebssystems mit hardwaregestützter Sicherheit zu integrieren.
Weitere Informationen >



Wichtigste Erkenntnisse und nächste Schritte

Sichere KI am Endpunkt mit Dell

Unternehmen sind zwar von KI begeistert, aber laut einer aktuellen Umfrage von Absolute unter CISOs hinkt die KI-Bereitschaft hinterher. Eine Analyse von Millionen von Geräten ergab, dass die PC-Population neue KI-Funktionen nicht umfassend aufnehmen kann. **Dell kann Abhilfe schaffen.**

Entwicklung und Bereitstellung von KI-Modellen auf einer sicheren, modernen Grundlage. Der Support für Windows 10 endet im Oktober 2025. PCs erhalten keine Sicherheitsupdates, keine Funktionen und keinen Support für Windows 10 mehr. Ältere Geräte erfüllen möglicherweise nicht die Anforderungen für Windows 11 und verfügen daher nicht über die neuesten Verbesserungen in den Bereichen Performance, Sicherheit und KI. Führen Sie ein Upgrade auf **Dell Pro** oder **Dell Pro Max basierend auf Intel® Core™ Ultra Prozessoren mit Intel vPro®** durch, um Sicherheitsvorteile zu erschließen und KI-Workloads mit **den weltweit sichersten AI PCs** schützen.* ►

Der Support für Windows 10 endet im Oktober.

Führen Sie ein Upgrade auf die neuesten Dell AI PCs mit Intel durch, um Sicherheitsvorteile und KI-Verbesserungen zu nutzen:

Dell Pro kaufen ● Dell Pro Max

*Die sichersten AI PCs der Welt**

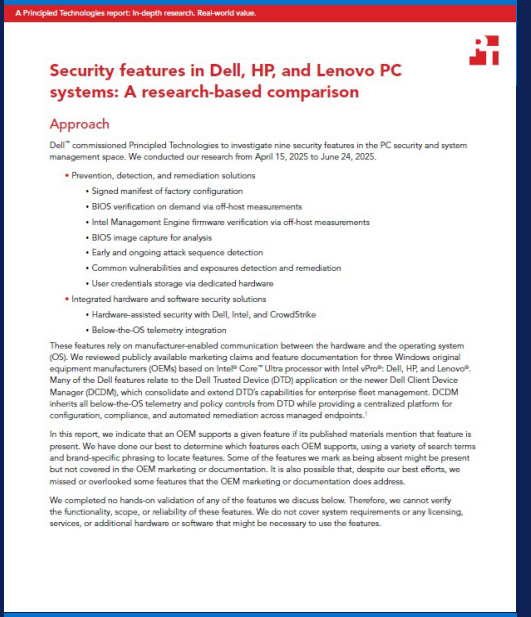
Entdecken Sie Software mit Mehrwehrt und Services, die Ihren Sicherheitsstatus zu verbessern:

Software und Integrationen

Services

BRANCHENFÜHREND

Principled Technologies hat festgestellt, dass die AI PC-Sicherheit von Dell und Intel gegenüber Mitbewerbern überlegen ist.


A Principled Technologies report: In-depth research. Real-world value.

Security features in Dell, HP, and Lenovo PC systems: A research-based comparison

Approach

Dell™ commissioned Principled Technologies to investigate nine security features in the PC security and system management space. We conducted our research from April 15, 2025 to June 24, 2025.

- Prevention, detection, and remediation solutions
  - Signed manifest of factory configuration
  - BIOS verification on demand via off-host measurements
  - Intel Management Engine firmware verification via off-host measurements
  - BIOS image capture for analysis
  - Early and ongoing attack sequence detection
  - Common vulnerabilities and exposures detection and remediation
  - User credentials storage via dedicated hardware
- Integrated hardware and software security solutions
  - Hardware-assisted security with Dell, Intel, and CrowdStrike
  - Below-the-OS telemetry integration

These features rely on manufacturer-enabled communication between the hardware and the operating system (OS). We reviewed publicly available marketing claims and feature documentation for three Windows original equipment manufacturers (OEMs) based on Intel® Core™ Ultra processor with Intel vPro®: Dell, HP, and Lenovo®. Many of the Dell features relate to the Dell Trusted Device (DTD) application or the newer Dell Client Device Manager (DCDM), which consolidate and extend DTD's capabilities for enterprise fleet management. DCDM inherits all below-the-OS telemetry and policy controls from DTD while providing a centralized platform for configuration, compliance, and automated remediation across managed endpoints.[1]

In this report, we indicate that an OEM supports a given feature if its published materials mention that feature is present. We have done our best to determine which features each OEM supports, using a variety of search terms and brand-specific phrasing to locate features. Some of the features we mark as being absent might be present but not covered in the OEM marketing or documentation. It is also possible that, despite our best efforts, we missed or overlooked some features that the OEM marketing or documentation does address.

We completed no hands-on validation of any of the features we discuss below. Therefore, we cannot verify the functionality, scope, or reliability of these features. We do not cover system requirements or any licensing, services, or additional hardware or software that might be necessary to use the features.

Studie lesen

Haftungsausschluss

* Basierend auf einer Drittanbieteranalyse von Principled Technologies, bei der Dell AI PCs auf Intel Prozessoren mit HP und Lenovo verglichen wurden, Juli 2025. Unterstützt durch eine interne Dell Analyse des weltweiten PC-Markts, Oktober 2024. Gilt für PCs mit Intel Prozessoren. Nicht alle Funktionen sind bei allen PCs verfügbar. Einige Funktionen müssen zusätzlich erworben werden.

Weitere Informationen:

Schreiben Sie uns eine E-Mail an Global.Security.Sales@Dell.com

Weitere Informationen: Dell.com/Endpoint-Security

Folgen Sie uns: LinkedIn @DellTechnologies | X @DellTech

Dell Endpoint Security

Das Thema Sicherheit ist für Unternehmen jeder Größe eine echte Herausforderung. **Binden Sie einen erfahrenen Sicherheits- und Technologiepartner für die Modernisierung der Endpoint Security ein**.

Dell Trusted Workspace trägt zum Schutz von Endpunkten bei, damit Sie eine moderne, Zero-Trust-fähige IT-Umgebung aufbauen können. Verkleinern Sie die Angriffsfläche und verbessern Sie die Ausfallsicherheit bei Cyberangriffen mit einem umfassenden Portfolio an Hardware- und Softwareschutz, exklusiv von Dell. Unser rundum koordinierter, abwehrbasierter Ansatz entschärft Bedrohungen, indem integrierte Schutzmaßnahmen mit kontinuierlicher Wachsamkeit kombiniert werden. Unsere Sicherheitslösungen wurden für die cloudbasierte Welt von heute konzipiert und sorgen für Produktivität seitens der EndnutzerInnen und eine starke IT.