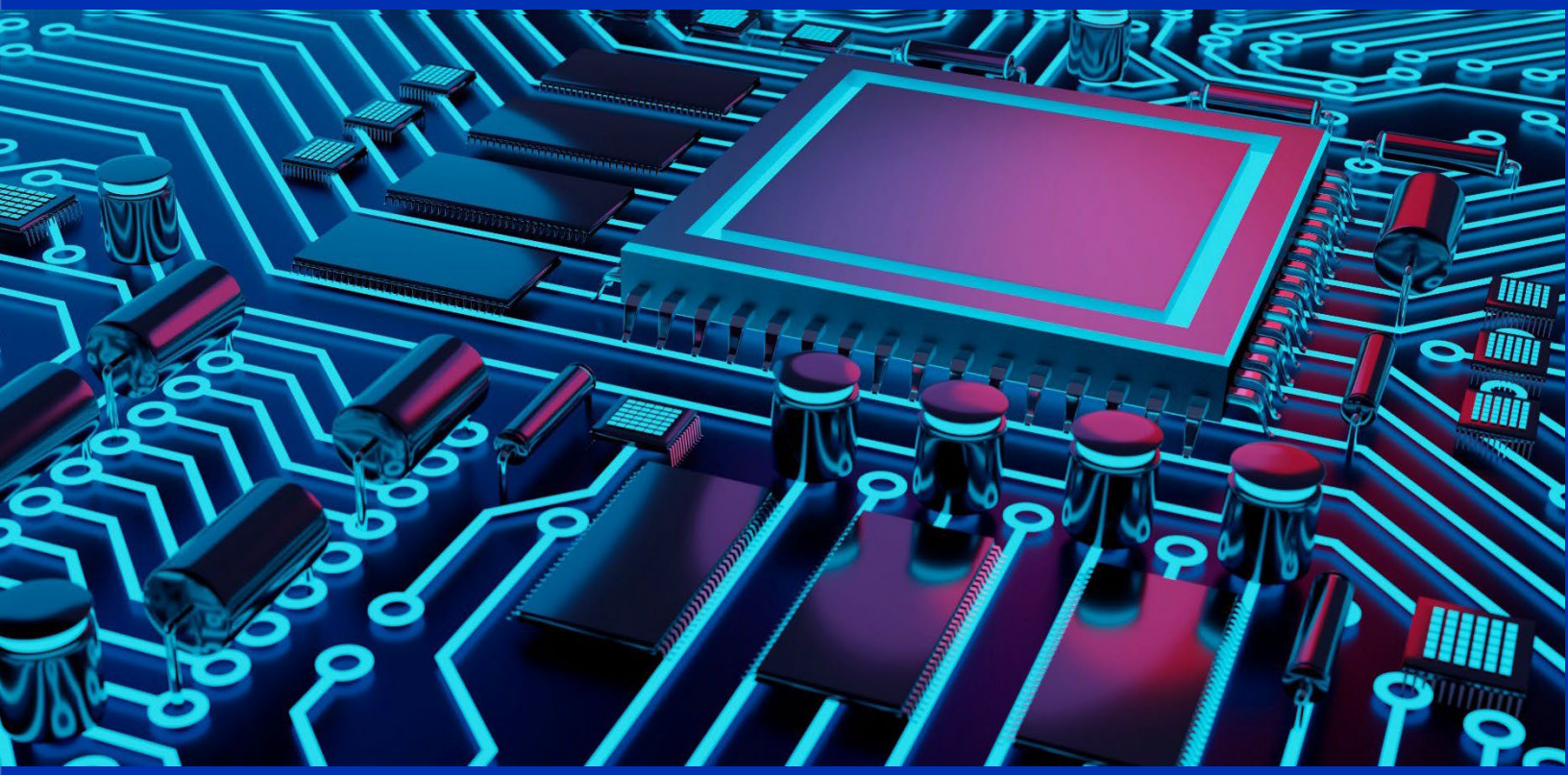
DELL Technologies intel

Umfassende Sicherheit ober- und unterhalb des BS

Die weltweit sichersten kommerziellen AI PCs* bereitgestellt von Dell und Intel®. Machen Sie Ihren Gerätebestand zukunftssicher und bleiben Sie Cyberangriffen mit mehreren Abwehrebenen einen Schritt voraus.

Juli 2025



Zusammenfassung

- Die Sicherheit von Geschäftsdaten zu gewährleisten, ist eine schwierige Aufgabe, die durch die zunehmende Verbreitung von Endgeräten außerhalb des Unternehmensnetzwerks und die ständige Weiterentwicklung von Bedrohungsvektoren noch erschwert wird.
- KI ist auf den Geräten angekommen und bringt nicht nur Raum für Innovationen sondern auch eine größere Angriffsfläche mit. Angesichts der Vielzahl von Modellen und KI-Funktionen besteht nun das Risiko, dass sensible Daten durch Anwendungen wie GenAI offengelegt werden.
- Dell und Intel setzen sich dafür ein, die Netzwerke von gewerblichen Kunden mit mehreren Abwehrebenen zu schützen.
- Dell kombiniert integrierte Hardware- und Firmwaresicherheit mit chipbasierten Schutzmaßnahmen von Intel, um die tiefsten Ebenen eines Geräts vor grundlegenden Angriffen zu schützen.
- Wir stärken diese „unterhalb des Betriebssystems“ liegenden Abwehrmaßnahmen mit intelligenten Softwarelösungen aus unserem Partner-Ökosystem für erweiterten Schutz vor Bedrohungen.
- Zusätzlich zu diesem Ansatz haben Dell und Intel in Praktiken und Policies investiert, um Plattformen auch nach ihrer Markteinführung und bei Angriffen durch böswillige Akteure kontinuierlich zu schützen.

Themen in diesem Whitepaper

Grundlage für mehr Sicherheit

Sicherer Entwicklungslebenszyklus: Dell und Intel entwickeln ihre Produkte mit Sicherheit als oberstem Gebot und testen sie vor der Markteinführung gründlich.

Sicherheit entlang der Lieferkette: Schutzmaßnahmen entlang der gesamten Lieferkette sorgen dafür, dass die Geräte nach Verlassen des Werks weiter geschützt sind.

Umfassendes Abwehrframework

Integrierte Sicherheit: Strenge Lieferkettenkontrollen und optionale Sicherheitsmaßnahmen sorgen dafür, dass Kunden ab dem ersten Start geschützt sind.

Integrierte Sicherheit:

- Hardware- und firmwarebasierte Sicherheitsfunktionen schützen Geräte vor Bedrohungen, die auf ihre grundlegenden Ebenen abzielen, beispielsweise das BIOS.
- Chipbasierte Schutzmaßnahmen bieten eine grundlegende Ebene, die die Zuverlässigkeit und Vertrauenswürdigkeit von AI PCs gewährleistet.

Integrierte Sicherheit: Softwarebasierte Sicherheit bietet erweiterten Schutz für Endpunkte, Netzwerke und Cloud-Umgebungen – entscheidend für die moderne Gerätesicherheit.

Fortlaufender Support: Dell und Intel arbeiten kontinuierlich daran, die Sicherheit unserer Produkte zu gewährleisten, Sicherheitslücken zu schließen und die chipbasierte Sicherheit innerhalb des Betriebssystems zu aktualisieren.

Wichtige Sicherheitstrends

1. In Endpoint Security Market Insights, Forrester Research, Inc., März 2025, erläutert das Unternehmen „Endpunkte … gehören zu den primären Zielen externer Angriffe auf Unternehmen, die in den letzten 12 Monaten eine Sicherheitsverletzung erlebt haben“.

2. Laut dem Global Threat Report 2025 von CrowdStrike machen dateilose Malware-Angriffe mittlerweile 79 % aller Angriffe aus. Dabei handelt es sich um Angriffe auf den Arbeitsspeicher, die aufgrund schwerer zu erkennen sind.

3. Laut einem Forschungsbericht der Enterprise Strategy Group vom Mai 2023 geben mehr als 75 % der Unternehmen an, dass sie mindestens einen Cyberangriff erlebt haben, der durch ein unbekanntes, nicht gemanagtes oder schlecht gemanagtes Endgerät verursacht wurde.

Einführung

Ihr Netzwerk ist nur so sicher wie sein schwächster Endpunkt

Sicherheit beginnt viel früher, als Sie vielleicht denken. Es scheint, als ob alle paar Monate ein anderes renommiertes globales Unternehmen Opfer einer größeren Sicherheitsverletzung wird. Auch die damit verbundene negative Berichterstattung fügt dem Ruf dieser Unternehmen ernsthaften Schaden zu. Auf jeden Fall reicht dies aus, um Unternehmensverantwortliche und SicherheitsexpertInnen in Sorge zu versetzen, dass auch sie gefährdet sind – sei es durch eine übersehene Sicherheitslücke in ihren Geräten oder eine unbekannte ausnutzbare Schwachstelle in ihrer Software. Sie können sich vielleicht darauf verlassen, dass Ihr IT-Team Ihre Netzwerke schützt und datenschutzkonforme Verfahren anwendet, aber wie können Sie all den Endgeräten und Anwendungen vertrauen, auf die sich Ihre Geschäftsaktivitäten stützen, wenn Sie keinen Einblick in deren Herstellung oder Entwicklung hatten?

Rein softwarebasierte Sicherheit reicht nicht aus. Eine sehr weit verbreitete und doch mangelhafte Herangehensweise zum Schutz der Geräteintegrität ist der Versuch, mit reinen Softwarelösungen ein falsches Sicherheitsgefühl zu erzeugen, ohne die zugrunde liegenden hardwarebasierten Sicherheitslücken wirklich anzugehen. Für Führungskräfte ist es wichtig, die Grenzen dieser Strategie zu verstehen: Wenn sie sich beim Schutz ihres Unternehmens nur auf Software verlassen, um ihr Unternehmen zu schützen, setzen sie die Hardware, auf der die Software ausgeführt wird, potenziellen Angriffen aus. Und wenn die Hardware nicht sicher ist, können die darauf laufenden Sicherheitsanwendungen und -technologien auch nicht sicher sein.

Andere Anbieter versuchen, einen sogenannten „Walled Garden“ zum Schutz der Geräte zu errichten, bei dem in die Anwendungen und Services Beschränkungen eingebaut werden, die die Flexibilität der NutzerInnen einschränken. Dies mag für PrivatanwenderInnen sinnvoll erscheinen, geht aber zulasten der Freiheit, die Geräte vollumfänglich nutzen zu können – ein Problem, das sich im kommerziellen Kontext noch verschärft. Dieser Ansatz kann auch dazu führen, dass AngreiferInnen zunehmend diese Systeme ins Visier nehmen und versuchen, Sicherheitslücken in gängigen Konfigurationen aufzuspüren und auszunutzen.

Einfach ausgedrückt: Was bei Geräten, die direkt für EndanwenderInnen bereitgestellt werden, funktioniert, scheitert oft in kommerziellen Umgebungen, die für Angreifer ein attraktiveres Ziel darstellen. Genau deshalb verfolgen Dell und Intel einen anderen, ganzheitlichen Sicherheitsansatz. Dell und Intel wissen, dass die einzige Möglichkeit für einen zuverlässigen Schutz von Unternehmensgeräten und -netzwerken in der Harmonisierung von hard- und softwarebasierten Sicherheitstechnologien liegt. Während unsere Teams sich zusammengetan haben, um ein ganzes Geflecht aus eng integrierten hard- und softwarebasierten Sicherheitsfunktionen zu entwickeln, haben andere Anbieter diese Investition möglicherweise nicht getätigt.

Hardwarebasierte Sicherheit für den kommerziellen AI PC

Jeder PC wird ein AI PC sein. Der Marktforschungsdienst Canalys prognostiziert, dass AI PCs in den kommenden sechs Jahren den gesamten PC-Markt übernehmen werden. Das bedeutet, dass PCs ohne integrierte KI-Funktionen bis 2030 nicht mehr verkauft werden. Um Ihr Unternehmen zukunftssicher zu machen, sollten Sie daher bereits jetzt Maßnahmen ergreifen. Die gute Nachricht: Dell und Intel unterstützen Kunden bei der Bewältigung der sich weiterentwickelnden IT- und Sicherheitslandschaft mit kommerziellen AI PCs, die die notwendigen grundlegenden Sicherheitsfunktionen, Geschwindigkeit und Effizienz bieten, um moderne Bedrohungen effektiv zu bekämpfen.

Das ist jedoch keine einfache Aufgabe. Die Komplexität und Bedenken beim Schutz von Geräten und Netzwerken können schnell überfordern – und neue KI-Technologien gestalten diese Aufgabe komplexer. Deshalb möchten wir unseren Kunden Geräte zur Verfügung stellen, bei deren Konzeption stets die Sicherheit im Vordergrund steht, damit sie sich auf das Wesentliche konzentrieren können – den Betrieb ihres Unternehmens. Die gemeinsame Entwicklungsarbeit von Dell und Intel erstreckt sich bereits über mehrere Jahrzehnte. Im Fokus stand dabei stets die Sicherheit der Daten unserer Kunden, insbesondere im B2B-Bereich. Durch seine Partnerschaft mit Intel hat sich Dell einen Ruf als führender Anbieter von Mitarbeitergeräten für Unternehmen jeder Größe und Branche erworben. Was steckt alles in einem kommerziellen KI-Gerät von Dell? Auf jeden Fall mehr als eine willkürliche Ansammlung von Funktionen. Intel und Dell kombinieren Technologien, Tools und Policies über den gesamten PC-Lebenszyklus hinweg, um unseren Kunden und ihren Unternehmen End-to-End-Sicherheit zu bieten.

Sicherheit per Design

Intel und Dell schauen bei der Entwicklung der Systeme von morgen über die aktuellen Bedrohungen hinaus, um die Angriffsfläche zu minimieren und die Geräte zu schützen.

Schutz während des Transports

Wir verfügen über entsprechende Technologien und Policies, um die Integrität der Geräte auch auf deren Weg zu Ihnen zu schützen. So kann die Sicherheit während der gesamten Prozesse der Beschaffung, Herstellung und Lieferung der Komponenten aufrechterhalten werden.

Gewappnet gegen künftige Bedrohungen

Wir setzen hardwarebasierte Sicherheit über Dell Trusted Devices und Intel vPro® Security-Funktionen ein, um Geräte zu schützen, die primäre Cybersicherheitsanwendungsfälle für Prävention, Erkennung, Reaktion, Recovery und Korrektur erfüllen. Darüber hinaus verfügen Dell und Intel über spezielle Sicherheitsteams, die die Produkte stichprobenartig untersuchen und neue Sicherheitslücken aufspüren, bevor sie von Angreifern entdeckt werden, und dann umgehend Patches bereitstellen, damit Sie und Ihr Team geschützt sind.

In diesem Whitepaper erfahren Sie, wie Dell und Intel gemeinsam kommerzielle AI PC-Plattformen mit integrierter Sicherheit auf tiefster Ebene entwickeln, um Ihre Geräte während ihres gesamten Lebenszyklus, bis zur nächsten Aktualisierung und darüber hinaus zu schützen.

Cybersicherheit und GenAI – ein zweischneidiges Schwert

So wie Cyberabwehrspezialisten GenAI für gute Zwecke nutzen, versuchen Cyberangreifer, ihre eigenen bösartigen Ziele voranzutreiben und raffiniertere Angriffe schneller und in großem Umfang zu starten.

Auch wenn GenAI-Anwendungsfälle noch in den Kinderschuhen stecken und täglich zunehmen, ist es wichtig, einige wichtige Konzepte im interkopf zu behalten. Erstens gibt es eine Reihe von Bedrohungen, die GenAI für Unternehmen darstellen kann, einschließlich:

- Probleme mit Datenschutz und -integrität
- Complianceprobleme
- und Verstöße gegen das geistige Eigentumsrecht

Darüber hinaus sehen wir eine Reihe von Möglichkeiten, wie GenAI im Kampf um die Sicherheit helfen kann, unter anderem:

- Erkennung von Advanced Threats
- Spezialisierte und gezielte Schulungen für MitarbeiterInnen und
- Automation

Dell und Intel arbeiten aktiv daran, eine bessere Bedrohungsmodellierung speziell für GenAI zu ermöglichen. Dies kann die Vermeidung von Datenverlusten, das Management von Datenrechten, erweiterte Phishing-Schutzmaßnahmen, Modellmanipulationen, behördliche Auflagen und Compliance umfassen – jeweils mit den entsprechenden Kontrollen.

Dell kann Ihnen auch helfen, Ihre GenAI-Landschaft in Bezug auf Sicherheit mit Programmen zum Sicherheitsmanagement und Penetrationstests zu testen, um mit der sich entwickelnden Bedrohungslandschaft Schritt zu halten.

Grundlage für mehr Sicherheit

Sicherer Entwicklungslebenszyklus

Der Schutz unserer Plattformen beginnt am Whiteboard

Planung, Bewertung und Analyse

Vor der Entwicklung neuer Plattformen und Chipsätze legen die ExpertInnen von Dell und Intel strenge Parameter für die Sicherheit fest, damit auch künftige Sicherheitsanforderungen erfüllt und geltende Sicherheitsbestimmungen eingehalten werden. Dieser Prozess beginnt mit einer interaktiven Diskussionsrunde, in der die zu erwartenden künftigen Sicherheits- und Datenschutzrisiken mit den passenden Gegenmaßnahmen ermittelt werden. Außerdem werden bei der Bewertung die Sicherheitsziele definiert, an denen sich unsere Architekturen messen lassen müssen. Anhand dieser Informationen entwickeln die Sicherheitsteams von Dell und Intel dann Bedrohungsmodelle. Dazu gehen sie diese konzeptionelle Architektur aus Angreifersicht an und suchen nach potenziellen Schwachstellen und Exploits, die behoben werden müssen. Wie sich gezeigt hat, bewirkt ein solches Vorgehen deutliche Verbesserungen beim Ermitteln und Behandeln potenzieller Sicherheitslücken im BIOS-, Firmware- und Hardwaredesign.

Sicherheitsorientiertes Design

Wenn die Bedrohungsbewertung abgeschlossen ist und Modelle erstellt wurden, um die Angriffsfläche und die Schwerpunkte für Tests zu ermitteln, beginnen die IngenieurInnen und TechnikerInnen mit der Entwicklung des Produktcodes. Die in der vorangegangenen Phase definierten Sicherheitsziele dienen in dieser Entwicklungsphase als Orientierungshilfe und zugleich als Kriterien, um festzustellen, ob das Produkt die Anforderungen unserer Kunden erfüllen kann.

Verifizierung und Tests

Sobald der Code so weit optimiert ist, dass er die zu Beginn des Entwicklungslebenszyklus festgelegten Sicherheitsziele erfüllt, schließt sich ein rigoroser Testprozess für das Produkt an. Diese Tests beginnen in der Regel mit der Überprüfung, ob der Code sicher ist, sowie mit einer statischen Codeanalyse. Dies ist ein automatisierter Prozess, bei dem spezielle Tools zum Auffinden und Beheben von Fehlern zur Anwendung kommen. Einige Produkte mit komplizierterem Code werden dann einem manuellen Prüfprozess unterzogen, bei dem SicherheitsexpertInnen den Produktcode Zeile für Zeile durchgehen, um zuvor unbekannte Fehler aufzuspüren und sicherzustellen, dass der Code auf sichere Weise entwickelt wurde. Zum Abschluss werden Teams aus erfahrenen HackerInnen für Penetrationstests, Fuzzing und andere Red-Team-Aktivitäten hinzugezogen, um potenzielle Sicherheitslücken zu finden, die in den vorhergehenden Phasen übersehen wurden. Die so aufgedeckten Schwachstellen werden ebenfalls anhand des Risikos behandelt, damit sichergestellt ist, dass alle ermittelten zusätzlichen Sicherheitslücken dokumentiert und korrigiert wurden.

Markteinführung und darauffolgende Phasen

Wenn das Produkt umfassend getestet wurde und nachweislich die zu Beginn definierten Sicherheitsziele erfüllt oder übertrifft, kann es auf den Markt gebracht werden. Diese Phasen stellen jedoch nur einen Ausschnitt aus dem Lebenszyklus der sicheren Entwicklung dar. Für Dell und Intel ist die Sicherheit unserer Plattformen ein fortlaufendes Bestreben. So suchen unsere Teams kontinuierlich nach Sicherheitslücken, um sie vor den möglichen AngreiferInnen zu finden, und entwickeln und veröffentlichen Sicherheitsupdates mit Patches für diese Lücken. Ein Beispiel für das Engagement von Dell und Intel für End-to-End-Sicherheit ist unsere Investition in eine sichere Lieferkette zwischen Montage und Auslieferung eines Geräts, denn die Lieferkette ist einer der am schnellsten wachsenden Angriffsvektoren für böswillige AkteurInnen. Im nächsten Abschnitt erfahren Sie, wie Dell und Intel die Risiken entlang ihrer Lieferketten minimieren, um sicherzustellen, dass das Gerät, das Sie erhalten, vom ersten Einschalten an sicher ist.

Lieferkettensicherheit

Eine sichere Lieferkette ist für Gerätesicherheit entscheidend

Zwischen dem Zeitpunkt, an dem ein Bauteil oder Gerät das Werk verlässt und an seinem Ziel ankommt, kann viel passieren. Jede Phase der Lieferkette stellt einen neuen Vektor dar, der Ihre Belegschaft, Ihr Unternehmen und Ihre KundInnen für potenzielle Angriffe anfällig macht. Dell und Intel haben Tools, Technologien und Prozesse entwickelt, um dafür zu sorgen, dass unsere Produkte sicher beim Kunden eintreffen, und eine Selbstverifizierung der Geräteauthentizität vor der Bereitstellung bei den MitarbeiterInnen zu ermöglichen.

Quelle
Dell wendet einen strengen Prozess zur Überprüfung von Partnern an, um die Qualität und Sicherheit von Geräten und deren Komponenten sicherzustellen. Diese Partner müssen zudem regelmäßig Audits durchlaufen, bei denen die Einhaltung der umfassenden Dell Standards für Lieferkettensicherheit überprüft wird.

Herstellung
Die von Dell beauftragten Gerätehersteller müssen nicht nur die Dell Standards für Lieferkettensicherheit einhalten, sondern Teile bei der Fertigung auch häufig testen, damit keine gefälschten Produkte in die Lieferkette gelangen. Um dieses Risiko noch weiter zu mindern, werden bestimmte besonders fälschungsgefährdete Komponenten mit eindeutigen PPID-Etiketten (Piece Part Identification) versehen. Darauf sind Informationen zum Lieferanten, die Teilenummer, das Ursprungsland und das Fertigungsdatum angegeben, damit Dell diese Komponenten identifizieren, authentifizieren, nachverfolgen und schließlich validieren kann. So wird sichergestellt, dass Kunden tatsächlich die versandten Produkte erhalten.

Lieferung
Dell schützt Fracht durch mehrstufige physische Sicherheit, u. a. mit manipulationssicheren Siegeln, Schließmechanismen und verschiedenen Trackinggeräten, die erkennen sollen, ob die enthaltenen Dell Geräte beim Transport manipuliert wurden.

Auch die Dell Geräte an sich sind mit Technologien zur Manipulationserkennung ausgestattet. Dell SafeSupply Chain-Lösungen umfassen Lieferkettensicherheit und Integritätskontrollen wie manipulationssichere Siegel und Festplattenlöschung auf NIST-Ebene, um das gute Image Ihres Unternehmens aufrechtzuerhalten.

Überprüfen
Die KI-Geräte von Dell werden mit kryptografisch signierten Plattformzertifikaten ausgeliefert, die zur Erfassung von Snapshot-Attributen der Plattformen bei Fertigung, Zusammenstellung, Tests und Integration dienen. Diese Plattformattribute werden dann unter Verwendung von Trusted Platform Module (TPM) als vertrauenswürdige Hardware („Root of Trust“) kryptografisch mit dem jeweiligen Gerät verknüpft.

Erfahren Sie mehr über die gemeinsamen Bemühungen von Dell und Intel zur Sicherung der Lieferkette. Hier finden Sie das Interview ***mit SiliconANGLE***

Dell hat TCG-Plattformzertifikate (Trusted Computing Group) innerhalb der Dell Secured Component Verification (SCV)-Lösung für kommerzielle AI PCs mit Intel Prozessoren implementiert (Zertifikat ist sowohl auf Geräten (für Bundesbehörden) als auch in der Cloud für gewerbliche Kunden verfügbar). SCV liefert der IT-Abteilung kryptografisch signierte Bestandszertifikate für unterstützte Dell Geräte. Mit sicheren Tools zur Selbstverifizierung trägt die bei Dell einzigartige Verifizierungsmethode SCV* dazu bei, vollständige Hardwareintegrität während des Transports zu den IT-Umgebungen zu gewährleisten. Außerdem können die Kunden damit überprüfen, ob die AI PCs von Dell und zentrale Komponenten so ankommen, wie sie bestellt und gefertigt wurden.

Umfassendes Abwehrframework

Sicherheit unterhalb der Betriebssystemebene

Integrierte Sicherheitstechnologien tragen dazu bei, Bedrohungen vorzubeugen, zu erkennen, darauf zu reagieren und deren Folgen zu überwinden

Ganzheitliche Sicherheit bedeutet, über das herkömmliche Modell des Softwareschutzes hinauszugehen, um mit neuen Arten von Bedrohungen der digitalen Sicherheit und des Datenschutzes Schritt zu halten. Durch die Kombination mit hardwarebasierten Sicherheitstechnologien „unterhalb des Betriebssystems“ bleibt jede Ebene des Compute-Stacks geschützt, da grundlegende Angriffe erkannt und verhindert werden, einschließlich der Bedrohungsvarianten, die am häufigsten entlang der Lieferkette auftreten. Schwerpunkt der gemeinsamen Entwicklungsarbeit von Dell und Intel war, diese Angriffsfläche durch ein komplexes Geflecht von Technologien sowohl auf Komponenten- als auch auf Plattformebene abzudecken.

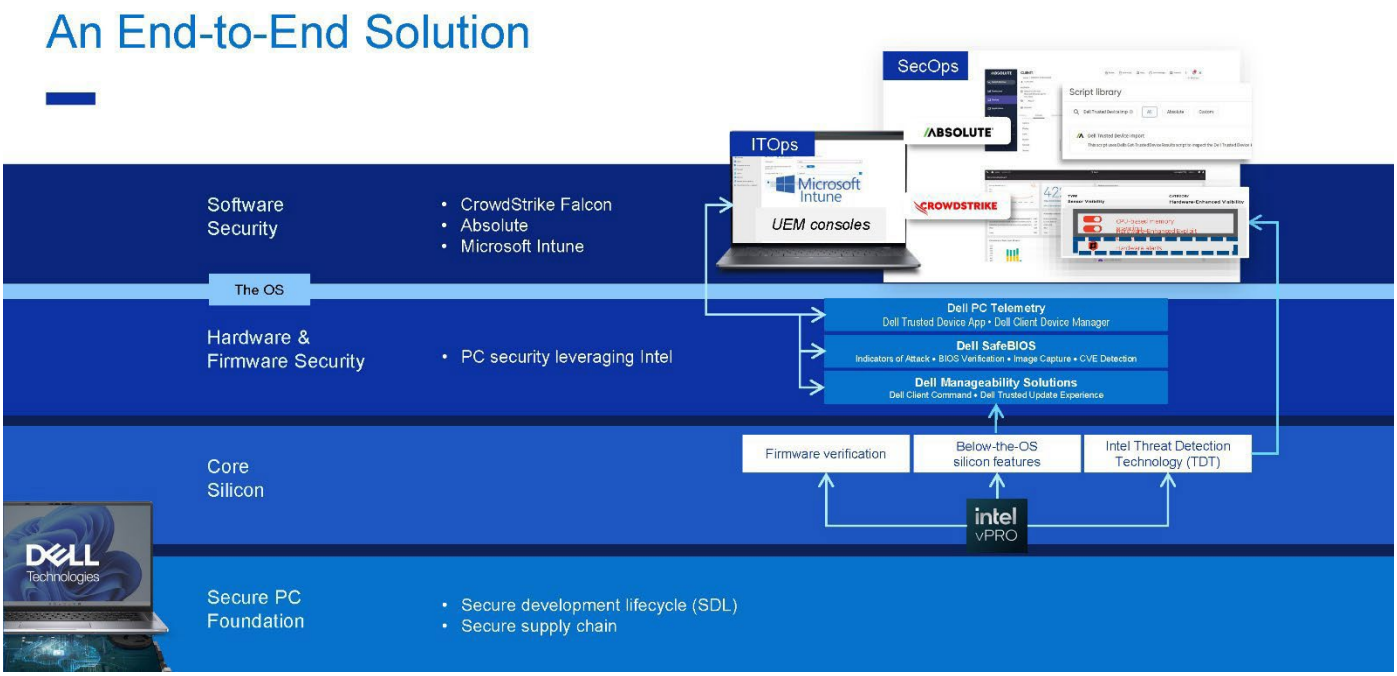


Abbildung 1: Effektive Sicherheit erfordert heute mehrere Ebenen von Angriffsbekämpfungsmaßnahmen. Dell und Intel arbeiten mit Softwarepartnern zusammen, um eine umfassende Abwehr bereitzustellen.

Wir haben die Lieferkette und die sichere AI PC-Grundlage, die Dell und Intel bieten, bereits behandelt. Sehen wir uns nun die mittleren Ebenen an.

Intel vPro® Security

Intel vPro Security ist in jedem Gerät von Dell enthalten, das auf der Intel vPro® Plattform ausgeführt wird, und bietet hardwareoptimierte Sicherheitsfunktionen, die dazu beitragen, alle Schichten im Compute-Stack zu schützen. Diese Sammlung von Sicherheitstechnologien trägt dazu bei, moderne Bedrohungen auf jeder Ebene abzuwehren: Hardware, BIOS/Firmware, Hypervisor, VMs, BS und Anwendungen.

Integrierte Hardware- und Firmwaresicherheit von Dell

Der Schutz des BIOS (Basic Input Output System) ist für die Gerätesicherheit von entscheidender Bedeutung. Wenn es AngreiferInnen gelingt, das BIOS eines Geräts zu kompromittieren, könnten sie aufgrund der einzigartigen und privilegierten Position des BIOS innerhalb der Gerätearchitektur die Kontrolle über das gesamte Gerät erlangen. Zum Schutz dieser kritischen Ebene besitzen kommerzielle KI-Geräte von Dell SafeBIOS, eine Suite mit mehrschichtiger Sicherheit auf Firmwareebene. Die zugrunde liegenden Funktionen von SafeBIOS verbessern Schutz, Erkennung und Recovery auf BIOS-Ebene.

Abbildung 2: Laut Principled Technologies stellen Dell und Intel die weltweit sichersten AI PCs bereit.*

Zu effektiver Sicherheit gehört auch ein Überblick über die aktuelle Sicherheitslage. Dell macht diese Ereignisse unterhalb des Betriebssystems von SafeBIOS auf Betriebssystemebene sichtbar, damit AdministratorInnen und EndnutzerInnen mit der Dell Trusted Device-Anwendung (DTD-App) Entscheidungen treffen können. Die DTD-App erkennt, ob das BIOS kompromittiert wurde, indem sie Messungen des ausgeführten BIOS-Images mit denen der in der Dell Umgebung gesicherten Goldkopie vergleicht, und bietet so eine marktweit einzigartige BIOS-Verifizierung außerhalb des Hosts. Darüber hinaus schützt die Firmware-Verifizierung der Intel Management Engine (ME), die ausschließlich auf kommerziellen Dell PCs verfügbar ist, vor unbefugtem Zugriff auf und Manipulation von hochprivilegierter Firmware.

Diese einzigartige PC-Telemetrie von Dell (verfügbar über den Dell Client Device Manager (DCDM) für verwaltete IT-Umgebungen oder die DTD-App-Konsole für nicht verwaltete Umgebungen) ist der Schlüssel zum Erfolg in der Sicherheitsgleichung. Diese Telemetrie ermöglicht die Integration in Drittanbieter-Konsolen wie CrowdStrike und Absolute für die Sicherheit sowie Microsoft Intune für die Verwaltung (siehe Abbildung 1). Tatsächlich ist Dell der einzige PC-Hersteller, der die Integration und Transparenz der Bedrohungserkennung auf Firmwareebene über Sicherheitskonsolen von Drittanbietern bietet.*

Dell mindert außerdem das wachsende Risiko von Identitätsdiebstahl und unbefugtem Zugriff auf sensible Workloads. Zu den ausgewählten kommerziellen Dell Geräten gehören Dell SafeID mit ControlVault 3+, ein einzigartiger, nach FIPS 140-3 Level 3 zertifizierter Sicherheitschip*, der Endnutzerzugangsdaten speichert und sie vom Betriebssystem isoliert, wodurch sie weitaus weniger anfällig für Angriffe sind.

Die Sicherheit unterhalb des Betriebssystems ist nur ein Teil des ganzheitlichen Ansatzes von Dell zur Sicherung von Geräten

Um die kommerziellen KI-Geräte von Dell vollständig zu schützen, haben Dell und Intel auch stark in die Überprüfung und Pflege eines Ökosystems branchenführender Softwaresicherheitslösungen investiert. Diese Funktionen bieten Schutz vor Advanced Threats, die von ausgefeilten Angreifern ausgehen, und bieten zusätzlichen Schutz auf Daten- und Anwendungsebene.

Auch hier können Dell und Intel Softwaretechnologien mit PC-Telemetrie unterhalb des Betriebssystems erweitern, um die Erkennung von Bedrohungen sowie die Reaktion darauf zu verbessern.

Sicherheit oberhalb der Betriebssystemebene

Integrierte Softwaresicherheit bietet erweiterten Bedrohungsschutz

Angesichts der potenziellen Ausbeute, die schon ein einziger erfolgreicher Angriff verspricht, sind Cyberangreifer hochmotiviert und machen im Laufe der Lebensdauer oft Dutzende von Versuchen auf einem einzigen Gerät. Über den Gerätebestand eines Unternehmens hinweg summiert sich dies zu einem ernsthaften Problem. Können Sie das Risiko eingehen, dass ein Angriff Ihre Abwehr durchbricht? Eines ist sicher: Keine Lösung kann Angriffe zu 100 % abwehren. Dies gilt für die Endpunkte in Ihrem Gerätebestand genauso wie die Netzwerke und Cloud-Umgebungen, in denen sie betrieben werden. Intelligente Softwarelösungen können dazu beitragen, Bedrohungen zu verhindern, zu erkennen, darauf zu reagieren und sich von ihren Folgen zu erholen, wo immer sie auftreten. Aus diesem Grund umfasst das Endpoint Security-Portfolio von Dell Trusted Workspace branchenführende Software, die die Beschaffung vereinfacht und Führungskräften alles bietet, was sie für die Verteidigung ihrer Endpunkte benötigen. Zu den Funktionen gehören:

- Prävention, Erkennung, Reaktion und Korrektur in Endpunkt-, Netzwerk- und Cloud-Umgebungen durch Nutzung von KI und maschinellem Lernen
- Geolokalisierung von Endpunkten, Geofencing, Remotedatenlöschung sowie automatische Fehlerkorrektur für kritische Anwendungen, innerhalb oder außerhalb des Netzwerks
- Security Service Edge-Lösungen für einen datenzentrierten Ansatz für Cloud-Sicherheit und -Zugriff, der Daten und NutzerInnen überall schützt

Die tief im Chip integrierten Sicherheitsfunktionen von Intel, z. B. die Intel Control-flow Enforcement Technology, schützen vor Angriffen auf das Betriebssystem, während andere Funktionen von Intel vPro® Security unterhalb der Betriebssystemebene Anwendungen und Daten schützen sowie Advanced-Threat-Schutz bieten.

Hardwaregestützte Sicherheit

Integrierte Sicherheit

Angreifer richten ihre Angriffe zunehmend auf den gesamten Computing-Stack eines Unternehmens, der bisher nur unzureichend einsehbar und kontrollierbar war. Diese sich weiterentwickelnden Bedrohungen umgehen die Sicherheitstools für Legacy-Endpoint Detection and Response (EDR), weshalb die PC-Sicherheit von entscheidender Bedeutung ist. Um modernen, sich schnell weiterentwickelnden Bedrohungen einen Schritt voraus zu bleiben, bedarf es einer umfassenden Zusammenarbeit innerhalb des Ökosystems, um herstellerübergreifende Schutzmaßnahmen für Angriffsflächen zu einer einheitlichen Lösung zu verbinden.

Diese Back-end-Integrationsarbeit ist jedoch komplex und erfordert einen hohen Zeit- und Ressourcenaufwand. Um dieses Problem zu lösen, haben Dell und Intel ihr tiefgreifendes Verständnis der Problembereiche von Angreifern und Kunden genutzt, um gemeinsam mit Partnern eine integrierte Hardware- und Softwarelösung namens „Hardwaregestützte Sicherheit“ zu entwickeln. Dell liefert nicht nur sichere AI PCs mit führenden Softwarepartnern, sondern bereichert mit seiner einzigartigen Gerätetelemetrie* das gesamte Sicherheitsökosystem und sorgt so für mehr Transparenz auf BIOS-Ebene in Ihrem Gerätebestand. Diese Integrationsfähigkeit ist entscheidend, um die IT-Sicherheitslücke zu schließen, mit der so viele Unternehmen heute zu kämpfen haben. Dank Dell, Intel und unserem Partnernetzwerk kommunizieren Hardware und Software miteinander, um die Sicherheit und Verwaltbarkeit des Gerätebestands zu verbessern.

Abbildung 3: Neue Cyberbedrohungen umgehen rein softwarebasierte Abwehrmaßnahmen. Verkleinern Sie die Angriffsfläche von Endpunkten mithilfe von hardwaregestütztem Schutz.

Hardwaregestützte Sicherheit mit Dell, Intel und CrowdStrike im Mittelpunkt

Dell, Intel und CrowdStrike haben gemeinsam Funktionen zur Erkennung und Abwehr von Bedrohungen entwickelt, die die Leistungsfähigkeit von Dell Trusted Devices, den weltweit sichersten kommerziellen AI PCs*, mit den Intel Chiptechnologien und den Funktionen von CrowdStrike, einem Unternehmen im Gartner Magic Quadrant 2024 kombinieren. Die mehrschichtige Lösung von CrowdStrike, Dell und Intel definiert die Endgerätesicherheit für Ihr Unternehmen neu und reicht über den Softwareschutz hinaus bis hin zur hardwaregestützten Sicherheit.

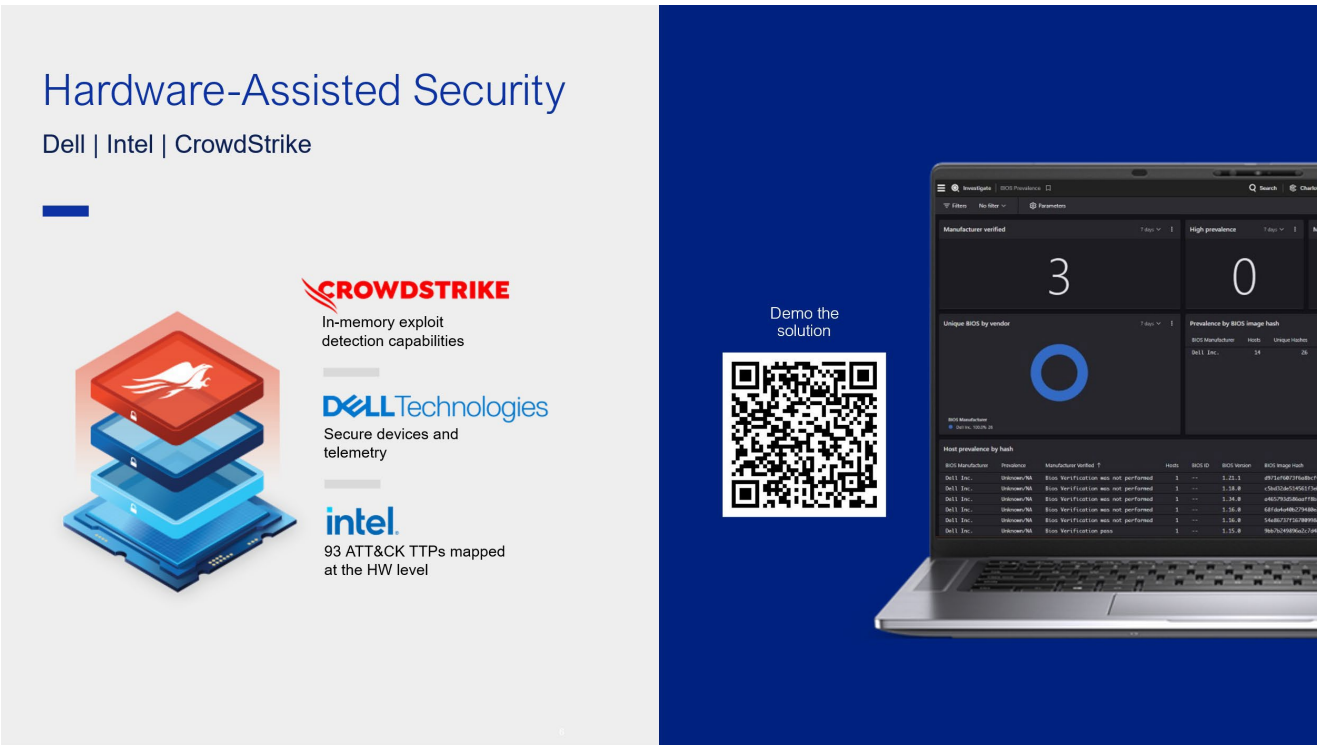


Abbildung 4: Mehrschichtige Sicherheit auf Dell AI PCs, integriert in CrowdStrike und Intel.

Zusätzlicher Nutzen der Integration von Intel und CrowdStrike auf Dell AI PCs

Verbesserung der Endpunktsicherheit durch KI und GPU-/NPU-Beschleunigung: Cyberbedrohungen werden immer ausgefeilter, und AI PCs sind darauf ausgelegt, durch die Verwendung von KI auf Geräten eine schnellere Bedrohungserkennung in Echtzeit zu ermöglichen und gleichzeitig die Abhängigkeit von Cloud-Services zu reduzieren. Tools wie CrowdStrike können die Malware-Erkennung auf integrierte Neural Processing Units (NPUs) auslagern und Bedrohungen schneller erkennen, ohne die CPU-Leistung zu beeinträchtigen. Mit lokaler Datenverarbeitung und erweiterten Anti-Phishing-Funktionen auf Intel-basierten AI PCs bleiben vertrauliche Informationen sicher und sind weniger externen Risiken ausgesetzt.

Einige Beispiele für die Arbeit von Intel und CrowdStrike (derzeit in der Proof-of-Concept-Phase, aber in den kommenden Monaten öffentlich verfügbar) zur Verbesserung der Endpunktsicherheit durch KI und NPU-Beschleunigung:

- Hardware Enhanced Exploit Detection (HEED): Verwendet Intel CPU-Telemetrie, um den Kontrollfluss von Anwendungen nachzuverfolgen und Angriffe auf den Arbeitsspeicher zu erkennen.
- Accelerated Memory Scanning (AMS): Nutzt die Intel Threat Detection Technology, um rechenintensive Arbeitsspeicherscans auf die integrierte Intel GPU auszulagern und so die Arbeitsspeicherscan-Leistung auf das bis zu Siebenfache zu steigern.

Mit diesen beiden Funktionen leistet Intel einen wesentlichen Beitrag zur Bereitstellung der KI-gestützten Indikatoren von CrowdStrike für Angriffe auf Endgeräte und die CrowdStrike-Sicherheitscloud. Diese Funktionen bieten CrowdStrike außerdem neue Einblicke in die Speicherschicht, sodass in Zukunft neue Scanerkennungsmodelle implementiert werden können, um die Sicherheit noch weiter zu verbessern.

Branchenvalidierte Verteidigung der AI PC-Sicherheit: Neue Untersuchungen von MITRE belegen, dass Ihre Wahl der PC-Hardware eine entscheidende Rolle dabei spielt, dass Sicherheitssoftware und Betriebssystemfunktionen Ihre Ressourcen effektiv schützen können.

Sicherheitsteams (SecOps) stellen leistungsstarke Agents über Endpunkt-PC-Bestände hinweg bereit, um jeden Prozess auf Anzeichen von Malware zu überprüfen. Sicherheitssoftwareanbieter bilden ihre Fähigkeiten anhand des MITRE ATT&CK-Frameworks ab, um aufzuzeigen, wo sie Lösungen bereitstellen. Managed Security Provider helfen Unternehmen bei der Priorisierung täglicher Warnmeldungen in XDR-, SIEM- und Co-Pilot-Sicherheitstools. Das klingt recht komplex, doch die Frage, inwieweit Hardwaresicherheit in bereits vorhandenen PCs vor realen Angriffen schützen kann, blieb bislang ungeklärt … bis jetzt.

Ende 2024 hat das MITRE Center for Informed Defense* (CTID) in Zusammenarbeit mit mehr als 30 ExpertInnen von Intel, Microsoft, CrowdStrike und ATTACK IQ die Bedeutung hardwareoptimierter Sicherheitssoftwarefunktionen anhand der Taktiken und (Sub-)Techniken des MITRE ATTACK-Frameworks erfasst und bewertet. Gemeinsam ordnete die Gruppe die Intel vPro® Sicherheitsfunktionen 150 kumulativen und einzigartigen Bedrohungstaktiken (Sub-)Techniken und Verfahren (TTPs) zu, bei denen PC-Hardware mit optimierter Sicherheitssoftware sofortigen Schutz bietet.

Für die Validierung von Zuordnungs- und Emulationstests verwendete MITRE einen Dell Pro mit einem Intel Core Ultra Prozessor (einschließlich der vollständigen Intel vPro Sicherheitsschutzmaßnahmen, die auf einem typischen Sicherheitssoftware-Stack der Enterprise-Klasse aktiviert sind), der die einzigartigen integrierten Abwehrmaßnahmen von Dell unterhalb des Betriebssystems ergänzt.

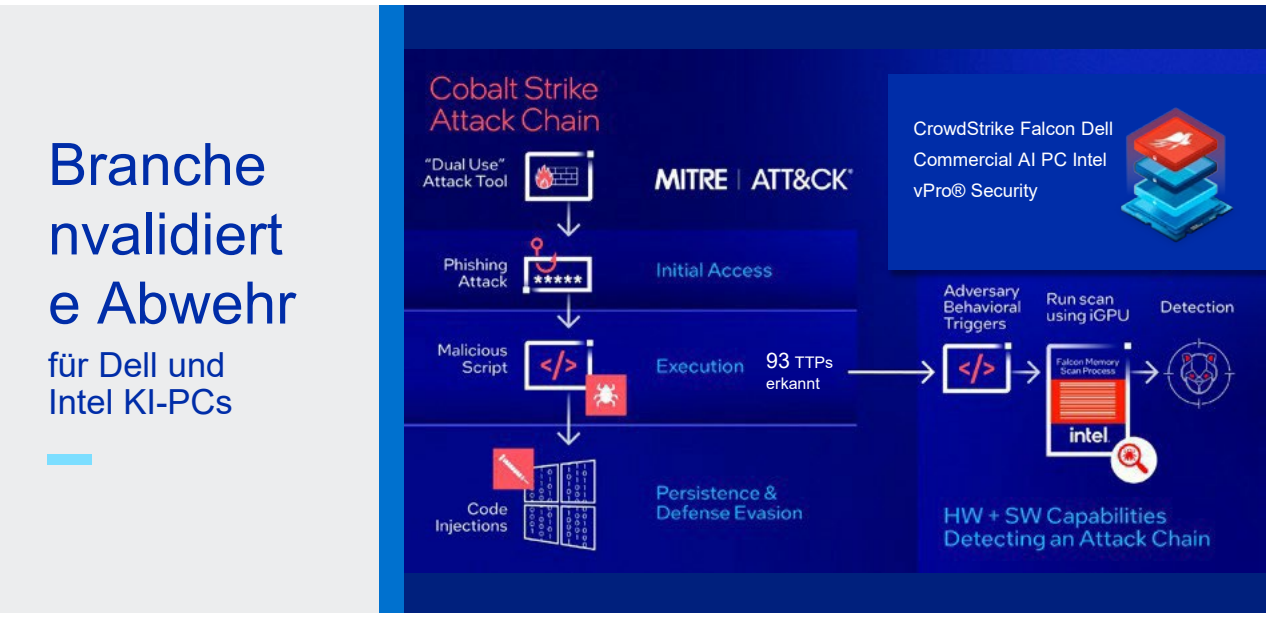


Abbildung 5: Hardwaregestützte Sicherheit funktioniert.

Im Beispielszenario (Cobalt Strike Attack Chain-Szenario) zeigen wir einen dateilosen Cobalt Strike-Angriff auf den Arbeitsspeicher und veranschaulichen, wie CrowdStrike Falcon mithilfe von Hardware Abhilfemaßnahmen bereitstellt. Wie bereits erwähnt, werden dateilose Malware-Angriffe immer beliebter. Fast 75 % aller Angriffstypen nutzen gültige Systemprozesse aus, wie zum Beispiel die Ausführung im Arbeitsspeicher, um herkömmliche EDR-Abwehrmaßnahmen zu umgehen. Dies ist ein gutes Beispiel dafür, wie die Hardware Ihres PCs dazu beiträgt, die erforderliche Rechenleistung bereitzustellen, um den Arbeitsspeicher zu scannen, ohne die Benutzererfahrung zu beeinträchtigen. **Für CrowdStrike, das die beschleunigten Speicherscan-Algorithmen der Intel Threat Detection Technology (Intel TDT) und seine Fähigkeit zur Auslagerung der Verarbeitung auf den integrierten Grafikprozessor der Intel Graphics Technology nutzt, führt dies zu einer Leistungssteigerung um das bis zu Siebenfache. Dies stellt ein gutes Nutzererlebnis sicher und bietet gleichzeitig die Kapazität, tiefer zu scannen und mehr als 93 TTPs zu erkennen.** (Hinweis: Die Arbeitsspeicherscan-Funktion von CrowdStrike funktioniert nur auf Intel vPro PCs.)

Einblicke in software- und hardwarebasierte Sicherheitsmaßnahmen können Unternehmen dabei unterstützen, das volle Potenzial moderner AI PCs zu erschließen. Die Ergebnisse belegen, dass die Auswahl der PC-Hardware einen erheblichen Einfluss auf die Fähigkeit der Sicherheitssoftware und Betriebssystemfunktionen hat, bestimmte Bedrohungen abzuwehren und Unternehmensressourcen vor fortschrittlichen Cyberangriffen zu schützen.

Die Sicherheitsframeworks von Dell und Intel oberhalb und unterhalb der Betriebssystemebene bieten einen ganzheitlichen Ansatz für den Schutz gewerblicher Geräte, aber SicherheitsexpertInnen wissen, dass kein Gerät absolut sicher ist. Aus diesem Grund sind wir branchenführend bei Sicherheitsinvestitionen nach der Veröffentlichung, um sicherzustellen, dass unsere Geräte nach der Veröffentlichung Jahre lang sicher bleiben.

Laufender Support

Dell und Intel investieren nach der Markteinführung in die fortlaufende Sicherheit ihrer Plattformen

Dell und Intel haben über einen längeren Zeitraum erheblich investiert, um Sicherheit im gesamtem Produktlebenszyklus zu gewährleisten. Auch nach der Markteinführung testen die Teams von Dell und Intel ihre Produkte weiterhin aktiv auf Sicherheitslücken. Intel arbeitet zu diesem Zweck mit ForscherInnen und Hochschulen zusammen, um mögliche Schwachstellen schneller als die AngreiferInnen zu erkennen, sie zu patchen und anschließend zu melden.

Die proaktive Produktsicherheit umfasst Maßnahmen zur internen Suche nach Schwachstellen sowie Anreize für die externe Sicherheitsforschungscommunity über Bug Bounty-Programme. Im Jahr 2024 entfielen 96 % der erkannten und behobenen Sicherheitslücken auf die Investitionen von Intel in die proaktive Produktsicherheit. Die verbleibenden 4 % der von Intel behobenen Sicherheitslücken wurden entweder nicht über das Intel Bug Bounty-Programm übermittelt oder von Partnern oder anderen Unternehmen eingereicht, die keine Prämienzahlungen verlangen. In allen Fällen arbeitete Intel mit Forschenden zusammen, um die öffentliche Bekanntmachung dieser Probleme zu koordinieren, sodass den Kunden am Tag der Veröffentlichung entsprechende Abhilfemaßnahmen zur Verfügung standen.

Als Reaktion auf die im Rahmen der umfassenden Programme gefundenen gängigen Sicherheitslücken und Bedrohungen (Common Vulnerabilities and Exposures, CVEs) veröffentlicht Intel regelmäßig sogenannte Intel Platform Updates für alle auf Intel Produkten ausgeführten Systeme. Dieser vierteljährliche Prozess umfasst Sicherheits- und Funktionsupdates für Mikrocode, Firmware und System-BIOS. Regelmäßige Updates ermöglichen es Intel Partnern, Hardware- und Firmwareupdates nach einem vorhersehbaren vierteljährlichen Zeitplan zu validieren und in ihre Plattformen zu integrieren, was zu einer koordinierten Offenlegung in der gesamten Umgebung führt.

Die Koordinierung der Offenlegung erkannter Sicherheitslücken in Produkten und der Reaktion darauf übernehmen die dedizierten Incident-Response-Teams für Produktsicherheit von Dell und Intel. Gemeinsam sorgen sie dafür, dass die CVEs schnell und sicher behandelt und die damit verbundenen Risiken effektiv gemindert werden.

Dell und Intel haben diese Investitionen getätigt, um Kunden durchgängigen Support zu bieten und deren IT-Teams zu entlasten. Wir haben ForscherInnen, SicherheitsarchitektInnen und CyberforensikanalystInnen eingestellt, damit Ihr Unternehmen sicher ist und Ihre Teams sich darauf konzentrieren können, Ihren MitarbeiterInnen zu Bestleistungen zu verhelfen.

96 % der 2024 behandelten Sicherheitslücken wurden durch die Investitionen von Intel gefunden

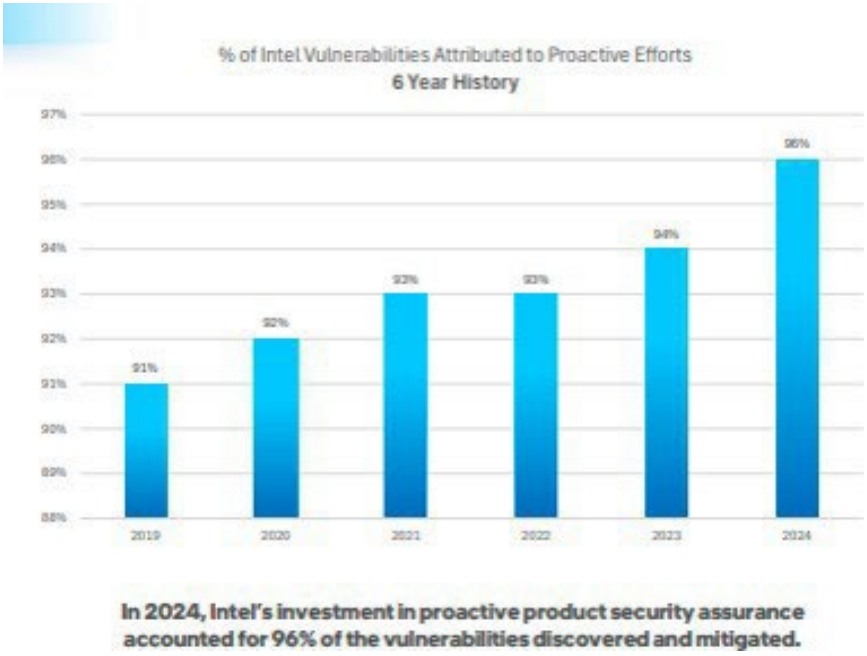
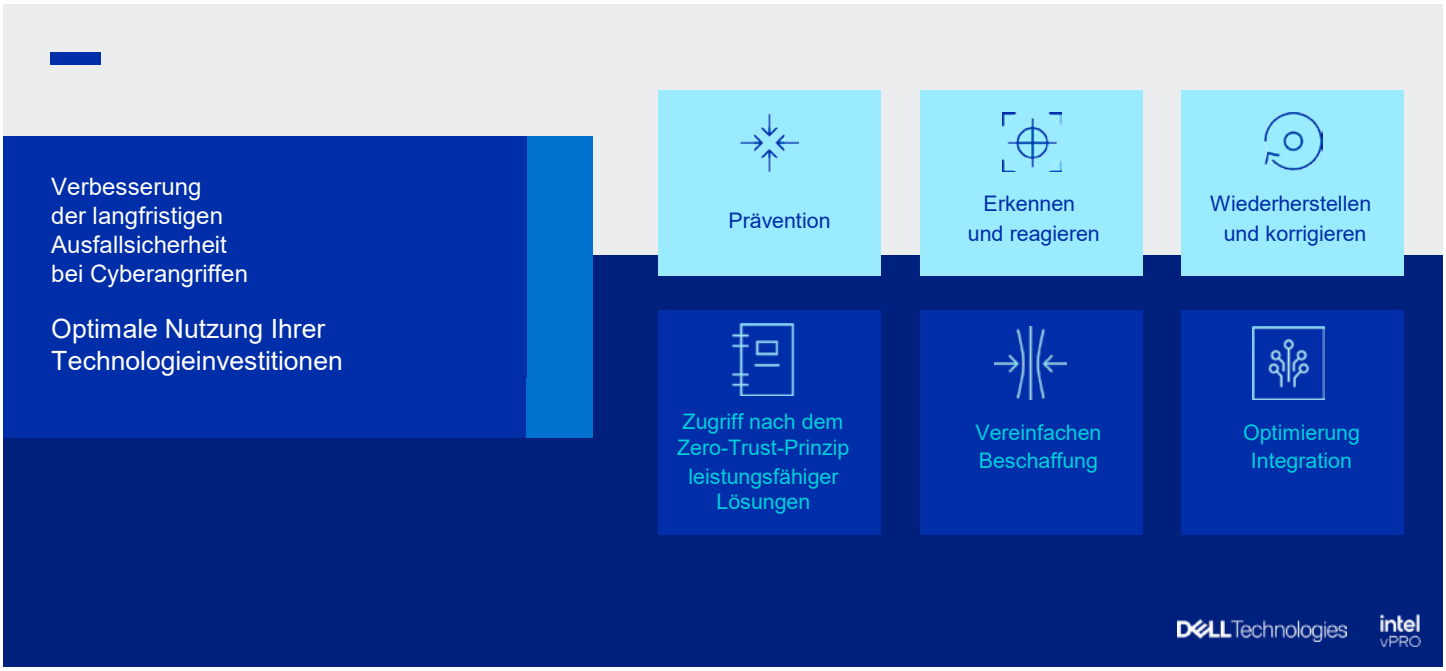


Abbildung 6: Prozentsatz der Intel Sicherheitslücken, die auf proaktive Maßnahmen zurückzuführen sind (Quelle: Intel Sicherheitsbericht 2024)

Fazit

Ergebnisse der Zusammenarbeit mit Dell und Intel



Dell und Intel konzentrieren sich auf Sicherheitsergebnisse und entwickeln Lösungen, die auf der gegnerischen Denkweise basieren. Ein wichtiges Endziel für Cyberangreifer ist Geld, das sie durch den Diebstahl und Verkauf von Daten oder durch Erpressung erlangen. Obwohl die Vorgehensweise variiert (MITRE ATT&CK®-Framework beobachtet neun allgemeine Erstzugriffsmethoden), entwickeln sich Kill Chains für Cyberangriffe auf sehr ähnliche Weise: Ausspionieren, Erstzugriff (durch Ausnutzen einer Sicherheitslücke = Schwäche oder eines Fehlers, den sie gefunden haben), Infiltrieren eines Netzwerks, seitliches Bewegen/Erlangen von höheren Zugriffsrechten, Herumschnüffeln und Sammeln von Informationen, Exfiltrieren von Daten.

Wir unterstützen Sie bei der Sicherung aller Workloads mit intelligenten Produkten, Lösungen und Services, die speziell für die Abwehr von Angriffen entwickelt wurden. Anstatt zu versuchen, 100 % der Angriffe zu blockieren (was unmöglich ist), gehen wir davon aus, dass Angriffe unvermeidbar sind, und richten unsere Abwehrmaßnahmen auf das Worst-Case-Szenario aus. Wir legen Wert auf Transparenz und Handlungsfähigkeit über den gesamte PC-Bestand hinweg. Dadurch bleiben unsere Kunden neuen Angriffsvektoren einen Schritt voraus.

Mit den Sicherheitslösungen für Endgeräte von Dell und Intel **erzielen Unternehmen wichtige Sicherheitsergebnisse**:

- **Verbesserung der langfristigen Ausfallsicherheit bei Cyberangriffen**
- **Optimale Nutzung Ihrer Technologieinvestitionen**

Erfüllen Sie beide Anwendungsfälle für Cybersicherheit …

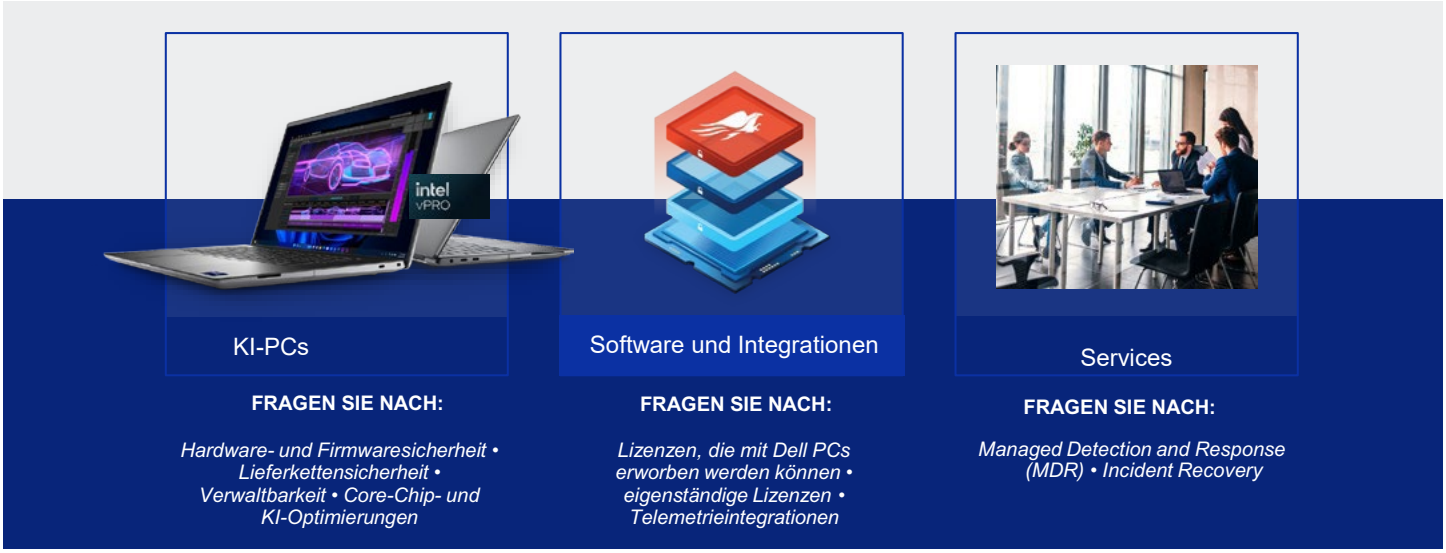
- **Reduzierung der Angriffsfläche**: Mindern Sie das Risiko, dass ein Angriff erfolgreich ist, und minimieren Sie die Sicherheitslücken und Einstiegspunkte, die zur Kompromittierung der Umgebung ausgenutzt werden können.
- **Verbesserung der Bedrohungserkennung und Reaktion darauf**: Identifizieren und beheben Sie potenzielle Sicherheitsvorfälle und bösartige Aktivitäten aktiv mit integrierten Abwehrebenen, die die Erkennung und Reaktion beschleunigen.
- **Möglichkeit zur Wiederherstellung und Behebung**: Erfassen Sie Daten zu Sicherheitsverletzungen, um zukünftige Bedrohungen zu analysieren und zu bekämpfen, und setzen Sie Endpunkte nach einem Sicherheitsvorfall wieder in einen bekannten, sicheren und betrieblichen Zustand zurück.

… und reduzieren Sie den Betriebsaufwand für die Sicherheit:

- Aufrechterhaltung der Vertrauenswürdigkeit von Geräten und Identitäten mit **Zero-Trust-fähigen Angeboten**
- **Vereinfachung der Beschaffung** durch Konsolidierung von Anbietern und Zugriff auf Hardware, Software und Services aus einer Hand
- Zeit- und Ressourceneinsparungen durch **optimierte Integration**

Ob Sie den Kampf für Cybersicherheit gewinnen oder verlieren, hängt davon ab, ob Sie in der Lage sind, Informationen über Bedrohungen zu erheben, zu analysieren und darauf zu reagieren. Die AngreiferInnen von heute sind innovativ. Da die meisten Sicherheitslösungen nur auf das Betriebssystem ausgerichtet sind, suchen Angreifer nach schwächeren Angriffspunkten, nämlich in den Schichten unterhalb des Betriebssystems und in der Lieferkette. Um diesen böswilligen AkteurInnen einen Schritt voraus zu sein und ihr Unternehmen zu schützen, müssen die Führungskräfte von heute unbedingt tief im Chip integrierte, hardwarebasierte Sicherheitstechnologien berücksichtigen, wenn sie ihren MitarbeiterInnen Geräte zur Verfügung stellen.

Erfahren Sie, welche Lösungen für Sie geeignet sind



Mit erstklassiger Sicherheit entlang der Lieferkette, mit hardwarebasierten Schutzmechanismen, mit Software zum Schutz vor Advanced Threats, verwalteten Services und kontinuierlichem Support sind Dell und Intel bereit, Ihnen und Ihrem Unternehmen Geräte anzubieten, die die Arbeit erledigen und dazu beitragen, dass Ihre Unternehmensdaten nicht im Dark Web landen.

* Die sichersten AI PCs: Basierend auf einer Drittanbieteranalyse von Principled Technologies, bei der Dell AI PCs auf Intel Prozessoren mit HP und Lenovo verglichen wurden, Juli 2025. Unterstützt durch eine interne Dell Analyse des weltweiten PC-Markts, Oktober 2024. Gilt für PCs mit Intel Prozessoren. Nicht alle Funktionen sind bei allen PCs verfügbar. Einige Funktionen müssen zusätzlich erworben werden.

Weitere Informationen zu den Lösungen von Dell

Kontakt zu Dell Technologies ExpertInnen

Weitere Ressourcen

An Unterhaltung teilnehmen