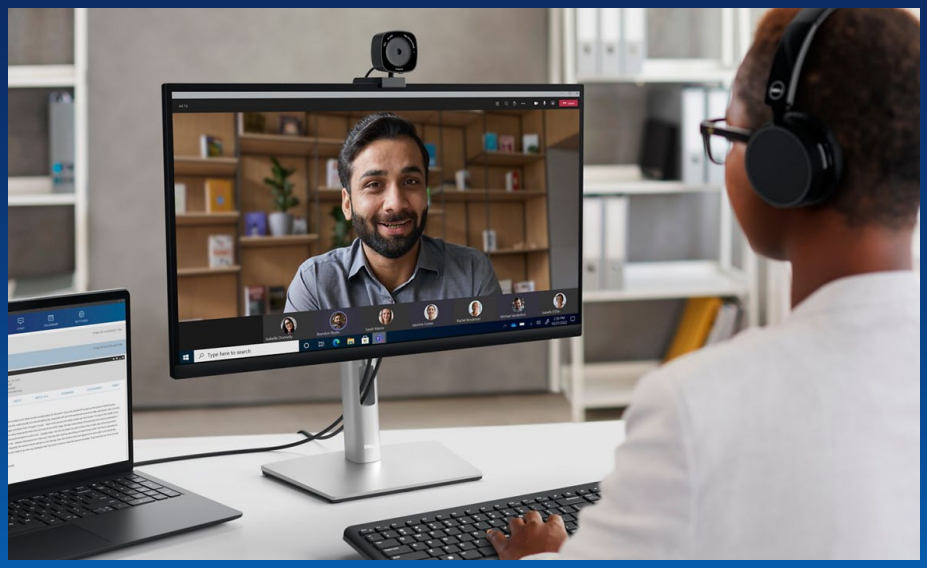
MEHR ENTDECKEN

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 →

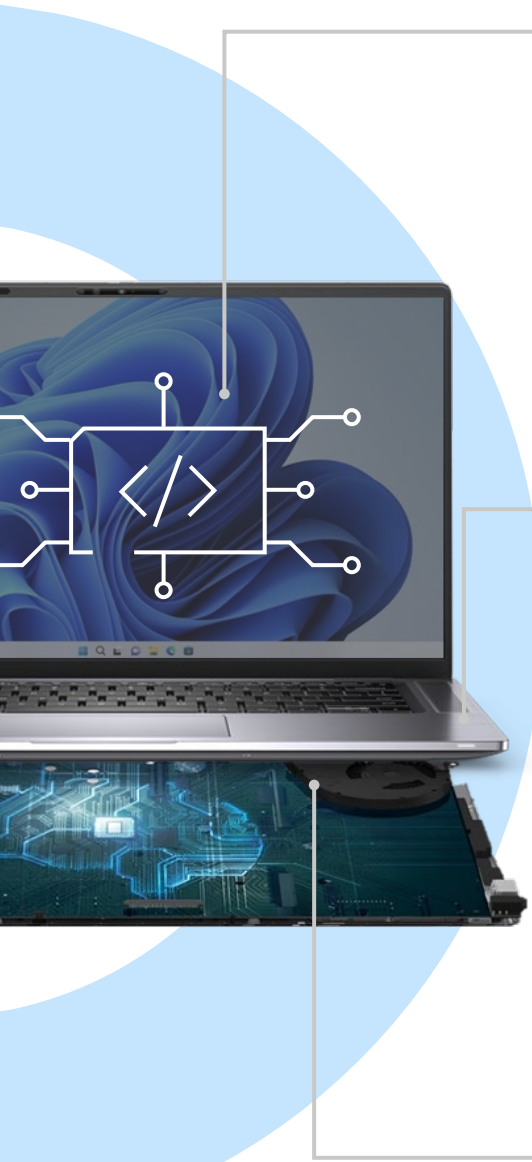
Die branchenweit sichersten PCs[1] →

Software für mehr Sicherheit in jeder 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 branchenweit sichersten 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]

Eingebaute **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 sie auftreten

Dell SafeGuard and Response

Dell SafeData

Schutz vor sich weiterentwickelnden Bedrohungen

Dell SafeBIOS

Dell SafeID

Dell SafeShutter

Auslieferung vertrauenswürdiger und unmanipulierter Hardware

Dell SafeSupply Chain

Dell Trusted Workspace – eingebaute und integrierte Sicherheit

Die branchenweit sichersten PCs[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.

Weitere Informationen →

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.

Schutz von Endnutzerzugangsdaten

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

Weitere Informationen →

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.

Weitere Informationen →

Aufspüren tickender Zeitbomben

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

Wahrung des Datenschutzes auf dem Bildschirm

Die per Sensor aktivierte Webcamfunktion **SafeShutter** öffnet und schließt die Kamera automatisch synchron mit den Videokonferenzanwendungen.

Höhere Sicherheit durch PC-Telemetrie

Minimieren Sie IT-Sicherheitslücken mit **Dell Trusted-Device-Software**. 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

Latitude →

OptiPlex →

Precision →

DELL Technologies

Dell Trusted Workspace – zusätzliche Sicherheit

Software für mehr Sicherheit in jeder Flotte

Vereiteln ausgeklügelter 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® →

VMware Carbon Black →

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

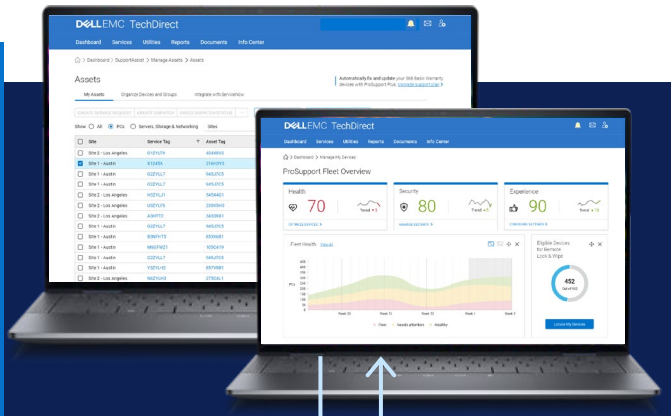
Sich weiterentwickelnde Cyberbedrohungen umgehen rein softwarebasierte Abwehrmaßnahmen. Minimieren Sie mit hardwaregestützten Schutzmaßnahmen die Angriffsfläche von Endpunkten.

Der Schutz vor modernen Bedrohungen erfordert die Kombination von hardware- und softwaregestützten Maßnahmen. Hier kommt Dell ins Spiel. In Zusammenarbeit mit branchenführenden Sicherheitspartnern kombiniert Dell umfassende Telemetrie auf Geräteebene mit hochmoderner Bedrohungserkennung, um die Sicherheit Ihrer Flotte zu verbessern.

- ✓ **Verkleinern der Angriffsfläche**
- ✓ **Verbessern der Bedrohungserkennung**
- ✓ **Wahren der Vertrauenswürdigkeit von Geräten**
- ✓ **Konsolidieren von Anbietern**

Zusätzliche Softwaresicherheit

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



DAS BS

Integrierte Hardware- und Firmwaresicherheit

Dell SafeBIOS

Dell Trusted-Device-Software

BIOS Verification | Imageerfassung | Indicators of Attack

Chipbasierte Funktionen („unterhalb des BS“) von Partnern

Eingebaute Lieferkettensicherheit

Dell SafeSupply Chain[1]

Secured Component Verification
Auf dem Gerät • In der 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
dell.com/endpoint-security

Kontakt
global.security.sales@dell.com

Weitere Informationen
Endpoint Security – Blogs →

Jetzt mitreden
LinkedIn/delltechnologies
X @delltech

Quellen und rechtliche Hinweise

[1] Basierend auf einer internen Analyse von Dell, September 2023. Gilt für PCs mit Intel Prozessoren. Nicht alle Funktionen sind bei allen PCs verfügbar. Einige Funktionen müssen zusätzlich erworben werden. Die Verfügbarkeit kann je nach Region variieren.

[2] Integrationen verfügbar für CrowdStrike Falcon Insight XDR und VMware Carbon Black Audit and Remediation.

DELL Technologies