Eindpuntbeveiliging is een onmisbaar onderdeel van uw Zero Trust-traject

Drie aanbevelingen ter voorbereiding op Zero Trust

Beknopte samenvatting

Zero Trust is een traject voor de lange termijn. Het is geen product of oplossing om te implementeren in uw organisatie, het is een strategisch framework voor beveiligingsbeheer dat in de loop der tijd wordt opgebouwd. Dit e-book biedt praktische tips voor IT-besluitvormers die de Zero Trust-transformatie aangaan en het is gericht op de rol die eindpuntbeveiliging speelt bij het leggen van een moderne, werkelijk veilige fundering van een wereld waarin overal kan worden gewerkt.

Inhoudsopgave

Cyber-troonrede

Beveiligingsbedreigingen nemen alsmaar toe als gevolg van de wereldwijd toenemende mate van remote/hybride werken en cloudgebruik.

Het is in de afgelopen jaren steeds ingewikkelder geworden om de data-assets van organisaties te beschermen. De cloud is een gamechanger geweest voor bedrijfsproductiviteit nu remote/hybride werken ingeburgerd is, maar dit brengt wel risico's met zich mee. De overgang van het beheren van infrastructuur op locatie naar het beheren van de cloud heeft de aanvalsmogelijkheden van kwaadwillenden vergroot, met verstrekkende gevolgen. Als een aanval slaagt bijvoorbeeld, wordt niet één klant getroffen, maar kunnen mogelijk alle klanten van die cloudservice en hun klanten worden getroffen, en dat in de hele toeleveringsketen. De winsten voor kwaadwillenden, hetzij landen of criminelen, kunnen enorm zijn, en daarom blijven ze zoeken naar nieuwe kwetsbaarheden om te misbruiken.

De wereldwijde kosten van schade als gevolg van cybermisdaad zal oplopen tot **10,5 biljoen USD in 2025**[i]

Verizon rapporteerde in een studie in 2022 **5200** bevestigde data-inbreuken – **1,3 keer meer gevallen dan het jaar ervoor**[ii]

De gevolgen van een wereld waarin overal kan worden gewerkt

Organisaties moeten een manier vinden om een voorsprong te nemen op de almaar ontwikkelende bedreigingen.

Wat zijn dan de gevolgen van een wereld waarin meer en meer op afstand wordt gewerkt? Twee punten:

Alle organisaties zijn kwetsbaar, ...

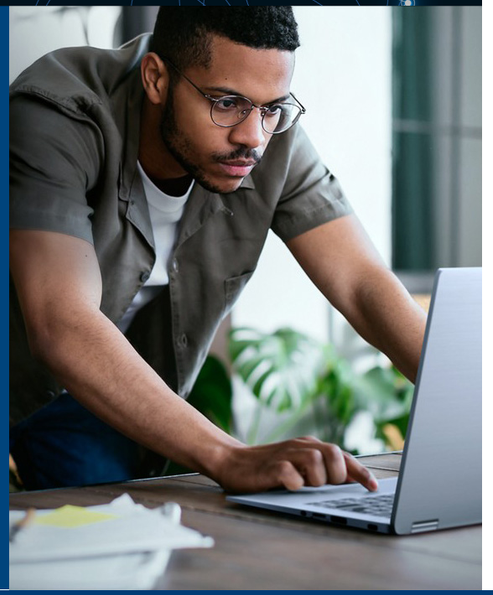
> "[A]ls een kwaadwillende aanvaller echt in uw systeem wil komen, hebben ze een hoge kans op succes."
>
> — *Admiraal Michael Rogers, voormalig directeur van de National Security Agency en voormalig bevelhebber van het Amerikaanse Cyber Command*[iii]

...en de kosten van een onjuiste bescherming kunnen fataal zijn.

> "De kosten van een data-inbreuk waren nog nooit zo hoog, met een gemiddelde van 4,35 miljoen USD in 2022, [12,7% hoger dan in 2020]."[iv]

Aanvalvectoren nemen toe, aanvalsmogelijkheden ook en geen enkel bedrijf kan helemaal beveiligd zijn. Organisaties moeten uitgaan van het ergste en hun verdediging aanscherpen in afwachten van de aanval die komen gaat.

69% van de organisaties heeft in enige mate last gehad van cyberaanvallen als gevolg van een slecht beheerde asset met internetverbinding.[v]



Beveiligings-strategieën moeten veranderen

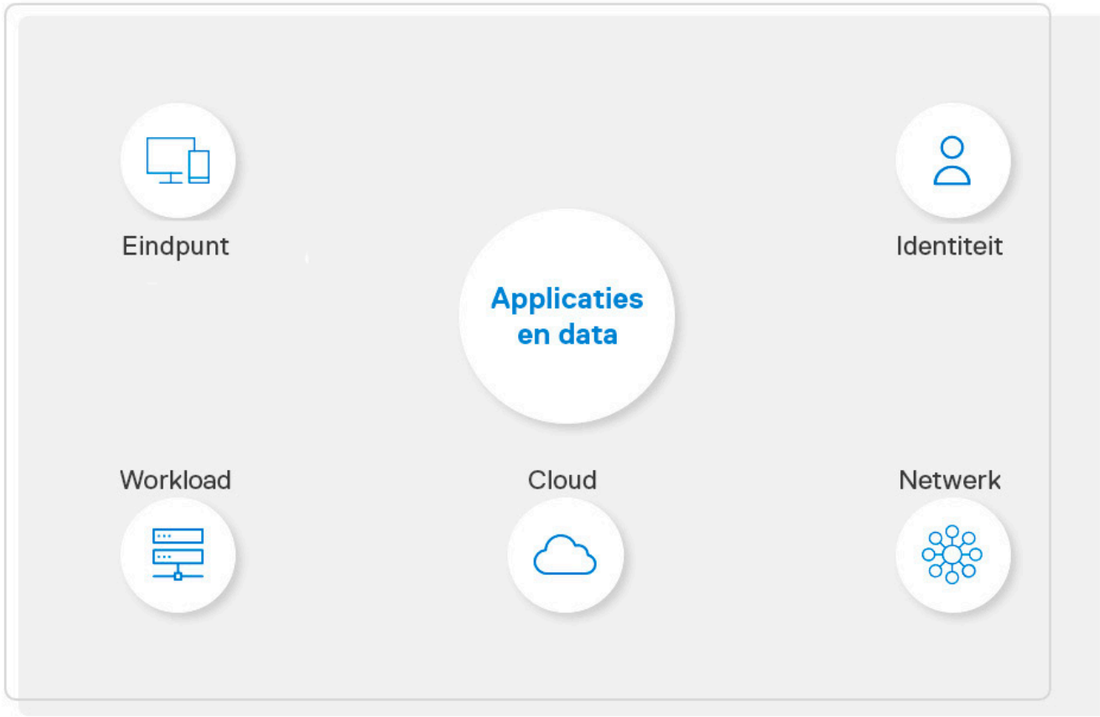
We moeten de cloudgebaseerde omgeving omarmen. Dat is precies waar Zero Trust om draait.

Traditionele beveiligingsmodellen werken niet meer. We leggen u uit waarom.

Voor een effectieve beveiliging moeten organisaties vijf controlepunten in de gaten houden: Eindpunt, Workload, Identiteit, Netwerk en Cloud. Het doel is om applicaties en data te beschermen.

De traditionele aanpak is meestal op silobasis, waardoor organisaties kwetsbaarder worden voor aanvallen.

Volgende...

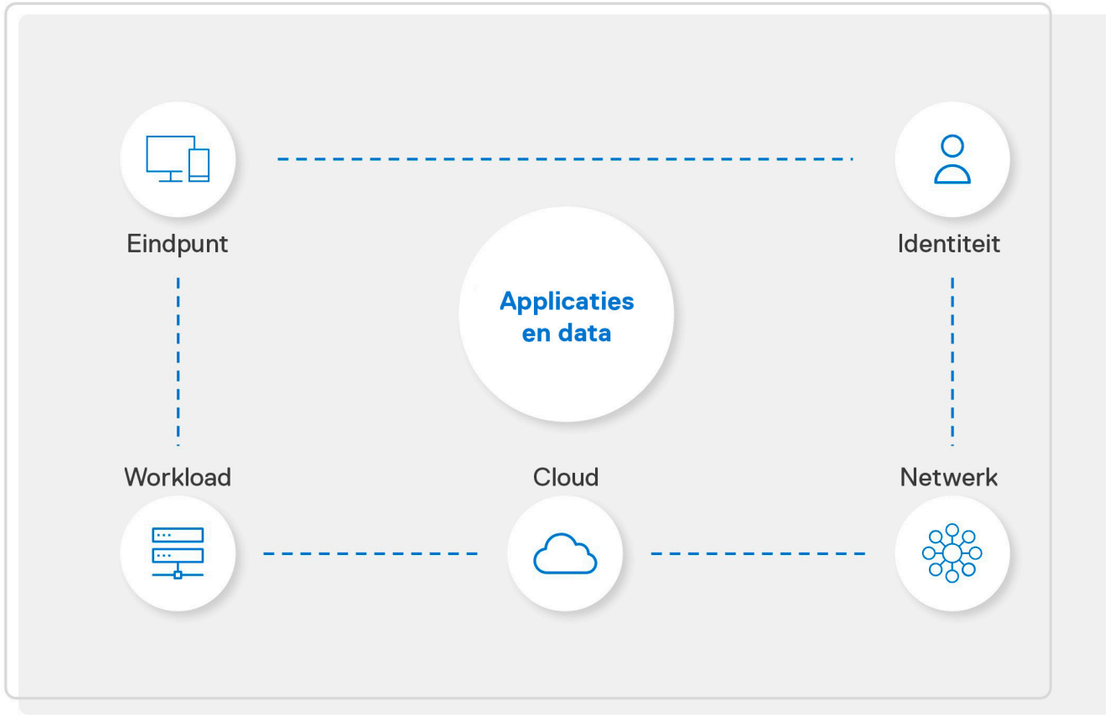


Beveiligings-strategieën moeten veranderen

We moeten de cloudgebaseerde omgeving omarmen. Dat is precies waar Zero Trust om draait.

Een moderne aanpak stuurt aan op meer beheersing, met beter communicatie tussen de controlepunten. Maar in omgevingen die meer en meer zijn gebaseerd op remote/hybride werken moeten we de perimeter versterken.

Volgende...

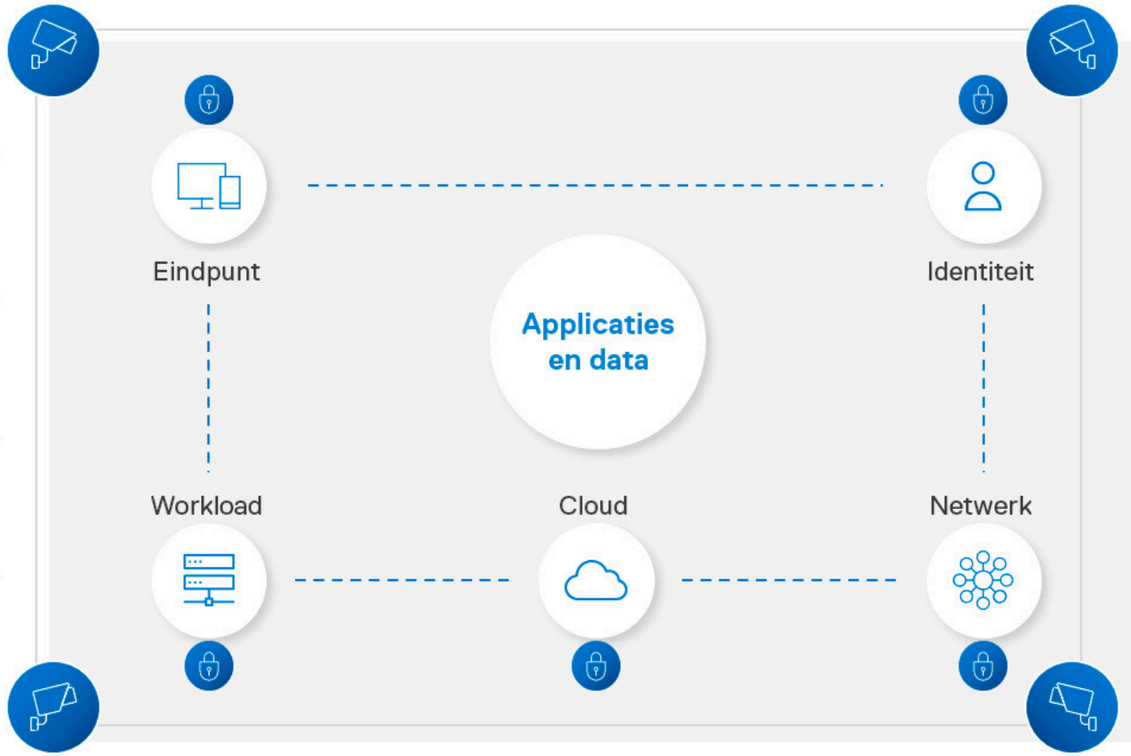


Beveiligings-strategieën moeten veranderen

We moeten de cloudgebaseerde omgeving omarmen. Dat is precies waar Zero Trust om draait.

Tegenwoordig werken medewerkers overal: thuis, in een café of hotel, vaak op een onbeveiligd wifi-netwerk met weinig tot geen connectiviteit en terug naar firewall beschermde kantoren en datacenters. Standaard verbinden ze vaak met een directe internetverbinding op hun apparaat naar cloudbestandsservers en Software-as-a-Service (SaaS)-applicaties om met bedrijfsdata te werken.

Nu aanvallen verfijnder worden en er meer aanvalsvectoren zijn, werken traditionele beveiligingsstrategieën op basis van impliciet vertrouwen niet meer. Dat is precies waar Zero Trust om draait.



De basisprincipes van Zero Trust begrijpen

Zero Trust is de nieuwe manier van denken over beveiliging. Het vervangt *impliciet* vertrouwen, wat betekent dat gebruikers na verificatie onbeperkt toegang hebben tot het netwerk. Zero Trust draait dit gegeven om en geeft juist organisaties zelf de expliciete controle over de IT-omgeving.

We leggen Zero Trust uit aan de hand van een bekend idee: gebouwbeveiligingsprotocollen.

U werkt in een bedrijfspand. Toen u werd aangenomen, kreeg u een badge en hebben ze u de beveiligingsprotocollen uitgelegd. U loopt elke dag het gebouw binnen. Er hangen overal camera's. U gebruikt uw badge op meerdere punten. Eenmaal aan uw bureau, gebruikt u een wachtwoord om uw computer te ontgrendelen.

Een werknemer arriveert bij het kantoorgebouw en haalt zijn badge tevoorschijn om naar binnen te gaan.

Volgende...

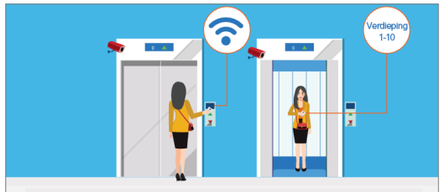
De basisprincipes van Zero Trust begrijpen

Zero Trust is de nieuwe manier van denken over beveiliging. Het vervangt *impliciet* vertrouwen, wat betekent dat gebruikers na verificatie onbeperkt toegang hebben tot het netwerk. Zero Trust draait dit gegeven om en geeft juist organisaties zelf de expliciete controle over de IT-omgeving.

We leggen Zero Trust uit aan de hand van een bekend idee: gebouwbeveiligingsprotocollen.

U werkt in een bedrijfspand. Toen u werd aangenomen, kreeg u een badge en hebben ze u de beveiligingsprotocollen uitgelegd. U loopt elke dag het gebouw binnen. Er hangen overal camera's. U gebruikt uw badge op meerdere punten. Eenmaal aan uw bureau, gebruikt u een wachtwoord om uw computer te ontgrendelen.

Een werknemer arriveert bij het kantoorgebouw en haalt zijn badge tevoorschijn om naar binnen te gaan.



Hij gebruikt zijn badge om toegang te krijgen tot de lift die naar zijn verdieping gaat.

Volgende...

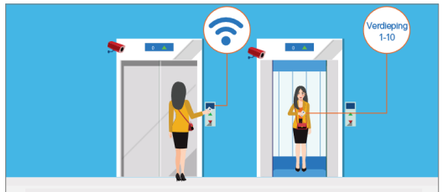
De basisprincipes van Zero Trust begrijpen

Zero Trust is de nieuwe manier van denken over beveiliging. Het vervangt *impliciet* vertrouwen, wat betekent dat gebruikers na verificatie onbeperkt toegang hebben tot het netwerk. Zero Trust draait dit gegeven om en geeft juist organisaties zelf de expliciete controle over de IT-omgeving.

We leggen Zero Trust uit aan de hand van een bekend idee: gebouwbeveiligingsprotocollen.

U werkt in een bedrijfspand. Toen u werd aangenomen, kreeg u een badge en hebben ze u de beveiligingsprotocollen uitgelegd. U loopt elke dag het gebouw binnen. Er hangen overal camera's. U gebruikt uw badge op meerdere punten. Eenmaal aan uw bureau, gebruikt u een wachtwoord om uw computer te ontgrendelen.

Een werknemer arriveert bij het kantoorgebouw en haalt zijn badge tevoorschijn om naar binnen te gaan.



Hij gebruikt zijn badge om toegang te krijgen tot de lift die naar zijn verdieping gaat.

De werknemer gebruikt zijn badge opnieuw om de geselecteerde verdieping te activeren in de lift.

Volgende...

 |

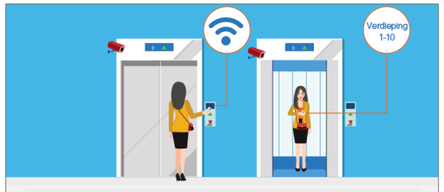
De basisprincipes van Zero Trust begrijpen

Zero Trust is de nieuwe manier van denken over beveiliging. Het vervangt *impliciet* vertrouwen, wat betekent dat gebruikers na verificatie onbeperkt toegang hebben tot het netwerk. Zero Trust draait dit gegeven om en geeft juist organisaties zelf de expliciete controle over de IT-omgeving.

We leggen Zero Trust uit aan de hand van een bekend idee: gebouwbeveiligingsprotocollen.

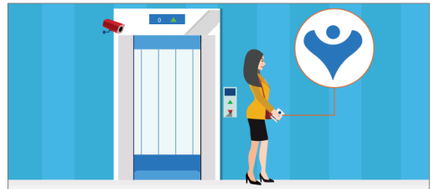
U werkt in een bedrijfspand. Toen u werd aangenomen, kreeg u een badge en hebben ze u de beveiligingsprotocollen uitgelegd. U loopt elke dag het gebouw binnen. Er hangen overal camera's. U gebruikt uw badge op meerdere punten. Eenmaal aan uw bureau, gebruikt u een wachtwoord om uw computer te ontgrendelen.

Een werknemer arriveert bij het kantoorgebouw en haalt zijn badge tevoorschijn om naar binnen te gaan.



Hij gebruikt zijn badge om toegang te krijgen tot de lift die naar zijn verdieping gaat.

De werknemer gebruikt zijn badge opnieuw om de geselecteerde verdieping te activeren in de lift.



Als de werknemer is aangekomen, loopt hij naar zijn kantoorsuite.

Volgende...

 |

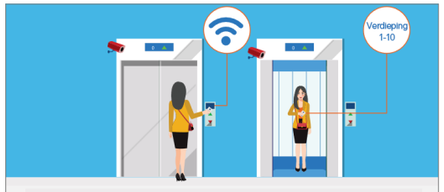
De basisprincipes van Zero Trust begrijpen

Zero Trust is de nieuwe manier van denken over beveiliging. Het vervangt *impliciet* vertrouwen, wat betekent dat gebruikers na verificatie onbeperkt toegang hebben tot het netwerk. Zero Trust draait dit gegeven om en geeft juist organisaties zelf de expliciete controle over de IT-omgeving.

We leggen Zero Trust uit aan de hand van een bekend idee: gebouwbeveiligingsprotocollen.

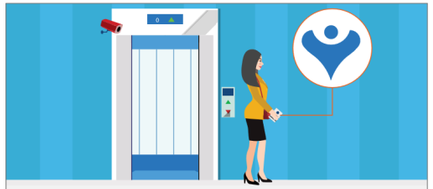
U werkt in een bedrijfspand. Toen u werd aangenomen, kreeg u een badge en hebben ze u de beveiligingsprotocollen uitgelegd. U loopt elke dag het gebouw binnen. Er hangen overal camera's. U gebruikt uw badge op meerdere punten. Eenmaal aan uw bureau, gebruikt u een wachtwoord om uw computer te ontgrendelen.

Een werknemer arriveert bij het kantoorgebouw en haalt zijn badge tevoorschijn om naar binnen te gaan.



Hij gebruikt zijn badge om toegang te krijgen tot de lift die naar zijn verdieping gaat.

De werknemer gebruikt zijn badge opnieuw om de geselecteerde verdieping te activeren in de lift.



Als de werknemer is aangekomen, loopt hij naar zijn kantoorsuite.

Hij swipet zijn ID-kaart om toegang te krijgen tot zijn suite.

Volgende...

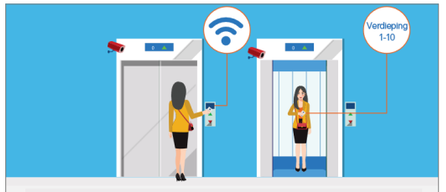
De basisprincipes van Zero Trust begrijpen

Zero Trust is de nieuwe manier van denken over beveiliging. Het vervangt *impliciet* vertrouwen, wat betekent dat gebruikers na verificatie onbeperkt toegang hebben tot het netwerk. Zero Trust draait dit gegeven om en geeft juist organisaties zelf de expliciete controle over de IT-omgeving.

We leggen Zero Trust uit aan de hand van een bekend idee: gebouwbeveiligingsprotocollen.

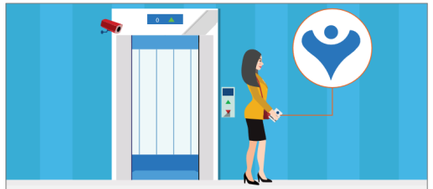
U werkt in een bedrijfspand. Toen u werd aangenomen, kreeg u een badge en hebben ze u de beveiligingsprotocollen uitgelegd. U loopt elke dag het gebouw binnen. Er hangen overal camera's. U gebruikt uw badge op meerdere punten. Eenmaal aan uw bureau, gebruikt u een wachtwoord om uw computer te ontgrendelen.

Een werknemer arriveert bij het kantoorgebouw en haalt zijn badge tevoorschijn om naar binnen te gaan.



Hij gebruikt zijn badge om toegang te krijgen tot de lift die naar zijn verdieping gaat.

De werknemer gebruikt zijn badge opnieuw om de geselecteerde verdieping te activeren in de lift.



Als de werknemer is aangekomen, loopt hij naar zijn kantoorsuite.

Hij swipet zijn ID-kaart om toegang te krijgen tot zijn suite.

De werknemer gaat naar zijn bureau en ontgrendelt de computer met behulp van een wachtwoord.

Volgende...

 |

De basisprincipes van Zero Trust begrijpen

Zo werkt Zero Trust.

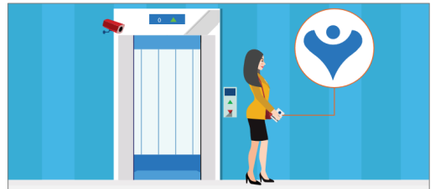
Uw werkgever heeft u op Dag Eén geïdentificeerd. Elke toegang die u sindsdien hebt aangevraagd, is geverifieerd om de assets van de organisatie (gebruikers, data etc.) te beschermen. Voor extra beveiliging controleren beveiligingsmedewerkers via monitors alle bewegingen in het gebouw. Afwijkend gedrag, bijvoorbeeld proberen een ruimte in te gaan waar u niet hoort te zijn, wordt onderzocht.

Maar tegenwoordig zien we meer en meer gebruikers, apparaten, apps en data buiten de bedrijfsnetwerken dan ooit tevoren. Als gevolg daarvan is de gebruikersidentiteit een blinde vlek geworden en is een gecompromitteerde identiteit vaak een belangrijk element bij inbreuken. Zero Trust haalt deze blinde vlek weg.

Een werknemer arriveert bij het kantoorgebouw en haalt zijn badge tevoorschijn om naar binnen te gaan.

Hij gebruikt zijn badge om toegang te krijgen tot de lift die naar zijn verdieping gaat.

De werknemer gebruikt zijn badge opnieuw om de geselecteerde verdieping te activeren in de lift.



Als de werknemer is aangekomen, loopt hij naar zijn kantoorsuite.

Hij swipet zijn ID-kaart om toegang te krijgen tot zijn suite.

De werknemer gaat naar zijn bureau en ontgrendelt de computer met behulp van een wachtwoord.

Zero Trust-principes toepassen

Eindpuntbeveiliging is een onmisbaar onderdeel van een Zero Trust-transformatie.

Om een effectieve Zero Trust-strategie te implementeren, moet u eindpunten beveiligen.

Volgens het MITRE ATT&CK®-framework zijn er negen ‘initiële toegangstechnieken’ die kwaadwillende gebruiken om toegang tot netwerken te krijgen *(zie illustratie)*.[vi] Onderzoek toont aan dat traditionele verdedigingsmaatregelen eindpunten in een cloudgebaseerde wereld niet veilig kunnen houden. Aanvallers hebben maar één toegangspunt nodig. Op eindpunten kunnen kwaadwillenden tientallen kwetsbaarheden misbruiken in de hele levenscyclus van een apparaat.

Als het aantal apparaten op een netwerk toeneemt, worden eindpunten een steeds grotere aanvalsvector.

Beveiligingsbeleid bij Zero Trust-modellen definieert “known good” (bekend goed) in elk detail, al het andere wordt geblokkeerd. Bedreigingsbeheer monitort op alle afwijkingen van bekend goed, markeert ongebruikelijk gedrag en start de juiste actie om de mogelijke dreiging het hoofd te bieden.

Illustratie 1/3

Zero Trust-principes toepassen

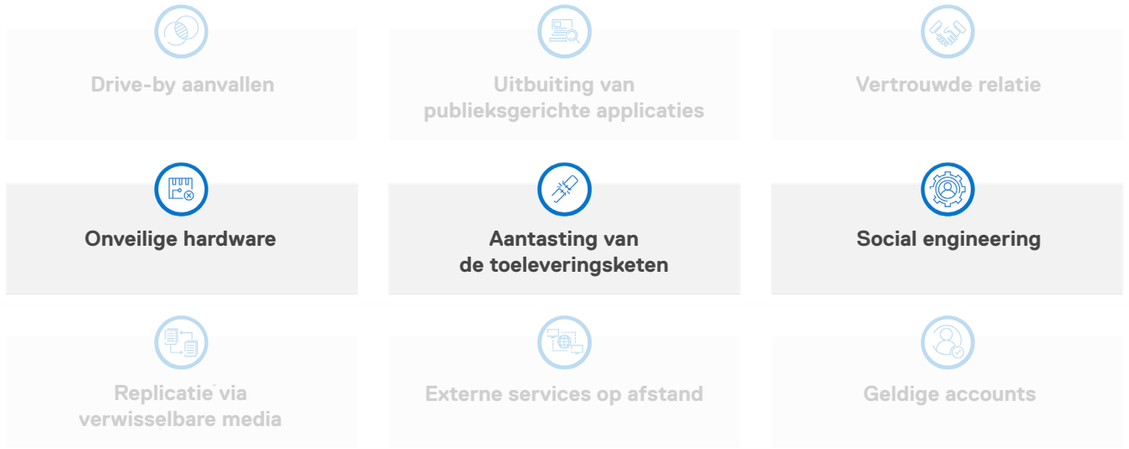
Eindpuntbeveiliging is een onmisbaar onderdeel van een Zero Trust-transformatie.

Om een effectieve Zero Trust-strategie te implementeren, moet u eindpunten beveiligen.

Volgens het MITRE ATT&CK®-framework zijn er negen ‘initiële toegangstechnieken’ die kwaadwillende gebruiken om toegang tot netwerken te krijgen *(zie illustratie)*.[vi] Onderzoek toont aan dat traditionele verdedigingsmaatregelen eindpunten in een cloudgebaseerde wereld niet veilig kunnen houden. Aanvallers hebben maar één toegangspunt nodig. Op eindpunten kunnen kwaadwillenden tientallen kwetsbaarheden misbruiken in de hele levenscyclus van een apparaat.

Als het aantal apparaten op een netwerk toeneemt, worden eindpunten een steeds grotere aanvalsvector.

Beveiligingsbeleid bij Zero Trust-modellen definieert “known good” (bekend goed) in elk detail, al het andere wordt geblokkeerd. Bedreigingsbeheer monitort op alle afwijkingen van bekend goed, markeert ongebruikelijk gedrag en start de juiste actie om de mogelijke dreiging het hoofd te bieden.



Illustratie 2/3

Zero Trust-principes toepassen

Eindpuntbeveiliging is een onmisbaar onderdeel van een Zero Trust-transformatie.

Om een effectieve Zero Trust-strategie te implementeren, moet u eindpunten beveiligen.

Volgens het MITRE ATT&CK®-framework zijn er negen ‘initiële toegangstechnieken’ die kwaadwillende gebruiken om toegang tot netwerken te krijgen *(zie illustratie)*.[vi] Onderzoek toont aan dat traditionele verdedigingsmaatregelen eindpunten in een cloudgebaseerde wereld niet veilig kunnen houden. Aanvallers hebben maar één toegangspunt nodig. Op eindpunten kunnen kwaadwillenden tientallen kwetsbaarheden misbruiken in de hele levenscyclus van een apparaat.

Als het aantal apparaten op een netwerk toeneemt, worden eindpunten een steeds grotere aanvalsvector.

Beveiligingsbeleid bij Zero Trust-modellen definieert “known good” (bekend goed) in elk detail, al het andere wordt geblokkeerd. Bedreigingsbeheer monitort op alle afwijkingen van bekend goed, markeert ongebruikelijk gedrag en start de juiste actie om de mogelijke dreiging het hoofd te bieden.

Illustratie 3/3

Drie aanbevelingen ter voorbereiding op Zero Trust

Bereid uw organisatie voor op een succesvolle Zero Trust-transformatie.

1

Stel de juiste beleidsregels en controles in om uw bedrijfsprioriteiten te ondersteunen.

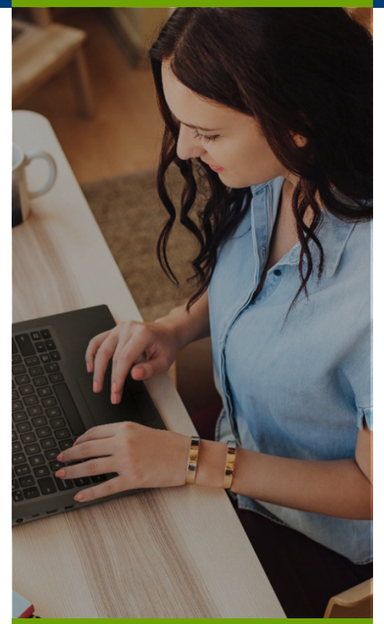
Beleidsengines en beleidsbeheer zijn cruciaal voor effectieve Zero Trust-implementaties. Maar geen enkele organisatie heeft een onbeperkt budget voor beveiliging, dus de eerste stap is om uw bedrijfsprioriteiten te bepalen. Wat zijn de meest kritieke assets en IP die u wilt beschermen? Weeg die aanvalsmogelijkheid af tegen het toegestane risico van uw organisatie.

Neem dan het beleid en de controles door die u nu gebruikt. Hedendaagse risico's hangen met de cloudgebaseerde wereld samen. Hoe is uw beleidsengine hierop afgesteld?

Als u beleid heeft om toegang tot uw belangrijkste assets te beheren, kunt u uw blik daarna verruimen.

MEER INFORMATIE

Bekijk deze video en zie hoe cyberexperts van Dell de belangrijkste beveiligingsrisico's van organisaties bespreken.



Met meer gebruikers, apps, data en apparaten buiten het bedrijfsnetwerk dan ooit tevoren zegt **82%** van de IT-besluitvormers dat ze hun beveiligingsbeleid hebben moeten herzien.[x]

Drie aanbevelingen ter voorbereiding op Zero Trust

Bereid uw organisatie voor op een succesvolle Zero Trust-transformatie.

2 Begin met veilige apparaten.

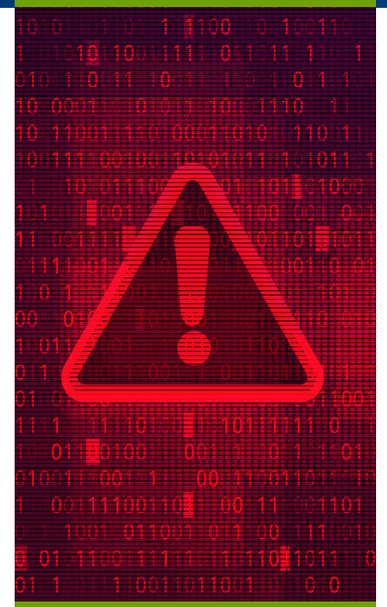
Baseer de Zero Trust-planning op een stevige basis. Versterk uw verdediging met apparaten die zijn ontworpen en ontwikkeld met het oog op beveiliging. Denk hierbij aan:

A. **Hardware- en firmware-gebaseerde beschermingen** die de eindpuntstack beveiligen en de zichtbaarheid vergroten (bijv. detecteren dat een BIOS is gecompromitteerd en IT waarschuwen). Voorzie uw organisatie van technologieën die de identiteit verifiëren bij elke nieuwe toegangsaanvraag, met een zo klein mogelijke impact op de gebruikersproductiviteit.

B. **Toeleveringsketenbeschermingen en integriteitscontroles** die elke stap van de PC-levenscyclus beveiligen. In de afgelopen jaren is gedemonstreerd dat toeleveringsketenaanvallen vernietigend kunnen werken. In een pure Zero Trust-architectuur begint authenticatie, verificatie en monitoring al in de toeleveringsketen. Werk samen met leveranciers die 1) veiligheidsprincipes toepassen en 2) u toestaan de integriteit van uw apparaten te valideren, van de aankoop tot de productie en levering.

MEER INFORMATIE

Lees voor meer informatie over best practices bij apparaatbeveiliging het whitepaper van Dell en Intel: Het bereiken van grootschalige beveiliging boven, in en onder het besturingssysteem.



In **2021** verspreidde een IT-beheerbedrijf een ransomware-aanval naar minstens **1.500** klanten.[xi]

Drie aanbevelingen ter voorbereiding op Zero Trust

Bereid uw organisatie voor op een succesvolle Zero Trust-transformatie.

3

Streef naar naadloze integratie en interoperabiliteit in uw hele ecosysteem.

Voor een effectieve beveiliging zijn op het hoogste niveau drie dingen cruciaal:

A. Integratie van alle verdedigingen in het hele IT-ecosysteem,

B. Real-time zichtbaarheid, en

C. Mogelijkheid om actie te ondernemen zodra het nodig is.

In onze cloudgebaseerde wereld, waarin zelfs de kleinste ongedekte kwetsbaarheid verstrekkende gevolgen kan hebben, is het belangrijk dat alle systemen potentiële bedreigingen kunnen herkennen *en* de mogelijkheid hebben om de benodigde acties te ondernemen.

Zijn uw systemen geïntegreerd, of werken ze in silo's? Kan uw beleidsengine een specifieke workflow in gang zetten als een IT-beheerder een melding krijgt van een corrupte BIOS op het netwerk? In een geïntegreerde omgeving moet automatisering direct een getroffen BIOS in quarantaine zetten, aanvullende toegang beperken en beginnen met patchen.

Hebt u zichtbaarheid in al uw eindpunten? In een perfecte situatie ontvangt u zinvolle telemetrie uit elke laag, van de toeleveringsketen (bijv. het laaddock) tot de firmware (bijv. sabotagepogingen op BIOS-niveau).

Maar die telemetrie is slechts zo goed als uw integraties. Kunt u actie uitvoeren op basis van uw data? Het is belangrijk om de juiste bronnen, bijv. ervaren cyberbeveiligingsmedewerkers, te hebben om de data en programmaworkflows te begrijpen die de problemen aanpakken.

41% van de organisaties implementeren Zero Trust[xii]

DELL Technologies

Belangrijke conclusies

Zero Trust is de toekomst van beveiliging.

- De nieuwe manier van werken heeft het aantal aanvalsvectoren verveelvoudigd.
- Een inbreuk is onafwendbaar. Minimaliseer de aanvalsmogelijkheden met verdedigingen die zijn voorbereid op de ergste scenario's.
- Zero Trust is een nieuwe manier van denken over beveiliging die organisaties de expliciete controle over de IT-omgeving geeft.
- Eindpuntbeschermingen die werken op Zero Trust-principes zijn cruciaal voor het behouden van een veilige, moderne basis.
- Bepaal uw meest cruciale assets om de opbouw van uw Zero Trust-architectuur te prioriteren.
- Gebruik apparaten van leveranciers die ingebouwde beschermingen bieden en die goed investeren in toeleveringsketencontroles.
- Beoordeel de interoperabiliteit van beveiliging en IT. Blijf workflows inbouwen om uw beveiliging te versterken.

Zet de volgende stap

Beveiliging is een groot onderwerp voor organisaties groot en klein. Neem een ervaren beveiligings- en technologiepartner in de arm om uw Zero Trust-transformatie te stroomlijnen.

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 ingebouwde bescherming te combineren met doorlopende waakzaamheid. Eindgebruikers blijven productief en IT kan vertrouwen op beveiligingsoplossingen die zijn gemaakt voor de moderne cloudgebaseerde wereld.

Neem contact met ons op: EndpointSecurity@Dell.com
Bezoek ons op: Dell.com/Endpoint-Security
Volg ons: LinkedIn @DellTechnologies | Twitter @DellTech

DELL Technologies

[i] Cybersecurity Almanac 2nd Edition. Cybersecurity Ventures, 2022 https://cybersecurityventures.com/cybersecurity-almanac-2022/

[ii] Ponemon Institute and IBM, Cost of a Data Breach Report, 2022 https://www.ibm.com/security/data-breach

[iii] American College of Cardiology, You Will Be Hacked. Plan Now: Cybersecurity in Health Care, 2021 https://www.acc.org/Latest-in-Cardiology/Articles/2021/11/01/01/42/Feature-You-Will-Be-Hacked-Plan-Now-Cybersecurity-in-Health-Care

[iv] Ponemon Institute and IBM, Cost of a Data Breach Report, 2022 https://www.ibm.com/security/data-breach

[v] ESG Complete Survey Results, Security Hygiene and Posture Management, 2022 https://www.esg-global.com/research/esg-complete-survey-results-security-hygiene-and-posture-management

[vi] MITRE ATT&CK https://attack.mitre.org/tactics/TA0001/

[vii] Futurum, Four Keys to Navigating the Hardware Security Journey, 2020 https://futurumresearch.com/research-reports/four-keys-to-navigating-the-hardware-security-journey/

[viii] Verizon Data Breach Investigations Report, 2022 https://www.verizon.com/business/resources/reports/dbir/2022/summary-of-findings/

[ix] Verizon Data Breach Investigations Report, 2022 https://www.verizon.com/business/resources/reports/dbir/2022/summary-of-findings/

[x] Absolute Endpoint Risk Report, 2021 https://www.absolute.com/go/reports/endpoint-risk-report/

[xi] TechTarget, 2021 https://www.techtarget.com/searchsecurity/news/252503605/Kaseya-1500-organizations-affected-by-REvil-attacks

[xii] Ponemon Institute and IBM, Cost of a Data Breach Report, 2022 https://www.ibm.com/security/data-breach