DELL Technologies

Moderne Cyberbedrohungen bekämpfen

mit integrierter Endpoint Security und Verwaltbarkeit

CROWDSTRIKE intel ABSOLUTE®

DELL Technologies

Zusammenfassung

Neue Angriffsvektoren schaffen neue Risiken. Mit mehreren aufeinander abgestimmten Schutzebenen bleiben Sie den modernen Bedrohungen Ihrer Endpunkte einen Schritt voraus. Erfahren Sie, wie Sie mit in Software integrierter Hardwaretelemetrie die Sicherheit und Verwaltbarkeit der gesamten Flotte verbessern. Einfach zu verwaltende Geräte und Lösungen wehren Angriffe schneller ab, unterstützen Zero-Trust-Prinzipien und ermöglichen sichere Innovationen.

Inhalt

Die Bedrohungslandschaft

Fallstudie

Im Jahr 2023 entdeckte Eclypsium einen Fehler in der Firmware von Hauptplatinen eines taiwanesischen Herstellers. Der Code, der eigentlich nur die Firmware auf dem neuesten Stand halten sollte, war unsicher implementiert. Es bestand das Risiko, dass der Mechanismus gekapert und zur Installation von Malware verwendet werden konnte.

Gründe, weshalb diese Entdeckung besonders beunruhigend war

- Kundendaten waren über Firmwaresicherheitslücke ungeschützt.
- Die Sicherheitslücke bestand in einem Bereich des Geräts, in dem es gewöhnlich schwierig war, Bedrohungen zu erkennen.
- Die Lücke konnte für einen Remoteangriff genutzt und die Überprüfung der Zugangsdaten umgangen werden.

Aus den Schlagzeilen ...

WIRED BACKCHANNEL BUSINESS CULTURE GEAR IDEAS MORE SIGN IN SUBSCRIBE

Millions of PC Motherboards Were Sold With a Firmware Backdoor

ExpertInnen schlagen Alarm: In Hunderten von Hauptplatinen lädt versteckter Code heimlich Software herunter. Damit ist Missbrauch buchstäblich vorprogrammiert.

Die Bedrohungslandschaft

Auswirkungen

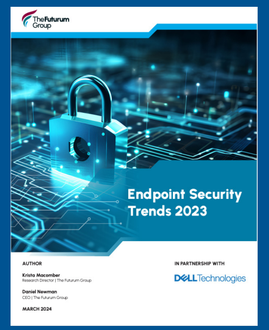
Ein wichtiger Grund, weshalb IT- und Sicherheitsteams nachts nicht schlafen können:

Gerätebasierte Angriffe.

Über diese ausgeklügelten, bösartigen Angriffe verschaffen sich AngreiferInnen privilegierten Zugriff. Zusätzlich können viele dieser Angriffe den herkömmlichen reinen Softwareschutz, z. B. Virenschutz, völlig unbemerkt deaktivieren.

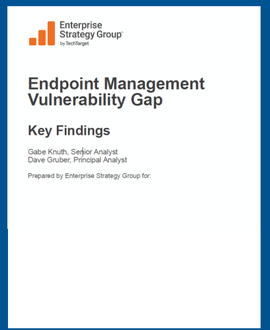
Wichtigste Bewertungskriterien von Unternehmen bei der Beschaffung neuer Hardware laut einer kürzlich unter IT- und SicherheitsexpertInnen weltweit durchgeführten Umfrage[1]:

Automatisierte Erkennung von BIOS-Firmwareereignissen



69 % der Unternehmen meldeten in den letzten zwölf Monaten mindestens EINEN Angriff auf Geräteebene. Das ist ein Anstieg um das 1,5-Fache gegenüber der Studie von 2020![2]

Konfigurationen mit hohem Risiko



Mehr als 75 % der Unternehmen meldeten mindestens einen Cyberangriff, der von einem unbekannten, nicht bzw. schlecht verwalteten Endpunkt ausgeht.[3]

Herausforderungen

Wodurch wird ein Gerät zu einem leichten Ziel?

Sichtbarkeit

Angriffe dieser Art sind schwer zu erkennen. Sie betreffen einen Teil des Geräts, der gewöhnlich nicht sichtbar und beobachtbar ist.

Handlungsfähigkeit

Oft haben Unternehmen zahlreiche Tools installiert, die isoliert voneinander arbeiten. Schnelle Reaktionen und Korrekturen sind eine echte Herausforderung und mit hohem manuellem Aufwand verbunden.

Lösung

Sichtbarkeit | **Handlungsfähigkeit**

Als einer der weltweit größten Technologieanbieter legt Dell viel Wert auf Sicherheit. Deshalb **achten wir schon bei der Entwicklung unserer PCs auf Sichtbarkeit und Handlungsfähigkeit**. So hält die IT- und Sicherheitsabteilung das Heft in den Händen.

Unsere PCs verfügen über **einzigartige integrierte Sicherheitsfunktionen** wie BIOS Verification[4] und Indicators of Attack[4]. Damit werden Bedrohungen erkannt noch bevor sie Schaden anrichten. Sichtbar gemacht werden sie mit **nur von Dell erhältlicher Gerätetelemetrie**.[4] Erkennt ein Dell PC mit Intel vPro® eine potenzielle Bedrohung auf Geräteebene, wird-die Information an das Betriebssystem weitergeleitet und kann schneller und effektiver untersucht und behandelt werden.

Branchenführend

Die sichersten PCs der Welt – natürlich von Dell[4]

Erfahren Sie, wie angesichts moderner Bedrohungen Geräte vertrauenswürdig bleiben.

Lesen Sie die Studie von Principled Technologies zur Gerätesicherheit →


Principled Technologies®

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

A comparison of security features in Dell, HP, and Lenovo PC systems

Approach

Dell™ commissioned Principled Technologies to investigate 10 security features in the PC security and system management space:

- Support for monitoring solutions
- BIOS security and protection features
  - Platform integrity validation
  - Device integrity validation via off-site measurements
  - Component integrity validation for Intel® Management Engine (ME) via off-site measurements
  - BIOS image capture for analysis
  - Built-in hardware cache for monitoring BIOS changes with security information and event management (SIEM) integration
- Microsoft Intune management
  - BIOS setting management integrations for Intune
  - BIOS access management security enhancements for Intune
- Remote management
  - Intel vPro® remote management
  - PC management using cellular data

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): Dell, HP, and Lenovo®. Many of the Dell features relate to the Dell Trusted Device application.

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.

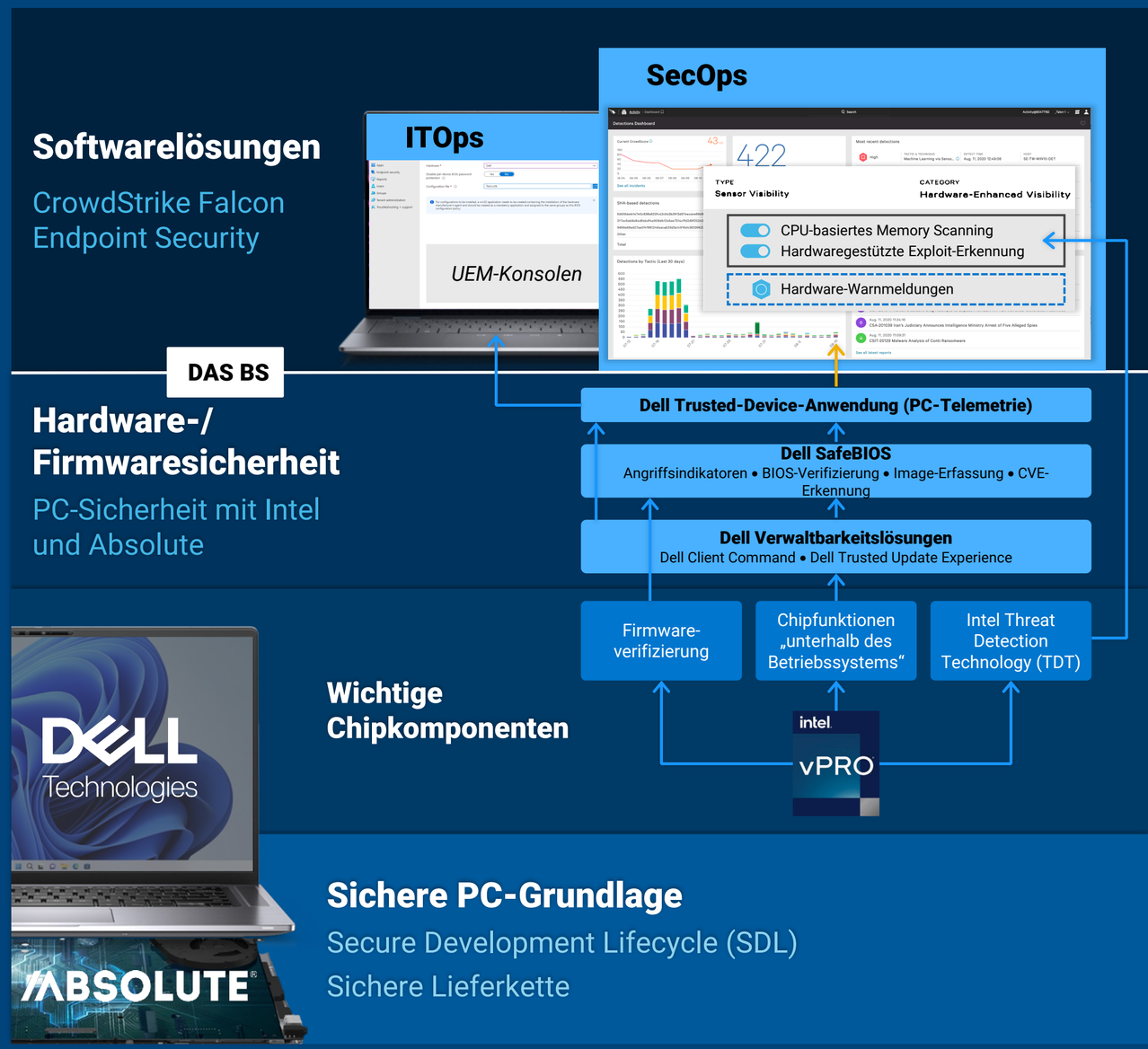
Lösung

Mit Sicherheit und Verwaltbarkeit Bedrohungen bekämpfen

Dell und sein Partnernetzwerk bringen Sichtbarkeit und Handlungsfähigkeit an den Arbeitsplatz. Dazu gehört:

- Sicherheit in der Lieferkette und integrierter Hardware- und Firmewareschutz von Dell
- Core-Chips und hardwarenaher Schutz von Intel
- Verwaltbarkeit über Dell und einheitliches Endgerätemanagement
- Schutz vor erweiterten Bedrohungen für Endpunkte, Netzwerke und die Cloud von Partnern wie CrowdStrike und Absolute

Die Umgebung nutzt die PC-Telemetrie als Bindeglied und hilft, die Lücke zwischen IT- und Sicherheitslösungen zu schließen, durch die sich Bedrohungen einschleichen können. Dieser Ansatz trägt nicht nur dazu bei, Angriffe zu verhindern, sondern kann auch Angriffe erkennen, darauf reagieren und sie beheben.



Anwendungsfälle und Gegenmaßnahmen

Anhand von zwei Anwendungsfällen (mit Angriffsszenarien und Gegenmaßnahmen) soll gezeigt werden, wie integrierte Sicherheit und Verwaltbarkeit die Ausfallsicherheit bei Cyberangriffen verbessern.

Zunächst geht es um einen Angriff auf die BIOS-Firmware. Hier wird deutlich, wie sich die Cyber Kill Chain[5] eines BIOS-Downgrade-Angriffs auswirken kann.

BIOS-Downgrade-Angriff

Erstzugriff: Replikation über Wechselmedien + Phishing

Schritt 1a

Bösartige Insider stehlen BS-Zugangsdaten über eine bestehende BIOS-Sicherheitslücke remote. Sie hacken das Gerät und führen ein Downgrade des BIOS durch.

Schritt 1b

Ein Angreifer initiiert einen Spear-Phishing-Angriff und stiehlt einen Sitzungstoken, wenn sich ein Admin versehentlich auf einer bösartigen Website authentifiziert.

Schritt 2

Zugriff über Zugangsdaten

AngreiferInnen erreichen Persistenz, indem sie zusätzliche Administratorkonten erstellen und sich im Netzwerk bewegen.

Schritt 3

Laterale Ausbreitung

AngreiferInnen bilden das Netzwerk ab und orten Systemmanagementserver.

Schritt 4

Exfiltration

Sie exfiltrieren Daten über einen Webservice.

Anwendungsfälle und Gegenmaßnahmen

Schutz vor BIOS-Downgrade

AngreiferInnen verschaffen sich heute schneller als je zuvor Zugang zum Netzwerk. Tatsächlich sank laut Global Threat Report von CrowdStrike die durchschnittliche eCrime-Breakout-Time (die nötige Zeit, um in ein System einzudringen und sich darin zu bewegen) von 84 Minuten im Jahr 2022 auf 62 Minuten im Jahr 2023. Die schnellste beobachtete Breakout-Zeit lag bei nur 2 Minuten und 7 Sekunden![6]

Hier erfahren Sie, wie Dell und unsere Partner Intel® und CrowdStrike dazu beitragen, einen BIOS-Downgrade-Angriff entlang der „Kill Chain“ mit Hardware-unterstützter Sicherheit abzufangen und abzuwehren.

Prävention | **Erkennen und reagieren** | **Wiederherstellen und korrigieren**

Sichere Lieferkette: Strenge Kontrollen schützen PCs von Design und Entwicklung über Beschaffung und Montage bis hin zur Lieferung. Dell und Intel arbeiten unermüdlich daran, Produkte so zu entwickeln, dass das Risiko von Sicherheitslücken und Manipulationen während des gesamten Lebenszyklus minimiert wird.




Security	Integrity	Quality	Resilience
• Secure development lifecycle • Software partners securely onboarded • Information exchange with partners securely • Quality Process Audit • Separation of Duties • Least Privilege Access	• Supplier accountability • Supplier due diligence • Piece-Part Identification • SAFECode • US Exec Order 14028 SBOM -SPDX	• Counterfeit prevention & detection • Enhanced manufacturing security program • Enterprise code signing • Secured Component Verification • Freight Tracking	• Silicon Root of Trust • Platform Firmware Resiliency Guidelines • BIOS Protection Guidelines • Built-in Supplier Redundancy

Anwendungsfälle und Gegenmaßnahmen

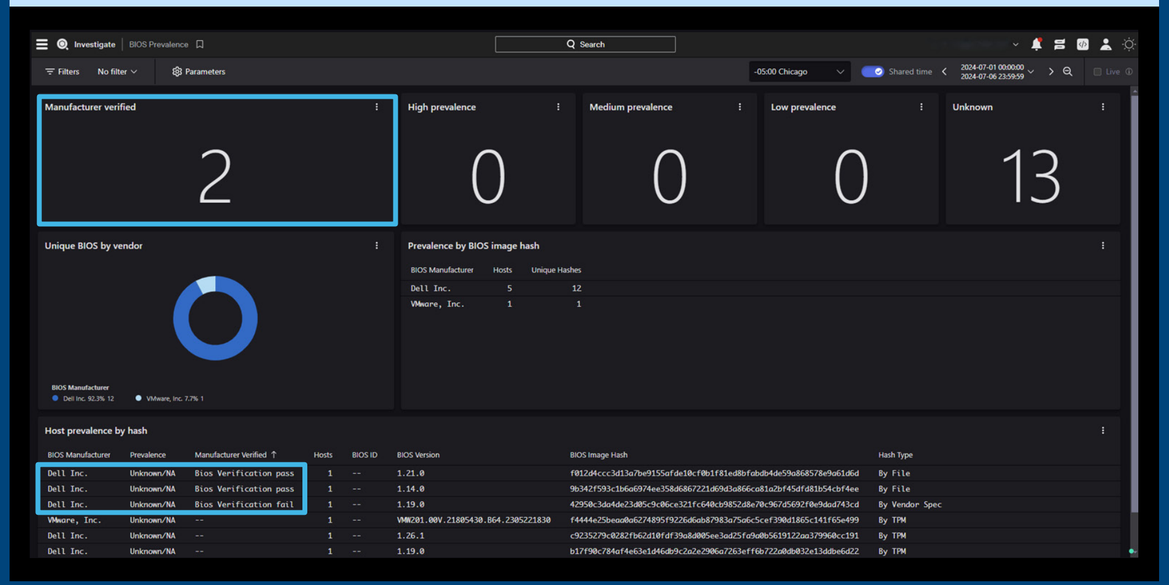
Schutz vor BIOS-Downgrade

AngreiferInnen verschaffen sich heute schneller als je zuvor Zugang zum Netzwerk. Tatsächlich sank laut Global Threat Report von CrowdStrike die durchschnittliche eCrime-Breakout-Time (die nötige Zeit, um in ein System einzudringen und sich darin zu bewegen) von 84 Minuten im Jahr 2022 auf 62 Minuten im Jahr 2023. Die schnellste beobachtete Breakout-Zeit lag bei nur 2 Minuten und 7 Sekunden![6]

Hier erfahren Sie, wie Dell und unsere Partner Intel® und CrowdStrike dazu beitragen, einen BIOS-Downgrade-Angriff entlang der „Kill Chain“ mit Hardware-unterstützter Sicherheit abzufangen und abzuwehren.

Prävention | **Erkennen und reagieren** | **Wiederherstellen und korrigieren**

BIOS-Bestätigung in der CrowdStrike Falcon-Plattform erkennen: Bei aktivierter Dell Gerätetelemetrie können AdministratorInnen Benachrichtigungen von integrierten Sicherheitsfunktionen wie BIOS Verification aus der Ferne in CrowdStrike Falcon anzeigen und verdächtige Aktivitäten schneller erkennen, bevor ein dauerhafter Schaden entsteht.



Anwendungsfälle und Gegenmaßnahmen

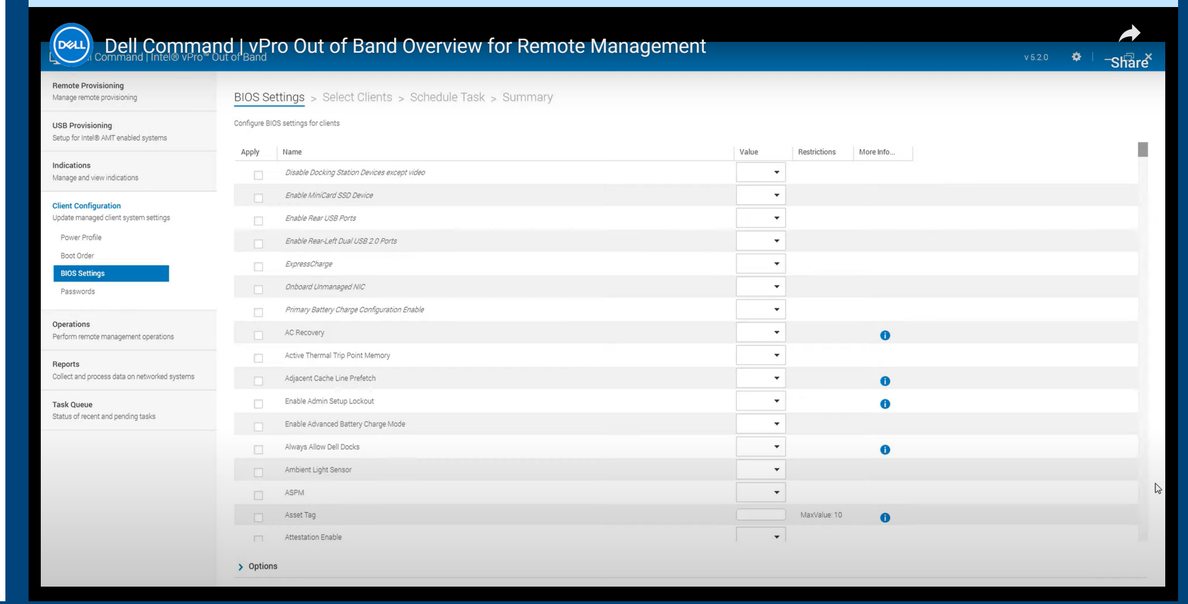
Schutz vor BIOS-Downgrade

AngreiferInnen verschaffen sich heute schneller als je zuvor Zugang zum Netzwerk. Tatsächlich sank laut Global Threat Report von CrowdStrike die durchschnittliche eCrime-Breakout-Time (die nötige Zeit, um in ein System einzudringen und sich darin zu bewegen) von 84 Minuten im Jahr 2022 auf 62 Minuten im Jahr 2023. Die schnellste beobachtete Breakout-Zeit lag bei nur 2 Minuten und 7 Sekunden![6]

Hier erfahren Sie, wie Dell und unsere Partner Intel® und CrowdStrike dazu beitragen, einen BIOS-Downgrade-Angriff entlang der „Kill Chain“ mit Hardware-unterstützter Sicherheit abzufangen und abzuwehren.

Prävention | **Erkennen und reagieren** | **Wiederherstellen und korrigieren**

BIOS-Downgrade korrigieren: Zukünftigen Bedrohungen für Out-of-Band-Systeme kann vorgebeugt werden. Mit der Dell Client Command Suite mit Intel vPro sind Remotekorrekturen möglich.



Anwendungsfälle und Gegenmaßnahmen

In diesem zweiten Anwendungsfall könnte der Schritt in der „Kill Chain“ eines Angriffs auf die Softwarelieferkette folgendermaßen ablaufen.

Angriff auf die Softwarelieferkette

Schritt 1

Erstzugriff: Lieferkette wird kompromittiert

Die AngreiferInnen fügen schädlichen Code in ein Softwaredienstprogramm (BIOS/Firmware) ein.

Schritt 2

Persistenz

Die KundInnen laden den schädlichen Code herunter, wenn sie ihre Geräte aktualisieren.

Die AngreiferInnen installieren Malware.

Schritt 3

Laterale Ausbreitung

Die AngreiferInnen übernehmen die Identität der NutzerInnen, die sie gerade angegriffen haben, und senden einen schädlichen Link an andere NutzerInnen. Diese klicken auf den Link und die AngreiferInnen stehlen ihre Zugangsdaten.

Schritt 4

Exfiltration

Die AngreiferInnen exfiltrieren Daten.

Anwendungsfälle und Gegenmaßnahmen

Die Lieferkette ist zu einem wichtigen Ziel für AngreiferInnen geworden. Diese Angriffe sind zwar nicht so häufig, können aber verheerende Folgen haben, da die Unternehmen noch herausfinden müssen, wie sie sich dagegen schützen können.

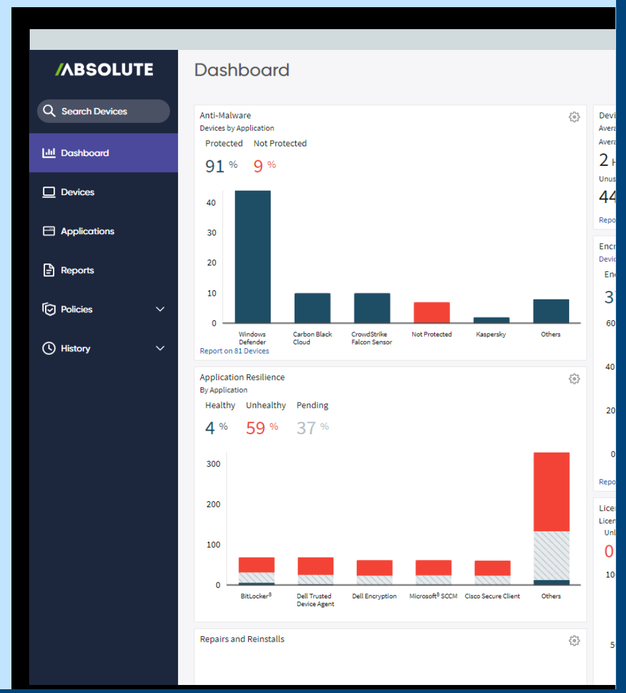
Alle Technologieanbieter müssen dafür sorgen, dass die von ihnen verkauften Produkte nicht ungewollt durch Sicherheitslücken Risiken für die NutzerInnen bergen.

Um Angriffe zu verhindern und Ausfallsicherheit für das Sicherheitspaket bereitzustellen, halten sich Dell und Intel® an die im sicheren Entwicklungszyklus[7] festgelegten strengen Prozesse und Protokolle. Zusätzliche Sicherheit in der Lieferkette, z. B. Dell Secured Component Verification[8] und Sicherheit auf Firmwareebene von Absolute (siehe rechts), sorgen bei KundInnen während des gesamten PC-Lebenszyklus für Vertrauen.

Prävention | **Erkennen und reagieren** | **Wiederherstellen und korrigieren**

Endpunktsichtbarkeit ab Werk: Sie sehen alle Geräte innerhalb und außerhalb des Netzwerks mit Absolute in den von Dell verwalteten Werken. Absolute Custom Factory Install (CFI) reduziert einen Schritt in der Bereitstellung und schützt Geräte, die etwa an Lager oder mehrere Endnutzerstandorte ausgeliefert werden. Risiken werden mithilfe eines vollständigen Überblicks über die Flotte auf einem cloudbasierten Dashboard minimiert.

- Einfaches Auffinden und Pflegen des kompletten Inventars der IT-Bestände und Anwendungen
- Lokalisierung und Zuordnung der gesamten Flotte
- Optimierung der Bestandsnutzung und Monitoring des Sicherheitsstatus
- Unterstützung verschiedener Plattformen (Windows, Mac und Chrome)
- Eingebettet in das BIOS von 27 führenden PC-OEMs



Anwendungsfälle und Gegenmaßnahmen

Die Lieferkette ist zu einem wichtigen Ziel für AngreiferInnen geworden. Diese Angriffe sind zwar nicht so häufig, können aber verheerende Folgen haben, da die Unternehmen noch herausfinden müssen, wie sie sich dagegen schützen können.

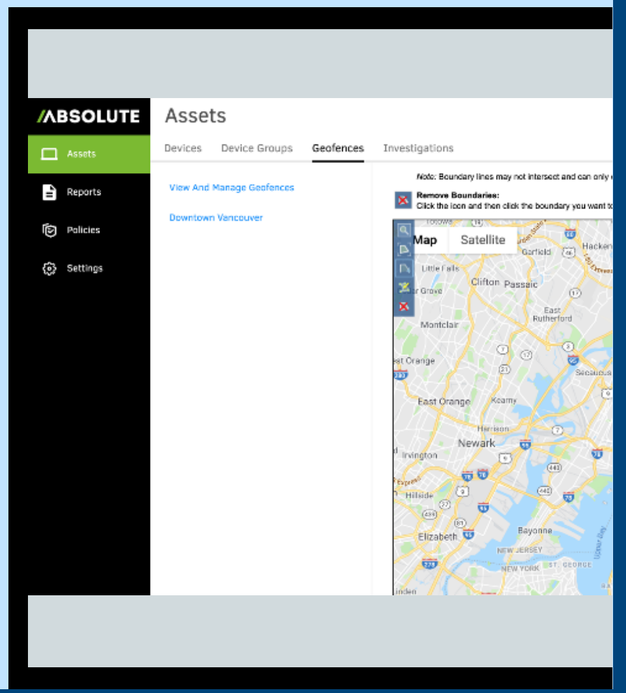
Alle Technologieanbieter müssen dafür sorgen, dass die von ihnen verkauften Produkte nicht ungewollt durch Sicherheitslücken Risiken für die NutzerInnen bergen.

Um Angriffe zu verhindern und Ausfallsicherheit für das Sicherheitspaket bereitzustellen, halten sich Dell und Intel® an die im sicheren Entwicklungszyklus[7] festgelegten strengen Prozesse und Protokolle. Zusätzliche Sicherheit in der Lieferkette, z. B. Dell Secured Component Verification[8] und Sicherheit auf Firmwareebene von Absolute (siehe rechts), sorgen bei KundInnen während des gesamten PC-Lebenszyklus für Vertrauen.

Prävention | **Erkennen und reagieren** | **Wiederherstellen und korrigieren**

Kontrolle von Endpunkten: Über Absolute können Sie erkennen, ob Endpunkte kompromittiert wurden (z. B. eine kritische Anwendung von Malware infiziert oder ein PC während des Transports verloren gegangen ist). Mit Remotemaßnahmen lassen sich die Bedrohungen dann sofort beseitigen. Sie können Geräte z. B. unbrauchbar machen und/oder die darauf befindlichen Daten löschen.

- Schutz für Geräte bei Überschreiten der festgelegten räumlichen Grenzen (Fences)
- Remoteschutz und -bereinigung kritischer Daten
- Datenlöschung am Ende der Nutzungsdauer mit Compliancezertifikaten
- Gerätesperrung als On-Demand-Schutzmaßnahme für kritische Daten
- Aktivierbarer Remoteschutz für Firmware



Anwendungsfälle und Gegenmaßnahmen

Die Lieferkette ist zu einem wichtigen Ziel für AngreiferInnen geworden. Diese Angriffe sind zwar nicht so häufig, können aber verheerende Folgen haben, da die Unternehmen noch herausfinden müssen, wie sie sich dagegen schützen können.

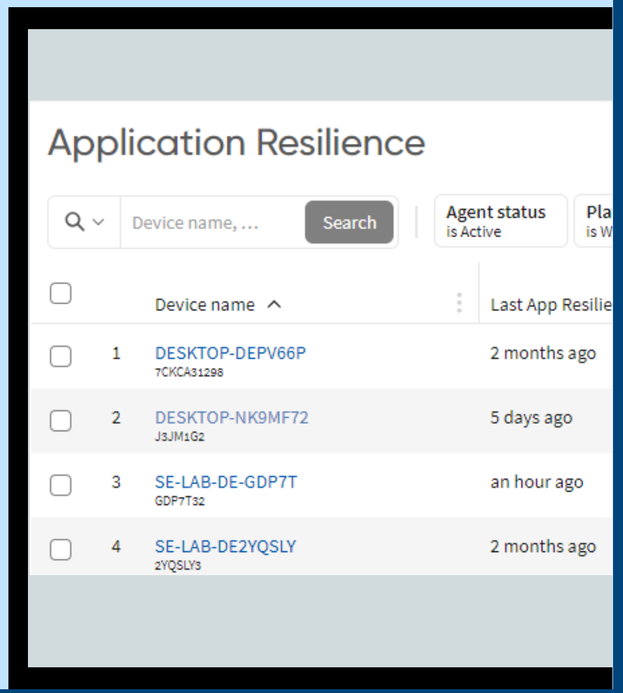
Alle Technologieanbieter müssen dafür sorgen, dass die von ihnen verkauften Produkte nicht ungewollt durch Sicherheitslücken Risiken für die NutzerInnen bergen.

Um Angriffe zu verhindern und Ausfallsicherheit für das Sicherheitspaket bereitzustellen, halten sich Dell und Intel® an die im sicheren Entwicklungszyklus[7] festgelegten strengen Prozesse und Protokolle. Zusätzliche Sicherheit in der Lieferkette, z. B. Dell Secured Component Verification[8] und Sicherheit auf Firmwareebene von Absolute (siehe rechts), sorgen bei KundInnen während des gesamten PC-Lebenszyklus für Vertrauen.

Prävention | **Erkennen und reagieren** | **Wiederherstellen und korrigieren**

Automatische Fehlerkorrektur: Mit der in die BIOS-Firmware von Dell integrierten Absolute Persistence können Sie nach einer erkannten Manipulation den ursprünglichen Zustand wiederherstellen. Absolute kann jeden kompromittierten Endpunkt und jede unterstützte Anwendung aus dem Application Resilience-Katalog (mehr als 80 Anwendungen) automatisch korrigieren oder erhalten. Der Katalog enthält auch viele weitere etablierte Schutzlösungen, etwa Dell Trusted Device oder Zscaler.

- Einfaches Auffinden und Entfernen sensibler Daten auf Endpunkten
- Geräteübergreifende Korrekturmaßnahmen mithilfe einer Bibliothek kundenspezifisch angepasster Skripte
- Monitoring und automatische Fehlerkorrektur für Anwendungen
- Umfangreicher, wachsender Application Resilience-Katalog mit Endpunktkontrollen von Drittanbietern
- Ermittlung und Lokalisierung von verlorenen oder gestohlenen Geräten mit dem Absolute Investigations Team



Wichtigste Erkenntnisse

Eine Flotte ist nur so sicher wie die einzelnen darin enthaltenen PCs.

Um moderne Bedrohungen bekämpfen zu können, müssen Geräte sicher gebaut sein und über integrierte Sicherheit verfügen.

Wo Endpoint Security und Verwaltbarkeit zusammenspielen, können Angriffe abgefangen, abgewehrt und bewältigt werden.

Sicherheit ist ein Teamsport. Nutzen Sie Hardware und Software für die beste Verteidigung.

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

Ihr nächster Schritt

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 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.

1. Quelle: Enterprise Strategy Group, eine Abteilung von TechTarget, Forschungsstudie im Auftrag von Dell Technologies, *Assessing Organizations' Security Journeys*, November 2023.
2. Quelle: Futurum Group, Endpoint Security Trends, 2023.
3. Quelle: Enterprise Strategy Group, eine Abteilung von TechTarget, Forschungsbericht *Managing the Endpoint Vulnerability Gap: The Convergence of IT and Security to Reduce Exposure*, Mai 2023.
4. Basierend auf einer internen Analyse von Dell, Oktober 2024. Gilt für PCs mit Intel Prozessoren. Nicht alle Funktionen sind bei allen PCs verfügbar. Einige Funktionen müssen zusätzlich erworben werden. Validiert von Principled Technologies. A comparison of security features, April 2024.
5. Quelle: What is the Cyber Kill Chain? Introduction Guide – CrowdStrike.
6. Quelle: CrowdStrike 2024 Global Threat Report.
7. Quelle: Three Considerations for Establishing Device Trust | Dell USA.
8. Quelle: How to Keep Device Trust Close to the Vest | Dell USA.