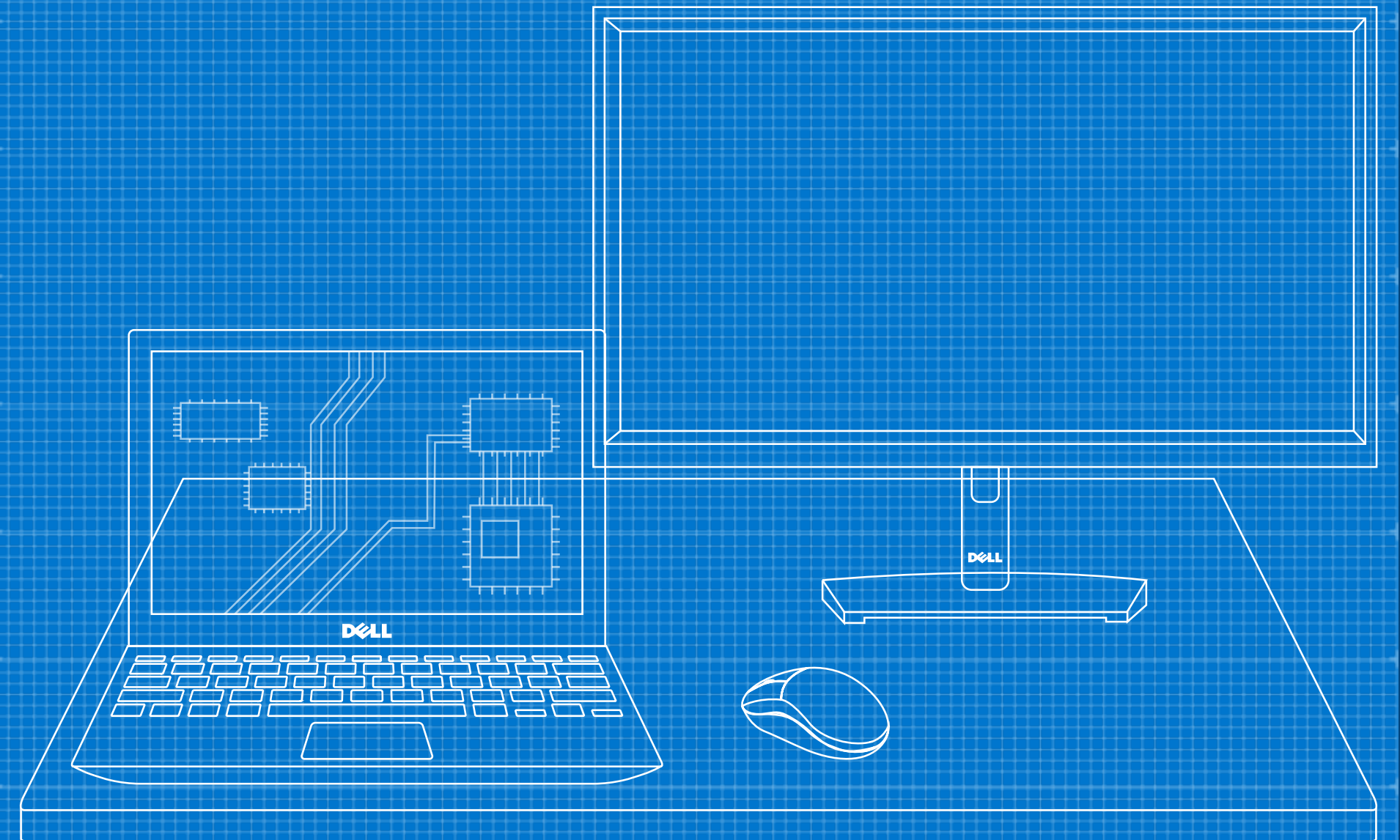


De anatomie van een vertrouwde werkruimte

Verbeter de beveiliging van al uw apparatuur
met meerdere defensieve lagen



Executive summary

Cyberaanvallen zijn onvermijdelijk, worden steeds geavanceerder en nemen ook toe in aantal. Eindpunt-apparaten, netwerken en cloudomgevingen zijn belangrijke doelwitten geworden.

Dit eBook biedt besluitvormers op het gebied van IT en beveiliging een aantal richtlijnen over welke elementen nodig zijn om de meest effectieve eindpuntbescherming te bieden in dit veranderende bedreigingslandschap.



Inhoudsopgave

- 1 [Het bedreigingslandschap](#)
- 2 [Uitdagingen](#)
- 3 [Beveiliging van de moderne werkruimte](#)
- 4 [De anatomie van een vertrouwde werkruimte](#)
- 5 [De benadering van Dell](#)
- 6 [Alles op een rijtje](#)
- 7 [Inzichten en actiepunten](#)



Het bedreigingslandschap

De overstap naar hybride werken heeft geleid tot nieuwe complexiteit en meer aanvalsvectoren, en **het aanvalsoppervlak bij eindpunten, netwerken en clouds is uitgebreid**.

Bovendien gebruiken aanvallers nu geavanceerde technieken die zijn gericht op verschillende lagen van de computerstack en die moeilijk zijn te onderscheiden van geldige systeemp processen. Via sommige methoden krijgen aanvallers zelfs geprivilegieerde toegang waarmee ze softwarebeveiligingen *volledig onopgemerkt* kunnen uitschakelen.

Veel organisaties zijn een Zero Trust-traject opgestart om deze bedreigingen te bestrijden. Maar om Zero Trust-principes te activeren, moet u ervoor zorgen dat al uw apparaten betrouwbaar zijn én blijven.

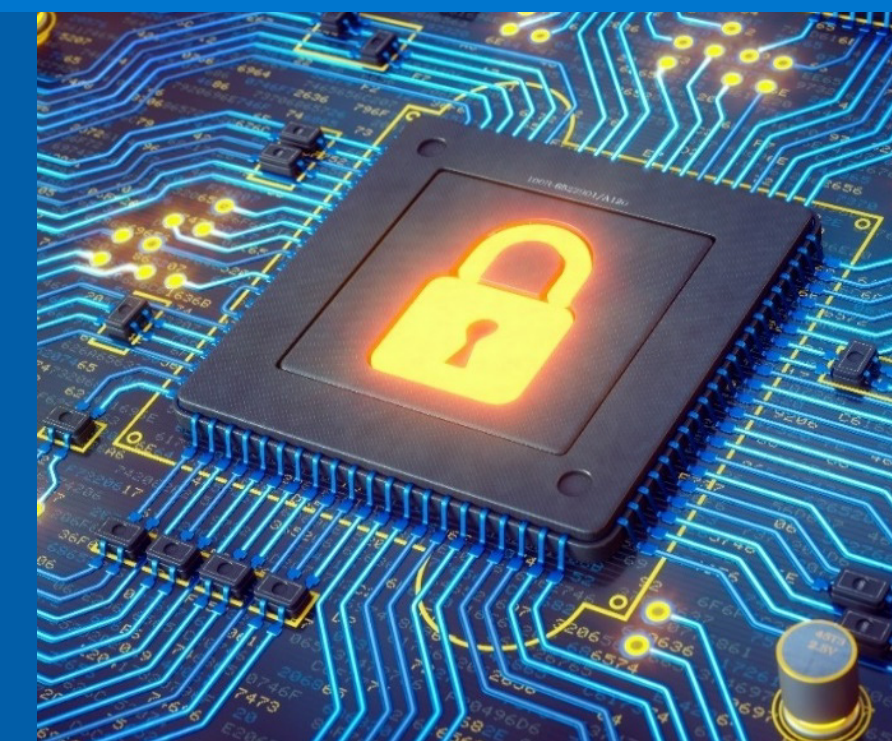
Hoe weet u dat uw apparaten betrouwbaar blijven nu aanvallen vaker voorkomen en er telkens nieuwe aanvalsvectoren worden gecreëerd met geavanceerde technologie?

¹CrowdStrike Global Threat Report, 2024.

²Dell Innovation Index, 2023.

Wist u dat?

75% van alle aanvallen in 2023 waren niet gebaseerd op malware¹



Slechts 41% van de ondervraagde organisaties kan in het volste vertrouwen zeggen dat beveiliging is geïntegreerd in hun technologie en applicaties²

Wilt u Zero Trust verkennen om de maturiteit van uw bedrijf op het gebied van cyberbeveiliging te vergroten? Zie ons eBook: [*Eindpuntbeveiliging is een onmisbaar onderdeel van uw Zero Trust-traject*](#).

Uitdagingen

Voor effectieve eindpuntbeveiliging is het belangrijk om uw tegenstanders en hun werkwijzen te begrijpen.

Gezien het winstpotentieel van een inbreuk **doen aanvallers vaak meerdere pogingen om dezelfde organisatie binnen te dringen. Hierbij gebruiken ze verschillende methoden en toegangspunten om hun kansen te vergroten.** Tijdens de levenscyclus van een enkel apparaat kunnen aanvallers bijvoorbeeld via tientallen vectoren profiteren van kwetsbaarheden.

Verouderde bescherming is ontoereikend om eindpunten veilig te houden. Naarmate organisaties één aanvalsoppervlak verharder, gaan bedreigingsactoren gewoon door met zachtere doelen. Naarmate de wereld steeds meer hybride werd, werden ook nieuwe aanvalsvectoren voor eindpunten geïdentificeerd door bedreigingsactoren, met verwoestende gevolgen.

Zie aanvalsvoorbeelden aan de rechterkant

Aanvallen op leveringsketen: Gericht op leveranciers om toegang te krijgen tot hun systemen, gegevens en/of netwerk en, in het verlengde daarvan, tot die van hun klanten. **VOORBEELD: Een aanval op de hardwareleveringsketen, gestart door sabotage met componenten:**

Aanvallers onderscheppen een pc-zending en verwisselen harde schijven.



IT implementeert de gecompromitteerde apparaten in het hele bedrijf.



De aanvaller installeert malware om aanmeldingsgegevens te extraheren wanneer gebruikers zich aanmelden.



Social-engineering-aanval: Eindgebruikers worden misleid om gevoelige informatie te verstrekken waarmee de aanvaller toegang krijgt tot apparaten en/of netwerken. **VOORBEELD: Een spoofingaanval, geïnitieerd door een phishing-e-mail:**

Een eindgebruiker trapt in een phishing-e-mail en verstrekt aanmeldingsgegevens op een vervalste webpagina.



De aanvaller gebruikt de geldige aanmeldingsgegevens om op afstand toegang te krijgen tot het netwerk.



De aanvaller exfiltreert gegevens via een webservice, versleutelt gestolen gegevens en bewaart deze voor losgeld.



Beveiliging van de moderne werkruimte

Als het gaat om eindpuntbescherming, zijn preventie, detectie en reactie, herstel en sanering nodig voor de verschillende fasen in de gehele levenscyclus van een apparaat - vanaf de inkoop van onderdelen en de productie van pc's tot aan verzending en implementatie, maar ook tijdens het gebruik en daarna. Stel u de grootte van dat gecombineerde aanvalsoppervlak eens voor!

De meest effectieve cyberbeveiligingsstrategie is gepland voor het worst-case-scenario. Deze strategie gaat ervan uit dat een inbreuk mogelijk is en integreert meerdere beveiligingslagen om de aanval zo snel en zo vaak mogelijk te verstoren. Deze aanpak bevat ook herstelmogelijkheden om het risico op herhaling te minimaliseren.

³Dell Innovation Index, 2023.

PREVENTIE

Zorg dat het doelwit kleiner wordt, met beschermingsmaatregelen die zijn ontworpen om aanvallen te blokkeren.

DETECTIE EN REACTIE

Ga altijd uit van een inbreuk en blijf waakzaam.

HERSTEL EN SANERING

Beperk de impact van een aanval en ga terug naar de normale gang van zaken.

Wist u dat:

Slechts 33%

van alle organisaties een holistische end-to-end beveiligingsstrategie hanteert waarin zowel hardware- als softwaregebaseerde beveiligingen zijn geïntegreerd?³



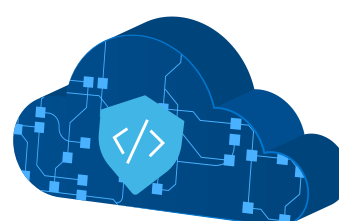
De anatomie van een vertrouwde werkruimte

Moderne eindpuntbeveiliging vereist drie dingen:

- 1 Softwarebeveiliging:** Tegenwoordig staan gebruikers, apparaten en gegevens meer dan ooit buiten het bedrijfsnetwerk. Softwarebeveiliging biedt niet alleen bescherming voor apparaten, maar breidt deze ook uit naar de netwerk- en cloudomgevingen waar kwaadaardige activiteiten vaak hun oorsprong vinden.
- 2 Hardwarebeveiliging:** Apparaten moeten geïntegreerde beveiligingsfuncties bevatten. Dit gaat over hardware- en firmwarebeveiliging waarmee een apparaat tijdens het gebruik wordt beschermd. Om de werkruimte te kunnen beschermen, moet functionaliteit zijn geïntegreerd die u zichtbaarheid en controle biedt over het apparaat.
- 3 Beveiliging van de leveringsketen:** Apparaten moeten met aandacht voor beveiliging worden gebouwd. Dit betekent dat we moeten samenwerken met leveranciers die a) het bedreigingslandschap begrijpen en b) deze kennis kunnen gebruiken naarmate het landschap evolueert. Door pc's veilig te ontwerpen, te ontwikkelen en te testen minimaliseren we het risico op kwetsbaarheden in producten. Met controles in de leveringsketen beperken we bovendien het risico op productenmanipulatie.

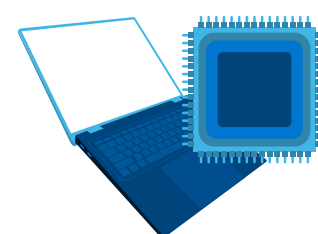
Meerdere beveiligingslagen ontleed

(Representatieve voorbeelden van genoemde beveiligingsmaatregelen)



Softwarebeveiliging

- Next-gen antivirus (NGAV)
- Eindpuntdetectie en -reactie (EDR)
- Uitgebreide detectie en reactie (XDR)
- Cloud-databescherming
- Netwerkbeveiliging
- Geautomatiseerd zelfherstel



Hardware- en firmwarebeveiliging

- Verificatie bij opstarten
- Runtime-verificatie
- Gebruikersidentificatie
- Beveiligingsmeldingen en waarschuwingen/telemetrie



Beveiliging van de leveringsketen

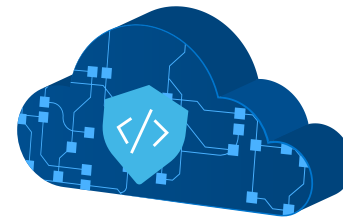
- Beveiligde werkwijzen voor de ontwikkelingsfase
- Beveiligde werkwijzen voor de leveringsketen
- Componentverificatie
- Manipulatiebestendige verpakking

Onze aanpak: Dell Trusted Workspace

Dell is een beveiligings- en IT-partner voor organisaties over de hele wereld. In tegenstelling tot puntoplossingen richt Dell zich op algemene beveiligingsresultaten en bouwt het een reeks oplossingen die 'kill chains' verstoren en u flexibeler maken tegen cyberaanvallen. **Dell Trusted Workspace** omvat:

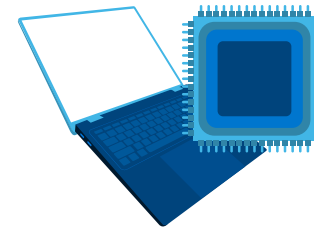
- Unieke **hardware- en firmwarebeveiligingen** die de pc's van Dell tot de veiligste zakelijke pc's ter wereld maken.⁴ (*Toegevoegde en geïntegreerde beveiliging*)
- Een ecosysteem van **toonaangevende softwarepartners** biedt geavanceerde bescherming tegen bedreigingen, zowel voor het apparaat als in het netwerk en de cloud. (*Toegevoegde beveiliging*)

⁴Gebaseerd op een analyse van Dell, 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. Gevalideerd door Principled Technologies. [A comparison of security features](#), april 2024.



Toegevoegde softwarebeveiliging van het partnerecosysteem

- **Dell SafeGuard and Response: CrowdStrike** en **Secureworks** bieden detectie, reactie en herstel van bedreigingen.
- **Dell SafeData: Netskope** biedt zichtbaarheid, monitoring en preventie van gegevensverlies voor cloudgebaseerde apps. **Absolute** maakt zelfherstel mogelijk voor apps en netwerken.



Geïntegreerde hardware- en firmwarebeveiliging op de veiligste zakelijke pc's ter wereld⁴

Voorbeeldfuncties voor de bescherming van apparaten tijdens gebruik:

- **Dell SafeBIOS** voor off-host BIOS-verificatie*, aanvalsindicatoren* en CVE-detectie* kunnen schadelijke activiteiten opsporen voordat deze de pc in gevaar brengen.
- **Dell SafeID** slaat gebruikersreferenties veilig op in een speciale beveiligingschip.*
- **Off-host firmwareverificatie** beschermt de integriteit van firmware met hoge bevoegdheden.*
- Met de **Dell Trusted Device app** integreert Dell apparaatmetrie met toonaangevende software om de beveiliging van al uw bedrijfsapparatuur te verbeteren.*



Ontworpen met-beveiliging voor de leveringsketen zorgt ervoor dat pc's al vanaf de eerste keer opstarten goed beveiligd zijn

- **Dell SafeSupply Chain** add-ons zoals Dell Secured Component Verification* (SCV) bieden extra zekerheid voor productintegriteit.

* Alleen bij Dell

Alles op een rijtje met Dell

Als u zowel hardware- als softwarematige tegenmaatregelen in positie hebt, verkleint u het aanvalsoppervlak met bescherming waarmee veel voorkomende aanvallen makkelijker worden voorkomen.

Detectie- en reactiemogelijkheden pakken sluipende aanvallen aan die hier doorheen kunnen glijpen.

Bij een aanval op de leveringsketen die op pagina 4 is besproken, kan de aanval door preventieve maatregelen, zoals **veilige leveringsketenpraktijken**, al vroeg in de 'kill chain' worden verstoord wanneer u met Dell werkt. Als een aanval doorglipt, zijn er ook aanvullende tegenmaatregelen, zoals **SCV**.

Bij een social-engineering-aanval kan een aanvaller direct worden gestopt en verdere toegang ontzegd dankzij **gebruikersverificatie op basis van hardware, zoals SafeID**. Dit kan dus zelfs ook als de aanvaller een gebruiker heeft misleid en beschikt over geldige aanmeldingsgegevens. Beveiligingssoftware zoals **Next-Gen Web Gateway** kan een extra beschermingslaag op basis van monitoring bieden.

Verweer tegen een aanval op de hardwareleveringsketen die wordt geïnitieerd doordat er met componenten is geknoeid.

Aanvallers onderscheppen een pc-zending en verwisselen harde schijven.



- **Beveiligde werkwijzen voor de leveringsketen**
- Manipulatiebestendige verpakking
- Deurvergrendelingen

IT implementeert de gecompromitteerde apparaten in het hele bedrijf.



- Secured Component Verification (SCV)
- Runtime-verificatie

De aanvaller installeert malware om aanmeldingsgegevens te extraheren wanneer gebruikers zich aanmelden.



- Beveiligingsbroker voor cloudtoegang
- Next-Gen Secure Web Gateway

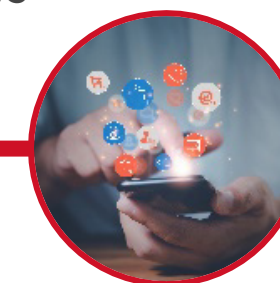
Verweer tegen een social-engineering-aanval die wordt geïnitieerd door een phishing-e-mail.

Een eindgebruiker trapt in een phishing-e-mail en verstrekt aanmeldingsgegevens op een vervalste webpagina.



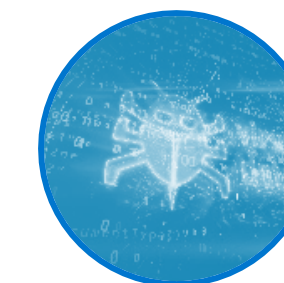
- NGAV
- EDR
- XDR

De aanvaller gebruikt de geldige aanmeldingsgegevens om op afstand toegang te krijgen tot het netwerk.



- **Multi-factorauthenticatie met SafeID**
- Zero Trust-netwerktogang

De aanvaller exfiltreert gegevens via een webservice, versleutelt gestolen gegevens en bewaart deze voor losgeld.



- Next-Gen Secure Web Gateway + Gedragsanalytics van gebruikersentiteit

Belangrijke voordelen

Inbreuken zijn onvermijdelijk.

Effectieve eindpuntbeveiliging gaat altijd uit van het worst-case-scenario en richt zich op het verstoren van 'kill chains', waar die zich ook voordoen, van apparaat tot het netwerk tot de cloud.

Geen enkele oplossing kan 100% van alle aanvallen blokkeren. Combineer hardware- en softwaremaatregelen voor de beste verdediging.

Uw beveiligingsniveau is gelijk aan dat van uw leveranciers. Vraag uw leveranciers om een overzicht van hun beveiligingsmaatregelen.



Meer informatie:

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

Ga dan naar: Dell.com/Endpoint-Security

Volg ons: LinkedIn [@DellTechnologies](https://www.linkedin.com/company/delltechnologies) | X [@DellTech](https://twitter.com/DellTech)

Zet de volgende stap

Beveiliging is een groot onderwerp voor organisaties groot en klein. **Schakel een ervaren beveiligings- en technologiepartner in 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. Verminder de aanvalsmogelijkheden met een uitgebreid portfolio hardware- en softwarebeschermingen, uitsluitend van 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.

