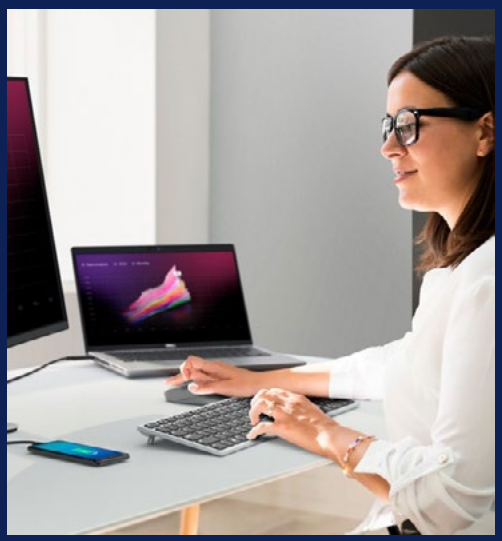
DELL Technologies

Unbegrenzte Möglichkeiten

Schutz Ihrer durch KI unterstützten Belegschaft mit Dell Technologies, Microsoft und Intel.



Windows 11

intel

Zusammenfassung

Der Wechsel zum hybriden Arbeitsmodell hat zu mehr Komplexität und neuen Angriffsvektoren geführt, denn Endpunkte, Netzwerke und Clouds erweitern die Angriffsflächen. Der Wettlauf um die Einführung von generativer KI (GenAI) erhöht den Einsatz noch weiter. So kommen immer neue Sicherheitsbedrohungen hinzu, darunter z. B. Datenlecks und Diebstahl geistigen Eigentums sowie ultraschnelle kontextbezogene Angriffe.

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 privilegierten Zugriff, sodass sie den Softwareschutz gänzlich unentdeckt umgehen können.

Zusammenarbeit ist das A und O

Kein Anbieter kann all diese Probleme alleine lösen. Deshalb arbeiten Dell, Intel und Microsoft strategisch zusammen, um die Unternehmen hier zu entlasten.

Unser ganzheitlicher Sicherheitsansatz integriert hardwarebasierte Funktionen „unterhalb der Betriebssystemebene", die zur Abwehr von Angriffen beitragen – mit chipbasierten Schutzmechanismen von Intel, die auf die tiefsten Ebenen eines Geräts abzielen.

Im Anschluss daran stellen wir sicher, dass Windows 11 sowie moderne Dell Geräte und Software zusammenarbeiten, um die Angriffsfläche zu verringern, die Systemintegrität aufrechtzuerhalten und die NutzerInnen und wertvolle Daten zu schützen.

Gemeinsam besser. Nur für Sie

Die einzigartige intrinsische Sicherheit von Dell Technologies vereint alle Innovationen unserer Partner Intel und Microsoft im Bereich Sicherheit. So können Sie Ihre hybrid arbeitenden MitarbeiterInnen vor neu aufkommenden Sicherheitsbedrohungen schützen.

Nur 33 % der IT-Verantwortlichen nutzen eine ganzheitliche End-to-End-Sicherheitsstrategie mit hardware- und softwarebasiertem Schutz.

Quelle: Dell Innovation Index, 2023.

Themen in diesem Whitepaper

Grundlage für mehr Sicherheit

Sicherer Entwicklungslebenszyklus

Dell Technologies, Intel und Microsoft arbeiten eng zusammen, um vom Chip bis zur Cloud Sicherheit zu integrieren. Ein Beispiel hierfür sind Dell Trusted-Devices – die branchenweit sichersten PCs.*

Sicherheit entlang der Lieferkette

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

* Basierend auf einer internen Analyse von Dell, September 2022.
Nicht alle Funktionen sind bei jedem PC verfügbar.
Einige Funktionen müssen zusätzlich erworben werden.

Umfassendes Verteidigungsframework – für Zero-Trust-Sicherheit

KI-gestützte Sicherheit

Nutzen Sie KI, um den Schutz der NutzerInnen zu automatisieren, und profitieren Sie von sofort einsatzbereiten, revolutionären Sicherheitslösungen.

Sicherheit unterhalb der Betriebssystemebene

Hardwarebasierte Sicherheitsfunktionen helfen Ihnen dabei, Geräte vor Bedrohungen zu schützen, die es auf ihre tiefsten Schichten abgesehen haben.

Sicherheit oberhalb der Betriebssystemebene

Sowohl softwarebasierte Sicherheitstechnologien als auch chipbasierte Schutzmechanismen sind für eine ganzheitliche Gerätesicherheit unverzichtbar.

Windows 11 -Sicherheit

Bietet sofortigen Schutz durch eng integrierte Software- und Hardwareebenen für Betriebssystem, Anwendungen, Identität und Cloud.

Laufender Support

Dell, Intel und Microsoft sorgen dafür, dass ihre Lösungen stets geschützt sind, indem sie Sicherheitslücken mithilfe von Patches schließen und die chipbasierte Sicherheit innerhalb des Betriebssystems aktualisieren.

Ihr Unternehmensnetzwerk ist so sicher wie sein schwächster Endpunkt

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, die in ihr Gerät eingebaut ist, oder eine unbekannte 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?

Dell, Microsoft 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.

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. Es ist wichtig, dass sich Unternehmensverantwortliche der Grenzen dieser Strategie bewusst sind. Wenn sie sich zum Schutz ihrer Unternehmen nur auf Software verlassen, bleibt die Hardware, auf der die Software ausgeführt wird, potenziell anfällig für Angriffe. 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 AngreiferInnen ein attraktiveres Ziel darstellen.

Genau deshalb verfolgen Dell, Microsoft und Intel einen anderen, ganzheitlichen Ansatz für Sicherheit.

Ihr Unternehmensnetzwerk ist so sicher wie sein schwächster Endpunkt

Dell, Microsoft und Intel bieten integrierte hardwarebasierte Sicherheit

Die Komplexitäten und Probleme, die mit dem Schutz von Geräten und Netzwerken einhergehen, sind besorgniserregend. 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, Microsoft 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 Microsoft und Intel hat sich Dell einen Ruf als führender Anbieter von Mitarbeitergeräten für Unternehmen jeder Größe und Branche erworben.

Was steckt alles in einem Dell Gerät? Auf jeden Fall mehr als eine willkürliche Ansammlung von Funktionen ... Wir 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
Microsoft, 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
Mit Dell Trusted-Device-Technologien und Intel® Hardware Shield-Funktionen setzen wir auf hardwarebasierte Sicherheit, um die Verteidigungsmechanismen der Geräte durch ein Framework aus Prävention, Erkennung und Reaktion zu stärken. Darüber hinaus verfügen Dell, Microsoft und Intel über spezielle Sicherheitsteams, die die Produkte stichprobenartig untersuchen und neue Sicherheitslücken aufspüren, bevor sie von AngreiferInnen entdeckt werden, und dann umgehend Patches bereitstellen, damit Sie und Ihr Team geschützt sind.

In diesem Whitepaper erfahren Sie, wie Dell, Microsoft und Intel zusammenarbeiten, um PC-Plattformen zu entwickeln, in denen Sicherheit bis in die tiefsten Schichten hinein integriert ist, um Ihre Geräte während ihres gesamten Lebenszyklus, bis zur nächsten Aktualisierung und darüber hinaus zu schützen.

Der Schutz unserer Plattformen beginnt am Whiteboard

Planung, Bewertung und Analyse

Vor der Konzeption der neuesten Plattformen, Chipsätze und Software legen die ExpertInnen von Dell, Microsoft und Intel strenge Parameter fest, die eine sichere Plattform aufweisen muss, um den Sicherheitsanforderungen der Zukunft gerecht zu werden und alle relevanten Vorschriften zu erfüllen. 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, Microsoft 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.

Der Schutz unserer Plattformen beginnt am Whiteboard

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 übersehene Fehler aufzuspüren und sicherzustellen, dass der Code auf sichere Weise entwickelt wurde.

Abschließend werden Teams aus erfahrenen HackerInnen für Penetrationstests und andere Red-Team-Aktivitäten hinzugezogen, um potenzielle Sicherheitslücken zu finden, die in den vorhergehenden Phasen übersehen wurden. Die so aufgedeckten Schwachstellen werden ebenfalls auf der Grundlage des jeweiligen 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 unser Engagement 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.

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. Jeder Schritt in 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.

Beschaffung

Dell wendet einen strengen Prozess zur Überprüfung von Partnern an, um die Qualität und Sicherheit von Geräten und deren Komponenten sicherzustellen. Die 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 Produktion auch häufig testen, damit keine gefälschten Produkte in die Lieferkette gelangen. Um dieses Risiko noch weiter zu minimieren, werden 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 Tracking-Tools, 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 Technologies Safe SupplyChain-Lösungen umfassen Lieferkettensicherheit und Integritätskontrollen wie manipulationssichere Siegel und Festplattenlöschung auf NIST-Ebene, um das gute Image Ihres Unternehmens aufrechtzuerhalten.

Eine sichere Lieferkette ist für Gerätesicherheit entscheidend

Überprüfung

Geräte von Dell werden mit kryptografisch signierten Plattformzertifikaten ausgeliefert, die Snapshot-Attribute von Plattformen während der Fertigung, Montage, Tests und Integration erfassen. Diese Plattformattribute werden dann kryptografisch mithilfe von Trusted Platform Module (TPM) als vertrauenswürdige Hardware („Root of Trust“) mit dem spezifischen Gerät verknüpft.

Dell hat Zertifikate der Trusted Computing Group-Plattform in die Lösung Dell Secured Component Verification (SCV) für PCs mit Intel Prozessoren Integriert. SCV liefert der IT-Abteilung kryptografisch signierte Bestandszertifikate für unterstützte Dell Geräte. Mit sicheren Tools zur Selbstverifizierung trägt SCV dazu bei, vollständige Hardwareintegrität während des Transports zu den IT-Umgebungen zu gewährleisten. Außerdem können die Kunden damit überprüfen, ob die PCs von Dell und zentrale Komponenten so ankommen, wie sie bestellt und gefertigt wurden.

In ähnlicher Weise ermöglicht auch Intel den Anbietern schon seit vielen Jahren Transparenz und Rückverfolgbarkeit der digitalen Lieferkette. Intel®Transparent Supply Chain (Intel®TSC) stellt TCG-Plattformzertifikate und Komponentendaten zur Unterstützung Intel basierter Plattformen über eine Cloud-API bereit, die der IT über das Intel®TSC-Webportal zur Verfügung steht. Auch wenn sich Dell und Intel für die Implementierung unabhängiger Lösungen entschieden haben, sind TCG-Plattformzertifikate ein gemeinsamer Bestandteil von Intel® TSC und Dell SCV. Diese Gemeinsamkeit bietet Kompatibilität und Interoperabilität, die es Unternehmen und Behörden ermöglichen, TCG-Plattformzertifikate einzusetzen, um die Sicherheit der digitalen Lieferkette für auf Intel basierende Geräte zu verbessern.

Umfassendes Verteidigungsframework – für Zero-Trust-Sicherheit

Unternehmen, die an der Verbesserung ihres Reifegrads bezüglich Cybersicherheit arbeiten, entwickeln hierfür eine umsetzbare Roadmap, in der Wege zur Reduzierung ihrer Angriffsfläche, zur Erkennung von und Reaktion auf Cyberbedrohungen sowie zur Implementierung von Methoden zur Recovery nach Cyberangriffen identifiziert werden – all dies unter Verwendung von Zero-Trust-Funktionen.

Um den immer ausgefeilteren Cyberbedrohungen zu begegnen, nutzt Dell die in unsere Lösungen und die unserer Partner – darunter Microsoft und Intel – integrierten Sicherheitsfunktionen, um Kunden bei der Umsetzung von Zero Trust im Einklang mit ihren Geschäftszielen zu unterstützen.

77 %

müssen noch eine Zero-Trust-Architektur evaluieren/entwickeln.*

* Innovation Index von Dell Technologies, 2023: https://www.dell.com/en-us/dt/perspectives/innovation-index.htm.

Deutlich einfachere Zero-Trust-Einführung für Ihre Belegschaft durch eine vollständig integrierte Architektur

Dell, Microsoft und Intel arbeiten zusammen, um eine nahtlose und sichere hybride Arbeitsumgebung zu schaffen, die es Kunden ermöglicht, die drei Grundsätze von Zero Trust zu erfüllen:

1. Explizite Überprüfung

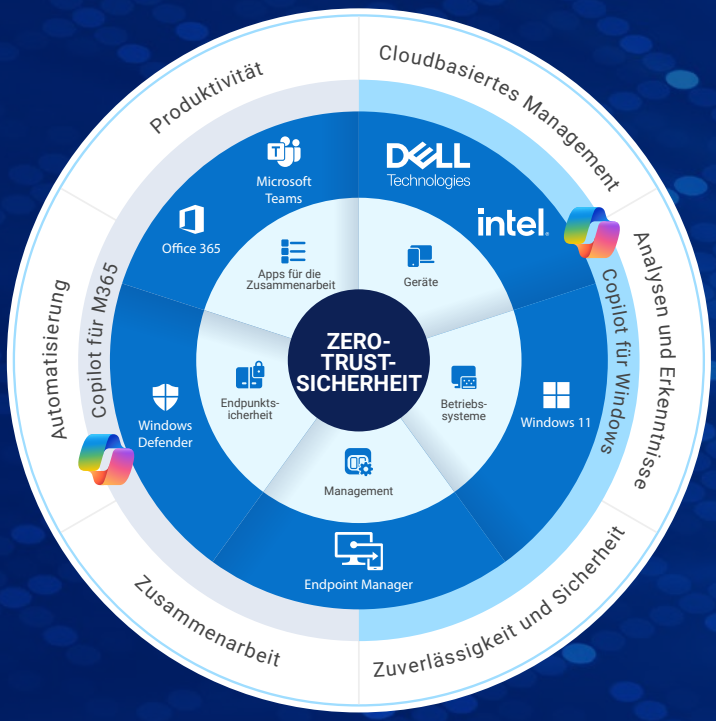
Basieren Sie die Authentifizierung und Autorisierung immer auf allen verfügbaren Datenpunkten, einschließlich Nutzeridentität, Standort, Geräteintegrität, Service oder Workload, Datenklassifizierung und Anomalien.

2. Zugriffserteilung mit den geringsten Rechten

Begrenzen Sie den Nutzerzugriff mit Just-in-Time und Just-enough-Access (JIT/JEA), risikobasierten adaptiven Policies und Data Protection, um sowohl Daten als auch die Produktivität zu schützen.

3. Annahme eines Verstoßes

Achten Sie beim Betrieb auf einem minimierten Blast-Radius und Segmentzugriff. Überprüfen Sie die End-to-End-Verschlüsselung und nutzen Sie Analysen, um transparente Einblicke zu erhalten, die Bedrohungserkennung zu erleichtern und die Abwehrmaßnahmen zu verbessern.



Unsere gemeinsamen Lösungen unterstützen Unternehmen bei der Umsetzung eines Zero-Trust-Sicherheitsmodells, indem sie jeden Zugriffsversuch verifizieren und strenge Sicherheitsrichtlinien basierend auf Identität, Gerätezustand, Standort und Risikostufe durchsetzen, wodurch das Risiko eines unbefugten Zugriffs verringert und die Auswirkungen von Sicherheitsverletzungen minimiert werden.

Dies wird erreicht durch die Integration von:

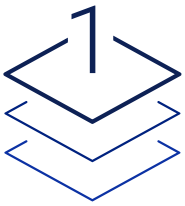
BIOS-/Firmwaresicherheit für Dell PCs, Hardwaresicherheit, Lieferkettensicherheit, Bedrohungsmanagementsoftware (EDR, XDR, VDR), Data-Protection-Software für Netzwerk und Cloud sind in Kombination mit Intel® Hardware Shield exklusiv auf der Intel vPro® Plattform erhältlich.

Die umfassende Suite an Tools und Technologien von Microsoft für Identitäts- und Zugriffsmanagement, Endpunktsicherheit, Netzwerksicherheit, Data Protection, Threat Intelligence, Sicherheitsanalyse, Durchsetzung von Policies sowie kontinuierliche Überwachung und Reaktion. Zu diesen Lösungen gehören Azure Active Directory, Microsoft Defender for Endpoint, Azure Firewall, Azure Information Protection, Microsoft Threat Intelligence, Azure Sentinel, Microsoft Endpoint Manager und Microsoft Security Center.

KI-gestützte Sicherheit

Bahnbrechende KI-gestützte Sicherheit – sofort einsatzbereit

Dell, Intel und Microsoft setzen auf KI, um den Schutz der NutzerInnen zu automatisieren, und bieten gemeinsam sofort einsetzbare revolutionäre Sicherheitslösungen an. Diese innovativen Maßnahmen wurden entwickelt, um die raffinierten Angriffe von heute zu erkennen und zu verhindern. Sie umfassen hardwarebasierte Sicherheit, erweiterte Verschlüsselung und Malwareschutz – alles basierend auf Intel® Core™ Ultra Prozessoren unter Intel vPro® und Windows 11 Pro-Betriebssystemen und nahtlos in moderne Dell Geräte integriert. Dieses Zusammenspiel verringert die Angriffsfläche erheblich, da mehrere Schutzebenen implementiert werden, die sich auf drei Schlüsselbereiche konzentrieren:



1. Unterhalb des Betriebssystems:

- Dell und Intel haben bei Dell SafeBIOS eng zusammengearbeitet – einem robusten Schutzmechanismus für BIOS- und Firmwareangriffe, der durch eine vom Host unabhängige Verifizierung die Integrität des BIOS mit Firmware auf Intel vPro® sicherstellt.
- Die neueste Intel vPro® Plattform reduziert die physische Angriffsfläche im Vergleich zu 4 Jahre alten Geräten um bis zu 70 %.*
- Dell Geräte mit Intel vPro® erhalten die Zertifizierung „Windows 11 Secured Core PC Level 3“, die eine Reihe nahtlos integrierter Schutzmaßnahmen umfasst.
- So bietet beispielsweise der Intel System Security Report dem Betriebssystem die Gewissheit, dass der Bootprozess sicher ausgeführt wird, und sorgt auf diese Weise von Anfang an für Integrität.
- Diese Schutzmechanismen sind im System integriert und sofort einsatzbereit.

2. Anwendungsschutz und Data Protection:

- Die Nutzerzugangsdaten werden durch fortschrittliche Funktionen geschützt, darunter z. B. die Isolierung der Zugangsdaten, ermöglicht durch Windows Hello und Intel Virtualisierungstechnologien.
- Die Verschlüsselung des gesamten Arbeitsspeichers mit mehreren Schlüsseln stattet virtuelle Windows 11-Maschinen mit verschlüsseltem Arbeitsspeicher aus, was die Prozesse und die zugehörigen Daten auf effektive Weise isoliert.
- Diese Schutzmaßnahmen sind für den sofortigen Einsatz vorkonfiguriert oder können bequem über das Windows-Sicherheitscenter angepasst werden.

3. Erkennung von Advanced Threats:

- Intel® Threat Detection zeichnet sich als die einzige chipfähige KI-Bedrohungserkennungslösung aus, die Ransomware- und Cryptojacking-Angriffe abwehren kann.
- Da Ransomware stark auf die CPU angewiesen ist, um geschäftskritische Inhalte zu verschlüsseln, nutzt Intel TDT die KI-gesteuerte Bedrohungserkennung, um die CPU-Telemetrie nach Angriffsindikatoren zu scannen und bösartige Prozesse sofort zu kennzeichnen, sodass sie von Sicherheitssoftware wie Microsoft Defender unter Quarantäne gestellt oder beendet werden können.

*13th Gen Intel® Core™ Processor Attack Study Report

KI-gestützte Sicherheit

Unsere Zusammenarbeit erstreckt sich auch auf das Angebot von Accelerated Memory Scanning zur frühzeitigen Erkennung von dateiloser Malware, was eine zusätzliche Sicherheitsebene zur Abwehr von Malwareangriffen bietet. Durch unsere Partnerschaft mit Microsoft Defender und der Intel Threat Detection Technology optimieren wir rechenintensive Scanprozesse, indem wir sie auf die GPU verlagern, sodass die CPU für ununterbrochene Produktivität frei ist. Im Falle eines potenziellen Angriffs kommuniziert die GPU proaktiv mit MSFT Defender und ermöglicht so einen umfassenderen Scanansatz.

Dies bietet den Unternehmen folgende **drei Vorteile**:

Reduzierung der Anzahl dateiloser Angriffe, die sich zum vorherrschenden Vehikel für verschiedene Cyberbedrohungen entwickelt haben

Frühzeitige Erkennung von Ransomware und anderen bösartigen Bedrohungen schon in der Phase des ersten Speicherzugriffs

Aufrechterhaltung eines hohen Nutzererlebnisses während der Sicherheitsscans

Mit Accelerated Memory Scanning können Unternehmen ihren Schutz vor neu aufkommenden Cyber-bedrohungen verbessern und zugleich für optimale betriebliche Effizienz und Nutzerproduktivität sorgen.

Die Zusammenarbeit zwischen Dell, Microsoft und Intel resultiert in umfassenden Sicherheitslösungen, die einen hardwarebasierten Schutz, sichere Bootprozesse, Anwendungs- und Datensicherheit sowie Funktionen zur Erkennung von Advanced Threats umfassen – alle mit großer Sorgfalt entwickelt, um den sich ständig weiterentwickelnden Cyberbedrohungen von heute zu begegnen.

Integrierte Sicherheitstechnologien tragen dazu bei, Bedrohungen vorzubeugen, zu erkennen und darauf zu reagieren.

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, Microsoft und Intel war, diese Angriffsfläche durch ein komplexes Geflecht von Technologien sowohl auf Komponenten- als auch auf Plattformebene abzudecken. Zusätzlich zu anderen Tools und Technologien von Dell und Intel bieten Intel® Hardware Shield und das SafeBIOS-Framework von Dell einen integrierten, hardwarebasierten Schutz für die NutzerInnen von Dell Geräten.

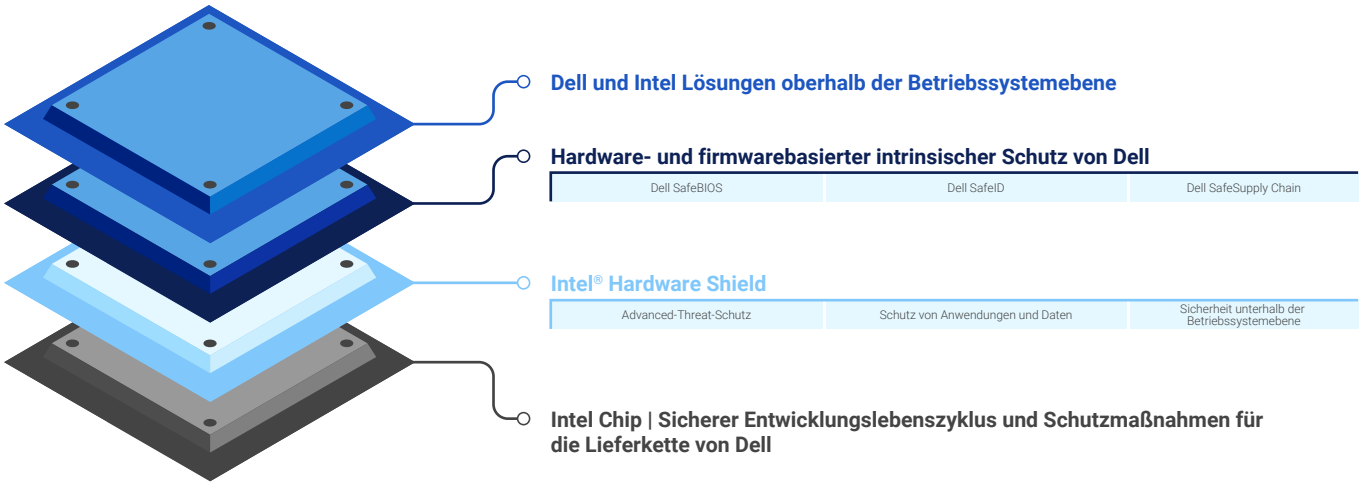


Abbildung 1: Intel® Hardware Shield und der hardwarebasierte Schutz von Dell sind Sicherheitsebenen, die vor grundlegenden Angriffen schützen.

Intel® Hardware Shield

Intel Hardware Shield 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.

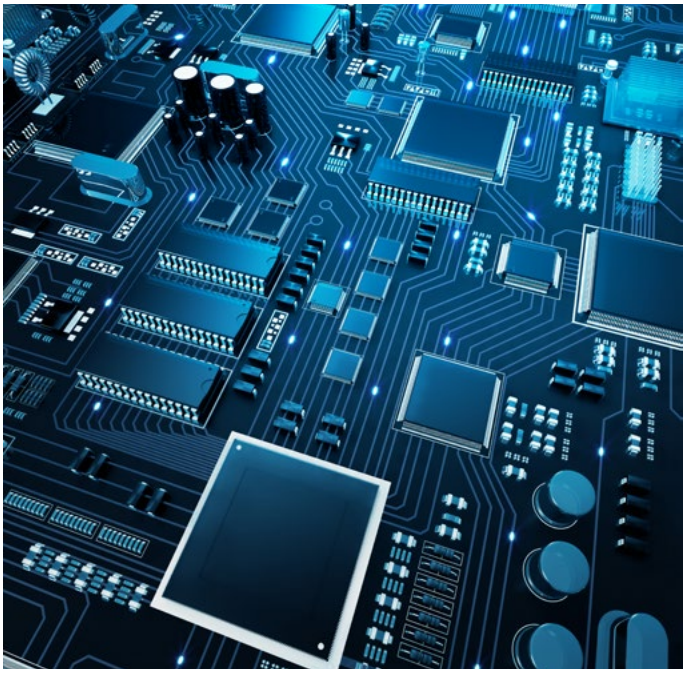
Intel Hardware Shield umfasst Funktionen für den Advanced-Threat-Schutz, für den Schutz von Anwendungen und Daten sowie für Sicherheit unterhalb der Betriebssystemebene mit über 20 innovativen Sicherheitstechnologien. Dell hat sich fast jede dieser Mechanismen zunutze gemacht, um Sicherheitslösungen zu entwickeln, die auf ihren grundlegenden Merkmalen aufbauen und den Kunden so mit die sichersten Geräte am Markt bieten. Zu diesen Lösungen gehören das Dell SafeBIOS Framework, Dell SafeID und Dell SafeSupply Chain, die zusammen ein noch höheres Maß an Schutz vor aktuellen und künftigen Bedrohungen bieten.

Integrierte Sicherheitstechnologien tragen dazu bei, Bedrohungen vorzubeugen, zu erkennen und darauf zu reagieren.

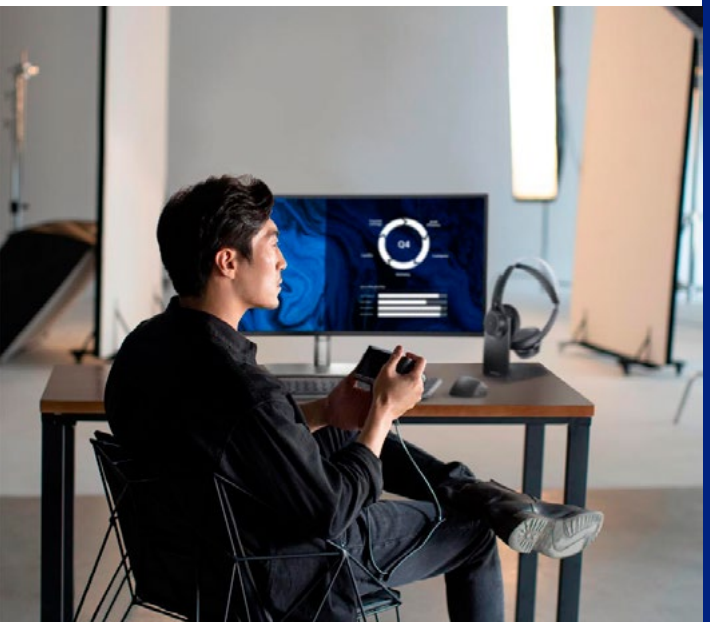
Dell SafeBIOS-Framework, Dell SafeID und Dell SafeSupply Chain

Der Schutz des BIOS ist für die Gerätesicherheit ungemein wichtig. 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. Um diese so kritische Ebene zu schützen, werden Dell Geräte mit SafeBIOS ausgeliefert. Dies ist eine Suite an Tools, die BIOS-Angriffe verhindern, erkennen, ob das BIOS kompromittiert wurde, und bei Feststellung von Unregelmäßigkeiten die IT-Abteilung benachrichtigen.

Ausgewählte Dell Geräte beinhalten außerdem Dell SafeID, das die Zugangsdaten der EndnutzerInnen in einem speziellen Sicherheitschip schützt, um sie vor Malware zu verbergen, die nach Zugangsdaten sucht und diese dann stiehlt – eine Sicherheitsverletzung, die das gesamte Unternehmensnetzwerk gefährden könnte. Für eine Extraportion Produktsicherheit bietet Dell optionale Add-on-Funktionen wie Secured Component Verification und mit Dell SafeSupply Chain eine manipulationssichere Verpackung.



Endpunktschutz mit Lösungen von Dell und Intel für Sicherheit oberhalb der Betriebssystemebene



Trotz der zunehmenden Bedrohung durch Angriffe unterhalb der Betriebssystemebene ist der Schutz oberhalb des Betriebssystems wichtiger als je zuvor. Da die Zahl der EndnutzerInnen, die remote und von unterwegs aus arbeiten, exponentiell zunimmt, benötigen Sie intelligente Lösungen, die Bedrohungen erkennen, verhindern und darauf reagieren, wo immer sie auch auftreten. Das Portfolio für Endpoint Security von Dell Trusted Workspace umfasst optionale Software wie Dell SafeGuard and Response mit Dell SafeData. So stehen Unternehmensverantwortlichen sämtliche Tools zur Verfügung, die sie zum Schutz ihrer Endpunkte benötigen. 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 Hardware Shield unterhalb der Betriebssystemebene Anwendungen und Daten schützen sowie Advanced-Threat-Schutz bieten.

Als Nächstes kommt die Softwaresicherheit von Microsoft ins Spiel, die von der Security Foundation bis zur Cloud reicht. Bei Windows 11 arbeiten Hardware und Software zusammen, um sensible Daten vom Core Ihres PCs bis hin zur Cloud zu schützen. Umfassender Schutz sorgt für die Sicherheit Ihres Unternehmens, unabhängig davon, wo gearbeitet wird. Auf der folgenden Seite sind die Schutzschichten in Windows 11 dargestellt.

Endpunktschutz mit Lösungen von Dell, Microsoft und Intel für Sicherheit oberhalb der Betriebssystemebene

Intel integriert dann die zusätzlichen Hardwareschutzmaßnahmen in jede Ebene der Sicherheitsvision von Microsoft. Im Anschluss daran werden diese in die Dell Client-Lösungen integriert.

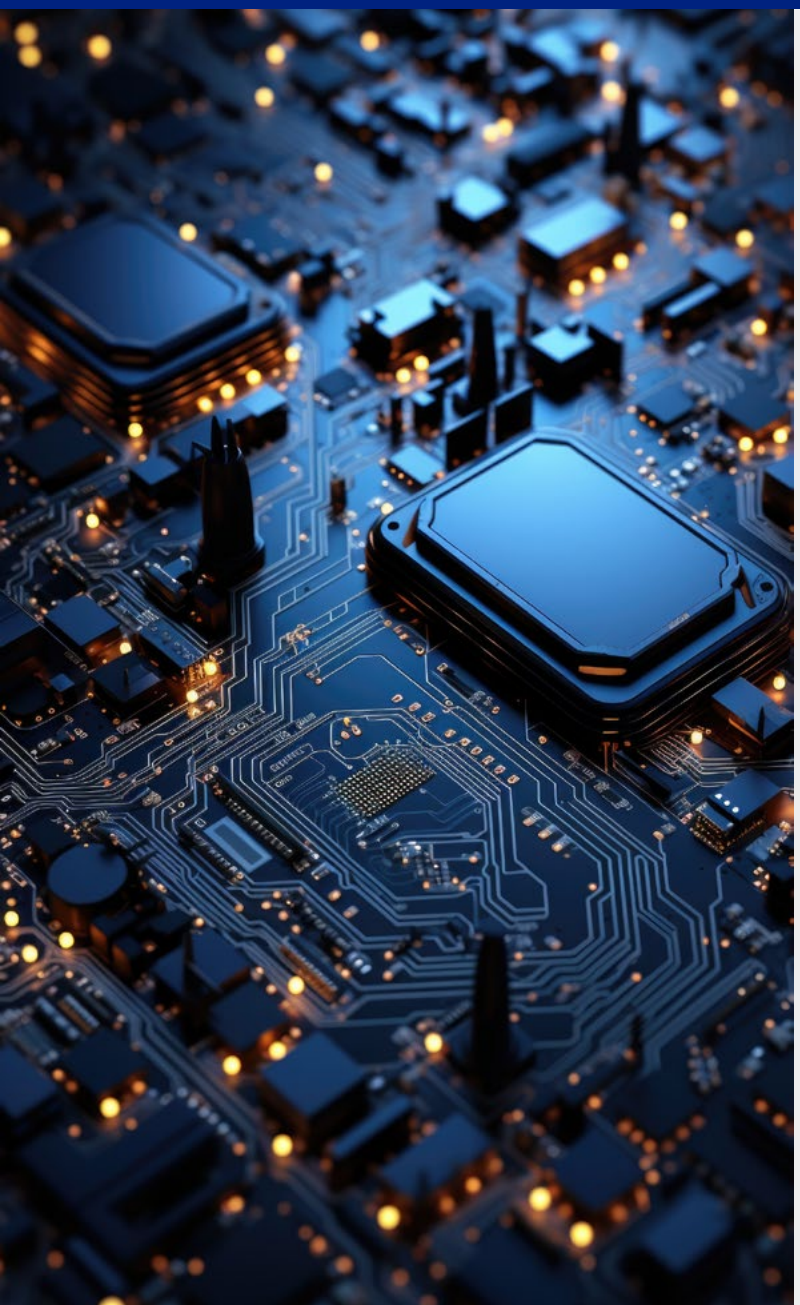
Eine Partnerschaft für leistungsstarken Standardschutz

Die einzigartige intrinsische Sicherheit von Dell Technologies vereint alle Innovationen unserer Partner Intel und Microsoft im Bereich Sicherheit. So können Sie Ihre hybrid arbeitenden MitarbeiterInnen vor neu aufkommenden Sicherheitsbedrohungen schützen.

Windows 11-Sicherheit

End-to-End-Schutz mit modernem Management:

Windows 11 ist das sicherste Windows aller Zeiten, da die meisten Sicherheitsfunktionen von Vornherein aktiviert sind. Die Hardware und Software arbeiten nahtlos zusammen, um sensible Daten vom Core Ihres PCs bis hin zur Cloud zu schützen, mit Schutzschichten auf jeder Ebene der Hardware, des Betriebssystems, der Anwendungen, der Identität und der Cloud. All dies verbessert die Produktivität, die Sicherheit und die Ausfallsicherheit – überall.

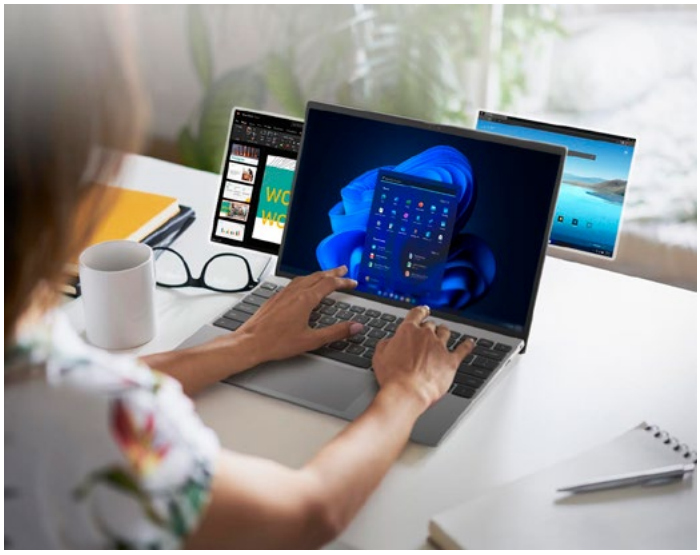


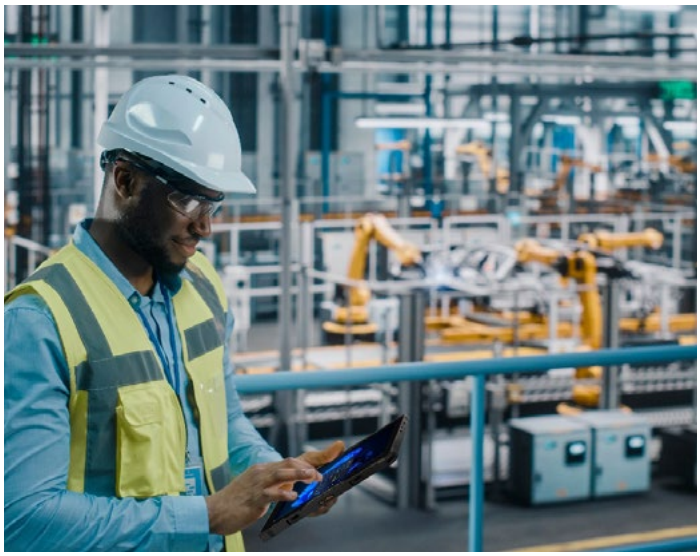
Hardware (Chip)

Root of Trust von Hardware
Das hardwarebasierte „Root of Trust“ hilft dabei, die Integrität des Systems zu schützen und aufrechtzuerhalten, während das Gerät eingeschaltet, die Firmware geladen und das Betriebssystem gestartet wird, und erfüllt damit wichtige Ziele der Systemsicherheit.

Trusted Platform Module (TPM)
Die TPM-Technologie (Trusted Platform Module) wurde entwickelt, um hardwarebasierte, sicherheitsrelevante Funktionen bereitzustellen. TPMs bieten Sicherheits- und Datenschutzvorteile für Systemhardware, Plattformverantwortliche und NutzerInnen. Windows Hello, BitLocker, System Guard (zuvor Windows Defender System Guard) und andere Windows-Funktionen stützen sich auf das TPM für Funktionen wie Schlüsselgenerierung, sicherer Storage, Verschlüsselung, Bootintegritätsmessungen und Nachweis.

Windows 11-Sicherheit





Betriebssystem

Systemsicherheit

Trusted Boot (Secure Boot + Measured Boot) Windows 11 erfordert, dass alle PCs die Secure-Boot-Funktion von Unified Extensible Firmware Interface (UEFI) verwenden. Wenn ein Windows 11-Gerät startet, arbeiten Secure Boot und Trusted Boot zusammen, um das Laden von Malware und kompromittierten Komponenten zu verhindern.

Verschlüsselung und Data Protection

BitLocker-Laufwerksverschlüsselung ist eine Data-Protection-Funktion, die in das Betriebssystem integriert ist und Bedrohungen durch Datendiebstahl oder die Offenlegung von Daten auf verlorenen, gestohlenen oder unsachgemäß außer Betrieb genommenen Computern abwehrt.

Secured-Core-PCs

In Zusammenarbeit mit Dell bietet Microsoft eine spezielle Gerätekategorie namens Secured-Core-PCs (SCPCs) an. Die Geräte werden hier mit zusätzlichen Sicherheitsmechanismen ausgeliefert, die auf der Ebene der Firmware oder des Cores des Geräts aktiviert sind, das Windows unterstützt.

Netzwerksicherheit

Um die Angriffsfläche eines Unternehmens zu verringern, verhindert der Netzwerkschutz in Windows, dass Personen auf gefährliche IP-Adressen und Domänen zugreifen, die u. U. Phishing, Exploits und andere bösartige Inhalte enthalten. Mithilfe von reputationsbasierten Services blockiert der Netzwerkschutz den Zugang zu potenziell schädlichen Domains und IP-Adressen mit niedriger Reputation.

Schutz vor Viren und Bedrohungen

Microsoft Defender SmartScreen Microsoft Defender SmartScreen schützt vor Phishing, Malware-Websites und -Anwendungen sowie vor dem Herunterladen potenziell bösartiger Dateien.

Windows 11-Sicherheit

Anwendung

Smart App Control
Smart App Control verhindert, dass NutzerInnen bösartige Anwendungen auf Windows-Geräten ausführen, indem es nicht vertrauenswürdige oder nicht signierte Anwendungen blockiert. Smart App Control geht über die bislang integrierten Browser-Schutzmechanismen hinaus, indem es eine weitere Sicherheitsebene hinzufügt, die direkt in den Kern des Betriebssystems auf Prozessebene eingebettet ist.

Anwendungsisolierung
Die Isolierung von Win32-Anwendungen ist eine neue Sicherheitsfunktion, die als öffentliche Vorschauversion verfügbar ist. Sie wurde als Isolierungsstandard auf Windows-Clients entwickelt. Sie setzt auf AppContainer auf und bietet mehrere zusätzliche Sicherheitsfunktionen, die die Windows-Plattform vor Angriffen schützen, die Sicherheitslücken in Anwendungen oder Bibliotheken von Drittanbietern ausnutzen.

Identität

Unterstützung einer kennwortlosen Anmeldung
Windows Hello ermöglicht die kennwortlose Anmeldung mit biometrischer oder PIN-basierter Verifizierung und bietet integrierte Unterstützung für den kennwortlosen Branchenstandard FIDO2. Windows Hello for Business erweitert Windows Hello um die Zusammenarbeit mit den ActiveDirectory- und Microsoft Entra ID-Konten eines Unternehmens. Es bietet Single-Sign-On-Zugriff auf Arbeits- oder Schulressourcen wie OneDrive for Business, Geschäfts-E-Mails und andere Businessanwendungen.

Erweiterter Schutz für Zugangsdaten
Zusätzlich zur Einführung der kennwortlosen Anmeldung können Unternehmen die Sicherheit von Nutzer- und Domainzugangsdaten in Windows 11 mit Credential Guard und Remote Credential Guard verbessern.

Transparenz und Kontrollen für Datenschutz
Gut sichtbare Symbole in der Taskleiste zeigen den NutzerInnen an, wenn Ressourcen und Anwendungen wie Mikrofone und Ortung verwendet werden. Eine Beschreibung der Anwendung und ihrer Aktivitäten wird in einer einfachen Kurzinformation angezeigt, die erscheint, wenn Sie mit dem Mauszeiger über ein Symbol fahren. Anwendungen können auch die neuen Windows-APIs nutzen, um die Funktion zur schnellen Stummschaltung zu unterstützen.

Windows 11-Sicherheit

Cloud

Microsoft Entra ID

Microsoft Entra ID (ehemals Azure Active Directory) ist eine umfassende cloudbasierte Identitätsmanagementlösung, die den sicheren Zugriff auf Anwendungen, Netzwerke und andere Ressourcen ermöglicht und vor Bedrohungen schützt.

Microsoft Intune

Microsoft Intune ist eine umfassende Lösung für das Endpunktmanagement, die dabei hilft, NutzerInnen, Anwendungen und Geräte zu schützen, bereitzustellen und zu verwalten. Intune vereint Technologien wie Microsoft Configuration Manager und Windows Autopilot, um die Bereitstellung, das Konfigurationsmanagement und Softwareupdates im gesamten Unternehmen zu vereinfachen.

Microsoft Azure Attestation-Service

Mithilfe des Remotenachweises lässt sich sicherstellen, dass Geräte die Sicherheitsrichtlinien einhalten und sich in einem vertrauenswürdigen Zustand befinden, bevor ihnen der Zugriff auf Ressourcen gewährt wird. Microsoft Intune ist in den Microsoft Azure Attestation Service integriert, um den Zustand von Windows-Geräten umfassend zu überprüfen und diese Informationen mit dem bedingten Zugriff von Microsoft Entra ID zu verbinden.

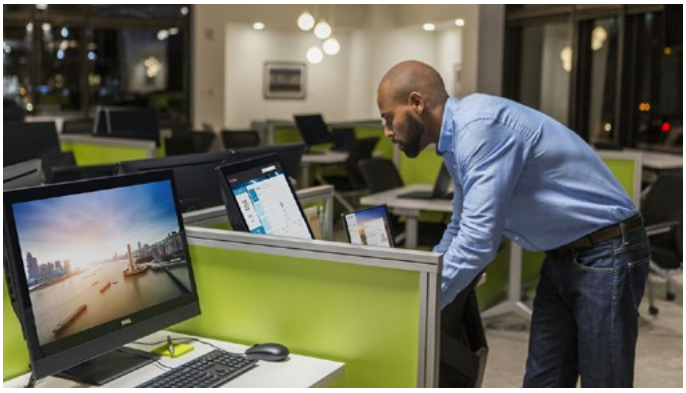
Dell, Microsoft und Intel investieren in fortlaufende Plattformsicherheit auch nach der Markteinführung

46,4 Mrd. USD unsere FuE-Ausgaben 2023* zusammengenommen

* Ausgaben für Forschung und Entwicklung im Jahr 2023 laut Macrotrends.net: Dell Technologies – 2,88 Mrd. USD, Intel – 16,046 Mrd. USD, Microsoft – 27,524 Mrd. USD.

Dell, Microsoft 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, Microsoft 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.

Als Teil dieses Engagements finanziert Intel eines der besten Bug-Bounty-Programme der Branche. Durch dieses Programm wurden 86 % der 2021 extern entdeckten Sicherheitslücken gefunden. Die im Rahmen dieses Programms und durch interne oder externe ForscherInnen gefundenen CVEs (Common Vulnerabilities and Exposures) werden in einer öffentlichen Datenbank protokolliert. Intel ist stolz auf seine Führungsposition beim Monitoring und Reporting von Sicherheitslücken nach der Markteinführung und hat mehr potenzielle Sicherheitslücken protokolliert und gepatcht als die meisten Mitbewerber. Chiphersteller können nicht dasselbe Maß an Transparenz und Gerätesicherheit bieten.



Als Reaktion auf die im Rahmen der umfassenden Programme gefundenen CVEs veröffentlicht Intel regelmäßig sogenannte Intel Platform Updates für alle auf Intel Produkten ausgeführten Systeme. Diese Veröffentlichung erfolgt in einem umfangreichen Prozess, der eine Validierung durch das Partnernetzwerk von Intel erfordert, das CSPs, ISVs, OEM/ODMs und SIs umfasst.

Die Koordinierung der Veröffentlichung 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, Microsoft 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.

Dell, Microsoft und Intel unterstützen Sie beim Schutz Ihres wachsenden Unternehmens

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 sich die meisten Sicherheitslösungen nur auf den Softwareschutz konzentrieren, nehmen die AngreiferInnen die Schichten unterhalb des Betriebssystems und die Lieferkette als neue Vektoren ins Visier, um Ihre Sicherheit zu kompromittieren und Unternehmen wie das Ihre auszunutzen.

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.

Dell, Microsoft und Intel arbeiten seit Jahrzehnten im Bereich der kommerziellen PCs zusammen und haben sich das Vertrauen unserer Kunden mit einigen der sichersten Geräte der Branche verdient. Unser Fachwissen und unsere gemeinsame Entwicklungsarbeit ermöglichen es uns, den HackerInnen durch unsere konsequente Forschung, Gewissenhaftigkeit und Innovation stets einen Schritt voraus zu sein. Als langjähriger Marktführer im Bereich kommerzieller Geräte erkennen wir mehr und verhindern auch mehr: Wir handeln ständig auf der Grundlage einer immensen Menge an Daten und Telemetrie, um die Sicherheit der Geräte unserer gemeinsamen Kunden kontinuierlich zu verbessern. Unsere kreativen Köpfe kommen regelmäßig zusammen, um zu erörtern, wie umfassende Sicherheit heute aussieht, wie sie morgen aussehen wird und welche Investitionen erforderlich sind, um sicherzustellen, dass unsere Produkte in puncto kommerzieller Cybersicherheit weiter führend bleiben.

Mit erstklassiger Sicherheit entlang der Lieferkette, mit hardwarebasierten Schutzmechanismen, mit Software zum Schutz vor Advanced Threats und kontinuierlichem Support sind Dell, Microsoft und Intel bereit, Ihnen und Ihrem Unternehmen Geräte anzubieten, die nicht nur die Arbeit erledigen, sondern auch dazu beitragen, dass Ihre Unternehmensdaten nicht im Dark Web landen. Sprechen Sie noch heute mit Ihrem/Ihrer Dell VertriebsmitarbeiterIn, um mehr über unsere Programme für kommerzielle Geräte zu erfahren sowie darüber, wie wir Ihnen dabei helfen können, Ihre Geschäftsziele zu erreichen.

Hier klicken für

unbegrenzte Möglichkeiten

DELL Technologies

Windows 11

intel