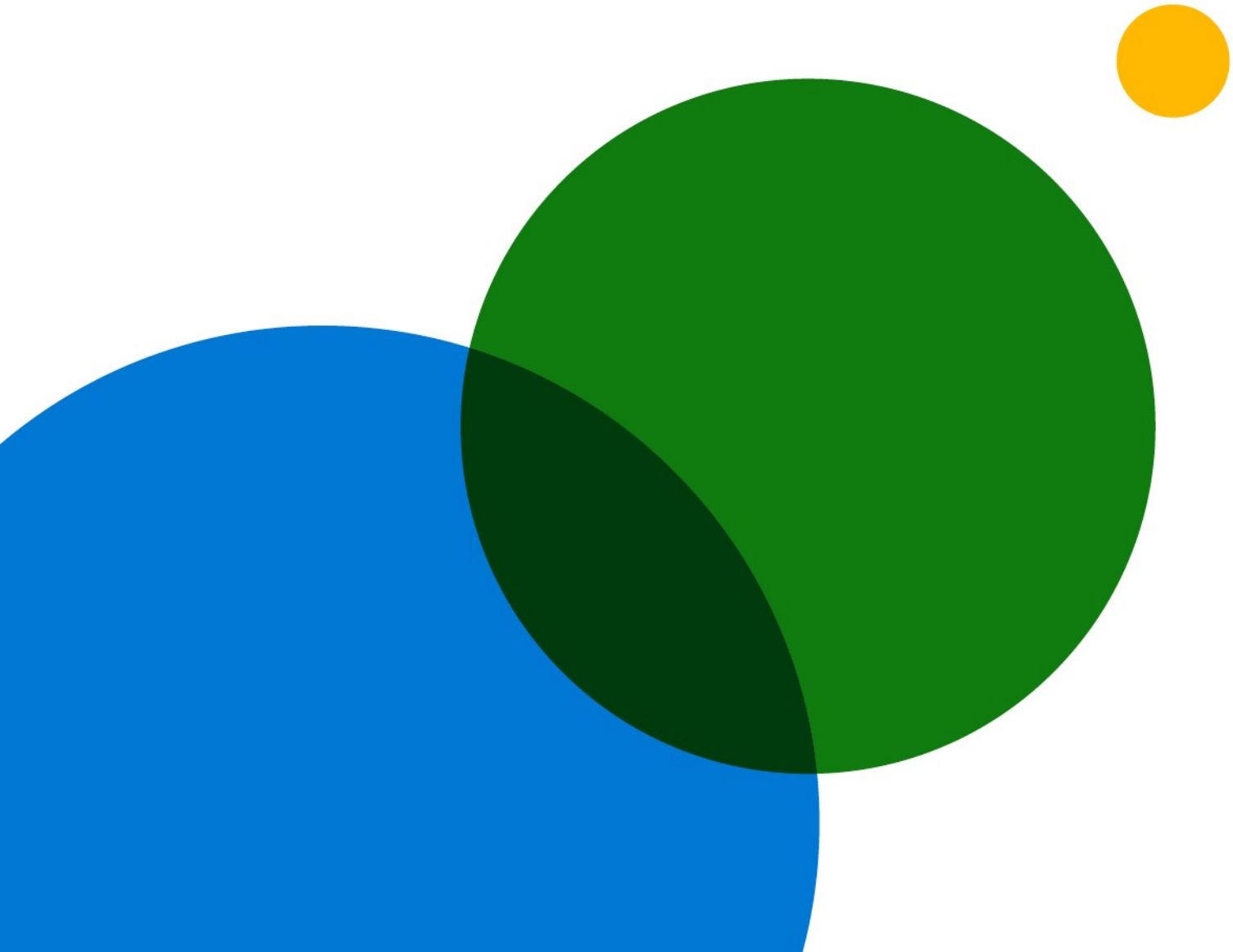
Microsoft Security

hypothesis

Rapport over de implementatie van Zero Trust



Inhoud

03
Introductie

04
Methode

05
Wat je moet weten over de implementatie van Zero Trust

06
Met wie we hebben gesproken

07
Algehele onderzoeksbevindingen

24
Gedetailleerde onderzoeksdoelstellingen en hoe we de doelgroep hebben geworven

Introductie

Vasu Jakkal / Corporate Vice President, Security, Compliance and Identity

In het afgelopen jaar heeft de cyberbeveiliging een opmerkelijke ontwikkeling doorgemaakt, met de opkomst van Zero Trust als leidende strategie voor onze branche en organisaties wereldwijd.

Aan het begin van de pandemie werd de werkplek bijna van de ene op de andere dag een externe werkplek. Hierdoor moesten veel organisaties zich razendsnel aanpassen om werknemers te ondersteunen, die zo goed en kwaad als het ging hun werk probeerden te doen. Dat deden ze met persoonlijke apparaten, via samenwerking met cloudservices en door data buiten de netwerkgrens van bedrijven te delen. Terwijl organisaties zich aan deze transformatie aanpasten, kregen ze ook te maken met steeds geavanceerdere cybercriminelen die hun doelgerichtheid, tactieken en middelen voortdurend verfijnden.

Nu is hybride werken de nieuwe realiteit. In deze nieuwe context, en met de snelle wijzigingen die er plaatsvinden, meldden de organisaties die deelnamen aan onze enquête ons dat ze vertrouwen op Zero Trust vanwege de verhoogde beveiliging en flexibele compliancemogelijkheden, snellere bedreigingsdetectie en -herstel en de mogelijkheden voor beveiligingsanalyse.

Een allesomvattende Zero Trust-architectuur wordt gebaseerd op de principes van expliciete verificatie, toegang met minimale bevoegdheden en 'assume breach' (uitgaan van een inbreuk). Hierbij worden beveiligingsmaatregelen ingebouwd voor identiteit, endpoints, apps, infrastructuur, netwerken en data, gekoppeld aan verhoogde zichtbaarheid, meer automatisering en orkestratie. We raden die strategie niet alleen aan bij onze klanten en partners, maar omarmen deze ook voor onze aanpak van wereldwijde beveiliging en softwareontwikkeling bij Microsoft.

Dit rapport licht toe hoe verschillende markten en branches Zero Trust kunnen invoeren. We hopen dat de bevindingen van dit onderzoek je kunnen helpen om je eigen Zero Trust-invoering te versnellen, licht werpen op de collectieve vooruitgang die je collega's hebben geboekt en inzichten bieden in de toekomstige ontwikkelingen op dit gebied.

Methode

Microsoft heeft Hypothesis Group, een bedrijf dat inzichten, ontwerp en strategie biedt, de opdracht gegeven om het Rapport over de implementatie van Zero Trust samen te stellen en hiervoor het onderzoek uit te voeren. Het onderzoek omvatte twee fasen. In de VS keken we allereerst naar de belangrijkste trends en de snelheid waarmee Zero Trust wordt ingevoerd, en tijdens de tweede fase hebben we meer markten toegevoegd om wereldwijde trends bloot te leggen.

Het allereerste onderzoek vond plaats in augustus 2020, waarbij we in de VS een online enquête van 15 minuten uitvoerden onder 300 SDM's (security decision-makers of beslissers op beveiligingsgebied) die betrokken zijn bij beslissingen over de Zero Trust-strategie bij ondernemingen uit verschillende sectoren. Naast deze online enquête zijn in september 2020 vijf online diepte-interviews afgenomen onder SDM's die in verschillende sectoren in de VS werkzaam zijn.

In april 2021 werd wereldwijd onderzoek gedaan in de VS, Duitsland, Japan en Australië/Nieuw-Zeeland onder een vergelijkbare groep SDM's. Meer dan 900 van hen namen deel aan een online enquête van 15 minuten met vragen over de invoering van hun Zero Trust-strategie, best practices, voordelen, problemen en hoe zij in de toekomst willen investeren.

Wat je moet weten over de implementatie van Zero Trust

01 / Organisaties zijn bereid om te profiteren van de Zero Trust-strategie, een trend die wordt versneld door de overstap op een hybride werkplek en COVID-19

SDM's verklaren dat het ontwikkelen van een Zero Trust-strategie hun hoogste beveiligingsprioriteit is. Daarbij geeft 96% aan dat dit cruciaal is voor het succes van hun organisatie. De belangrijkste beweegredenen om een Zero Trust-strategie in te voeren, zijn het verbeteren van hun algehele beveiligingsaanpak en de ervaring van de eindgebruiker. De overstap naar een hybride werkplek, versneld door COVID-19, stimuleert ook de trend van bredere invoering van een Zero Trust-strategie: 81% van de ondernemingen is begonnen met de overstap naar een hybride werkplek, waarvan 31% deze al heeft voltooid. 94% maakt zich echter zorgen over deze overstap, met name voor wat betreft misbruik door werknemers, de toegenomen IT-workloads en cyberaanvallen. Gezien deze zorgen, zijn belangrijke overwegingen om een strategie op te baseren: meer training voor werknemers en meervoudige verificatie (MFA of Multi-Factor Authentication) om een soepele gebruikerservaring en overgang te garanderen.

02 / Met een Zero Trust-strategie beschikken organisaties over flexibiliteit in waar ze kunnen beginnen met de implementatie, zodat de aanpak kan worden afgestemd op hun behoeften

Minder dan 15% van de organisaties is begonnen met het implementeren van een Zero Trust-strategie op hetzelfde beveiligingsrisicogebied. Dit komt grotendeels doordat de implementatie wordt benaderd als een allesomvattend proces voor alle pijlers en mogelijkheden van de beveiligingsarchitectuur, en niet als een reeks uiteenlopende, afzonderlijke technologieën. Ook de volgorde waarin afzonderlijke onderdelen van Zero Trust binnen een beveiligingsrisicogebied worden geïmplementeerd varieert sterk, waarbij beveiligingsprofessionals aanzienlijk van mening verschillen over welke onderdelen ze als eerste willen implementeren.

03 / Hoewel de Zero Trust-strategie op grote schaal wordt ingevoerd en organisaties betere mogelijkheden biedt om bedreigingen te beheren, moet er nog veel werk worden verzet

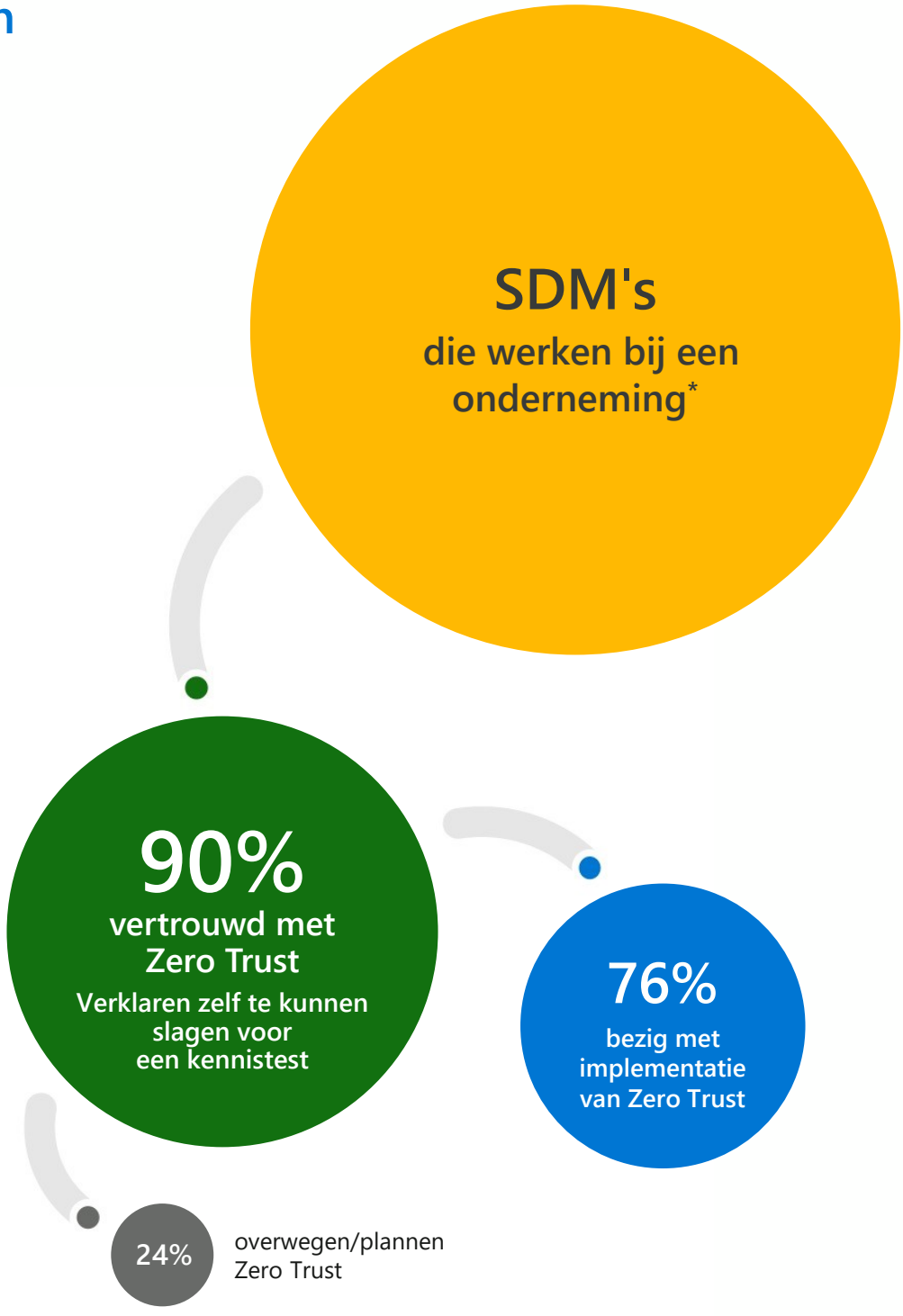
76% van de organisaties is ten minste begonnen met de implementatie van een Zero Trust-strategie, terwijl 35% beweert dat de implementatie is voltooid. De organisaties die echter beweren dat de implementatie is voltooid, geven ook toe dat ze niet klaar zijn met de implementatie van een Zero Trust-strategie op alle beveiligingsrisicogebieden en voor alle beveiligingsonderdelen. De Zero Trust-strategie is overtuigend, omdat deze meer flexibiliteit biedt, bedreigingen sneller kunnen worden gedetecteerd en de mogelijkheden worden vergroot om de beveiliging voor IoT (Internet of Things) en OT (Operational Technology) te beheren. De invoering is groeiende in de VS (van 70% in augustus 2020 tot 79% in april 2021). De VS hebben ook een voorsprong voor wat betreft de implementatie van Zero Trust vergeleken met andere landen die de invoering later zijn gestart. Ook geven organisaties in de VS aan dat ze minder worden beperkt door lagere budgetten. Maar hoewel 57% van de organisaties beweert dat ze voorop lopen wat betreft implementatie, heeft ongeveer de helft nog meer werk te verzetten, omdat ze Zero Trust niet volledig hebben geïmplementeerd op alle beveiligingsrisicogebieden en voor alle beveiligingsonderdelen.

04 / Wat de toekomst betreft, blijft de Zero Trust-strategie een topprioriteit die zorgvuldige besluitvorming vereist voor wat betreft werknemers en leveranciers

De Zero Trust-strategie zal de komende twee jaar naar verwachting de hoogste beveiligingsprioriteit blijven en organisaties verwachten tevens hun investeringen te zullen verhogen. Het overwinnen van de problemen met hun werknemers (waaronder personeel werven voor beveiligingsteams en steun van het management) is een cruciale factor voor het behalen van optimaal rendement uit de investeringen in Zero Trust. Waar het gaat om de leveranciersstrategie, hebben beveiligingsbeslissers een lichte voorkeur voor het werken met holistische of geconsolideerde leveranciers, aangezien de selectie van leveranciers vaak afhankelijk is van de beschikbaarheid van interne expertise. Voordelen van deze 'best-in-suite'-aanpak (een keuze voor uiteenlopende producten van één leverancier) zijn meer expertise, resources en eenvoud, hoewel de implementatie ervan langer kan duren, de integratie in de bestaande beveiligingsarchitectuur moeilijker kan zijn en de potentiële kwetsbaarheid toeneemt.

Met wie we hebben gesproken

Wereldwijd



*1000+ werknemers in de VS; 500+ werknemers in Duitsland, Japan, Australië/Nieuw-Zeeland

Algehele onderzoeks-bevindingen

Organisaties zijn klaar om te profiteren van de Zero Trust-strategie

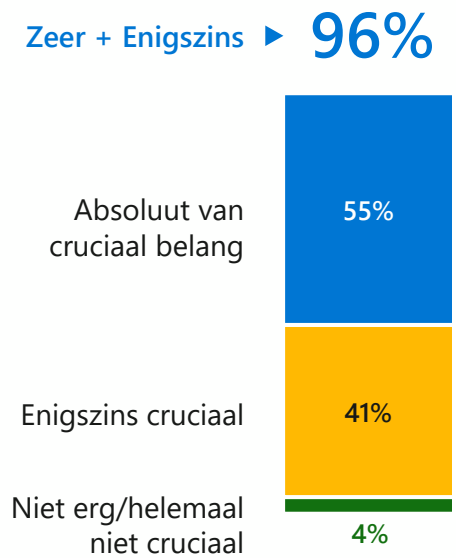
De Zero Trust-strategie is de hoogste beveiligingsprioriteit voor alle markten en sectoren, waarbij een aantal organisaties de afgelopen jaren een Zero Trust-strategie heeft geïntroduceerd. Hoewel Zero Trust door iedereen een hoge prioriteit wordt verleend (53%), is dit een bijzonder hoge prioriteit voor organisaties in de Verenigde Staten (56%) en Duitsland (53%).

Bijna alle beveiligingsprofessionals (96%) zijn ervan overtuigd dat een Zero Trust-strategie cruciaal is voor het succes van hun organisatie. (Zie bewijsstuk 1) Naast het versterken van hun algehele beveiliging en het verbeteren van de ervaring voor eindgebruikers, kiezen beveiligingsprofessionals voor de Zero Trust-strategie om de beveiligingsprocedures voor werknemers te vereenvoudigen. (Zie Bewijsstuk 2)

Zoals een Amerikaanse beveiligingsbeslisser in de horeca verklaart: "*Het doel is om onze algehele beveiliging te verbeteren, maar het draait allemaal om het versoepelen van de eindgebruikerservaring, zodat het leven van eindgebruikers wat gemakkelijker wordt.*"

Bovendien ziet 31% van de beveiligings-professionals de Zero Trust-strategie als een belangrijk instrument voor de aanstaande overstap op een hybride werkplek na de pandemie. Vooral in Australië/Nieuw-Zeeland (44%) is dit een belangrijke beweegreden.

Bewijsstuk 1. Zero Trust is cruciaal



Bewijsstuk 2. Beweegredenen voor Zero Trust

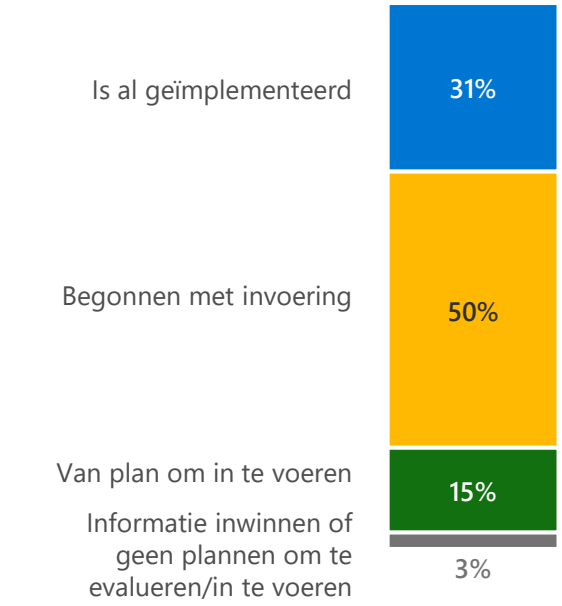
Belangrijkste beweegredenen	
Verbeteren van algehele beveiliging	47%
Ervaring en productiviteit van eindgebruikers verbeteren	44%
De manier transformeren waarop beveiligingsteams samenwerken	38%
Beveiligingsstack vereenvoudigen	35%
Kosten van beveiliging verlagen	35%

De overstap naar een hybride werkplek leidt tot een bredere acceptatie van de Zero Trust-strategie

81% van de ondernemingen is begonnen met de overstap naar een hybride werkplek, die door 31% al volledig is voltooid. De percentages voor volledige invoering zijn echter niet consistent op alle markten: terwijl Australië en Nieuw-Zeeland het voortouw nemen met 37%, ligt Duitsland ver achter, met slechts 20% van de organisaties die al zijn overgestapt op een hybride model. (Zie Bewijsstuk 3)

Ondanks dat de mondiale markten de hybride werkplek in een ongelijk tempo invoeren, verwacht de overgrote meerderheid (91%) van de organisaties die de transitie nog niet hebben voltooid, dat dit de komende vijf jaar een feit zal zijn. Van cruciaal belang is dat 94% zich zorgen maakt over de transitie. Misbruik door werknemers, grotere IT-workloads en een verhoogd risico op cyberaanvallen staan daarbij boven aan de lijst met zorgen. (Zie Bewijsstuk 4)

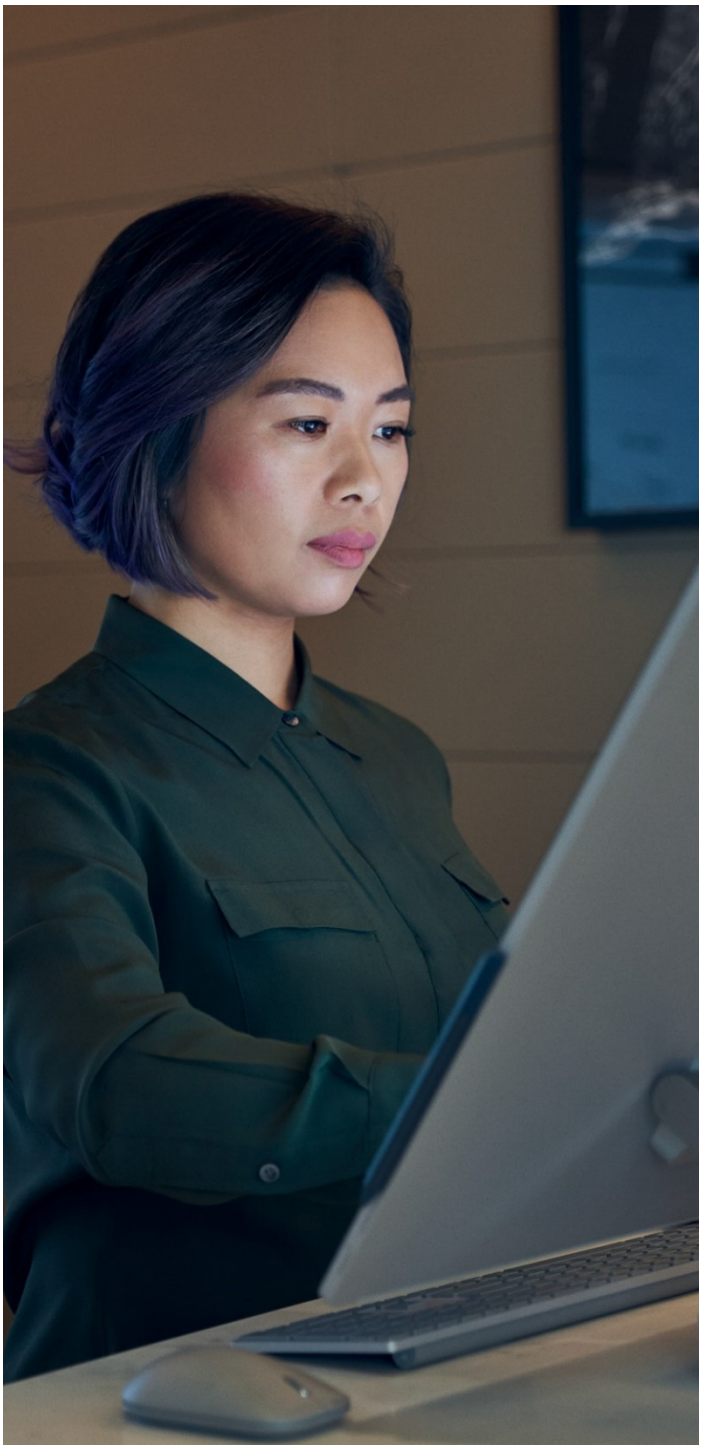
Bewijsstuk 3. Voornemens hybride werkplek



Bewijsstuk 4. Zorgen over de hybride werkplek

Medewerkers die onveilige apps downloaden	37%
Een toename van de IT-workload	37%
Ransomware-aanvallen	36%
Phishingaanvallen	35%
Ongepast gebruik van persoonlijke apparaten	34%
Onbevoegde toegang tot data	31%
Niet alle apparaten kunnen beheren	30%
Gebruik van persoonlijke e-mail-accounts	30%
Non-compliance van regelgeving voor data	24%

COVID-19 heeft geleid tot nieuwe overwegingen die de overstap naar de Zero Trust-strategie versnellen



In een poging om potentiële problemen te minimaliseren, benadrukken stakeholders het belang van meer training voor werknemers (54%) (met name in Japan (61%) en Duitsland (58%)) en meervoudige verificatie (MFA) (50%) (met name in de Verenigde Staten (52%) en Duitsland (56%)) om een soepele gebruikerservaring en transitie te garanderen.

Omdat veilig extern en hybride werken kan worden ondersteund door de Zero Trust-strategie, heeft COVID-19 de invoering van een Zero Trust-strategie voor 72% van de organisaties versneld, hoewel niet alle markten gelijk opgaan. Hoewel de pandemie bij ongeveer zeven van de tien organisaties in de VS (76%), Japan (71%) en Australië/Nieuw-Zeeland (69%) zorgde voor een intensivering van de acceptatie, is de implementatiegraad in Duitsland opmerkelijk lager geweest (62%), mogelijk als gevolg van een langzamere overgang naar een hybride werkplek.

Zero Trust wordt wereldwijd breed toegepast en groeit in de VS

Zero Trust is niet zomaar een modewoord; het is een realiteit. 76% van de organisaties is minimaal begonnen met de implementatie van deze strategie en 35% meent dat de strategie volledig is geïmplementeerd. Deze data schetst echter een te optimistisch beeld, omdat veel organisaties die menen dat de implementatie is voltooid, naar eigen zeggen nog niet klaar zijn met de invoering op alle beveiligingsrisicogebieden. Op dit moment hebben de VS een voorsprong bij de invoering van de Zero Trust-strategie ten opzichte van andere markten en deze blijft snel groeien: vergeleken met augustus 2020 nam de implementatie van de Zero Trust-strategie in de VS toe van 70% tot 79%, een aanzienlijke sprong vooruit in slechts acht maanden.
(Zie Bewijsstuk 5)

Hoewel de Zero Trust-strategie momenteel overheerst in de beveiligingsruimte, is de alomtegenwoordigheid ervan relatief nieuw. 82% van de bedrijven heeft in de afgelopen drie jaar Zero Trust-strategieën geïmplementeerd, waarvan 21% in de afgelopen 12 maanden. Daarbij moet worden opgemerkt dat 26% van de Amerikaanse organisaties meer dan drie jaar geleden is begonnen met de implementatie, vergeleken met 19% van de Japanse organisaties, 6% van de organisaties in Australië/Nieuw-Zeeland en 3% van de organisaties in Duitsland. Deze vroegere implementatie in de VS, in combinatie met ruimere budgetten, kan een verklaring vormen waarom organisaties in de VS vooroplopen bij de invoering van Zero Trust in vergelijking met organisaties op andere markten. Zo kan ook de relatief trage ontwikkeling van Zero Trust in Duitsland een verklaring vormen voor de lage invoeringscijfers: 97% van de Duitse organisaties is pas in de afgelopen drie jaar met de implementatie begonnen.

Bewijsstuk 5. Zero Trust-implementatie

	VS (2020)	VS	DE	JP	AUS/NZ
Zero Trust-implementatie	70%	79%	75%	76%	71%
• Volledig geïmplementeerd	27%	44%	19%	32%	28%
• Wordt uitgevoerd	43%	35%	56%	44%	43%

35% volledig geïmplementeerd

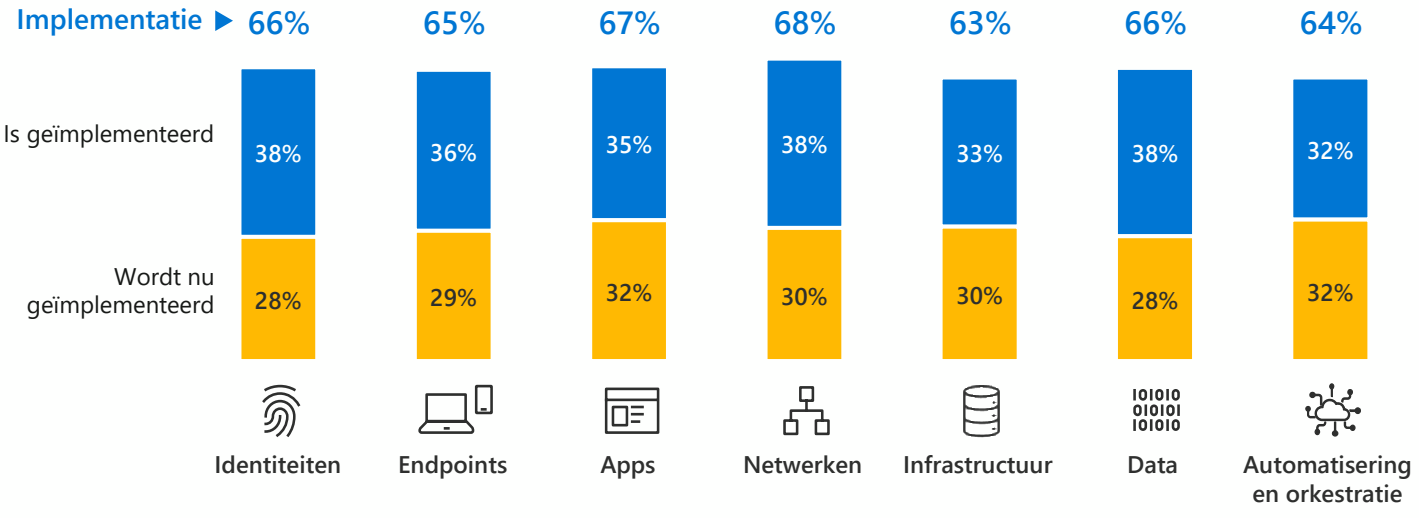
42% implementatie wordt uitgevoerd

Er is geen uniforme aanpak voor de implementatie van Zero Trust, zodat organisaties feitelijk overal kunnen beginnen

Geen enkel beveiligingsrisicogebied (identiteiten, endpoints, apps, netwerken, infrastructuur, data, automatisering en orkestratie) vormt een duidelijk primair uitgangspunt voor de Zero Trust-strategie, aangezien minder dan 15% begint met hetzelfde beveiligingsrisicogebied. Dat organisaties verschillende aspecten als eerste aanpakken hangt waarschijnlijk samen met hun behoeften en beschikbare interne resources. Uiteindelijk willen ze de Zero Trust-strategie toepassen op alle gebieden met een beveiligingsrisico om nog meer bescherming tegen bedreigingen te kunnen garanderen, en wordt Zero Trust dus gezien als een allesomvattende strategie die niet in één keer kan worden voltooid. (Zie Bewijsstuk 6)

Bedrijven moeten niet alleen de beveiligingsrisico's globaal aanduiden in hun Zero Trust-strategie , maar moeten ook alle afzonderlijke onderdelen van de beveiliging identificeren die prioriteit moeten krijgen. Endpoints, apps, netwerken, data en automatisering/orkestratie vormen geen overduidelijk uitgangspunt; de meningen van beveiligingsprofessionals verschillen aanzienlijk voor wat betreft de onderdelen die ze als hun hoogste prioriteit beschouwen. Sterke verificatie wordt echter meestal eerst geïmplementeerd voor identiteiten en bedreigingsdetectietools vormen een duidelijke prioriteit binnen de infrastructuur. (Zie Bewijsstuk 7)

Bewijsstuk 6. Huidige implementatie van Zero Trust: beveiligingsrisicogebieden



	Identiteiten	Endpoints	Apps	Netwerken	Infrastructuur	Data	Automatisering en orkestratie
Gemiddelde rangschikking (Als eerste begonnen)	1.1	0.9	0.8	1.1	1.1	1.1	1.0

Bewijsstuk 7. Implementatie van Zero Trust-onderdelen (Top 3) – Als nummer 1 gerangschikt (als eerste geïmplementeerd)

Identiteiten	
Sterke verificatie (bijv. meervoudige verificatie, verificatie zonder wachtwoord)	32%
Geautomatiseerd detecteren en verhelpen van risico's	27%
Adaptief toegangsbeleid om toegang tot resources te verlenen	22%

Endpoints	
Beleid/controles voor preventie van dataverlies voor alle onbeheerde en beheerde apparaten	27%
Realtime risico-evaluatie van apparaten/ detectie van endpointbedreigingen	26%
Apparaten worden geregistreerd bij een identiteitsprovider	24%

Apps	
Voortdurende detectie en risico-evaluatie van schaduw-IT	23%
Gedetailleerde toegangscontrole voor je apps (zoals beperkte zichtbaarheid of alleen-lezen)	22%
Op beleid gebaseerd toegangsbeheer voor apps	20%

Netwerken	
Beveiligd toegangsbeheer om netwerken te beschermen	25%
Bedreigingsbescherming en filteren op basis van contextgebaseerde signalen	24%
Al het verkeer wordt versleuteld	20%

Infrastructuur	
Toegang van beveiligingsteam tot bedreigingsdetectietools	25%
Bescherming van cloudworkloads voor hybride en multi-cloud	19%
Gedetailleerde zichtbaarheid en toegangsbeheer voor alle workloads (virtuele machines, servers, enz.)	17%

Data	
Toegangsbeslissingen worden beheerd door de engine voor beveiligingsbeleid	21%
Data wordt geclassificeerd en gelabeld	21%
De gevoeligste bestanden worden permanent beveiligd met encryptie	20%

Automatisering en orkestratie	
Totale zichtbaarheid via een gecentraliseerd platform voor onderzoek en respons	29%
Bedreigingsdata wordt verzameld en geanalyseerd voor meerdere domeinen (identiteiten, endpoints, apps, netwerken, infrastructuur)	28%
Geautomatiseerd onderzoek en respons is ingeschakeld	22%

We beschouwen het niet als zomaar een reeks technologieën, maar als een strategie en benadering om elke gebruikersresource, of die zich nu binnen of buiten of netwerk bevindt, als niet-vertrouwd te beschouwen totdat deze kan worden geverifieerd."

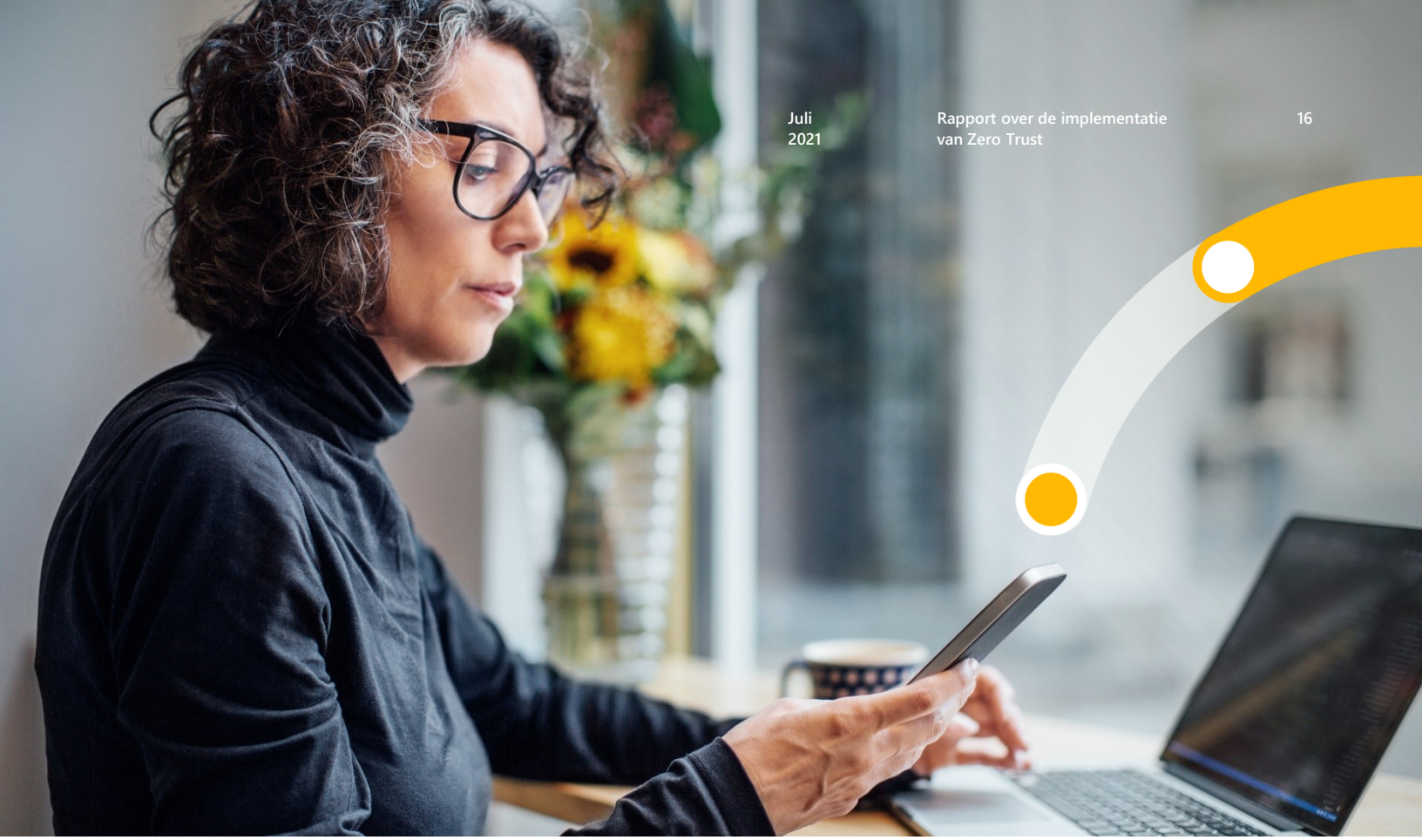
Amerikaanse SDM
Horeca

Als organisaties beginnen met de implementatie van een Zero Trust-strategie, zijn de grootste voordelen een grotere flexibiliteit, snelheid en bescherming; voordelen op het gebied van resources zijn minder gebruikelijk

Nadat de Zero Trust-strategie is geïmplementeerd, profiteren organisaties van meer flexibiliteit (37%), snelheid (35%) en bescherming van klantdata (35%). (Zie Bewijsstuk 8) Maar directe voordelen voor werknemers, waaronder een beveiligingsteam dat meer tijd overhoudt (27%) en een kleinere behoefte aan middelen om de infrastructuur te beheren (22%), worden minder vaak bereikt.

Nog belangrijker: organisaties zijn ervan overtuigd dat hun Zero Trust-strategie hen zal helpen de meeste bedreigingen en veranderingen in de omgeving te beheren, met name met betrekking tot IoT- en OT-beveiliging (47%).

Bewijsstuk 8. Voordelen van Zero Trust



Organisaties hebben er alle vertrouwen in dat ze optimaal kunnen profiteren van hun Zero Trust-strategie

79% heeft vertrouwen in hun vermogen om beveiligingsbedreigingen als geheel af te handelen, hoewel dit vertrouwen afneemt wanneer de bedreiging een falsificatie van de waarheid vormt: SDM's hebben het minst vertrouwen in het afhandelen van bedreigingen met betrekking tot synthetische identiteiten (20%) en deepfakes (10%).

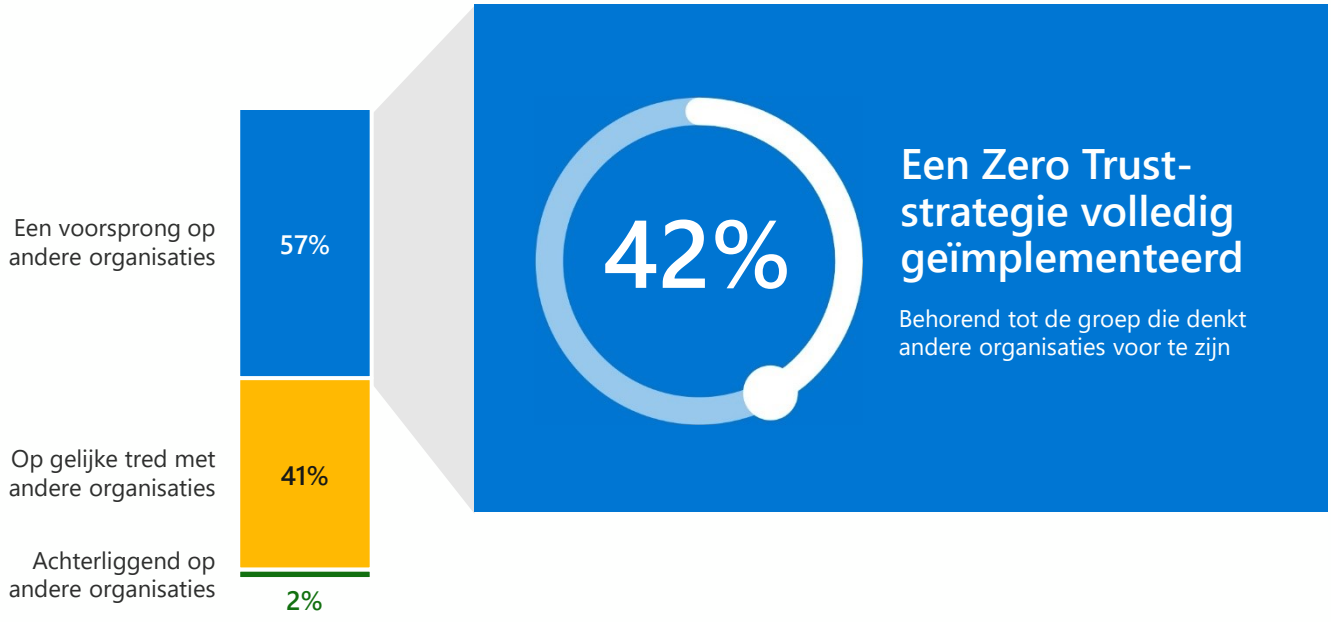
Gezien de voordelen die kunnen worden behaald, roept Zero Trust over het algemeen positieve reacties op. Op de vier markten zien SDM's de aanpak van hun organisaties tegelijkertijd als praktisch en ambitieus, waarbij ze deze beschrijven als zelfverzekerd (37%) en efficiënt (31%), maar ook motiverend (25%), inspirerend (25%) en enerverend (25%). Met name in Japan beschrijven beveiligingsprofessionals Zero Trust als veeleisend (27%) én transformationeel (25%), wat suggereert dat de voordelen, hoewel niet eenvoudig te behalen, verreikend zijn zodra de Zero Trust-strategie is geïmplementeerd.

Veel organisaties zijn ervan overtuigd dat ze vooroplopen met hun Zero Trust-implementatie, maar er is nog steeds meer werk te verzetten

Hoewel slechts 35% van de organisaties hun Zero Trust-strategie volledig heeft geïmplementeerd, zegt 52% dat ze een voorsprong hebben op hun planning en is 57% ervan overtuigd een voorsprong te hebben op andere organisaties. Organisaties denken met name een bijzonder grote voorsprong op anderen te hebben in Japan (66%) en Australië/Nieuw-Zeeland (63%). Hoewel het vertrouwen op alle markten groot is, lijkt er een kloof te bestaan tussen perceptie en realiteit: van de organisaties die ervan overtuigd zijn een voorsprong te hebben op andere organisaties, beweert slechts 42% dat de Zero Trust-strategie volledig is geïmplementeerd. (Zie Bewijsstuk 9)

Hoewel veel organisaties vertrouwen hebben in hun Zero Trust-strategie en denken voorbereid te zijn om toekomstige beveiligingsbedreigingen het hoofd te bieden, is er nog steeds veel werk te doen om de strategie op alle risicogebieden volledig te implementeren. Van de organisaties die van mening zijn dat hun Zero Trust-strategie volledig is geïmplementeerd, heeft bijna de helft de strategie bijvoorbeeld niet op alle risicogebieden geïmplementeerd, waarbij met name voor infrastructuur en identiteiten de kans het kleinst is dat de strategie is geïmplementeerd.

Bewijsstuk 9. Vergelijking van Zero Trust-implementaties



	VS	DE	JP	AUS/NZ
Voorsprong	59%	46%	66%	63%
Gelijke tred	40%	52%	34%	32%
Achterop	2%	2%	0%	6%

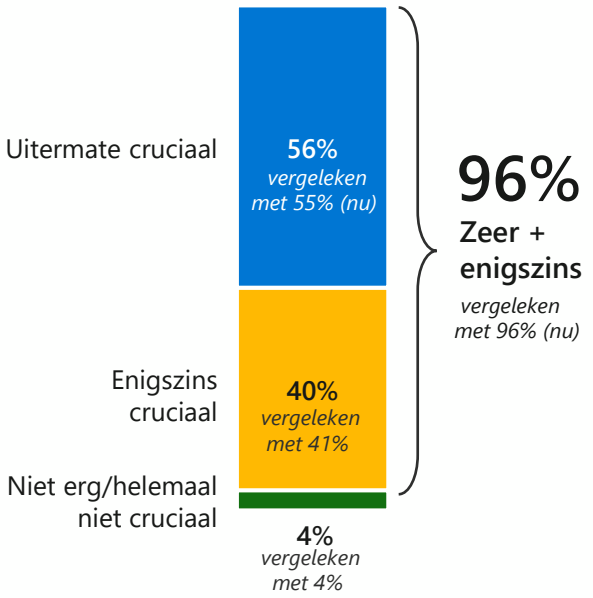
Microsoft Security hypothesis

Voor de komende twee jaar blijft de Zero Trust-strategie een topprioriteit op het gebied van beveiliging

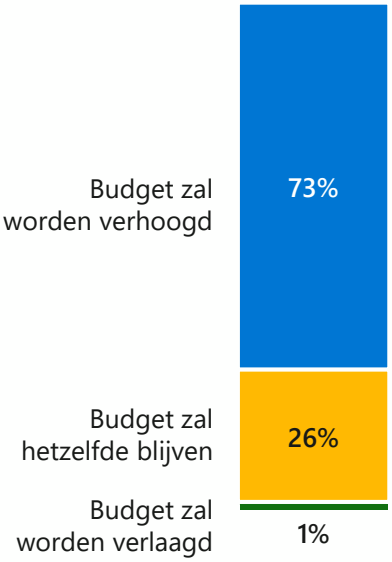
Organisaties zijn uitermate serieus over implementatie van een Zero Trust-strategie en beslissers zeggen dat dit de komende twee jaar de hoogste beveiligingspri-oriteit blijft. Het relatieve belang van de Zero Trust-strategie als beveiligingsinitiatief zal naar verwachting toenemen (53% tot 58%) in 2023, omdat SDM's verwachten dat de strategie van cruciaal belang zal blijven voor het algehele succes (96%). (Zie Bewijsstuk 10)

Het idee dat Zero Trust cruciaal zal blijven leeft met name onder Japanse organisaties, waarvan 70% zegt dat de Zero Trust-strategie de komende twee jaar zeer cruciaal zal zijn, vergeleken met het algemene gemiddelde van 56%. Naar verwachting zullen ook de budgetten voor de Zero Trust-strategie groeien, waarbij 73% van de organisaties verwacht het budget te zullen verhogen. Dit percentage ligt echter iets lager in Duitsland (67%), waar 31% verwacht dat hun budget hetzelfde zal blijven. (Zie Bewijsstuk 11)

Bewijsstuk 10. Hoe cruciaal is Zero Trust in de komende twee jaar?

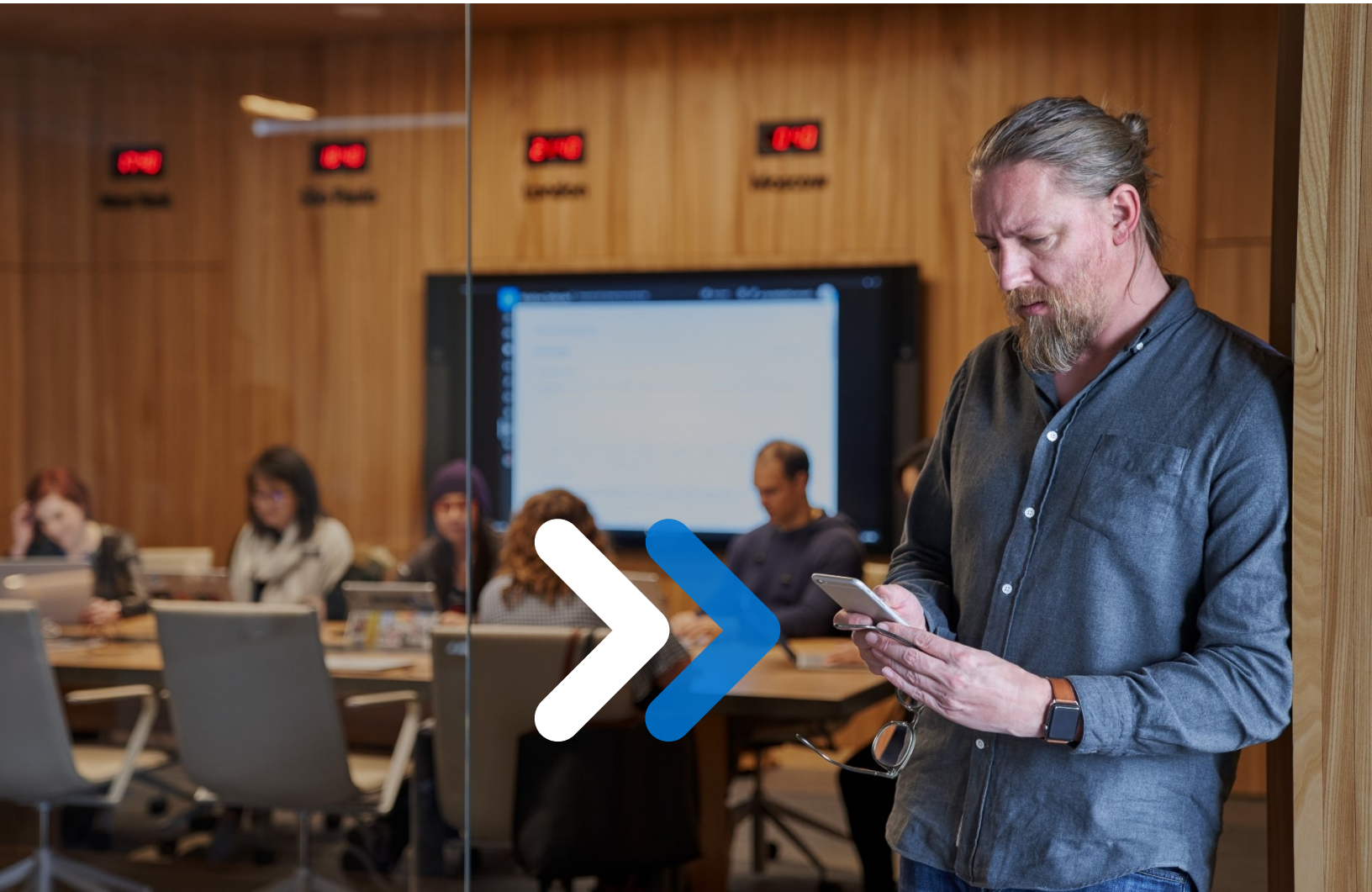


Bewijsstuk 11. Verwacht Zero Trust-budget in de komende twee jaar



Het aantonen van het succes van een Zero Trust-strategie kan verdere investeringen stimuleren

Organisaties die Zero Trust met open armen hebben ontvangen, verwachten dat ze hun investeringen in de komende twee jaar zullen verdubbelen, en organisaties die nog niet zijn begonnen met het invoeren, lopen het risico dat ze verder achterop raken. Deze organisaties lopen niet alleen achter bij organisaties die Zero Trust volledig hebben geïmplementeerd qua prioritering hiervan in hun beveiligingsplannen (42% vs. 66%) en de verwachting dat het budget zal worden verhoogd (66% vs. 72%), maar hebben ook aanzienlijk minder vertrouwen in het beheer van IoT- en OT-beveiliging in de toekomst (40% vs. 53%).



Het overwinnen van problemen met werknemers is dé cruciale factor om de Zero Trust-investering aanzienlijk te verhogen

Ondanks de grote stappen voorwaarts in de invoering van Zero Trust-strategieën, moeten organisaties een groot aantal uitdagingen overwinnen als ze echte voortgang willen boeken met de implementatie. (Zie Bewijsstuk 12) Problemen op het gebied van resources en leiderschap komen het meest voor binnen deze categorieën. De tijd die nodig is om Zero Trust-strategieën te implementeren en een gebrek aan steun van de directie staan bovenaan de lijst met obstakels, waarbij dit laatste aspect vooral opvallend is in Australië/Nieuw-Zeeland (65%).

Bovendien spelen budgettaire beperkingen, door 45% van de organisaties als een obstakel beschouwd, waarschijnlijk ook een rol bij uitdagingen op het gebied van resources en leiderschap.

Zo noemt 21% van de SDM's problemen bij het aantonen van het ROI van een investering in Zero Trust als een obstakel voor implementatie, wat op zijn beurt kan leiden tot een gebrek aan steun van de directie. Omdat markten buiten de VS meer budgettaire beperkingen hebben (60% van de organisaties in Japan; 57% van de organisaties in Duitsland; 57% van de organisaties in Australië/Nieuw-Zeeland), heeft dit mogelijk een rimpeleffect, wat kan leiden tot een lagere implementatiegraad en tragere voortgang voor Zero Trust-strategieën in Japan, Duitsland en Australië/Nieuw-Zeeland in vergelijking met de VS.

Bewijsstuk 12. Obstakels voor Zero Trust

Problemen met resources 60%	Leiderschap 53%	Technologisch 46%	Leverancier 46%	Budgetbeperkingen 45%
20% Implementatie duurt te lang	**20%** Gebrek aan steun van allerhoogste leiding als geheel	**21%** Problemen bij het integreren van beveiligingsoplos-singen	**21%** Heeft support bij de implementatie nodig van leveranciers	**21%** Kosten van implementatie van een Zero Trust-strategie
19% Gebrek aan intern verandermanagement	**19%** Gebrek aan steun van stakeholders	**19%** Incompatibiliteit met oudere systemen	**21%** Ondervindt moeite met het identificeren van de juiste leveranciers	**21%** Moeite om ROI aan te tonen
18% Meer leermate-riaal nodig	**19%** Hulp nodig om een overtuigende businesscase samen te stellen	**19%** Moeilijkheden met opschalen voor de hele organisatie	**17%** Kan geen innovatieve partners vinden	**14%** Budget is niet toereikend
17% Niet nodig voor een organisatie van onze omvang	**18%** Gebrek aan steun binnen de organisatie			
16% Beschikt niet over het juiste talent om goed te implementeren				

" Het kostte veel moeite om steun te krijgen, maar toen we eenmaal als stakeholders overeenkwamen dat we in dit project zouden investeren, stond iedereen er ook echt achter."

Amerikaanse SDM
FinTech

Beslissers op het gebied van beveiliging hebben een lichte voorkeur voor holistische of geconsolideerde aanbieders

Als het gaat om Zero Trust-leveranciersstrategie, hebben organisaties de keuze uit een best-in-suite- of best-in-breed-aanpak. De eerste strategie omvat de aankoop van een suite met producten voor de volledige Zero Trust-architectuur van een holistische of geconsolideerde leverancier, een oplossing die volgens SDM's meer expertise en resources biedt, evenals eenvoud voor organisaties die intern te kampen hebben met een gebrek aan resources. Problemen met deze aanpak zijn echter toegenomen kwetsbaarheid en gebrek aan flexibiliteit. (Zie Bewijsstuk 13)

Bij deze laatste strategie, best-in-breed, worden individuele onderdelen van de Zero Trust-technologie bij gespecialiseerde leveranciers gekocht. In tegenstelling tot best-in-suite, is deze strategie gebaseerd op leveranciers die op verschillende gebieden zijn gespecialiseerd. Als zodanig bieden ze grotere flexibiliteit en sluiten hun oplossingen beter aan bij de strategie van de organisatie. Volgens beveiligingsprofessionals is best-in-breed echter duurder, zijn hiervoor meer resources vereist en wordt de zichtbaarheid belemmerd. Deze nadelen leiden uiteindelijk tot problemen op leveranciers- en begrotingsgebied. (Zie Bewijsstuk 14)

Hoewel organisaties grotendeels in twee kampen uiteenvallen, werkt een kleine meerderheid van de SDM's (55%) liever met holistische (best-in-suite) leveranciers. (Organisaties in Australië/Nieuw-Zeeland neigen echter tot de tegenovergestelde richting, waarbij 52% de voorkeur geeft aan de best-in-breed.)

Bewijsstuk 13. Voordelen en obstakels voor best-in-suite, gerangschikt in Top 2

⊕ Voordelen van best-in-suite	
Leverancier heeft branchespecifieke expertise voor alle oplossingen	24%
Meer resources beschikbaar om een Zero Trust-strategie te helpen plannen	23%
Vereenvoudigde beveiligingsstack	22%

⊖ Nadelen van best-in-suite	
Vertrouwen op één leverancier verhoogt de kwetsbaarheid	34%
Vereist complexere integratie met verouderde architectuur	33%
Minder flexibiliteit voor gespecialiseerde functies	29%

Bewijsstuk 14. Voordelen en obstakels voor best-in-breed, gerangschikt in Top 2

⊕ Voordelen van best-in-breed	
Flexibiliteit om de beste oplossingen voor elk onderdeel van de Zero Trust-strategie te verkrijgen	33%
Kan de oplossing beter afstemmen op de architectuur of strategie van mijn organisatie	30%
Meer mogelijkheden voor innovatie met verschillende leveranciers	26%

⊖ Nadelen van best-in-breed	
Hogere kosten	29%
Geen mogelijkheden om data tussen verschillende oplossingen te delen	26%
Groot aantal oplossingen die interne teams moeten implementeren en beheren	26%

Afsluiting

Beveiligingsrisico's komen niet alleen vaker voor, maar hebben ook negatievere gevolgen. Daarom kiezen organisaties op allerlei markten en in uiteenlopende branches voor een Zero Trust-strategie, die is gebaseerd op het motto "niemand en niets vertrouwen en altijd controleren". De Zero Trust-strategie is de belangrijkste beveiligingsprioriteit voor organisaties die hun algehele beveiliging en de ervaring voor eindgebruikers willen verbeteren, de productiviteit willen verhogen, beveiligingsprocedures voor werknemers gebruiksvriendelijker willen maken en de kosten willen terugdringen. Hoewel de voordelen van een Zero Trust-strategie duidelijk zijn aangetoond, staan beperkte resources en scepsis bij de leiding universele implementatie in de weg.

Invoering van een Zero Trust-strategie is de afgelopen drie jaar in een stroomversnelling geraakt, deels als gevolg van de COVID-19-pandemie. Een cruciale factor is de overstap op externe en hybride werkplekken. Deze trend leidt tot bredere invoering van een Zero Trust-aanpak, die beveiliging van systemen en data kan waarborgen, ook voor medewerkers die hiertoe extern toegang verkrijgen, soms op persoonlijke apparaten. Versnelde implementatie als gevolg van COVID is een goede indicator van hoe goed organisaties voorbereid zijn op Zero Trust in het algemeen. Hierbij valt het op dat organisaties die deze strategie tijdens de pandemie hebben omarmd, deze op meer beveiligingsrisicogebieden hebben geïmplementeerd dan de overige organisaties.

Desondanks hebben zelfs de organisaties die het verst in het traject van Zero Trust-implementatie zijn, nog veel werk te verzetten. De misvattingen van organisaties over hun eigen volwassenheid op Zero Trust-gebied kunnen sommige ondernemingen kwetsbaar maken op bepaalde gebieden, zonder dat ze zich hiervan zelf bewust zijn.

Een meerderheid van de organisaties op verschillende markten is van mening dat het cruciale belang van een Zero Trust-strategie alleen maar verder zal toenemen en verwacht dat hun budgetten navenant zullen toenemen. Deze verwachte verschuiving in prioriteiten is van cruciaal belang voor met name niet-Amerikaanse markten, waar zorgen op budgettair gebied een opvallende belemmering voor invoering vormen. Het streven naar volledige implementatie kan financieel en logistiek een overweldigende uitdaging lijken, maar de voordelen van een Zero Trust-aanpak zijn gewoonweg onmiskenbaar, en Microsoft staat klaar om organisaties te begeleiden en ondersteunen bij hun traject naar een veelbelovende toekomst.

Als je meer wilt weten over Zero Trust en een evaluatie wilt maken van de volwassenheid op Zero Trust-gebied van je organisatie, ga je naar

aka.ms/zerotrust

Gedetailleerde onderzoeksdoelstellingen en hoe we de doelgroep hebben geworven

De doelstellingen van het onderzoek waren onder andere:

Inzicht verkrijgen in de huidige status van Zero Trust-benaderingen

Houdingen, best practices, voordelen en uitdagingen voor uiteenlopende Zero Trust-benaderingen blootleggen

De toekomst van Zero Trust-benaderingen verkennen

Meer context bieden voor innovaties en trends in Zero Trust-benaderingen

Om aan de screeningcriteria te voldoen, moesten SDM's aan de volgende vereisten voldoen:

Verantwoordelijk zijn voor de beveiliging in hun organisatie, waaronder cyberbeveiliging, beveiligingsactiviteiten, bescherming tegen bedreigingen, identiteitsbeheer, risicobeheer, applicatiebeveiliging, Digital Forensics en incidentrespons

Voltijds werken bij een organisatie op ondernemingsniveau (1000+ werknemers in de VS; 500+ werknemers in DE/JP/AU/NZ)

Leeftijdsgroep 25-75

Vertrouwd met Zero Trust

Betrokken zijn bij besluitvorming voor de ontwikkeling/implementatie van Zero Trust-strategieën

Van de 911 SDM's die zijn geïnterviewd voor het onderzoek van april 2021:

Werden in de VS 477 SDM's geïnterviewd

Werden in Duitsland 201 SDM's geïnterviewd

Werden in Australië/Nieuw-Zeeland 126 SDM's geïnterviewd

Werden in Japan 107 SDM's geïnterviewd

Opmerking: dit onderzoek is uitgevoerd tijdens de wereldwijde COVID-19 pandemie, waarbij in uiteenlopende regio's uiteenlopende escalatie/beperkende maatregelen gold/golden.