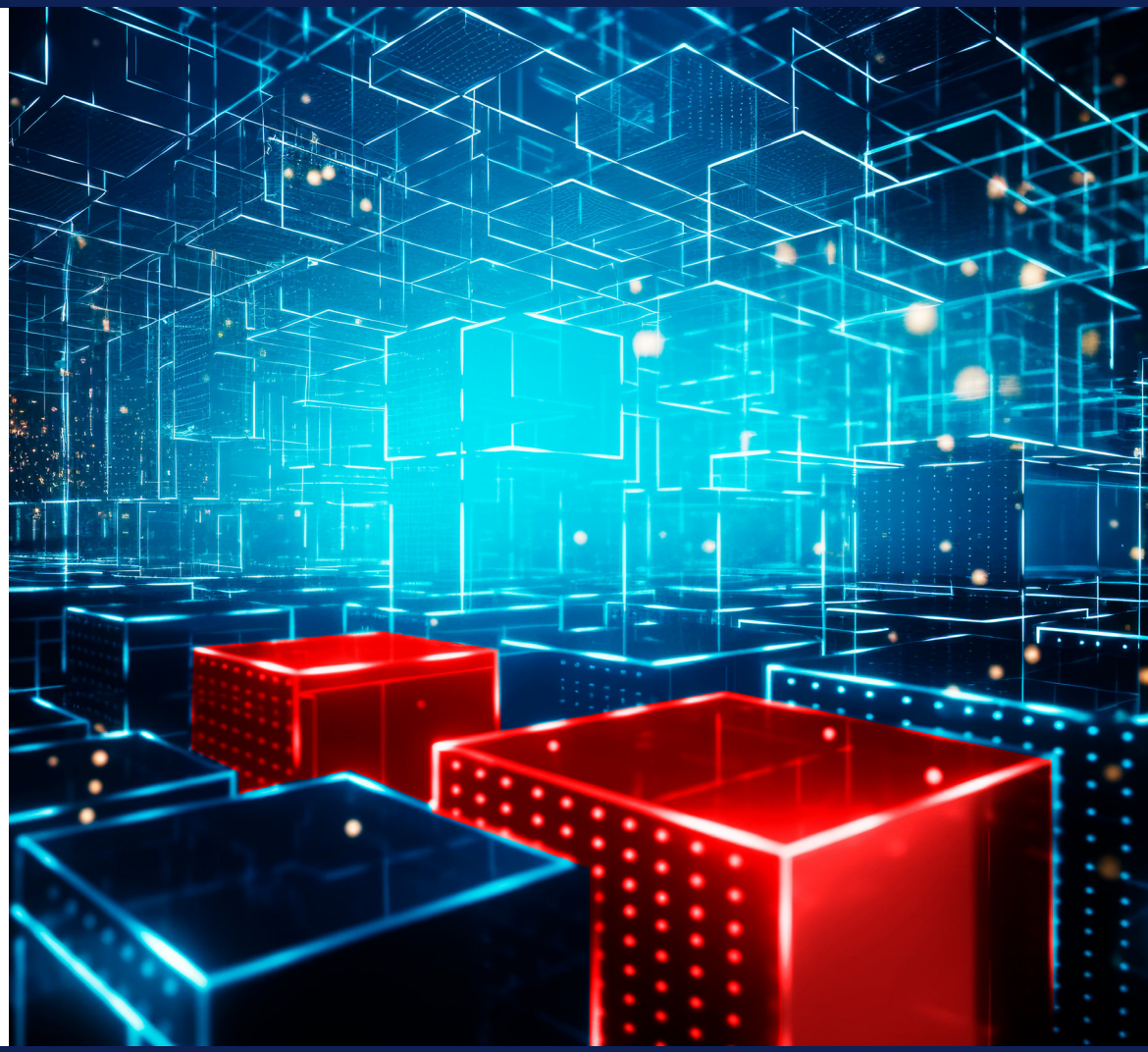
Het gebruik van AI op het eindpunt beveiligen

Verdedig AI-workloads op het apparaat met veilige, moderne apparaten en een aanvallersmentaliteit.



Executive summary

AI op het apparaat biedt enorme voordelen, maar brengt ook cyberrisico's met zich mee. In dit eBook bespreken we hoe u uw organisatie veilig kunt positioneren om te profiteren van AI-innovatie op het eindpunt.

Inhoudsopgave

Het aanvalsoppervlak van AI op het apparaat

Beveiligingsrisico's op het eindpunt

Noodzakelijke tegenmaatregelen

Best practices toepassen op uw computerpark

Belangrijkste punten en vervolgstappen

Het aanvalsoppervlak van AI op het apparaat

Wat kan worden aangevallen

Alle opkomende technologieën brengen cyberbeveiligingsrisico's met zich mee om één reden: het is een nieuw terrein. U hebt te maken met het onbekende. We zagen het eerder al bij cloudcomputing, blockchain en tal van andere technologieën. Hetzelfde geldt nu voor AI op het apparaat. De sleutel tot het beheersen van dat risico is, zoals altijd, zicht krijgen op het onbekende.

Voordat we kunnen praten over de beveiliging die nodig is om het aanvalsoppervlak te verkleinen, is het belangrijk om eerst te begrijpen wat we eigenlijk aan het beveiligen zijn en waarom. Denk aan een systeem van leidingen in een commercieel gebouw waarin meerdere bedrijven gevestigd zijn. Die leidingen transporteren water, gas, enzovoort, door het hele gebouw, en dienen verschillende toepassingen. Als de inhoud van die leidingen wordt besmet of verstoord, kan die zijn functie niet vervullen. En als de leidingen zelf beschadigd of aangetast zijn, kunnen ze hun functie ook niet vervullen. Zowel de leidingen als hun inhoud moeten in goede staat zijn om de behoeften van hun specifieke toepassingen te kunnen ondersteunen.►

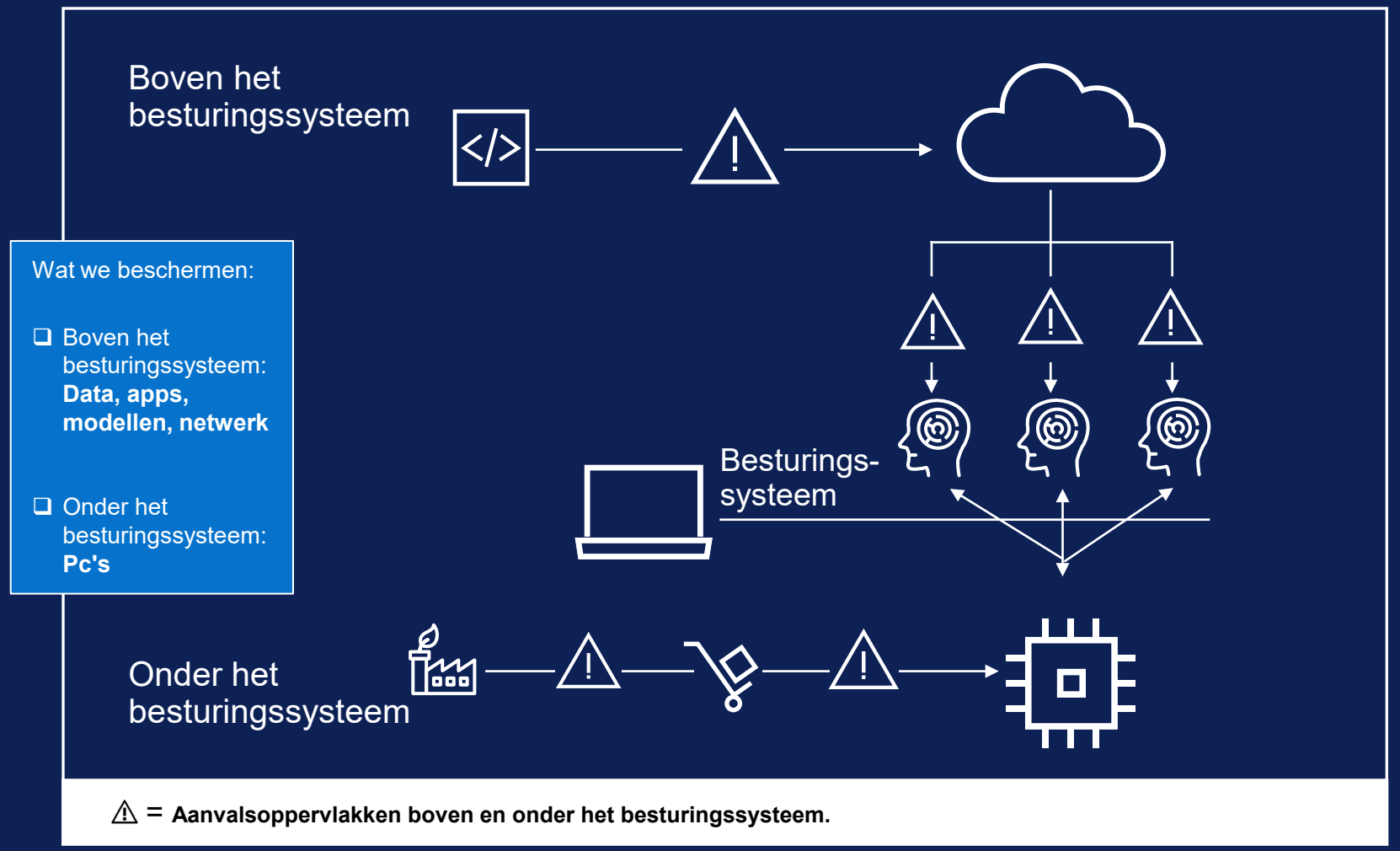
Het aanvalsoppervlak van AI op het apparaat, vervolg

Wat kan worden aangevallen, vervolg

Terug naar AI op het eindpunt:

- De leidingen vormen uw infrastructuur: uw pc's, uw bedrijfsnetwerken. De manier en de plek waarop u werkt.
- De inhoud die door de leidingen stroomt, zijn de data, apps en modellen die allerlei AI-toepassingen aandrijven. Dat zijn de assets en resources die u nodig hebt om uw werk te doen.

En u raadt het al. Cyberaanvallers richten zich op allebei. Zij kunnen intellectueel eigendom (IP) stelen en daarmee losgeld eisen, of data of modellen vergiftigen om de processen te verstoren. In beide gevallen zijn de gevolgen ernstig: van financiële schade en imagoverlies tot het risico op toezicht door toezichthouders of regelgevende instanties.►



Beveiligingsrisico's op het eindpunt

Tactieken die aanvallers gebruiken om toegang te krijgen

Laten we nu kijken naar methoden die aanvallers kunnen gebruiken om toegang te krijgen tot beide doelwitten.

Compromittering van het apparaat. Zoals we zien in het rapport Endpoint Security Market Insights, van Forrester Research, Inc., maart 2025, behoren pc's tot de belangrijkste doelwitten van moderne cyberdreigingen. Dit type aanval kan al plaatsvinden lang voordat het AI-werk op het apparaat begint, bijvoorbeeld via een **aanval op de hardware- of softwareleveringsketen**. Er zijn tientallen, zo niet honderden punten in de toeleveringsketen waar een kwaadwillende partij componenten kan manipuleren, denk aan circuits, firmware, enzovoort, om zwakke plekken in te bouwen die later misbruikt kunnen worden. Stelt u zich eens voor dat een investeringsmaatschappij een gloednieuwe levering pc's ontvangt met vervalste componenten erin.

Compromittering van identiteit. Datalekken waarbij gestolen of gecompromitteerde inloggegevens zijn gebruikt, behoren tot de snelst groeiende aanvalsmethoden van dit moment. Dat is niet verrassend. Aanvallers die geldige inloggegevens gebruiken, kunnen inloggen op een pc, zich vrij bewegen binnen het bedrijfsnetwerk en lange tijd onopgemerkt blijven. Volgens het meest recente Cost of a Data Breach-rapport van IBM duurde het gemiddeld 292 dagen om dit soort datalekken te identificeren en beheersen, het langste van alle onderzochte aanvalsvectoren. Dat soort diepgaande toegang is simpelweg te waardevol voor dreigingsactoren om te negeren. Uit onderzoek van Zscaler blijkt dat kwaadwillenden hun technieken voor diefstal van inloggegevens aan het verfijnen zijn. Ze zetten daarbij generatieve AI in om phishingaanvallen op te schalen en te verbeteren. Wanneer deze ongeautoriseerde toegang wordt gebruikt voor toegang tot gevoelige trainingsdata, inferentiedata of rechtstreeks tot modellen, spreken we van een **aanval op de modelleveringsketen**.

Bedreiging van binnenuit. Uit recent onderzoek blijkt dat **kwaadwillende aanvallen van binnenuit**, vergeleken met andere aanvalsvectoren, hebben geleid tot de hoogste kosten, gemiddeld USD 4,99 miljoen. Houd er rekening mee dat aanvallen van binnenuit kunnen voorkomen in de hardwareleveringsketen, de softwareleveringsketen en de modelleveringsketen.►

Gemiddelde tijd voordat een eindgebruiker op een **phishing**-mail klikt: minder dan 60 seconden*

Gemiddelde tijd om een **gecompromitteerde identiteit** te ontdekken en te beheersen: 292 dagen**

Kwaadwillende aanvallen van binnenuit kosten gemiddeld USD 4,99 miljoen**

*Bron: Verizon DBIR, 2024
**Bron: IBM Cost of a Data Breach, 2024

Noodzakelijke tegenmaatregelen

Wat het risico beperkt

Geen van deze aanvalsdoelwitten is fundamenteel nieuw. Ook de einddoelen van aanvallers zijn dat niet. Zoals altijd willen we ons richten op het beveiligen en veerkrachtig houden van uw computerpark. **Het toepassen van meerdere beveiligingslagen** kan helpen om het aanvalsoppervlak te verkleinen en elk verdacht gedrag onmiddellijk in kaart te brengen.

Een **Zero Trust-mentaliteit** beperkt de risico's in uw computerpark. Deze principes – nooit vertrouwen, altijd verifiëren en continu bewaken – helpen u om een stap voor te blijven op aanvallers. Het is onmogelijk om 100% van de aanvallen te blokkeren. Voor een sterke beveiligingsmentaliteit hebt u **zichtbaarheid en controle** nodig over uw volledige IT-ecosysteem.

Met dat framework in gedachten, is het tijd om uw infrastructuur opnieuw te beoordelen, met name systemen en processen die interacteren met AI. Welke tegenmaatregelen minimaliseren het risico op compromittering van apparaten, compromittering van identiteit en bedreigingen van binnenuit?►

Zero Trust-principes helpen u tegen risico's te beschermen en de impact van cyberactiviteiten te beperken

- Ga uit van het worst-case-scenario
- Geen impliciet vertrouwen
- Voortdurende authenticatie

Noodzakelijke tegenmaatregelen, vervolg

Wat het risico beperkt, vervolg

Er zijn twee hoofdcategorieën van tegenmaatregelen.

"Beveiliging onder het besturingssysteem" beschermt de AI-apparaten waarop u werkt. We kunnen dit in twee onderdelen opsplitsen:

- Bescherm uw computerpark met apparaten die **veilig zijn ontworpen**. Dit betekent het gebruik van AI PC's die 'secure by design' zijn, ontwikkeld volgens beveiligingsprincipes en binnen een beveiligde leveringsketen.
- Bescherm uw computerpark met apparaten met **ingebouwde beveiliging**. Veilige AI PC's beschikken over geïntegreerde beveiligingslagen die direct uit de verpakking zichtbaarheid bieden, tot op BIOS- en silicium-niveau.

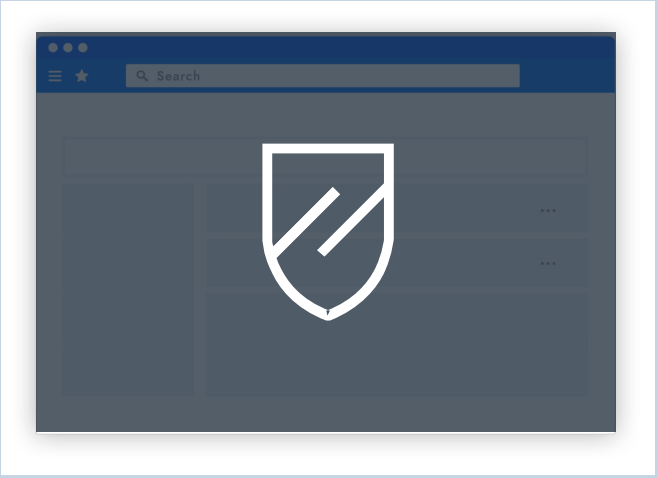
"Beveiliging boven het besturingssysteem" beschermt de toegang tot AI-modellen. Verdedig de data en modellen *waarmee* u werkt en de bedrijfsnetwerken *waarin* u werkt met **softwarebeveiliging**. Het is essentieel om de beveiligingsactiviteiten rond machine learning te beschermen en het netwerkverkeer van geïmplementeerde AI-workloads te bewaken.►

Beveiliging onder het besturingssysteem

Veilige AI PC's

Hardware- en firmwarebeveiliging, beveiliging van de leveringsketen, core silicon

Beveiliging boven het besturingssysteem



Softwarebeveiliging

Extra beveiligingslaag voor eindpunten, netwerken en cloudomgevingen

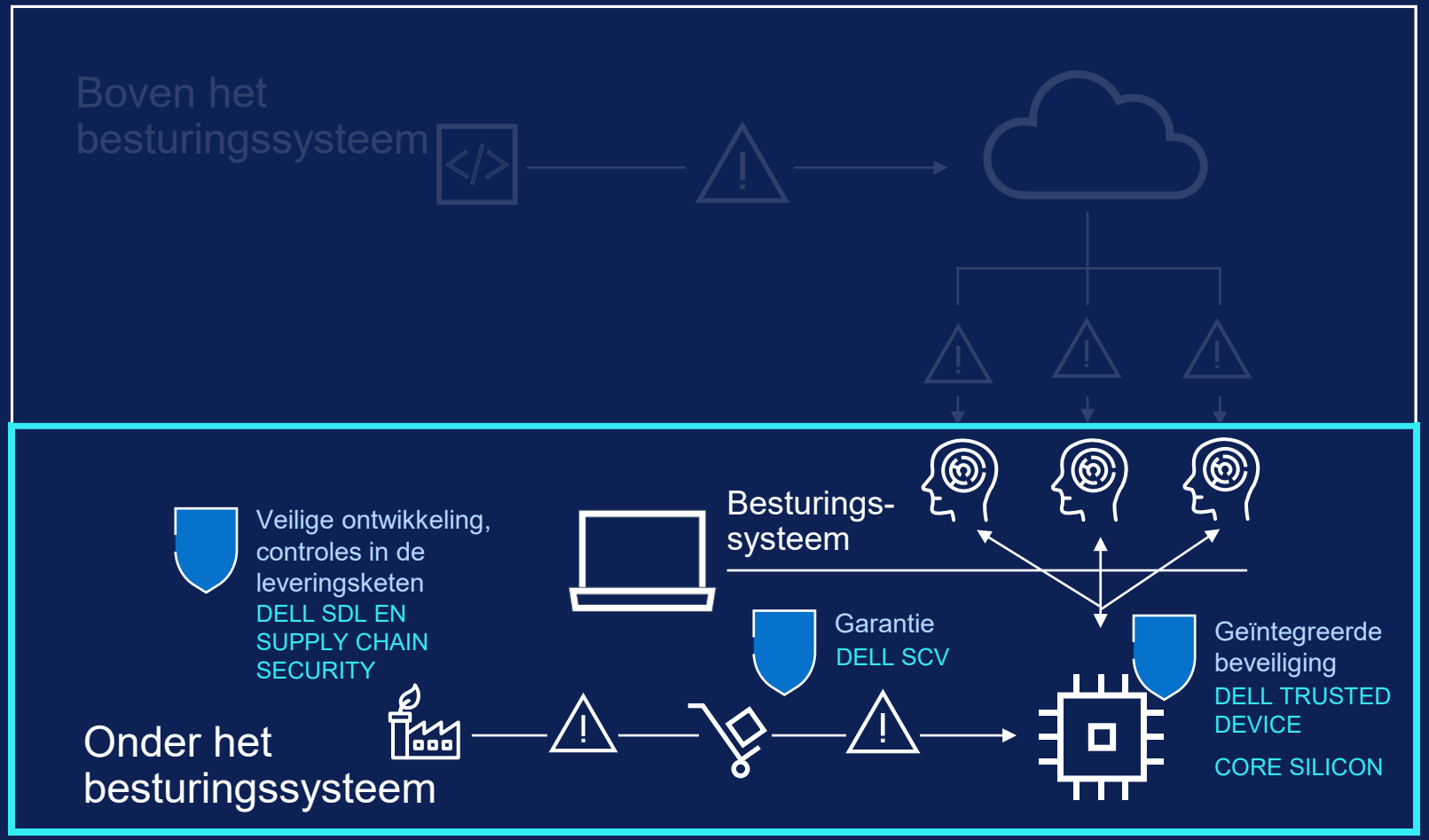
Beveiligingsservices en expertise beschikbaar om alles samen te voegen.

Best practices toepassen op uw computerpark

Hoe Dell AI PC's fundamentele beveiliging bieden voor uw computerpark

Dit is waar Dell Trusted Workspace u kan helpen. Onze technici ontwerpen en ontwikkelen de beveiliging van onze zakelijke AI PC's met een diepgaand begrip van de aanvallersmentaliteit.

Onder het besturingssysteem zorgen veilig ontwerp, robuuste controle van de leveringsketen en optionele leveringsketengarantie ervoor dat pc's vanaf de eerste opstart veilig zijn. Ingebouwde hardware- en firmwarebeveiliging beschermen de pc tijdens gebruik, bijv. de unieke* sabotagedetectie op BIOS-niveau van Dell (Dell SafeBIOS) en wachtwoordloze toegangsbeveiliging op basis van inloggegevens (Dell SafeID), die beschermen tegen ongeautoriseerde toegang. Daarnaast dragen de Intel®-siliciumtechnologieën bij aan een sterke basis voor de bescherming van verschillende aspecten van AI op AI PC's. Zo helpt Intel bij het beveiligen van AI-data in rust op het apparaat, door middel van versnelling van modelversleuteling op de schijf.►



Best practices toepassen op uw computerpark, vervolg

Hoe Dell AI PC's fundamentele beveiliging bieden voor uw apparatuur, vervolg

Om deze beveiliging onder het besturingssysteem aan te vullen, kan de Persistence-technologie van onze partner Absolute in de fabriek worden geïntegreerd voor nog meer zichtbaarheid en controle gedurende de hele pc-levenscyclus. Dit maakt bijvoorbeeld geolocatie van apparaten tijdens transport mogelijk en zelfherstel van kritieke applicaties in het slechtste scenario.

Dell heeft bovendien een ecosysteem van softwarepartneroplossingen samengesteld, waaronder CrowdStrike Falcon XDR en absolute Secure Access, die Zero Trust-principes activeren om uw modelleveringsketen te beschermen tegen ongeautoriseerde toegang **boven het besturingssysteem**. Met deze oplossingen kunt u beleid maken en afdwingen via granulaire toegangscontroles (bijv. rolgebaseerde toegangscontrole of RBAC) om het risico te beperken dat kwaadwillende insiders toegang krijgen tot uw AI-modellen of deze manipuleren.▶

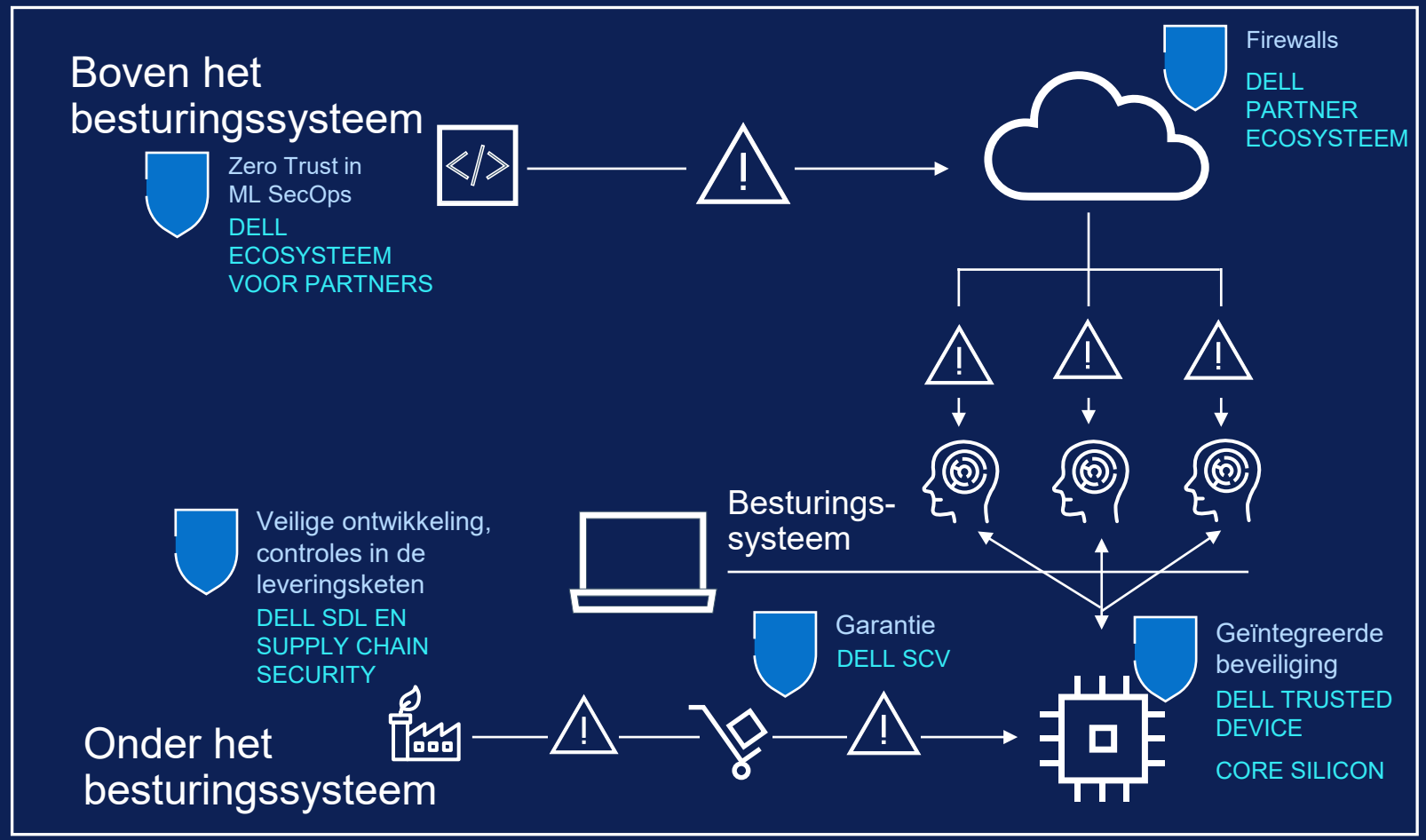
Best practices toepassen op uw computerpark, vervolg

Hoe Dell AI PC's fundamentele beveiliging bieden voor uw apparatuur, vervolg

Dit alles samen vormt ***beveiliging voor AI.*** Deze mogelijkheden beschermen AI-workloads op het apparaat tegen cyberaanvallen, zodat u zich kunt blijven richten op innovatie en zakelijk succes.►

Stop geavanceerde eindpuntaanvallen met gecoördineerde hardware- en softwarebeveiliging

Dell werkt samen met Intel en CrowdStrike om de beveiligingslagen onder en boven het besturingssysteem te integreren met door hardware ondersteunde beveiliging. *Meer informatie >*



Belangrijkste punten en vervolgstappen

Beveilig AI op het eindpunt met Dell

Bedrijven zijn enthousiast over AI, maar de AI-gereedheid blijft achter. Dit blijkt uit een recente enquête onder CISO's, uitgevoerd door Absolute. Een analyse van miljoenen apparaten toont aan dat het huidige pc-landschap niet in staat is om nieuwe AI-mogelijkheden op brede schaal te ondersteunen. **Dell kan u helpen alles samen te brengen.**

Ontwikkel en implementeer AI-modellen op een veilige, moderne basis. Ondersteuning voor Windows 10 eindigt in oktober 2025. Pc's ontvangen dan geen beveiligingsupdates, updates van functies en Windows 10-ondersteuning meer. Oudere apparaten voldoen mogelijk niet aan de Windows 11-vereisten en hebben niet de nieuwste geïntegreerde prestatie- en beveiligings- en AI-verbeteringen. Upgrade naar **Dell Pro** of **Dell Pro Max op basis van Intel® Core™ Ultra processors met Intel vPro®** om beveiligingsvoordelen te ontgrendelen en AI-workloads te beschermen met **'s werelds veiligste zakelijke AI PC's.*** ►

Ondersteuning voor Windows 10 eindigt in oktober.

Upgrade naar de nieuwste Dell AI PC's op Intel om beveiligingsvoordelen en AI-verbeteringen te ontgrendelen:

Koop Dell Pro ● Dell Pro Max

*'s Werelds veiligste zakelijke AI PC's**

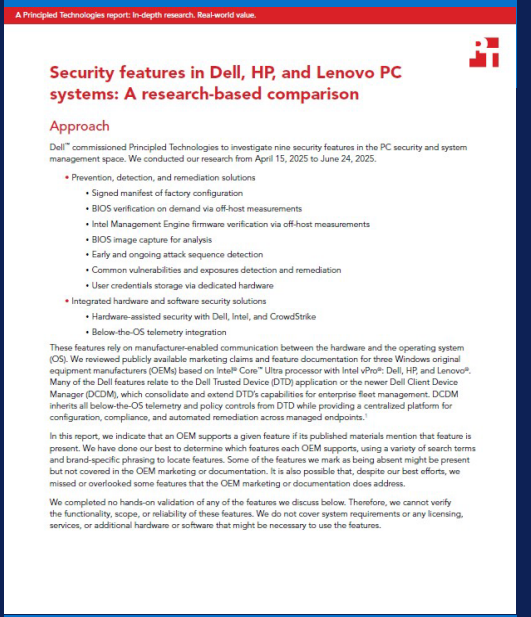
Ontdek aanvullende software en services om uw beveiligingsmentaliteit te versterken:

Software en integraties

Services

LEIDERS IN DE BRANCHE

Principled Technologies heeft vastgesteld dat Dell en Intel op het gebied van zakelijke AI PC-beveiliging beter presteren dan hun concurrenten


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

Security features in Dell, HP, and Lenovo PC systems: A research-based comparison

Approach

Dell™ commissioned Principled Technologies to investigate nine security features in the PC security and system management space. We conducted our research from April 15, 2025 to June 24, 2025.

- Prevention, detection, and remediation solutions
  - Signed manifest of factory configuration
  - BIOS verification on demand via off-host measurements
  - Intel Management Engine firmware verification via off-host measurements
  - BIOS image capture for analysis
  - Early and ongoing attack sequence detection
  - Common vulnerabilities and exposures detection and remediation
  - User credentials storage via dedicated hardware
- Integrated hardware and software security solutions
  - Hardware-assisted security with Dell, Intel, and CrowdStrike
  - Below-the-OS telemetry integration

These features rely on manufacturer-enabled communication between the hardware and the operating system (OS). We reviewed publicly available marketing claims and feature documentation for three Windows original equipment manufacturers (OEMs) based on Intel® Core™ Ultra processor with Intel vPro®: Dell, HP, and Lenovo®. Many of the Dell features relate to the Dell Trusted Device (DTD) application or the newer Dell Client Device Manager (DCDM), which consolidate and extend DTD's capabilities for enterprise fleet management. DCDM inherits all below-the-OS telemetry and policy controls from DTD while providing a centralized platform for configuration, compliance, and automated remediation across managed endpoints.[1]

In this report, we indicate that an OEM supports a given feature if its published materials mention that feature is present. We have done our best to determine which features each OEM supports, using a variety of search terms and brand-specific phrasing to locate features. Some of the features we mark as being absent might be present but not covered in the OEM marketing or documentation. It is also possible that, despite our best efforts, we missed or overlooked some features that the OEM marketing or documentation does address.

We completed no hands-on validation of any of the features we discuss below. Therefore, we cannot verify the functionality, scope, or reliability of these features. We do not cover system requirements or any licensing, services, or additional hardware or software that might be necessary to use the features.

Lees het onderzoek

Disclaimers

*Gebaseerd op een analyse van derden door Principled Technologies bij het vergelijken van zakelijke AI PC's van Dell op Intel processors met HP en Lenovo, juli 2025. Ondersteund door interne analyse van Dell van de wereldwijde pc-markt, oktober 2024. Van toepassing op pc's met Intel processors. Niet alle functies zijn beschikbaar voor alle pc's. Extra aankoop vereist voor sommige functies.

Meer informatie:

Neem contact met ons op: Global.Security.Sales@Dell.com.

Bezoek ons: Dell.com/Endpoint-Security

Volg ons: LinkedIn @DellTechnologies | X @DellTech

Over Dell Endpoint Security

Beveiliging is een groot onderwerp voor organisaties groot en klein. **Werk samen met een ervaren beveiligings- en technologiepartner om de beveiliging van eindpunten te moderniseren**.

Dell Trusted Workspace helpt om eindpunten te beveiligen voor een moderne IT-omgeving die klaar is voor Zero Trust. Beperk het aanvalsoppervlak en verbeter uw cybertolerantie met een uitgebreid portfolio van hardware- en softwarebescherming, exclusief beschikbaar via Dell. Onze zeer gecoördineerde verdedigingsgebaseerde aanpak pakt bedreigingen aan door geïntegreerde bescherming te combineren met doorlopende waakzaamheid. Eindgebruikers blijven productief en IT kan vertrouwen op beveiligingsoplossingen die zijn gemaakt voor de moderne cloudgebaseerde wereld.