

Aufbau eines vertrauenswürdigen Geräts

Warum Dell PCs die sichersten KI-PCs der Welt sind ¹



BEDROHUNGLANDSCHAFT UND HERAUSFORDERUNGEN

Neue Angriffsvektoren unterhalb des Betriebssystems schaffen neue Risiken

Endpunktgeräte sind ein wesentlicher Einfallstor für Sicherheitsverletzungen. Mit der wachsenden Angriffsfläche beim hybriden Arbeiten sind die Bedenken hinsichtlich der Sicherheit auf Geräteebene in den letzten Jahren stark gestiegen. Angreifer zielen zunehmend auf die Lieferkette sowie auf Rootkits und andere Firmwareschwachstellen ab, die von herkömmlicher EDR-Software allein kaum erkannt werden können.



Gerätebasierte Bedrohungen haben seit 2020 um das 1,5-fache zugenommen.²

Wichtigste Bewertungskriterien bei der Beschaffung neuer PCs:

- Automatisierte Erkennung von BIOS-Ereignissen³
- Umgang mit Konfigurationen mit hohem Risiko³

Um moderne Bedrohungen zu bekämpfen, müssen Geräte sicher aufgebaut sein und über integrierte Sicherheit verfügen, um Angriffe abfangen und abwehren zu können.

DIE LÖSUNG

Vorbeugung, Erkennung, Reaktion auf und Wiederherstellung nach grundlegenden Angriffen mit den sichersten PCs der Welt ¹

Eine Flotte ist nur so sicher wie die einzelnen darin enthaltenen PCs. Aber was macht ein Gerät vertrauenswürdig und sicher? Transparenz und Umsetzbarkeit. Zugriff auf mehr Daten führt zu einer fundierten Entscheidungsfindung und trägt dazu bei, selbst die heimtückischsten aufkommenden Bedrohungen abzufangen. Automatisierung ermöglicht eine schnellere Lösung potenzieller Probleme.

Die Hardware- und Firmwareabwehrfunktionen der Dell PCs auf der Intel und der AMD-Plattform sind darauf ausgelegt, diese Transparenz und Handlungsfähigkeit für Ihre gesamte Flotte bereitzustellen.

Aufbau eines Dell Trusted-Device

Vorteile



Schutz ab dem ersten Start durch strenge Lieferkettenkontrollen



Aufrechterhaltung der BIOS-Integrität mit umfassender Transparenz auf Firmware-Ebene



Schutz der Identität der EndnutzerInnen vor Malware, die darauf abzielt, Zugangsdaten zu stehlen



Anreicherung von Daten auf Betriebssystemebene mit Telemetrie unterhalb des Betriebssystems zur Beschleunigung von Erkennung, Reaktion und Korrektur

Höhere Sicherheit durch PC-Telemetrie

Verkleinern Sie die IT-Sicherheitslücke und 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](#) →

Aufrechterhaltung der BIOS-Integrität

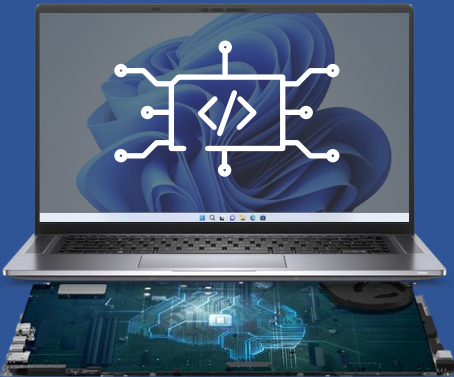
Mit der BIOS-Verifizierung, nur bei Dell, Bedrohungen entdecken und abwehren. Bewerten und reparieren Sie mit BIOS Image Capture ein beschädigtes BIOS und gewinnen Sie Einblicke, die die Gefährdung durch zukünftige Bedrohungen reduzieren.¹

[Weitere Informationen](#) →

Aufspüren tickender Zeitbomben

Indicators of Attack ist eine nur von Dell angebotene Frühwarnfunktion, die nach verhaltensbasierten Bedrohungen sucht, bevor diese Schaden anrichten können.¹

[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.¹

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.¹

[Weitere Informationen](#) →

Sichern von Endnutterzugangsdaten

Verifizieren Sie den Nutzerzugriff mit dem dedizierten und nur bei Dell erhältlichen Sicherheitschip SafeID, der Nutzerzugangsdaten vor Malware verbirgt.¹

[Weitere Informationen](#) →

Sicherheit während des gesamten PC-Lebenszyklus

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.¹

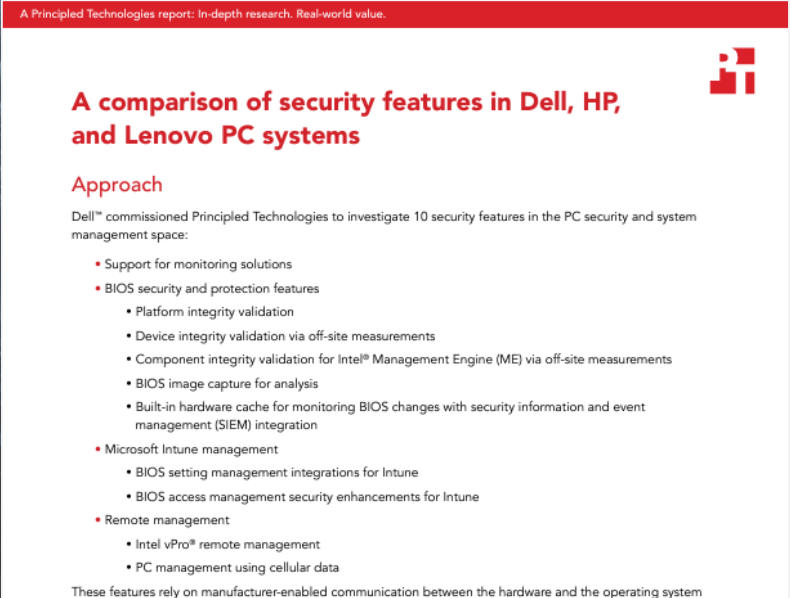
[Weitere Informationen](#) →

BRANCHENFÜHREND

Kein PC-Hersteller bietet die gleiche Transparenz auf BIOS-Ebene wie Dell.¹

Erfahren Sie, wie angesichts moderner Bedrohungen Geräte vertrauenswürdig bleiben.⁴

[Weitere Informationen](#) →



Weitere Informationen zu Dell Trusted-Devices



[Laptops](#) →



[Desktop-PCs](#) →



[Workstations](#) →

Sicheres Arbeiten an jedem Ort mit Dell Trusted Workspace



Eingebaute und integrierte Hardwaresicherheit



Zusätzliche Softwaresicherheit

Besuchen Sie uns

dell.com/endpoint-security

Kontakt

global.security.sales@dell.com

Weitere Informationen

[Endpoint Security – Blogs](#) →

An Unterhaltung teilnehmen

[in delltechnologies](#)

[X @delltech](#)