Solution Brief

Endpunktsicherheit

Mit Hardware-gestützter Sicherheit die Angriffsfläche am Endpunkt minimieren

Wie Sie ausgefeilte Endpunkt-Angriffe mit koordinierten Schutzmaßnahmen in Soft- und Hardware effektiv abwehren

Die wichtigsten Vorteile

- **Verringerung der Angriffsfläche um 70 %**[1] Dell PCs, die mit Intel® Core™ und Intel® Core™ Ultra Prozessoren ausgestattet sind, können komplette Bedrohungsklassen auf der Intel vPro® Plattform eliminieren. Verbessern und erweitern Sie die Schutzfunktionen der CrowdStrike Falcon® Plattform über den gesamten Stack hinweg.
- **Verbesserte Erkennung von Bedrohungen** Angriffsindikatoren (Indicators of attack, IOA) werden dank hardware-gestützter Exploit-Erkennung frühzeitig identifiziert.
- **Einsatz von Zero-Trust-fähigen Lösungen** Stellen Sie die Integrität von Geräten sicher, indem Sie den Sicherheitsstatus über Fernzugriff (SaaS) auf die Hardware-Telemetrie überwachen und Below-the-OS-Warnungen erhalten.
- **Optimierte Sicherheitsinvestitionen** Nutzen Sie die Vorteile und die Effizienzgewinne, die sich aus der Konsolidierung verschiedener Sicherheitslösungen ergeben.
- **Vereinfachte Aktivierung** Stellen Sie CrowdStrike Falcon® Lösungen auf einem Dell Gerät bereit, das auf der Intel vPro® Plattform basiert, und aktivieren Sie ganz einfach die Funktionen zur Überwachung Ihrer Geräte.

Zusammenfassung

Cyber-Bedrohungen sind inzwischen so ausgereift, dass sie herkömmliche Sicherheits-Software, die sich auf das Blockieren bekannter Malware konzentriert, leicht umgehen können. Viele Angriffe können diese älteren Tools einfach aushebeln. Hinzu kommt, dass Angreifer heute raffinierte Methoden einsetzen, die auf verschiedene Schichten des Computing-Stacks abzielen und sich in legitime Systemprozesse einschleichen. Diese Malware-freien Angriffe machen inzwischen 75 %[2] aller Cyber-Attacken aus. Darüber hinaus zeigen Untersuchungen von IBM, dass bis zu 90 % der erfolgreichen Attacken von einem Endgerät ausgehen.[3]

Und schließlich liegen viele Unternehmensendpunkte, die auf SaaS-Anwendungen zugreifen, aufgrund der zunehmenden hybriden Arbeitsmodelle außerhalb des herkömmlichen, abgesicherten Unternehmensnetzwerks. Dieses Zusammenspiel führt dazu, dass sich die Angriffsfläche effektiv vergrößert, und treibt die Einführung Cloud-nativer Software für Endpoint Detection and Response (EDR) und Extended Detection and Response (XDR) voran. Um den immer neuen und neuartigen Bedrohungen einen Schritt voraus zu sein, ist jedoch ein eng vernetztes Ökosystem erforderlich – sowohl auf Hardware- als auch auf Software-Ebene –, um einen nahtlosen, mehrschichtigen Schutz für die gesamte Angriffsfläche zu gewährleisten.

Aus diesem Grund haben Dell, Intel und CrowdStrike gemeinsam leistungsstarke Funktionen zur Erkennung und Abwehr von Bedrohungen entwickelt. Diese kombinieren die Stärken von Dell Trusted Devices, den branchenweit sichersten kommerziellen PCs[4], mit der Leistung von Intel® Prozessoren und der branchenführenden Endpunktsicherheits- und XDR-Plattform von CrowdStrike.[5]

Mit ihrer mehrschichtigen Lösung, die über den Software-Schutz hinausgeht und die Sicherheit hardware-basiert unterstützt, definieren CrowdStrike, Dell und Intel gemeinsam die Sicherheit von Endgeräten im Unternehmen ganz neu.

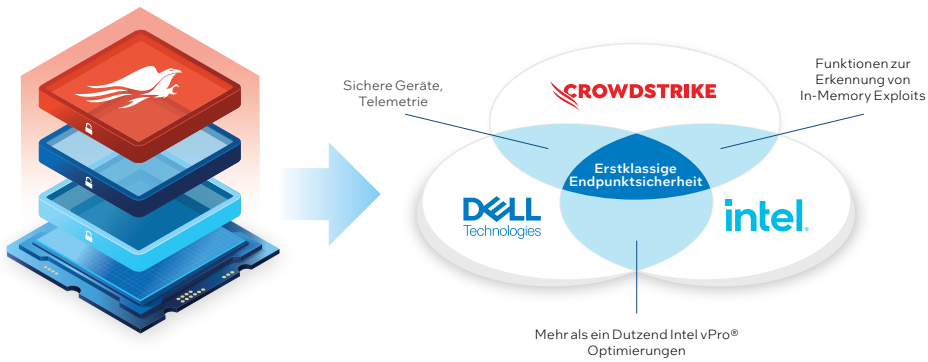

Abbildung 1. Mehrere Schutzschichten, die zusammenarbeiten

Die wachsende Angriffsfläche des PCs

Während Unternehmen daran arbeiten, die eine Angriffsfläche abzusichern, nehmen Bedrohungsakteure schon neue, leichtere Ziele ins Visier. Die Methoden für Exploit bzw. Initial Access sowie für bösartige Aktivitäten nach dem Exploit sind inzwischen sehr viel schwerer zu entdecken. Oftmals nutzen Angreifer legitimen Code, um sich einen ersten Zugang zu verschaffen, indem sie beispielsweise bereits in den Speicher geladene Befehle wiederverwenden. Immer häufiger werden nach dem Exploit schädliche Aktivitäten ausgeführt, bei denen keinerlei Malware auf den Endpunkt übertragen wird, z. B. durch In-Memory Code Injection, Living-off-the-Land(LotL)-Binaries und Skripte.

Malware-freie Methoden können den Weg freimachen für heimtückische Advanced Persistent Threats (APTs), Ransomware und weit verbreitete Dual-Use-Tools wie Cobalt Strike oder Sliver C2, die die Umgebung auskundschaften, bevor die eigentlich schädliche Payload ausgeführt wird. Speziell der Einsatz von Cobalt Strike bei Cyber-Angriffen ist um 161 % gestiegen. Scheinbar hat sich das Tool „in cyber-kriminellen Kreisen voll etabliert".[6]

Auch **Angriffe unterhalb des Betriebssystems** haben mit der Verbreitung hybrider Arbeitsmodelle zugenommen. In einer kürzlich durchgeführten Umfrage unter IT-Verantwortlichen weltweit berichteten 69 % der Befragten von mindestens einem Angriff auf Geräte-/BIOS-Ebene in den letzten zwölf Monaten. Das ist ein Anstieg um das 1,5-Fache gegenüber der Studie von 2020.[7]

Evolution von Defense-in-Depth – Hardware-gestützter Schutz der Angriffsfläche

Um diese komplexen Bedrohungen zu bekämpfen, ist eine enge Verzahnung von Hardware- und Software-Schutz erforderlich. Angesichts der Komplexität und des Umfangs der aktuellen Angriffe ist eine mehrschichtige, tiefgehende Abwehr von entscheidender Bedeutung. Wenn ein Angriff die erste Verteidigungslinie umgeht, gibt es weitere Schichten, die die Cyber Kill Chain unterbrechen können. Die gute Nachricht ist, dass die Hersteller in Sachen PC-Hardware-Sicherheit ebenfalls große Fortschritte gemacht haben. In die Hardware sind native Schutzmechanismen integriert, die ganze Angriffsklassen ausschalten und CPU-Telemetriedaten an Konsolen zum Bedrohungs-Management weiterleiten können, sodass schnell reagiert werden kann. Laut einer von IOActive durchgeführten Studie haben kommerzielle PCs von Dell mit Intel® Core™ Prozessoren der 13. Generation auf der Intel vPro® Plattform eine um bis zu 70% verringerte Angriffsfläche gegenüber der 6. Generation.[1]

Mit jeder neuen Generation bietet Intel vPro® neue Schutzfunktionen, die Sicherheitslösungen wie die CrowdStrike Falcon® Plattform noch effektiver machen. SecOps-Teams, die die Cybersecurity-Software von CrowdStrike auf Dell-PCs mit Intel vPro® Plattform einsetzen, erhalten eine einzigartige Suite integrierter Hardware- und Software-Funktionen zum Schutz der wachsenden Angriffsfläche.

Die einzelnen Technologien in Aktion

Intel vPro®: Für Unternehmen konzipiert

Seit mehr als 16 Jahren bietet die Intel vPro® Plattform eine umfassende, siliziumbasierte Lösung für den Schutz von Unternehmens-PCs und ist weltweit auf mehr als 300 Millionen Endgeräten im Einsatz.

Auf jeder Ebene wird eine sichere Grundlage geschaffen: Hardware, BIOS/Firmware, Hypervisor, VM, Betriebssystem und Anwendungen. Hinzu kommen KVM-Remote-Steuerung, temporäre Boot-Umleitung, Leistungsregler und nahtlose Firmware-Updates für die Verwaltung und Reparatur von Systemen in Remote- bzw. hybriden Arbeitsumgebungen. Die Intel vPro® Plattform verfügt über validierte Schutzmechanismen, die mit einer Vielzahl von Sicherheitsstandards getestet wurden, und bietet insgesamt 43 integrierte Abwehrmaßnahmen aus dem MITRE ATT&CK-Framework.[8]

Die in Intel vPro® enthaltene Intel® Thread Detection Technology (Intel® TDT) verstärkt den Schutz auf Hardware-Ebene. Mit KI-gestützten Sicherheitsfunktionen hilft Intel® TDT, Ransomware, Cryptomining und sogar Memory-Scanning-Angriffe effektiv abzuwehren.

Dell: Der branchenweit sicherste kommerzielle PC

Dell Trusted Workspace reduziert die Angriffsfläche von Unternehmens-PCs durch mehrschichtigen Schutz. Die „Built-with"-Sicherheit innerhalb der Lieferkette schafft eine vertrauenswürdige PC-Grundlage. SafeSupply-Chain-Lösungen bieten nicht nur einen sicheren Entwicklungszyklus und strenge Kontrollen der Lieferkette, sondern garantieren auch die Produktintegrität (z. B. die Dell-eigene Secured Component Verification).

Darüber hinaus verhindern und erkennen die einzigartigen integrierten hardware- und firmware-basierten Schutzmechanismen von Dell wie SafeBIOS grundlegende Angriffe unterhalb des Betriebssystems und bieten einzigartige Funktionen wie Off-Host-BIOS-Verifizierung und IOA. Dank SafeID verfügt das Gerät über einen speziellen Sicherheitschip mit FIPS Level 3 zum Schutz von Anmeldeinformationen und zur Benutzerauthentifizierung. Zusammen mit diesen BIOS-Schutzmechanismen und der Intel® Management Engine bietet die Anwendung Dell Trusted Device (DTD) zusätzliche, nur von Dell angebotene Funktionen wie die Off-Host-Verifizierung von Firmware.

Die integrierte Software-Sicherheit schließlich wird über ein Ökosystem von branchenführenden Partnern wie CrowdStrike bereitgestellt und bietet integrierten Schutz vor komplexen Bedrohungen. Für Kund:innen, die zusätzliche Unterstützung benötigen, bietet Dell Managed Detection and Response Support und Services rund um die Uhr.

Falcon Insight® XDR/EDR: Threat Detection und Response ganz einfach

CrowdStrike Falcon Insight® XDR sorgt für eine vollständige Transparenz der Endpunkte im gesamten Unternehmen – in Echtzeit. Es beschleunigt Sicherheitsprozesse und ermöglicht es Unternehmen, den Aufwand für die Bearbeitung von Warnmeldungen zu minimieren und die Zeit für die Analyse und Reaktion auf Angriffe zu reduzieren. Falcon Insight® XDR bietet Visibilität und ermöglicht tiefgreifende Analysen mithilfe KI-nativer Funktionen zur automatischen Erkennung verdächtiger Aktivitäten sowie zur Unterbindung getarnter Angriffe und Sicherheitsverstöße.

Falcon Insight® XDR nutzt Cloud-native Services zur dynamischen Verhaltenserkennung und Reaktion in Echtzeit. Der innovative, auf IOA basierende Ansatz von CrowdStrike bietet sofortigen Mehrwert. Die Falcon® Plattform verwendet IOA sowie Hardware- und andere Telemetriedaten, die vom kompakten Falcon® Agenten übermittelt werden, um unbekannte bösartige Verhaltensweisen abzuwehren. Die Angriffsindikatoren zielen darauf ab, die Intention eines Angreifers unabhängig von der verwendeten Malware oder dem Exploit zu erkennen. Die Optimierungen für die Intel vPro® Plattform bringen weitere Hardware-Sicherheitsfunktionen mit sich, die den innovativen IOA-Ansatz von CrowdStrike noch verbessern. Neben dem komplexen Netzwerk aus verhaltensbasierten IOA sendet Falcon® dem Agenten auch KI-gestützte Erkennungsmeldungen. Die KI-basierten Angriffsindikatoren werden mithilfe von Machine-Learning-Modellen generiert, die anhand riesiger Datensätze trainiert werden. Dazu gehören auch Verhaltensmuster und Telemetriedaten, die durch bestimmte Funktionen gewonnen werden. Diese wurden mithilfe von Intel® Prozessoren, auf denen der Falcon® Agent läuft, optimiert.

So funktioniert hardware-gestützte Sicherheit

Wie in Abbildung 2 dargestellt kann CrowdStrike Falcon® XDR/EDR Geräte-Telemetriedaten von kommerziellen Dell-PCs mit Intel vPro® sowie Intel® TDT nutzen, um selbst die bestgetarnten Angriffe zu erkennen.

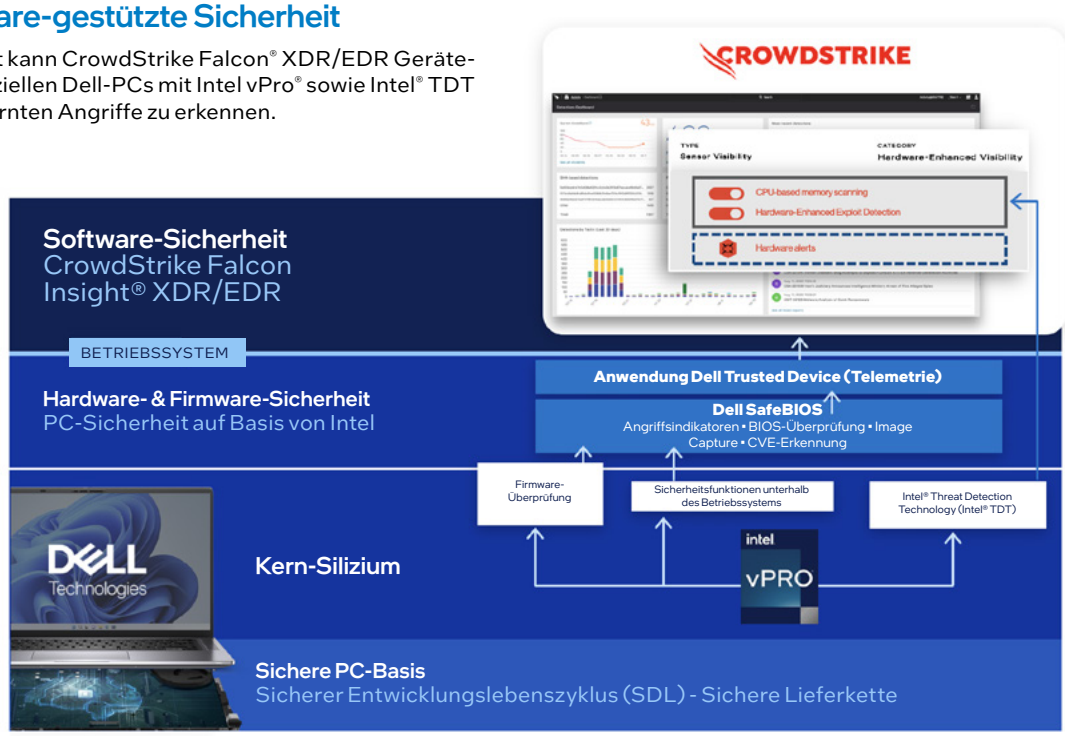

Abbildung 2. Schließen Sie die IT-Sicherheitslücke – mit Hardware- und Software-Schutzmaßnahmen, die ineinandergreifen

Anwendungsfälle

Wir nehmen zwei Angriffsszenarien unter die Lupe und zeigen auf, wie Hard- und Software-Funktionen ineinandergreifen, um die Kill Chain zu durchbrechen, bevor Schaden entsteht:

Anwendungsfälle	Beschreibung	Hardware-gestützte Abwehrmaßnahmen
Dateilose Malware-Angriffe	**Dateilose Malware-Angriffe** sind inzwischen die bevorzugte Methode bei Cyber-Attacken. Diese Methoden, zu denen LotL (native Tools/ Skriptmissbrauch) und die Execution in Memory gehören, können herkömmliche EDR-Software-Lösungen umgehen. So kann beispielsweise bei einem E-Mail-Phishing-Angriff durch Anklicken eines Links eine Cobalt-Strike-Beacon-Payload bereitgestellt werden, die den Erstzugriff ermöglicht und quasi „durch die Hintertür" (Backdoor) eine dauerhafte Command-and-Control-Infrastruktur einrichtet. Mit herkömmlicher EDR-Software, die nach Malware-Signaturen auf der Festplatte sucht und grundlegende Speicherprüfungen durchführt, aber nicht an KI-IOA gekoppelt ist, bleibt dies unter Umständen unerkannt. Das ultimative Ziel eines Cyberangriffs kann die Exfiltration von Daten durch Ransomware, der Zugriff auf das unternehmens-eigene VPN durch DLL-Hijacking, die Übernahme des Anwendungsspeichers durch ROP-Angriffe oder die Fehlerinjektion durch SMM-Angriffe auf BIOS-Ebene sein.	Die kommerziellen PCs von Dell bieten die Transparenz und Handlungsfähigkeit, die erforderlich sind, um diese Angriffe zu vereiteln. Sie nutzen proprietäre BIOS-/Firmware-Schutzmechanismen und die Intel® Control-Flow Enforcement Technology (Intel® CET), um die gesamte Klasse der ROP-Angriffe zu unterbinden. Die Hardware Enhanced Exploit Detection (HEED) von CrowdStrike nutzt die Intel® Processor Trace (Intel® PT) CPU-Telemetrie und weitet den Speicherschutz für Code-Injection-Verfahren auf alle PCs im Unternehmen aus. Darüber hinaus hat CrowdStrike die Art und Weise, wie dateilose Angriffe früh in der Angriffskette gestoppt werden können, neu überdacht. CrowdStrike nutzt dafür die beschleunigten Speicher-Scan-Algorithmen von Intel® TDT sowie dessen Fähigkeit, die Verarbeitung auf den integrierten Grafikprozessor von Intel® Graphics Technology zu verlagern. Die daraus resultierende 4- bis 7-fache Leistungssteigerung[9] trägt dazu bei, eine reibungslose Benutzererfahrung sicherzustellen, während CrowdStrike's dynamische IOA auf die Speicherebene angewendet werden – das gibt es so nur auf PCs mit Intel® Prozessoren. Wenn dateilose Angriffe versuchen, tiefer in den Stack einzudringen, nutzt Dell SafeBIOS die Intel® System Resource Defense Technologie der Intel vPro® Plattform, um Systemrechte einzuschränken und den böswilligen Zugriff auf das Betriebssystem zu verhindern.
Fundamentale Angriffe	In dem Maße, in dem sich die Sicherheit auf Ebene des Betriebssystems immer weiter verbessert, verlagern sich Angreifer immer mehr auf **fundamentale Angriffe**. Oft nutzen sie Rootkits und andere Schwachstellen in der Firmware, um verheerende Privilege-Escalation-Angriffe durchzuführen und sich Rechte anzueignen – diese Attacken können mit herkömmlicher EDR-Software allein kaum entdeckt werden. Insbesondere, wenn es viele Remote-Mitarbeitende in einer Organisation gibt, ist diese Art von Angriffen sehr schwer zu erkennen und zu beheben.	Kommerzielle PCs von Dell bieten dank integrierter Sicherheitsfunktionen eine erste Verteidigungslinie. SafeBIOS IOA und die Off-Host-Firmware-Überprüfung der Intel® Converged Security & Management Engine (Intel® CSME) verschaffen IT-SecOps-Teams beispielsweise einen besseren Eindruck von der Vertrauenswürdigkeit eines Geräts. Durch Nutzung der Telemetriedaten der Anwendung Dell Trusted Device kann CrowdStrike Falcon Insight® XDR dazu beitragen, potenzielle Firmware-Manipulationen und Abweichungen vom bekannten intakten Image aufzudecken, sodass fundamentale Angriffe besser erkannt werden können. Zur Schadensbehebung nutzt die Dell Client Command Suite die Out-of-Band-Verwaltungsfunktionen der Intel vPro® Plattform, um Administrator:innen mit einer KVM-Remote-Steuerung auszustatten. So können sie ein Gerät aufwecken, sein Hauptlaufwerk löschen oder ein von Intel® Firmware Guard unterstütztes Firmware-Update einleiten, um das Risiko eines Systemabsturzes zu minimieren. In Kombination bieten die Lösungen von Dell, Intel und CrowdStrike eine einzigartige, mehrschichtige Defense-in-Depth, die die Arbeit von SecOps-Teams unterstützt und Schutz, Abwehr und Beseitigung neuer Cyber-Bedrohungen wirkungsvoll verbessert.

Tabelle 1. Angriffsszenarien

Einfache Aktivierung

Dank der dreifachen Zusammenarbeit zwischen Dell, Crowdstrike und Intel bietet die Benutzeroberfläche der Falcon® Plattform IT-Administrator:innen einen Bildschirm für Präventionsrichtlinien, auf dem sie sowohl HEED- als auch Accelerated-Memory-Scanning(AMS)-Funktionen aktivieren können. Um sämtliche Unternehmens-PCs zu schützen, können IT-Administrator:innen zusätzlich zur Erkennung auch Richtlinien zur Vorbeugung hinzufügen. Wenn die Anwendung Dell Trusted Device (DTD) aktiviert ist, wird die Erkennung und Reaktion zusätzlich durch Telemetriedaten von unterhalb des Betriebssystems gespeist. Sicherheitsbenachrichtigungen und -warnungen auf Geräteebene werden in Dell Konsolen (über die Windows Ereignisanzeige) angezeigt. Administrator:innen können Schwachstellen auf BIOS-Ebene auch per Fernzugriff in der Falcon® Konsole anzeigen und dabei auf dieselben DTD Telemetriedaten zurückgreifen.

Den Wert Ihrer Sicherheitsinvestitionen maximal ausschöpfen

Auf kommerziellen Dell PCs mit der Intel vPro® Plattform verbessert CrowdStrike Falcon® die Effizienz und Leistung von XDR-/EDR-Lösungen. Dell Kund:innen können CrowdStrike Falcon® Lösungen im Paket mit Dell Hardware erwerben. Wählen Sie die passende Lösung für Ihr Unternehmen aus (Tabelle 2).

Sie können CrowdStrike Falcon® Lösungen auch jederzeit zu bereits vorhandener Hardware hinzukaufen.

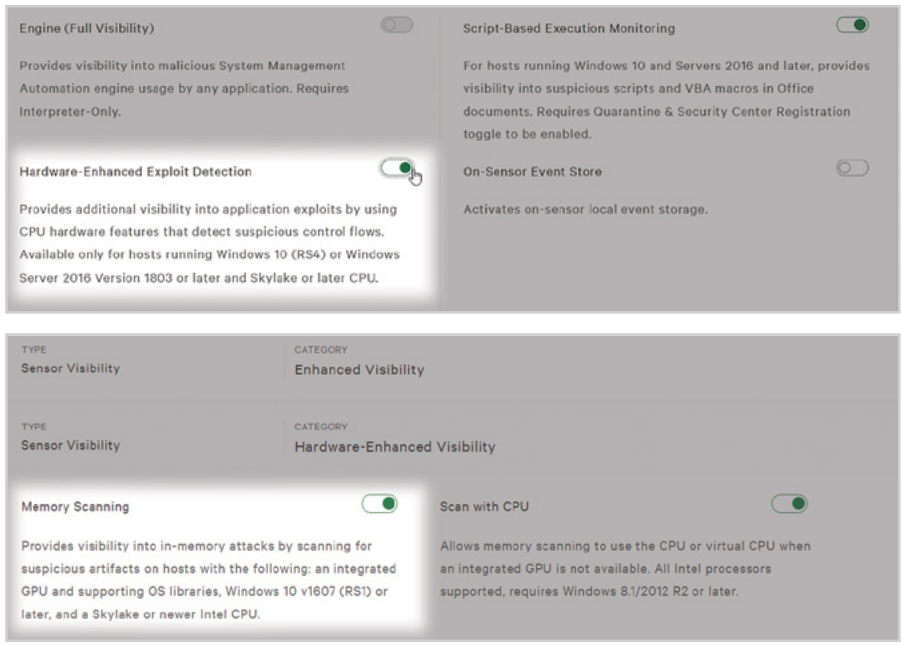

Abbildung 3. Mit Präventionsrichtlinien können Administrator:innen HEED- und AMS-Funktionen aktivieren und von der Zweifachnutzung profitieren.

Zielgruppe	Lösungen
Unternehmen	Dell: Latitude, OptiPlex, Precision and Rugged, Intel vPro® Enterprise

Tabelle 2. Empfohlene Kombinationen

Weitere Informationen

Sehen Sie sich das Demo-Video an

oder kontaktieren Sie uns direkt: global.security.sales@Dell.com

Lösung bereitgestellt von:

intel. DELL Technologies CROWDSTRIKE

[1] Neue PCs mit Intel vPro® bieten eine Reduzierung der Angriffsfläche um schätzungsweise 70 % im Vergleich zu vier Jahre alten Geräten. Basierend auf der im März 2023 veröffentlichten Studie „Intel vPro 13th Gen Attack Surface Study" von IOActive (im Auftrag von Intel), die Intel vPro® Geräte mit Intel® Core™ Prozessoren der 13. Generation vergleicht mit 4 Jahre alten PCs mit Intel® Prozessor und Windows. Weitere Informationen finden Sie unter www.intel.com/performance-vpro. Die Ergebnisse können von Fall zu Fall abweichen.

[2] Quelle: CrowdStrike 2024 Global Threat Report

[3] Quelle: IBM Endpunktsicherheit

[4] Quelle: Basierend auf internen Analysen von Dell, September 2023. Gilt für PCs mit Intel® Prozessoren. Nicht alle Funktionen sind auf allen PCs verfügbar. Einige Funktionen müssen zusätzlich erworben werden.

[5] Quelle: Gartner Magic Quadrant, 2022

[6] Quelle: Cobalt Strike Usage Explodes Among Cybercrooks. Threatpost

[7] Quelle: The Futurum Group, Endpoint Security Trends, 2023

[8] Quelle: Mit jeder Plattform entwickelt Intel seine Sicherheitsfunktionen weiter und bietet Neuerungen und Updates für bestehende Funktionen. Intel verfügt über die erste und einzige hardware-basierte Erkennung von Bedrohungen dieser Art. Sie ergänzt die vorhandene Sicherheits-Software und ermöglicht eine hochwirksame Erkennung von Ransomware, Cryptojacking-Attacken, Supply-Chain-Angriffen und sogar Zero-Day-Angriffen. Darüber hinaus arbeitet Intel mit dem größten Ökosystem zur Etablierung von Silizium-Sicherheitsfunktionen als Teil einer Defense-in-Depth-Strategie zusammen. Des Weiteren haben Expert:innen von Intel und Coalfire die Hardware-Sicherheitsfunktionen auf Intel vPro® Systemen mit Sicherheitsstandards (NIST, MITRE, TCG) verglichen, wobei sich unter diesen Funktionen 43 MITRE ATT&CK-Abwehrmaßnahmen befinden.

[9] Quelle: CrowdStrike AMS Blog, März 2022. Crowdstrike fand heraus, dass die Intel® Threat Detection Technology das Scannen um das 7-fache beschleunigen kann, was zu einer schnelleren Erkennung von dateilosen Angriffen führt, der häufigsten Einstiegsmethode. Die mit Falcon durchgeführten Tests zur Auslagerung von Speicher-Scans auf den integrierten Grafikprozessor im Vergleich zu CPU-Scans werden in einem aktuellen Blogartikel von CrowdStrike beschrieben. Weitere Informationen finden Sie unter www.intel.com/performance-vpro. Die Ergebnisse können von Fall zu Fall abweichen.

05/24/DCC/PDF