ERKUNDEN

Dell Trusted Workspace

Sicheres Arbeiten an jedem Ort

mit Hardware- und Softwareschutz für die cloudbasierte Welt von heute

Durch hybrides Arbeiten werden Unternehmen neuen Angriffsvektoren ausgesetzt. Da die Angriffstechniken immer ausgefeilter werden, erfordert eine effektive Endpoint Security heute mehrere Ebenen zum Schutz von Gerät, Netzwerk und Cloud.

Verkleinern Sie mit einem umfassenden Portfolio an Maßnahmen zum Schutz von Hardware und Software die Angriffsfläche und bleiben Sie modernen Bedrohungen einen Schritt voraus.

Weitere Informationen zum Portfolio →

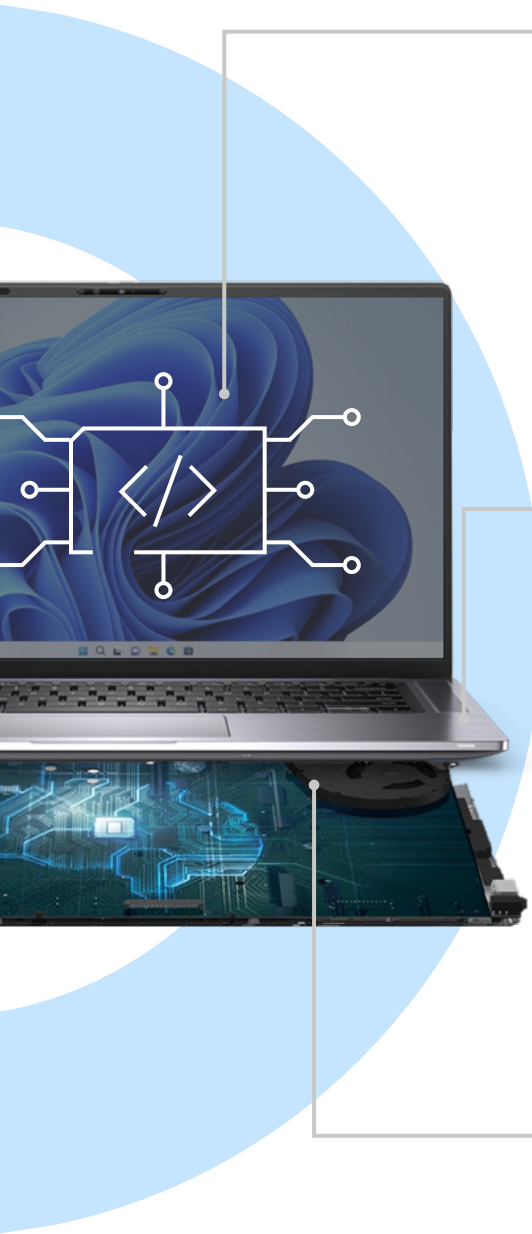
Die sichersten KI-PCs der Welt[1] →

Software für mehr Sicherheit für jede Flotte →

DELL Technologies

Dell Trusted Workspace

Mehrere Schutzebenen



Zusätzliche **Softwaresicherheit**

Erweitern Sie den Bedrohungsschutz mit Software eines Netzwerks sorgfältig ausgewählter Partner. Profitieren Sie von den Vorteilen und der Effizienz des konsolidierten Erwerbs von Sicherheitslösungen.

Integrierte **Hardware- und Firmwaresicherheit**

Erkennen und verhindern Sie grundlegende Angriffe mit den weltweit sichersten KI-PCs.[1] Umfassende Abwehrmechanismen auf BIOS-/Firmware- und Hardwareebene schützen das Gerät während der Verwendung.

Nur Dell integriert PC-Telemetrie in branchenführende Software, um die Sicherheit der gesamten Flotte zu erhöhen.[1]

Konzipiert mit **Lieferkettensicherheit**

Ihr Gerät ist ab dem ersten Start für maximale Sicherheit konzipiert, sodass Sie sorgenfrei arbeiten können. Durch Design, Entwicklung und Tests von sicheren PCs wird das Risiko von Sicherheitslücken in Produkten verringert. Strenge Lieferkettenkontrollen reduzieren das Risiko von Produktmanipulationen.

Bedrohungen vermeiden, erkennen und darauf reagieren – ganz gleich wo

Dell SafeGuard and Response

Dell SafeData

Schutz vor sich weiterentwickelnden Bedrohungen

Dell SafeBIOS

Dell SafeID

Auslieferung vertrauenswürdiger und unmanipulierter Hardware

Dell SafeSupply Chain

DELL Technologies

Dell Trusted Workspace Eingebaute und integrierte Sicherheit

Die sichersten KI-PCs der Welt[1]

Sicherheit ab dem ersten Start

Strenge Lieferkettenkontrollen nach den neuesten Standards und optionale Add-ons wie die nur von Dell zur Verfügung gestellte **Secured Component Verification** sichern die PC-Integrität. Mehr erfahren →

Überprüfung der Firmwareintegrität

Die exklusiv von Dell angebotene **Firmwareverifizierung** über hardwarebasierte Sicherheit in Intel Prozessoren schützt vor unbefugtem Zugriff auf hochprivilegierte Firmware und deren Manipulation. Mehr erfahren →

Sichern von Endnutzerzugangsdaten

Verifizieren Sie den Nutzerzugriff mit dem dedizierten und nur bei Dell erhältlichen Sicherheitschip **SafeID**, der Nutzerzugangsdaten vor Malware verbirgt. Mehr erfahren →

Aufrechterhaltung der BIOS-Integrität

Nutzen Sie die ausschließlich von Dell bereitgestellte BIOS Verification-Funktion **SafeBIOS.** Bewerten Sie ein beschädigtes BIOS, reparieren Sie es und gewinnen Sie Einblicke, die die Gefährdung durch künftige Bedrohungen reduzieren. Mehr erfahren →

Aufspüren tickender Zeitbomben

Indicators of Attack ist eine nur von Dell angebotene Frühwarnfunktion zur verhaltensbasierten Erkennung von Bedrohungen, bevor diese Schaden anrichten können.

Weitere Informationen →

Erkennung bekannter Sicherheitslücken

Die nur bei Dell verfügbare **Erkennung weit verbreiteter Sicherheitslücken und Risiken (Common Vulnerabilities and Exposures, CVEs)** überwacht öffentlich bekannte BIOS-Sicherheitslücken und empfiehlt Updates, um Risiken zu begrenzen. Mehr erfahren →

Principled Technologies *Von Principled Technologies validierte Branchenführung*

Verkleinern Sie die IT-Sicherheitslücke mit PC-Telemetrie

Bereichern Sie Softwarelösungen mit Einblicken von unterhalb der Betriebssystemebene. Nur Dell integriert PC-Telemetrie in Software branchenführender Anbieter, um die Sicherheit der gesamten Flotte zu erhöhen.[1] Weitere Informationen →

Weitere Informationen zu Dell Trusted-Devices

Laptops →

Desktop-PCs →

Workstations →

* Die Studienergebnisse sind nur für Intel basierte Geräte verfügbar.

DELL Technologies

Dell Trusted Workspace – zusätzliche Sicherheit

Software für mehr Sicherheit für jede Flotte

Vereiteln Sie ausgeklügelte Cyberangriffe mit Dell SafeGuard and Response

Vermeiden und erkennen Sie Bedrohungen und reagieren Sie auf diese – ganz gleich, wo sie auftreten. Künstliche Intelligenz und maschinelles Lernen erkennen und blockieren Angriffe auf Endpunkte proaktiv, während SicherheitsexpertInnen dabei helfen, identifizierte Bedrohungen am Endpunkt, im Netzwerk und in der Cloud aufzudecken und abzuwehren.

Partner

CrowdStrike Falcon® →

Sophos | Secureworks® Taegis™ XDR →

Schutz der Daten auf dem Gerät und in der Cloud mit Dell SafeData

Unterstützen Sie NutzerInnen bei der standortunabhängigen, sicheren Zusammenarbeit. Netskope verfolgt einen datenzentrierten Ansatz für Cloud-Sicherheit und -Zugriff, der Daten und NutzerInnen überall schützt, während Absolute der IT Transparenz, Schutz und Persistenz außerhalb der Unternehmensfirewall bietet.

Partner

Automatische Fehlerkorrektur für Endpunkte, Anwendungen und Netzwerke mit Absolute →

Weitere Informationen zu Security Service Edge-Lösungen mit Netskope →

Weitere Informationen zu Dell Security Services

Bei Dell können Kunden Sicherheit in Eigenregie managen oder diese Aufgabe SpezialistInnen überlassen. Mit unserer vollständig gemanagten 360°-SecOps-Lösung verhindern Sie Sicherheitsbedrohungen in der IT-Umgebung, wehren sie ab und stellen die Umgebung nach einem Angriff wieder her.

Weitere Informationen zu Managed Detection and Response Pro Plus →

DELL Technologies

Dell Trusted Workspace Hardwaregestützte Sicherheit

Integrierte Sicherheit

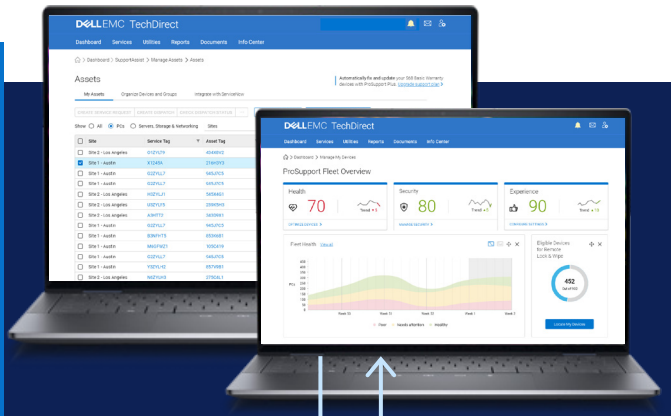
Neue Cyberbedrohungen umgehen rein softwarebasierte Abwehrmaßnahmen. Minimieren Sie mit hardwaregestützten Schutzmaßnahmen die Angriffsfläche von Endpunkten.

Zum Schutz vor modernen Bedrohungen müssen hardware- und softwarebasierte Abwehrmaßnahmen zusammenarbeiten. Und hier kommt Dell ins Spiel. Wir arbeiten mit branchenführenden Sicherheitspartnern zusammen und kombinieren umfassende Gerätetelemetrie mit neuester Bedrohungserkennung, um die Sicherheit Ihrer Flotte zu erhöhen.

- ✓ **Verkleinerung der Angriffsfläche**
- ✓ **Verbesserung der Bedrohungserkennung**
- ✓ **Wahrung des Gerätevertrauens**
- ✓ **Konsolidierung der Anbieter**

Zusätzliche Softwaresicherheit

Nur Dell integriert PC-Telemetrie in branchenführende Software, um die Sicherheit der ganzen Flotte zu verbessern.[1, 2]



DAS BS

Integrierte Hardware- und Firmwaresicherheit

Dell SafeBIOS

Dell Trusted-Device-Anwendung

BIOS Verification | CVE-Erkennung | Angriffsindikatoren (Indicators of Attack, IoA)

Chipfunktionen „unterhalb des Betriebssystems“ von Partnern

Konzipiert mit Lieferkettensicherheit

Dell SafeSupply Chain[3]

Secured Component Verification
On Device • On Cloud

DELL Technologies

Sicheres Arbeiten an jedem Ort mit **Dell Trusted Workspace**

Eingebaute und integrierte Hardwaresicherheit

Zusätzliche Softwaresicherheit

Verkleinern Sie mit mehreren Schutzebenen die Angriffsfläche und verbessern Sie die langfristige Ausfallsicherheit bei Cyberangriffen.

Besuchen Sie uns
dell.com/endpoint-security

Kontakt
global.security.sales@dell.com

Weitere Informationen
Endpoint Security – Blogs →

An Unterhaltung teilnehmen
LinkedIn /delltechnologies
X @delltech

Quellen und rechtliche Hinweise

[1] Basierend auf einer internen Analyse von Dell, Oktober 2024 (Intel) und März 2025 (AMD). Gilt für PCs mit Intel und AMD-Prozessoren. Nicht alle Funktionen sind bei allen PCs verfügbar. Einige Funktionen müssen zusätzlich erworben werden. Intel basierte PCs von Principled Technologies validiert. Vergleich der Sicherheitsfunktionen, April 2024.
[2] Integrationen sind für CrowdStrike Falcon Insight XDR und Absolute verfügbar. [3] Verfügbarkeit je nach Region

DELL Technologies