Cybertolerantie in actie

Benchmarking van de wereldwijde paraatheid van ondernemingen voor beveiligen, detecteren en herstellen
Insight-discussie
Januari 2026

DELL Technologies

Agenda

- Doelstellingen en bedrijfsstatistieken
- De achterstand op het gebied van cybertolerantie
- Beveiligen
- Detecteren
- Herstellen
- Complexiteit, cultuur en de toekomst

Bedrijfsdoelstellingen

- Om Dell te positioneren als een thought leader en strategische partner voor cybertolerantie
- Om opnieuw de beslissing te bevestigen om van het label "databescherming" over te stappen op "cybertolerantie"

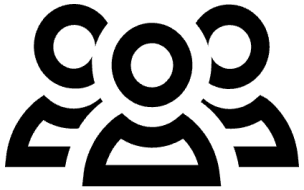
Onderzoeksdoelen

- Beoordeel de volwassenheid en integratie van strategieën voor cybertolerantie
- Beoordeel de effectiviteit van de beveiligings-, detectie- en herstelpraktijken van organisaties
- Inzicht in barrières voor het verbeteren van cybertolerantie, waaronder gebrek aan vaardigheden, budget en complexiteit
- Onderzoeken hoe organisaties hun IT-omgeving beveiligen en data beschermen tegen ransomware-bedreigingen

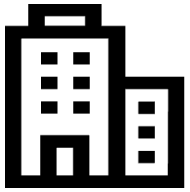
Wie hebben we ondervraagd?

Respondenten werden ondervraagd in juli en oktober 2025

850 IT-besluitvormers van wereldwijde organisaties



Organisaties met meer dan 1.000 werknemers



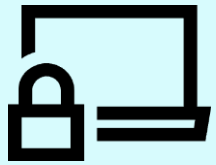
Organisaties komen uit verschillende publieke en particuliere sectoren

Respondenten zijn: bestuursleden, senior managers op C-niveau, middenkader

Belangrijkste conclusies

39%

van de organisaties heeft een volledig uitgewerkte en voortdurend geoptimaliseerde strategie voor cybertolerantie



Continue optimalisatie is essentieel – zonder dit kunnen strategieën snel verouderd raken ten opzichte van zich ontwikkelende bedreigingen, waardoor organisaties een groter risico lopen.

46%

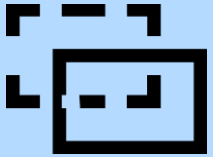
erkent dat de back-updata niet zo goed beveiligd zijn als zou moeten

Het versterken van back-upbescherming is essentieel om ervoor te zorgen dat herstel mogelijk blijft wanneer primaire systemen in gevaar komen.

Beveiligen

30%

gebruikt een uitgebreid platform voor het detecteren van bedreigingen in het netwerk, de back-up en de primaire storage



Zonder uniforme detectie kunnen de zichtbaarheid van bedreigingen en de reactietijden trager zijn, waardoor het risico op onopgemerkte inbreuken toeneemt.

Detecteren

55%

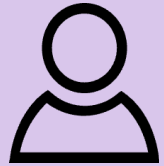
van degenen die maandelijks of vaker gesimuleerde cyberaanvallen uitvoerden, is succesvol hersteld na een oefening/cyberincident

Regelmatig testen helpt teams zich voor te bereiden op het echte werk. Regelmatig testen helpt teams zich voor te bereiden op de praktijk.

Herstellen

63%

denkt dat het management de paraatheid van hun organisatie voor een groot cyberincident overschat



Te veel zelfvertrouwen kan investeringen vertragen, de planning van reacties vertragen en kritieke kwetsbaarheden onopgelost laten.

Deel 1: de achterstand op het gebied van cybertolerantie

Inzicht in het probleem en de urgentie om te evolueren

Het voortdurend optimaliseren van weerbaarheidsstrategieën verbetert het herstel, maar succes is niet gegarandeerd

99,5%

heeft een of andere vorm van cybertolerantiestrategie

39%

is van mening dat deze volledig is uitgewerkt en voortdurend wordt geoptimaliseerd (een volwassen strategie)

57%

kon tijdens hun laatste test of incident niet effectief ingrijpen en herstellen

Organisaties met een volledig ontwikkelde strategie voor cybertolerantie hebben **2,6 keer meer kans om** succesvol te herstellen

65% vs. **25%**

63%

is van mening dat **het management hun paraatheid** voor een groot cyberincident overschat

Waarom dit nu belangrijk is

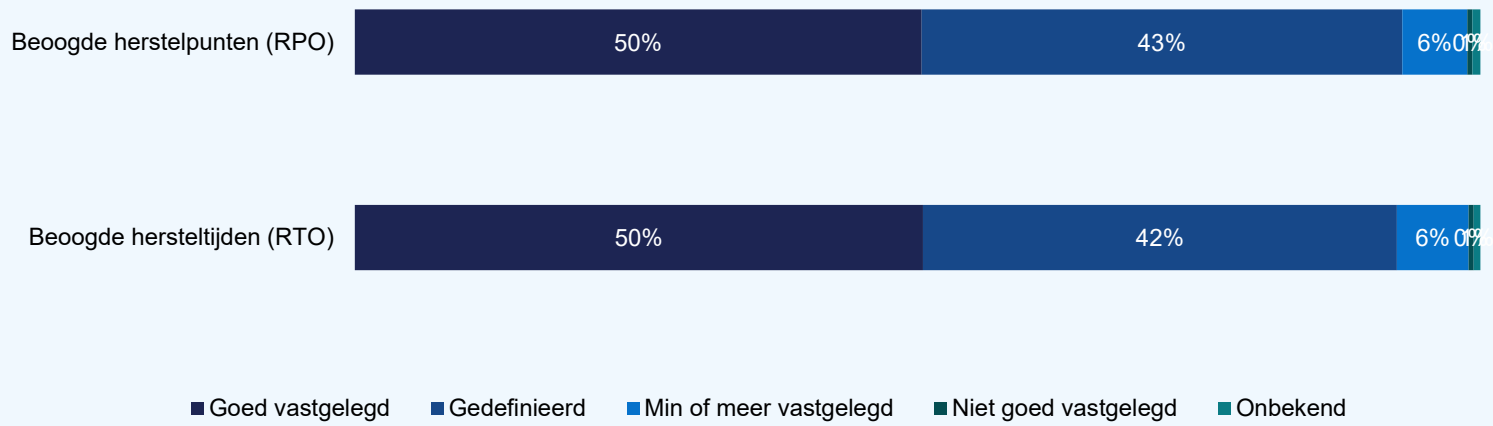
97%

erkent dat hun organisatie de beveiliging voortdurend moet versterken naarmate de bedreigingen evolueren

78%

is van mening dat hun organisatie zich meer richt op het voorkomen van aanvallen dan op het voorbereiden op het herstellen ervan

De mate waarin organisaties het volgende hebben vastgelegd:



32%

heeft **beide gebieden** goed vastgelegd.

Van degenen met een volledig ontwikkelde strategie voor cybertolerantie heeft

58%

heeft zowel een goed vastgelegde RTO als RPO

Deel 2: beveiligen

Aanvallen voorkomen en de digitale omgeving versterken

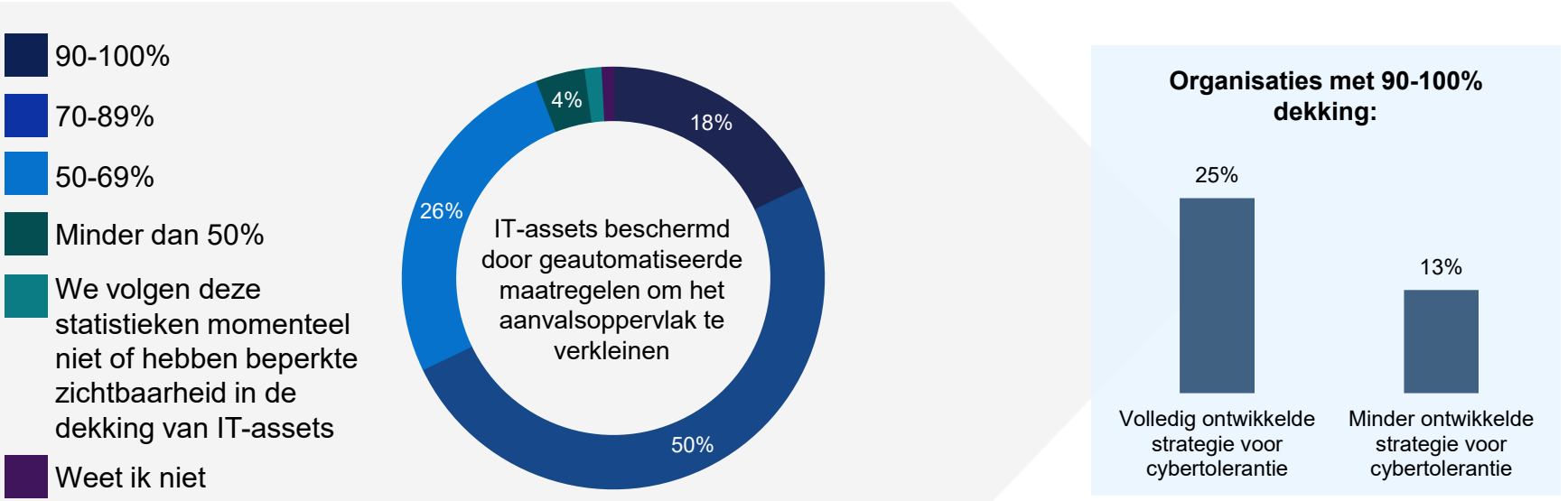
Gebrek aan zichtbaarheid en ontoereikende bescherming

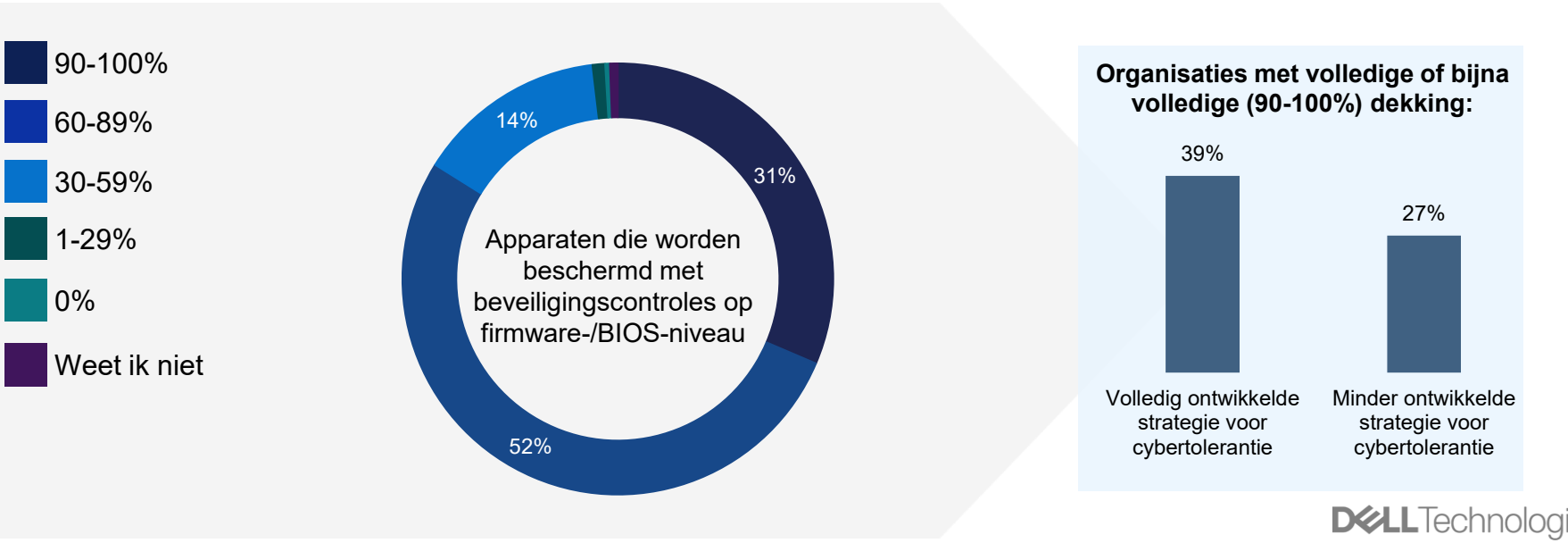
46%

erkent dat hun back-updata niet zo goed beveiligd zijn als zou moeten

N.v.t.	**59%**
EMEA	**43%**
LATAM	**41%**
APJ	**39%**

Voortdurende optimalisaties zorgen niet voor het wegwerken van tekorten, maar geven organisaties wel een belangrijk voordeel op het gebied van veerkracht





Van integriteit vóór implementatie tot herstel na een aanval: versterk beide kanten van de beveiliging

Processen/methoden die door organisaties worden gebruikt om de integriteit van IT-hardware/software te waarborgen

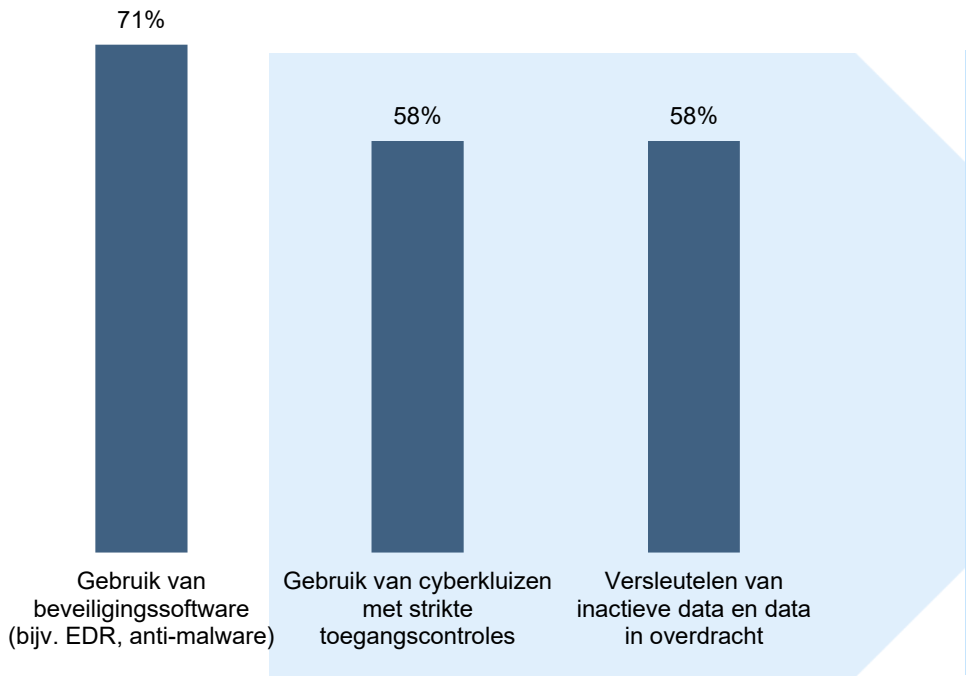
72%

vertrouwt op leveranciers voor certificeringen en verklaringen en voor systemen met ingebouwde tools die de integriteit van componenten controleren

64%

voert interne audits of handmatige evaluaties uit tijdens staging/implementatie

Methoden die door organisaties worden gebruikt om kritieke data te beveiligen tegen ransomware-aanvallen



Organisaties met volledig ontwikkelde veerkrachtstrategieën gebruiken vaker:

- **Dataversleuteling (59% vs.57%)**
- **Cyberkluizen (63% vs.55%)**

dan organisaties met minder ontwikkelde veerkrachtstrategieën

Deel 3: detecteren

Bedreigingen detecteren en erop reageren voordat ze impact hebben

Het gebruik van AI en automatisering kan bedreigingen blootleggen voordat ze back-ups in gevaar brengen

38%

van organisaties gebruiken AI/ML-tools met proactieve risicobeperkende en responsmaatregelen

Organisaties met een volledig ontwikkelde cybertolerantiestrategie doen dit **3,1 keer vaker**

65% vs. **21%**

48%

van de organisaties gebruikt **maakt uitgebreid gebruik van AI/ML om back-updata te scannen** op tekenen van inbreuk

Uitgebreid gebruik van AI/ML komt **2,3 keer zo vaak voor in organisaties met een volledig ontwikkelde strategie voor cybertolerantie**

72% vs. **32%**

83%

denkt dat bedreigingsactoren **steeds vaker back-ups aanvallen** tijdens ransomware-aanvallen

62% geeft prioriteit aan investeringen in automatisering en door AI/ML aangedreven bedreigingsdetectie

Onvolledige zichtbaarheid verhoogt risico's

54%

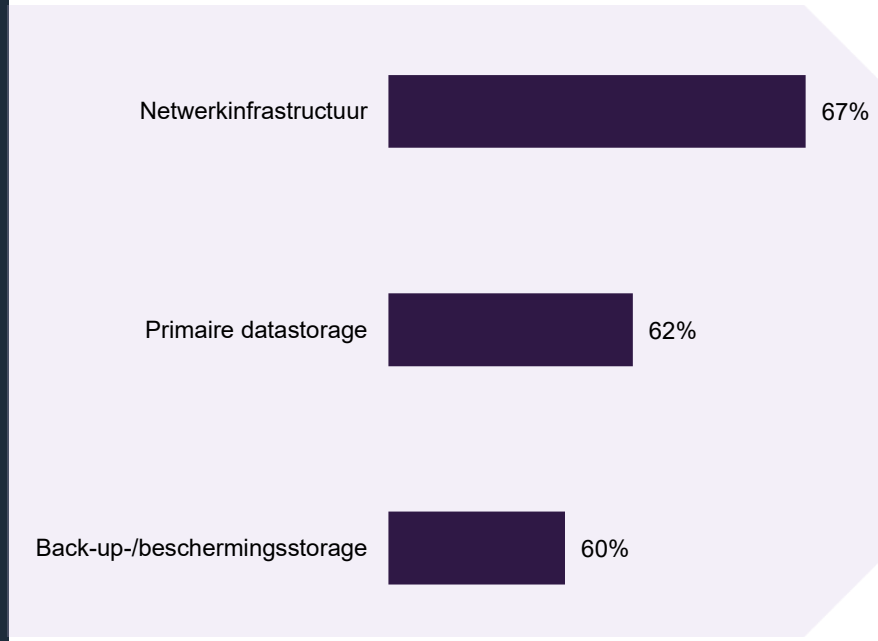
zegt dat ze veel inzicht hebben in verdachte activiteiten of gecompromitteerde data binnen hun back-upsystemen

74% organisaties met een volledig ontwikkelde strategie voor cybertolerantie

vs.

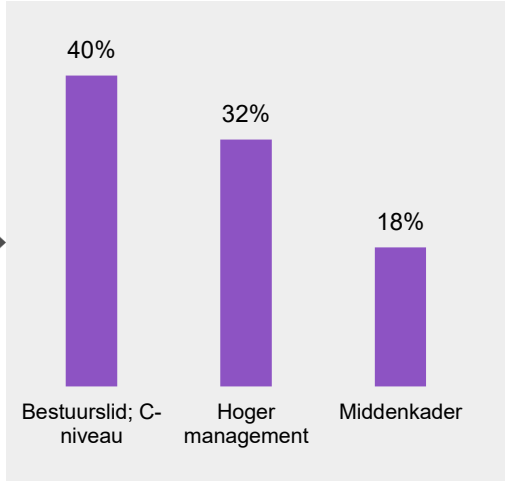
42% van de organisaties met een minder ontwikkelde strategie voor cybertolerantie

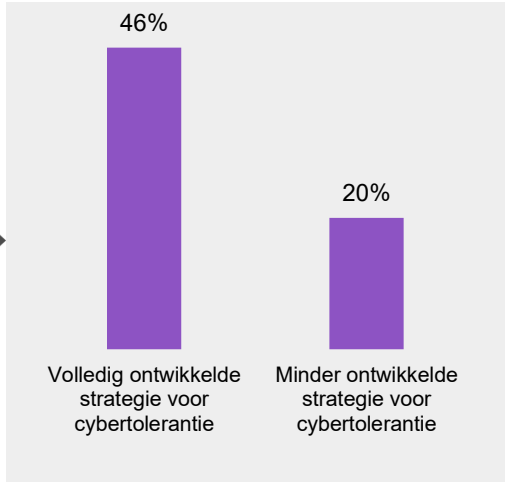
Organisaties met een robuust platform voor bedreigingsdetectie op de volgende gebieden



30%

beschikt over een uitgebreid platform **voor alle 3 de gebieden**





Deel 4: herstellen

Snel herstellen, binnen de SLA-verwachtingen

Status van herstel: veel organisaties voldoen aan de doelstellingen, maar voortdurende verbetering is essentieel om gelijke tred te houden met de toenemende bedreiging

40%

is succesvol ingeperkt en hersteld met minimale impact

Waarbij **bestuursleden (53%)** sneller geneigd zijn dit aan te geven dan **middenkader (30%)**

54%

van organisaties heeft de **RTO/RPO-doelen gehaald**

Per functie: bestuursleden (66%) versus middenkader (45%)

Nr. 4

De belangrijkste drijfveer voor investeringen in cyberbeveiliging is een **recent cyberincident of bijna-incident** binnen de organisatie

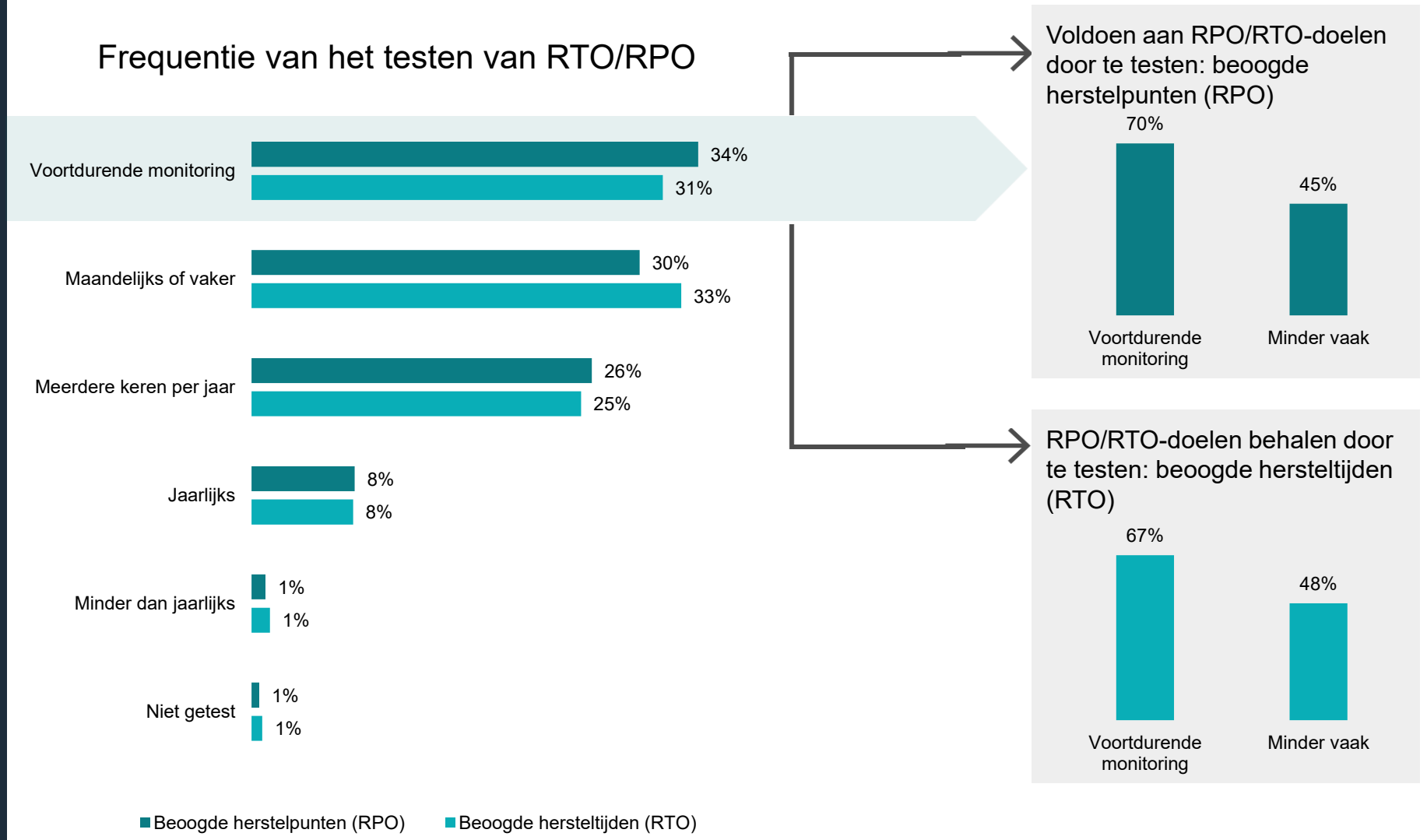
57% verbetert de veerkrachtmogelijkheden om **te voldoen aan wettelijke of nalevingsvereisten**

Regelmatig testen kan het herstel verbeteren

Uiteindelijk zorgt een cultuur van alertheid en voortdurende verbetering voor veerkracht.

SNR Manager, Consumer Services-organisatie, Brazilië

Testen is cruciaal voor veerkracht en geeft organisaties een betere kans om te herstellen



Testen is essentieel voor veerkracht

48%

verklaarde dat de cyberbeveiligingstests van hun organisatie geen realistische simulatie zijn van moderne aanvalstechnieken

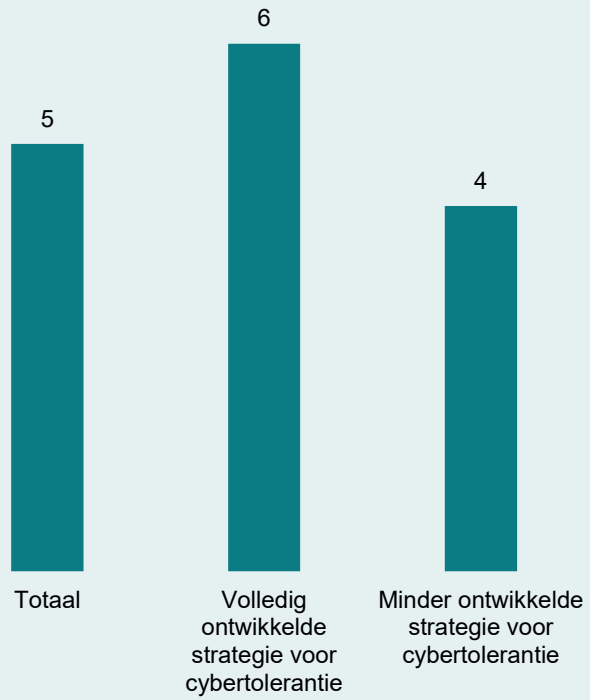
53% van bestuursleden; C-niveau

vs.

48% van middenkader

Regelmatig trainen is essentieel om het herstel te bevorderen, maar organisaties moeten voortdurend plannen maken voor veranderende bedreigingen.

Gemiddeld aantal keren per jaar dat de organisatie gesimuleerde cyberaanvallen uitvoert



55%

van degenen die **maandelijks of vaker gesimuleerde cyberaanvallen uitvoerden, is succesvol hersteld** na een oefening/cyberincident

35%

van degenen die **minder dan maandelijks gesimuleerde cyberaanvallen uitvoerden, is succesvol hersteld** na een oefening/cyberincident

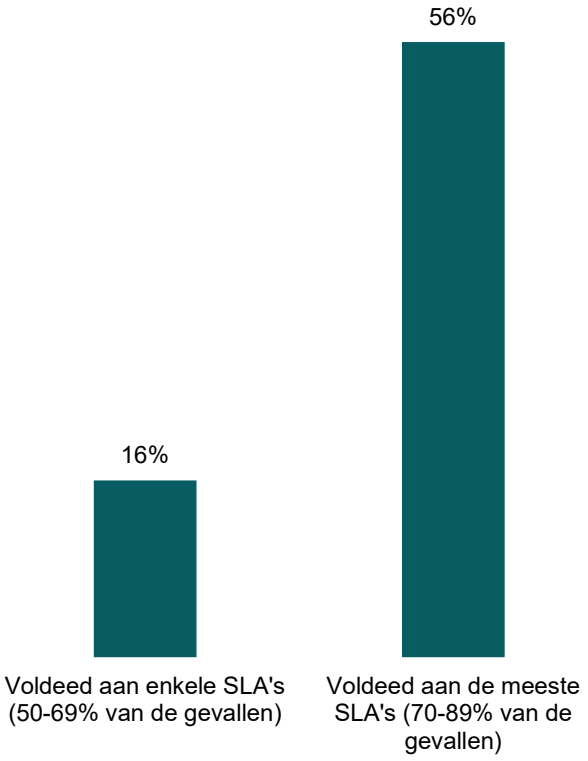
> *De noodzaak om alle potentiële bedreigingsoppervlakken integraal te testen en te evalueren in plaats van zich te concentreren op de dekking en het testen van specifieke punten.*
>
> Senior Manager, IT Technology and Telecoms, Verenigd Koninkrijk

> *Cyberaanvallen herinneren ons eraan hoe belangrijk het is om regelmatig beveiligingsoefeningen uit te voeren.*
>
> *Training in beveiligingsbewustzijn is versterkt, zodat elke werknemer potentiële bedreigingen kan identificeren.*
>
> Bestuurslid, bouw en vastgoed, Australië

DELL Technologies

SLA's zijn het bewijs: organisaties met volledig ontwikkelde strategieën komen hun herstelbeloften na

Frequentie waarmee organisaties voldoen aan SLA's voor herstel van kritieke systemen



2x

Organisaties met een volledig ontwikkelde cybertolerantiestrategie hebben meer kans om consequent aan hun SLA's te voldoen

36% vs. **18%**

Op basis van functie:

Deel 5: complexiteit, cultuur en de toekomst

Organisatorische barrières en toekomstige investeringsplannen

Complexiteit, gebrek aan vaardigheden en te veel zelfvertrouwen vormen een bedreiging voor de cybertolerantie, maar AI en training kunnen hierbij helpen

Belangrijkste uitdagingen:

Complexe IT-omgeving	49%
Budgetbeperkingen	42%
Gebrek aan deskundig personeel	39%
Fragmentatie van leveranciers en tools	38%
Lage prioriteit van leidinggevenden	23%

Grotere organisaties worden vaker geconfronteerd met dit probleem:

- 50% 5000 of meer werknemers
- 50% 3000 - 4999 werknemers
- 46% 1000 - 2999 werknemers

63%

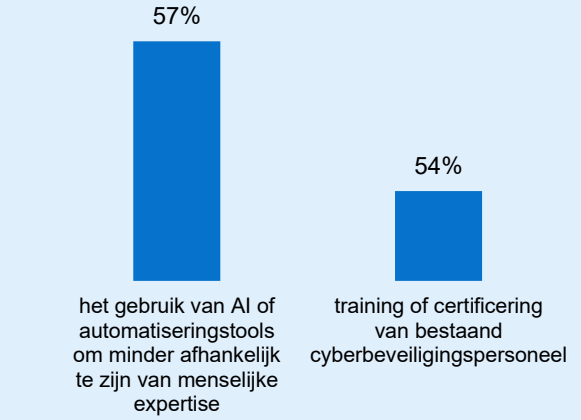
denkt dat het management de paraatheid van hun organisatie voor een groot cyberincident overschat

96%

erkent dat ze tekortkomingen hebben in hun vaardigheden of expertise op het gebied van cyberbeveiliging

MAAR...

Organisaties handelen door:



Vooruitblik op investeringen

Nr. 1

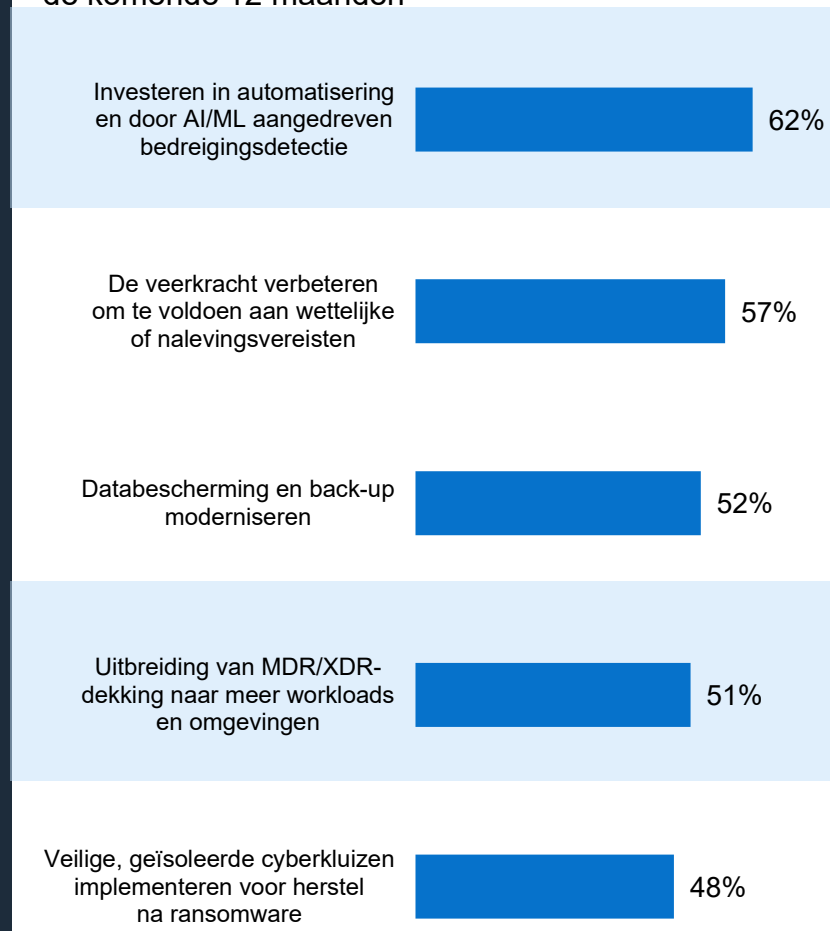
De drijvende kracht achter investeringen is het veranderende bedreigingslandschap

97%

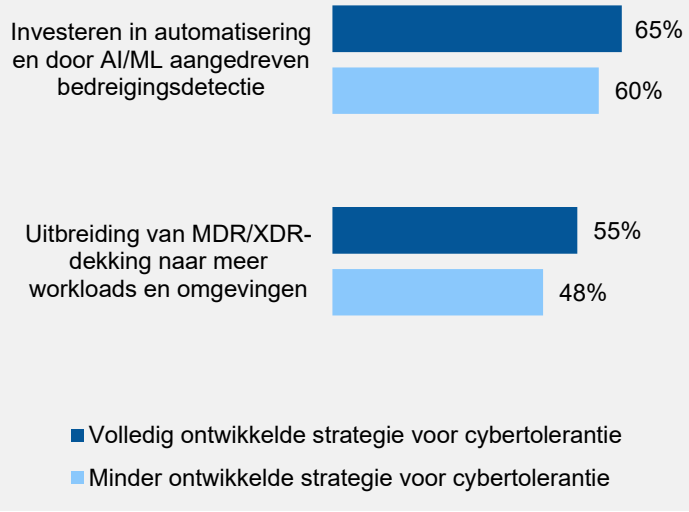
"Mijn organisatie moet voortdurend de beveiliging versterken naarmate bedreigingen zich ontwikkelen"

Om een stabiele positie te behouden, zijn voortdurende investeringen en optimalisatie de juiste weg voorwaarts

Prioritaire investeringen in cyberweerbaarheid voor de komende 12 maanden



Volwassen cybertolerante organisaties investeren voortdurend

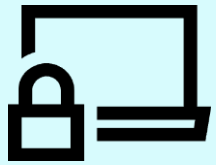


Belangrijke voordelen

Belangrijkste conclusies

39%

van de organisaties heeft een volledig uitgewerkte en voortdurend geoptimaliseerde strategie voor cybertolerantie



Continue optimalisatie is essentieel – zonder dit kunnen strategieën snel verouderd raken ten opzichte van zich ontwikkelende bedreigingen, waardoor organisaties een groter risico lopen.

46%

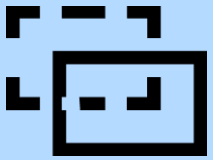
erkent dat de back-updata niet zo goed beveiligd zijn als zou moeten

Het versterken van back-upbescherming is essentieel om ervoor te zorgen dat herstel mogelijk blijft wanneer primaire systemen in gevaar komen.

Beveiligen

30%

gebruikt een uitgebreid platform voor het detecteren van bedreigingen in het netwerk, de back-up en de primaire storage



Zonder uniforme detectie kunnen de zichtbaarheid van bedreigingen en de reactietijden trager zijn, waardoor het risico op onopgemerkte inbreuken toeneemt.

Detecteren

55%

van degenen die maandelijks of vaker gesimuleerde cyberaanvallen uitvoerden, is succesvol hersteld na een oefening/cyberincident

Regelmatig testen helpt teams zich voor te bereiden op het echte werk. Regelmatig testen helpt teams zich voor te bereiden op de praktijk.

Herstellen

63%

denkt dat het management de paraatheid van hun organisatie voor een groot cyberincident overschat

Te veel zelfvertrouwen kan investeringen vertragen, de planning van reacties vertragen en kritieke kwetsbaarheden onopgelost laten.