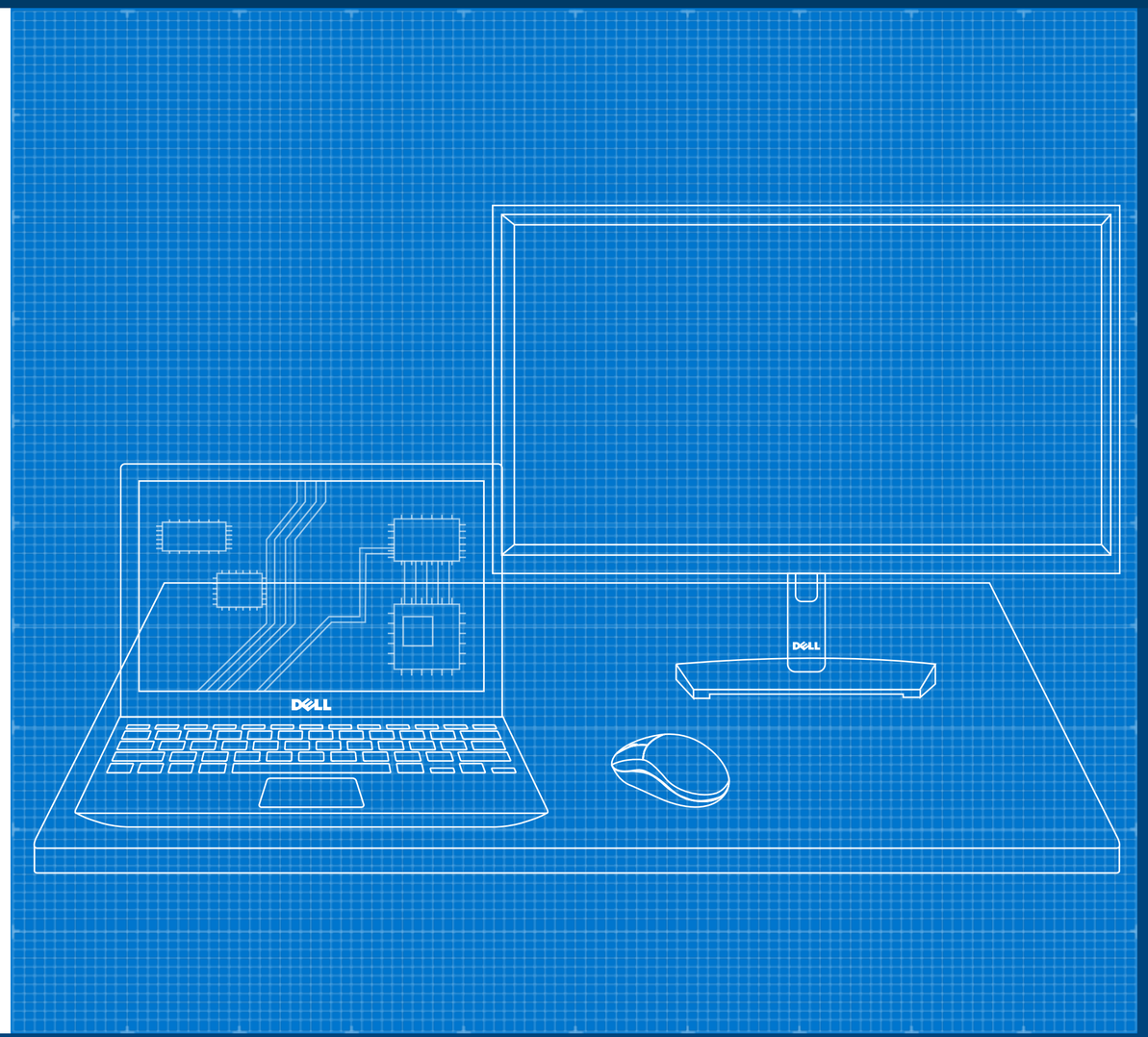
DELL Technologies

Die Gestaltung einer sicheren Arbeitsumgebung

Sorgen Sie für mehr Sicherheit in Ihrer gesamten Flotte – mit mehreren Abwehrebenen.



Zusammenfassung

Cyberangriffe sind unvermeidbar – und sie nehmen an Häufigkeit sowie Ausgereiftheit zu. Endgeräte, Netzwerke und Cloud-Umgebungen sind zu Hauptzielen geworden.

Dieses E-Book richtet sich an EntscheidungsträgerInnen in den Bereichen IT und Sicherheit. Es bietet eine Anleitung mit allen Elementen, die für den effektivsten Endpunktschutz in der sich stets weiterentwickelnden Bedrohungslandschaft erforderlich sind.

Inhaltsverzeichnis

Die Bedrohungslandschaft

Der Wechsel zum hybriden Arbeitsmodell hat zu mehr Komplexität und neuen Angriffsvektoren geführt – **Endpunkte, Netzwerke und Clouds sind erweiterte Angriffsflächen.**

Zudem setzen die AngreiferInnen nun ausgefeilte Techniken ein, die auf verschiedene Ebenen des Compute-Stacks abzielen und sich als valide Systemprozesse „tarnen“. Einige dieser Methoden ermöglichen den AngreiferInnen sogar Zugriff, sodass sie den Softwareschutz *gänzlich unentdeckt* umgehen können.

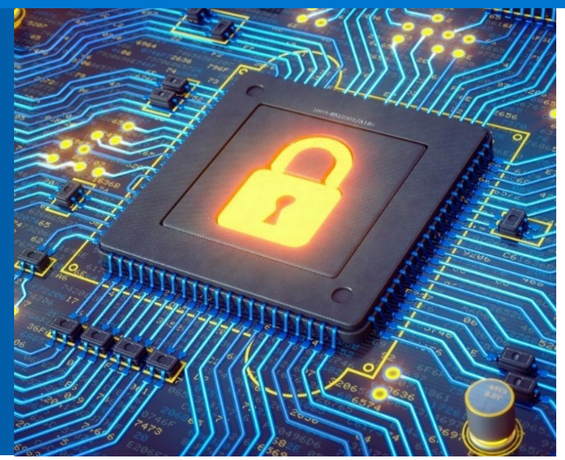
Viele Unternehmen haben einen Zero-Trust-Weg eingeschlagen, um diese Bedrohungen zu bekämpfen. Allerdings ist es für die Aktivierung der Zero-Trust-Prinzipien erforderlich, das Gerätevertrauen zu wahren.

Aber wie wahren Sie das Gerätevertrauen, wenn Angriffe immer häufiger auftreten und moderne Technologie neue Angriffsvektoren erzeugt?

[1] CrowdStrike Global Threat Report, 2023.
[2] Dell Innovation Index, 2023.

Schon gewusst?

71 % der Angriffe in 2022 basierten nicht auf Malware, das ist eine Zunahme von 9 % zum Vorjahr.[1]



Nur 41 % der befragten Unternehmen sind davon überzeugt, dass Sicherheit in ihre Technologie und Anwendungen integriert ist.[2]

Sie möchten mehr über Zero Trust erfahren, um die Ausgereiftheit Ihrer Cybersicherheit zu verbessern? Dann lesen Sie unser E-Book *Endpoint Security als wesentlicher Bestandteil von Zero Trust*.

Herausforderungen

Für eine effektive Endpoint Security müssen Sie wissen, was die AngreiferInnen motiviert und wie sie arbeiten.

Da eine Sicherheitsverletzung potenziell hohen Gewinn verspricht, **unternehmen die AngreiferInnen häufig mehrere Versuche beim gleichen Unternehmen. Sie nutzen dabei unterschiedliche Methoden und Einstiegspunkte, um ihre Erfolgschancen zu erhöhen.** Beispielsweise können die AngreiferInnen über den Lebenszyklus eines einzigen Geräts versuchen, die Sicherheitslücken über Dutzende Vektoren auszunutzen.

Legacy-Abwehrmaßnahmen reichen nicht mehr aus, um die Endpunkte zu schützen. Wenn die Unternehmen die Abwehr einer Angriffsfläche verstärken, versuchen es die BedrohungsakteurInnen einfach bei leichteren Zielen. Mit dem Wechsel zur hybriden Arbeitswelt haben sie neue Angriffsvektoren für Endpunkte gefunden, die verheerende Ausfälle nach sich zogen.

Siehe Beispiele rechts

Angriff auf die Lieferkette: zielt auf Lieferanten ab, um Zugriff auf deren Systeme, Daten und/oder Netzwerk und, im Endeffekt, auf deren Kunden zu erhalten. **BEISPIEL: Angriff auf eine Hardwarelieferkette, ermöglicht durch die Manipulation einer Komponente:**

Die AngreiferInnen fangen einen PC-Versand ab und tauschen die Festplatten.

Die IT stellt die kompromittierten Geräte im Unternehmen bereit.

Die AngreiferInnen installieren Malware, um die Zugangsdaten während des Anmeldevorgangs der NutzerInnen zu extrahieren.

Social-Engineering-Angriff: trickst die EndnutzerInnen aus, damit sie vertrauliche Informationen preisgeben, die dann den Geräte- und Netzwerkzugriff ermöglichen. **BEISPIEL: Spoofing-Angriff, ermöglicht durch eine Phishing-E-Mail:**

Ein/e EndnutzerIn fällt auf eine Phishing-E-Mail herein und gibt Zugangsdaten auf einer Spoofing-Webseite ein.

Die AngreiferInnen nutzen die gültigen Zugangsdaten, um sich remote Zugriff zum Netzwerk zu verschaffen.

Sie schleusen Daten über einen Webservice aus, verschlüsseln sie und fordern Lösegeld dafür.

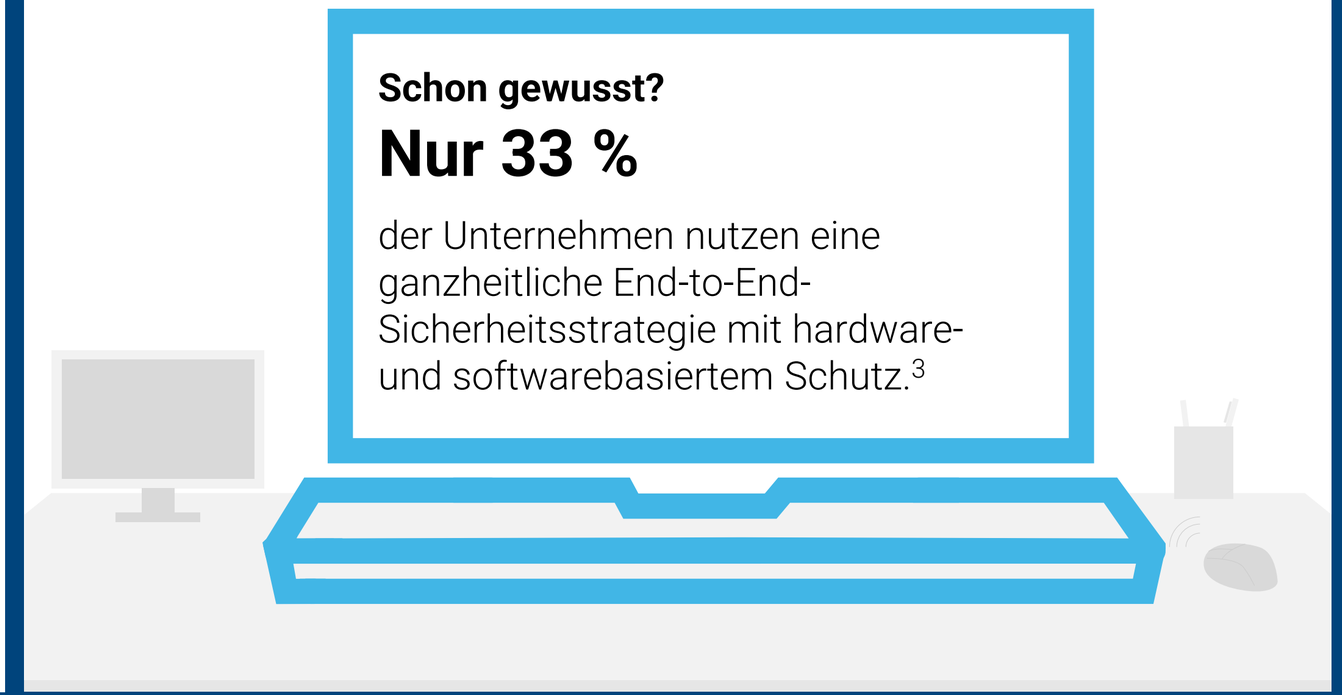
Schutz für die moderne Arbeitsumgebung

In Bezug auf den Endpunktschutz sind Prävention, Erkennung und Reaktion sowie Recovery und Korrektur in verschiedenen Phasen über den gesamten Lebenszyklus eines Geräts erforderlich – von der Beschaffung und Fertigung der PCs über den Versand und die Bereitstellung, während der Nutzung und bis zur Stilllegung. Stellen Sie sich nur die Größe dieser kombinierten Angriffsfläche vor!

Die effektivste Cybersicherheitsstrategie plant für das Worst-Case-Szenario vor. Es wird davon ausgegangen, dass eine Sicherheitsverletzung möglich ist. Daher werden mehrere Schutzebenen implementiert, um den Angriff so schnell und so häufig wie möglich zu stoppen. Zudem minimieren die enthaltenen Korrekturfunktionen das Risiko eines Wiederholungsangriffs.

[3] Dell Innovation Index, 2023.

PRÄVENTION	ERKENNUNG UND REAKTION	RECOVERY UND KORREKTUR
Bieten Sie weniger Angriffsfläche, indem Sie für die Abwehr von Angriffen entwickelte Maßnahmen nutzen.	*Gehen Sie stets von einer Sicherheits-verletzung aus und bleiben Sie wachsam.*	*Mindern Sie die Folgen eines Angriffs und kehren Sie zum normalen Geschäfts-betrieb zurück.*



Die Gestaltung einer sicheren Arbeitsumgebung

Für moderne Endpoint Security sind drei Elemente erforderlich:

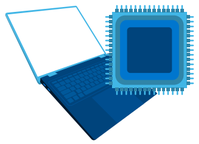
1. **Softwaresicherheit:** Heutzutage befinden sich mehr NutzerInnen, Geräte und Daten außerhalb der Unternehmensnetzwerke als je zuvor. Softwaresicherheit schützt nicht nur die Geräte, sondern erweitert den Schutz auch auf Netzwerk- und Cloud-Umgebungen, in denen bösartige Aktivitäten häufig ihren Ursprung haben.
2. **Hardwaresicherheit:** Die Geräte müssen über integrierte Sicherheitsfunktionen verfügen. Das bezieht sich auf Hardware- und Firmwaresicherheit, die das Gerät während der Nutzung schützt. Zum Schutz der Arbeitsumgebung benötigen Sie integrierte Funktionen, die Ihnen Sichtbarkeit in und Kontrolle über das Gerät bieten.
3. **Lieferkettensicherheit:** Die Geräte müssen sicher gefertigt werden. Das heißt, mit Lieferanten zusammenzuarbeiten, die a) die Bedrohungslandschaft verstehen und b) diese Kenntnisse auf die sich entwickelnde Landschaft anwenden können. Der Schutz von Design, Entwicklung und Tests von PCs minimiert das Risiko für Sicherheitslücken in Produkten und Lieferketten-kontrollen reduzieren das Risiko von Produktmanipulationen.

Darstellung der verschiedenen Sicherheitsebenen

(Repräsentative Beispiele der aufgeführten Sicherheitsmaßnahmen)

Softwaresicherheit

- Virenschutz der nächsten Generation (NGAV)
- Endpoint Detection and Response (EDR)
- Extended Detection and Response (XDR)
- Data Protection für die Cloud
- Netzwerkschutz
- Automatische Fehlerkorrektur



Hardware-/Firmwaresicherheit

- Überprüfung zur Startzeit
- Überprüfung zur Laufzeit
- Nutzerauthentifizierung
- Sicherheitsbenachrich-tigungen und Warnmel-dungen/Telemetrie

Lieferkettensicherheit

- Sichere Entwicklungspraktiken
- Sichere Lieferkettenpraktiken
- Komponentenprüfungen
- Manipulationssichere Verpackung

Unser Ansatz: Dell Trusted Workspace

Dell ist Sicherheits- und IT-Partner für Unternehmen weltweit. Im Gegensatz zu Punktlösungen legt Dell den Schwerpunkt auf die Sicherheitsergebnisse. Wir haben eine Suite mit Lösungen entwickelt, die Kill Chains unterbrechen und Ihre Ausfallsicherheit bei Cyberangriffen erhöhen.

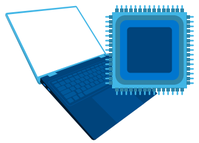
Dell Trusted Workspace umfasst Folgendes:

- Einzigartiger **Hardware- und Firmwareschutz** – das macht Dell zum Anbieter der branchenweit sichersten PCs[4] *(eingebaute und integrierte Sicherheit)*
- Partnernetzwerk mit **branchenführender Software** für Advanced Threat Protection – für Geräte sowie Netzwerk- und Cloud-Umgebungen *(zusätzliche Sicherheit)*

[4] 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.

Zusätzliche Softwaresicherheit durch Partnernetzwerk

- **Dell SafeGuard and Response: CrowdStrike, VMware Carbon Black** und **Secureworks** bieten Bedrohungserkennung, -reaktion und -korrektur.
- **Dell SafeData: Netskope** sorgt für Sichtbarkeit, Monitoring und die Verhinderung von Datenverlusten bei cloudbasierten Apps. **Absolute** aktiviert die automatische Fehlerkorrektur für Apps und Netzwerke.



Integrierte Hardware- und Firmwaresicherheit in den branchenweit sichersten PCs[4]

Beispielfunktionen für den Schutz während der Gerätenutzung:

- **Dell SafeBIOS** fängt bösartige Aktivitäten mithilfe von Off-Host BIOS Verification* und Indicators of Attack* ab, bevor sie den PC schädigen können.
- **Dell SafeID** schützt die Nutzerzugangsdaten auf einem dedizierten Chip.
- **Firmwareverifizierung unabhängig vom Host** schützt die Integrität von Firmware mit besonderen Berechtigungen.*
- Mit der **Dell Trusted-Device-Software** integriert Dell die Gerätetelemetrie in branchenführende Software, um die Sicherheit der ganzen Flotte zu verbessern.*

Eingebaute Lieferkettensicherheit sorgt dafür, dass die PCs ab dem ersten Start geschützt sind.

- **Dell SafeSupply Chain-**Add-ons wie Dell Secured Component Verification bieten eine zusätzliche Absicherung für die Produktintegrität.

** Nur bei Dell erhältlich.*

Eine umfassende Lösung von Dell

Mit sowohl hardware- als auch softwarebasierten Gegenmaßnahmen verkleinern Sie die Angriffsfläche durch eine Abwehr, die gängige Angriffe verhindert.

Erkennungs- und Reaktionsfunktionen fangen versteckte Angriffe ab, die sonst vielleicht „durchkommen“ würden.

Bei einem Angriff auf die Lieferkette (wie auf Seite 4 besprochen): Bei einer Zusammenarbeit mit Dell können präventive Maßnahmen wie z. B. **sichere Lieferkettenpraktiken** einen Angriff frühzeitig in der Kill Chain stoppen. Falls ein Angriff „durchkommt“, greifen die zusätzlichen Gegenmaßnahmen, wie z. B. **SCV** (Secured Component Verification).

Bei einem Social-Engineering-Angriff: Selbst wenn es den AngreiferInnen gelingt, EndnutzerInnen auszutricksen, damit sie gültige Zugangsdaten preisgeben, kann eine **hardwarebasierte Nutzerverifizierung wie SafeID** den Angriff stoppen und weiteren Zugriff verweigern. Sicherheitssoftware wie **Next-Gen Secure Web Gateway** bietet eine weitere Ebene für den Monitoringschutz.

Abwehren eines Angriffs auf die Hardwarelieferkette, ermöglicht durch die Manipulation einer Komponente

Die AngreiferInnen fangen einen PC-Versand ab und tauschen die Festplatten.

- **Sichere Lieferkettenpraktiken**
- Manipulationssichere Verpackung
- Türschlösser

Die IT stellt die kompromittierten Geräte im Unternehmen bereit.

- Sichere Komponenten-verifizierung (Secured Component Verification, SCV):
- Überprüfung zur Laufzeit

Die AngreiferInnen installieren Malware, um die Zugangsdaten während des Anmeldevorgangs der NutzerInnen zu extrahieren.

- Cloud Access Security Broker
- Next Generation Secure Web Gateway (NG-SWG)

Abwehren eines Social-Engineering-Angriffs, ermöglicht durch eine Phishing-E-Mail

Ein/e EndnutzerIn fällt auf eine Phishing-E-Mail herein und gibt Zugangsdaten auf einer Spoofing-Webseite ein.

- NGAV
- EDR
- XDR

Die AngreiferInnen nutzen die gültigen Zugangsdaten, um sich remote Zugriff zum Netzwerk zu verschaffen.

- Multifaktor-Authentifizierung mit SafeID
- Zero Trust Network Access

Sie schleusen Daten über einen Webservice aus, verschlüsseln sie und fordern Lösegeld dafür.

- Next Generation Secure Web Gateway + Verhaltensanalysen von Nutzerentitäten

Wichtigste Erkenntnisse

Sicherheitsverletzungen sind unvermeidbar. Effektive Endpoint Security geht immer vom Worst-Case-Szenario aus und konzentriert sich darauf, Kill Chains zu stoppen, wo immer sie auftreten – vom Gerät über das Netzwerk bis zu Cloud.

Keine Lösung blockiert 100 % der Angriffe. Eine Kombination aus hardware- und softwarebasierten Gegenmaßnahmen bietet die bestmögliche Abwehr.

Sie sind immer nur so sicher wie Ihre Lieferanten. Fordern Sie Ihre Lieferanten auf, ihre Sicherheitsmaßnahmen darzulegen.

Latitude-Laptops und -2-in-1-PCs

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.