

▶ ONTDEK

Dell Trusted Workspace



Veilig overal werken

met hardware- en softwarebescherming die is gebouwd voor de cloudgebaseerde wereld van vandaag.

Hybride werk heeft organisaties blootgesteld aan nieuwe aanvalsvectoren. Naarmate aanvallers steeds geavanceerdere technieken gebruiken, zijn er tegenwoordig meerdere verdedigingslagen nodig voor een effectieve eindpuntbeveiliging van apparaten, netwerken en de cloud.

Verklein het aanvalsoppervlak en blijf moderne bedreigingen voor met een uitgebreid portfolio aan hardware- en softwarebeveiliging.

[Meer informatie over portfolio →](#)



['s Werelds meest veilige zakelijke pc's¹ →](#)



[Software om de beveiliging van ieder apparaat te verbeteren →](#)

Meerdere beschermingslagen



Toegevoegd **Softwarebeveiliging**

Combineer geavanceerde bescherming tegen bedreigingen met software uit een vakkundig geselecteerd partnerecosysteem. Profiteer van de voordelen en efficiëntie wanneer u uw beveiligingsaankopen consolideert.

Geïntegreerd **Hardware- en firmwarebeveiliging**

Voorkom en detecteer fundamentele aanvallen met de veiligste zakelijke pc's in de branche.¹ Diepgaande verdediging op BIOS-/firmware- en hardwareniveau zorgt ervoor dat het apparaat ook tijdens gebruik goed beschermd blijft.

Alleen Dell integreert de pc-telemetrie met toonaangevende software om de beveiliging van alle apparaten in de onderneming te verbeteren.¹

Ontworpen met **Beveiliging van leveringsketen**

Werk vol vertrouwen in de wetenschap dat uw apparaat goed beveiligd is, al vanaf de eerste keer opstarten. Veilig ontwerp, ontwikkeling en het testen van pc's om het risico op kwetsbaarheden in het product tot een minimum te beperken. Rigoureuze controles van de leveringsketen verminderen het risico op productsabotage.



Voorkom, detecteer en reageer op dreigingen, waar ze zich ook voordoen

Dell SafeGuard and Response

Dell SafeData



Blijf beschermd tegen evoluerende bedreigingen

Dell SafeBIOS

Dell SafeID

Dell SafeShutter

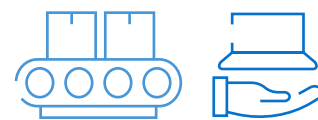


Bij Trust-hardware weet u zeker dat er niet is geknoeid met de geleverde hardware

Dell SafeSupply Chain

Dell Trusted Workspace Gebouwd met en geïntegreerde beveiliging

Veiligste zakelijke pc's in de branche¹



Wees veilig vanaf de eerste keer opstarten

Strikte, geavanceerde controles van de leveringsketen en optionele add-ons, zoals de unieke **Secured Component Verification** van Dell, bieden zekerheid over de integriteit van de pc.

[Meer informatie](#) →

Verifieer de firmware-integriteit

Exclusieve **firmwareverificatie** van Dell. Deze hardwaregebaseerde beveiliging bevindt zich in Intel-processors en beschermt tegen ongeoorloofde toegang tot en manipulatie van firmware met hoge bevoegdheden.

Beveilig de referenties van eindgebruikers

Controleer de toegang van gebruikers met het unieke **SafeID** van Dell, een speciale beveiligingchip die gebruikersreferenties verborgen houdt voor malware.

[Meer informatie](#) →

Behoud van BIOS-integriteit

Detecteer bedreigingen en bestrijd ze met **SafeBIOS**, de unieke BIOS-verificatie van Dell. Beoordeel een beschadigd BIOS, herstel het en krijg inzichten die de blootstelling aan toekomstige bedreigingen verminderen.

[Meer informatie](#) →

Ontdek tikkende tijdbommen

Indicators of Attack is een functie voor vroegtijdige waarschuwing die alleen door Dell wordt aangeboden. Deze functie scant bedreigingen die op gedrag zijn gebaseerd voordat ze schade kunnen veroorzaken.

Behoud schermprivacy

De **SafeShutter** webcam met sensoren wordt automatisch geopend of gesloten, en gesynchroniseerd met toepassingen voor videoconferencing.

Verbeter de beveiliging met pc-telemetrie

Verklein de kloof op het gebied van IT-beveiliging met Dell Trusted Device-software. Alleen Dell integreert pc-telemetrie met toonaangevende softwareleveranciers om de beveiliging van de volledige computeromgeving te verbeteren.¹ [Ontdek meer](#) →

Ontdek Dell Trusted Devices



[Latitude](#) →



[OptiPlex](#) →



[Precision](#) →

Dell Trusted Workspace Toegevoegde beveiliging

Software om de beveiliging van ieder apparaat te verbeteren



Voorkom geavanceerde cyberaanvallen met **Dell SafeGuard and Response**

Voorkom, detecteer en reageer op dreigingen, waar ze zich ook voordoen. Kunstmatige intelligentie en machine learning detecteren en blokkeren proactief aanvallen op eindpunten, terwijl beveiligingsexperts helpen bij het opsporen en herstellen van geïdentificeerde bedreigingen op het eindpunt, op het netwerk en in de cloud.

Partners

[CrowdStrike Falcon®](#) →

[VMware Carbon Black](#) →

[Secureworks® Taegis™ XDR](#) →

Bescherm data op het apparaat en in de cloud met **Dell SafeData**

Zorg ervoor dat gebruikers overal veilig kunnen samenwerken. Netskope gebruikt cloudbeveiliging en -toegang vanuit een datacentrische invalshoek, waarbij data en gebruikers overal worden beschermd, terwijl Absolute IT zichtbaarheid, bescherming en persistentie biedt buiten de bedrijfsfirewall.

Partners

Zelfherstel voor eindpunten, apps en netwerken met [Absolute](#) →

Ontdek Security Service Edge-oplossingen met [Netskope](#) →

Ontdek Dell Security Services

Met Dell kunnen klanten hun beveiliging zelf beheren of dat overlaten aan specialisten. Gebruik onze volledig beheerde, 360° SecOps-oplossing die speciaal is ontworpen om beveiligingsbedreigingen in de IT-omgeving te voorkomen, erop te reageren en te herstellen.

[Ontdek meer over Managed Detection and Response Pro Plus](#) →



Dell Trusted Workspace Door hardware ondersteunde beveiliging

Geïntegreerde beveiliging

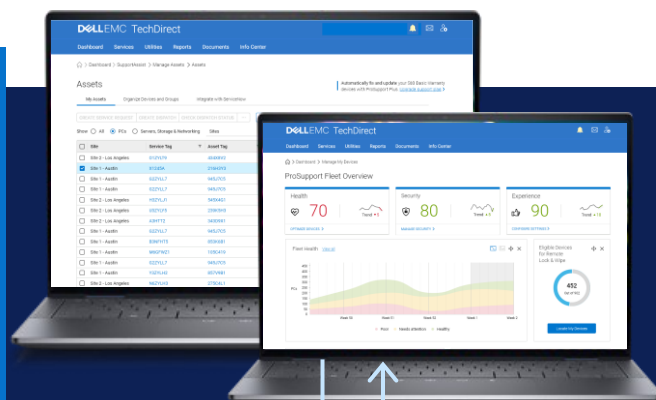
Evoluerende cyberdreigingen omzeilen beveiliging die alleen is gebaseerd op software. Verklein het aanvalsoppervlak van eindpunten met **beveiliging die door hardware wordt ondersteund**.

Om bescherming te bieden tegen moderne bedreigingen, moeten hardware en software samen een verdedigingslinie bouwen. Dell kan u hierbij helpen. We werken samen met toonaangevende beveiligingspartners en combineren uitgebreide telemetrie op apparaatniveau met geavanceerde bedreigingsdetectie om de beveiliging van al uw apparatuur te verbeteren.

- ✓ Beperk het aanvalsoppervlak
- ✓ Verbeter de bedreigingsdetectie
- ✓ Behoud de mate van vertrouwen bij apparaten
- ✓ Consolideer alle leveranciers

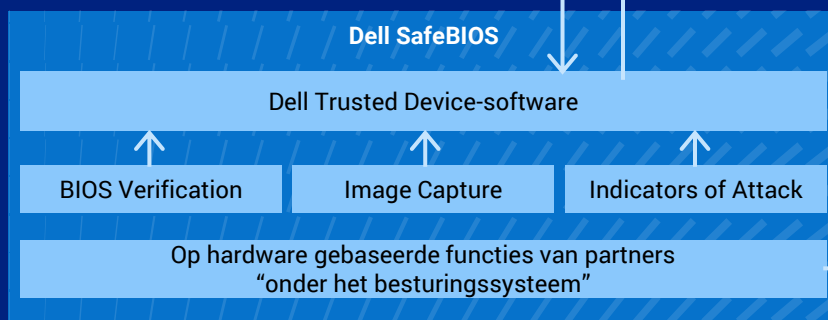
Toegevoegd
Softwarebeveiliging

Alleen Dell integreert de pc-telemetrie met toonaangevende software om de beveiliging van alle apparaten in de onderneming te verbeteren^{1 2}



HET OS

Geïntegreerde hardware- en firmwarebeveiliging



Ontworpen met
Beveiliging van leveringsketen

Dell SafeSupply Chain¹

Verificatie van beveiligde onderdelen
Op apparaat • Op de cloud

Werk overal veilig met **Dell Trusted Workspace.**



Hardwarebeveiliging in
ontwerp en geïntegreerd



Toegevoegde
softwarebeveiliging

Verklein het
aanvalsoppervlak
en verbeter de
cybertolerantie op
de lange termijn
met meerdere
verdedigingslagen.

Ga naar:

dell.com/endpoint-security

Contact:

global.security.sales@dell.com

Ontdek meer:

[Blogs over eindpuntbeveiliging →](#)

Neem deel aan het gesprek

[LinkedIn/delltechnologies](#)

[X @delltech](#)

Bronnen en disclaimers

¹Op basis van een interne analyse van Dell, september 2023. Van toepassing op pc's met Intel processors. Niet alle functies zijn beschikbaar voor alle pc's. Extra aankoop vereist voor sommige functies. Beschikbaarheid verschilt per regio.

²Integraties beschikbaar voor CrowdStrike Falcon Insight XDR en VMware Carbon Black Audit & Remediation.