DE STAAT VAN INNOVATIE IN SECURITY 2025

Het vertrouwensdilemma: innovatie in een risicomijdende sector

SECURITY
INNOVATION STORIES

Mogelijk gemaakt door:

BEYOND PRODUCTS

Contents

Introductie

Waarom dit onderzoek?

Bram de Bruijn

Founder Security Innovation Stories & Beyond Products

Een jaar geleden publiceerden we "Security Innovation Stories" met succesverhalen van innovatieve security bedrijven. Na elk interview hoorden we steeds: "Praat ook met deze persoon!" Dat veranderde de website van een eenvoudige webwinkel voor de verkoop van het boek in een levendig platform voor kennisdeling en inspiratie.

Het tweede doel was onszelf als marketers in cybersecurity scherp te houden - wat we aanvankelijk zagen als een win-win. Maar het is uitgegroeid tot veel meer. We geloven inmiddels dat echte vooruitgang in security vraagt om sterk leiderschap en open kennisdeling; met dit rapport en onze website hopen we daar een waardevolle bijdrage aan te leveren.

Ten derde viel ons op dat er in cybersecurity veel wordt gesproken over toenemende dreigingen en de noodzaak van innovatie, maar dat nieuwe oplossingen vaak moeizaam voet aan de grond krijgen. We besloten te onderzoeken wat innovatie precies tegenhoudt.

Om deze vraag te beantwoorden, combineerden we een survey onder 33 security professionals met diepte-interviews met meer dan 70 experts uit het veld. Dit gaf ons zowel kwantitatieve data als rijke inzichten in de uitdagingen waarmee security innovatie te maken heeft.

Al deze informatie schetst een helder beeld van de uitdagingen in de markt:

- Vanuit het perspectief van de koper (H2) zien we hoe CISO's worstelen met het evalueren en implementeren van nieuwe oplossingen.
- Het perspectief van de leverancier (H3) toont de obstakels bij het in de markt zetten van innovaties.
- De regelgevende omgeving (H4) blijkt een cruciale rol te spelen in het remmen of stimuleren van vernieuwing.
- Dit alles komt samen in een toekomstperspectief (H5) met concrete aanbevelingen voor verbetering.

Dit rapport wordt aangeboden door *Beyond Products*, het bedrijf achter *Security Innovation Stories*.

1 De innovatiekloof

Het macro-niveau: de afnemende positie van Nederland

Nederland behoort nog steeds tot de wereldtop op het gebied van cybersecurity, maar er zijn signalen dat deze positie in gevaar komt. Door de International Telecommunication Union (ITU) wordt Nederland weliswaar bestempeld als "role model" in de Global Cybersecurity Index, maar in de gezaghebbende National Cyber Power Index van het Belfer Center zakte Nederland van de 5e naar de 6e plaats tussen 2020 en 2022.

We hebben zeker reden tot trots: Nederlandse cybersecurity bedrijven zoals Fox-IT, SecurityMatters, RedSocks, Cybersprint, Northwave en Secura zijn internationaal toonaangevend. Onze wetgeving, technische capaciteiten en private sector vormen nog steeds een sterk fundament. Maar dit fundament staat onder druk.

Als we kijken naar de investeringen in de sector (zie afbeelding 1) , dan zien we dat terwijl de Verenigde Staten en Israël fors investeren in cybersecurity, Europa - en dus ook Nederland - achterblijft. Het aantal IT-patentaanvragen is weliswaar stabiel sinds 2013, maar stilstand is achteruitgang.

Zorgwekkender is het groeiende personeelstekort. Security bedrijven luiden de noodklok over de moeizame werving van gekwalificeerd personeel. Dit tekort vormt een directe bedreiging voor onze innovatiekracht en concurrentiepositie.

Investeringen in IT security bedrijven in 2023

	United States	European Union	Israel
Inwoners	334,9 miljoen	449,2 miljoen	9,7 miljoen
GDP	27,36 biljoen	17 biljoen	509,9 miljard
Early stage investment	223	59	38

Afbeeding 1. Onderzoek van Mike Privette, Return on Security.

> ***"In 2023, Europe saw 59 early-stage cybersecurity investments. This pales in comparison to the United States' 233 early-stage investments in the same period. Perhaps most telling is that Israël – a country with less than 2% of Europe's population – generated 38 early-stage cybersecurity investments, demonstrating a per-capita investment rate far exceeding that of Europe."***
>
> **- Mike Privette, Founder van Return on Security**
> Meer lezen? Lees dit artikel van Mike Privette.

De afnemende concurrentiepositie van Nederland en Europa in cybersecurity heeft verschillende structurele oorzaken. Waar de Verenigde Staten en Israël kunnen bouwen op grote geïntegreerde markten en een cultuur van risicovol investeren, worstelt Europa met versnippering en een meer behoudende aanpak. Dit belemmert niet alleen de groei van bestaande bedrijven, maar remt ook de ontwikkeling van nieuwe innovaties en startups.

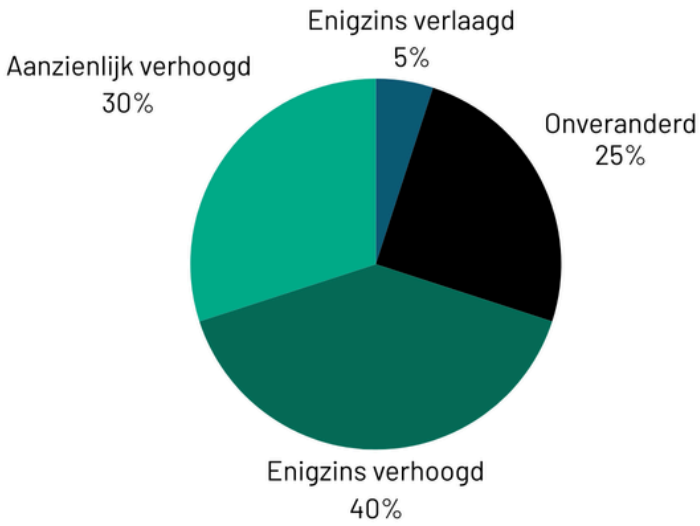
- **De versnippering van de Europese markt** zorgt ervoor dat cybersecurity bedrijven in elk land opnieuw moeten beginnen met het opbouwen van hun netwerk en klantenbestand. Deze fragmentatie maakt het lastig om snel op te schalen en verhoogt de kosten voor expansie aanzienlijk.
- **De beperkte omvang van de Nederlandse thuismarkt** maakt het moeilijker om de kritische massa te bereiken die nodig is voor snelle groei. Cybersecurity startups moeten vrijwel direct internationaal gaan om voldoende schaal te bereiken, wat extra uitdagingen met zich meebrengt.
- **De conservatieve investeringscultuur** in Europa leidt tot kleinere investeringsrondes en een focus op snellere winstgevendheid in plaats van groei. Europese investeerders zijn traditioneel meer risicomijdend dan hun Amerikaanse tegenhangers en hebben minder ervaring met het opschalen van bedrijven.

Om onze toppositie te behouden zijn stappen nodig. In het verleden behaalde resultaten bieden geen garantie voor de toekomst. Zonder gerichte investeringen in onderwijs, innovatie en het aantrekken van talent dreigt Nederland zijn vooraanstaande rol in cybersecurity te verliezen. De tijd van stilstand is voorbij – het is nu tijd voor actie.

Het micro-niveau: de huidige staat van innovatie

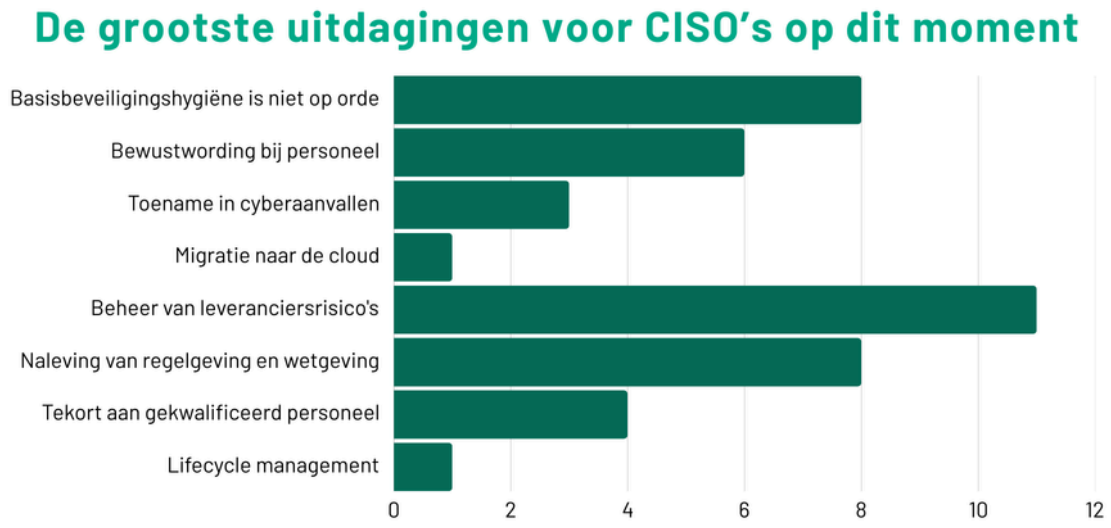
Als we inzoomen op de markt zien we een discrepantie tussen hoe security leveranciers hun eigen innovatievermogen beoordelen en hoe CISO's hier tegenaan kijken. Waar leveranciers zichzelf gemiddeld een 8,2 geven voor innovativiteit, kennen CISO's hen slechts een 6,9 toe. Deze kloof werd treffend geïllustreerd door één CISO die opmerkte dat leveranciers vaak simpelweg "AI" aan hun product toevoegen en het vervolgens als revolutionair in de markt zetten.

Ondanks deze kritische blik op innovatie, ziet de toekomst er vanuit budgettair oogpunt positief uit (zie afbeelding 2). Voor 2025 voorziet maar liefst 70% van de CISO's een budgetverhoging, waarvan 30% zelfs een aanzienlijke stijging verwacht. Een kwart geeft aan dat hun budget gelijk blijft, terwijl slechts één CISO een budgetverlaging voorspelt. Deze financiële ruimte biedt leveranciers de kans om hun innovatieve ambities waar te maken en het vertrouwen van CISO's te herwinnen.



Afbeelding 2. Resultaten uit de Security Innovation Stories Survey.

De focus van CISO's ligt echter niet waar veel leveranciers die zouden wellicht verwachten. In plaats van geavanceerde technologische innovaties zoals quantum computing, richten CISO's zich primair op praktische uitdagingen (zie afbeelding 3). Bovenaan hun prioriteitenlijst staat het beheer van leveranciersrisico's, gevolgd door compliance met wet- en regelgeving en het waarborgen van fundamentele security-maatregelen. Dit suggereert dat leveranciers hun innovatie-inspanningen mogelijk beter kunnen richten op het ondersteunen van deze dagelijkse security-uitdagingen.



Afbeelding 3. Resultaten uit de Security Innovation Stories Survey.

De kloof tussen perceptie en realiteit vraagt om betere communicatie tussen leveranciers en CISO's. Waar leveranciers hun innovatieve kracht mogelijk overschatten, kunnen CISO's wellicht meer openstaan voor nieuwe ontwikkelingen. Met toenemende budgetten in 2025 is er een unieke kans om dit wederzijds begrip te versterken. In het volgende hoofdstuk verkennen we hoe deze dialoog kan worden verbeterd, en hoe beide partijen kunnen bijdragen aan een sterkere Nederlandse cybersecurity sector.

> ***"Post-quantum bijvoorbeeld, daar denken veel mensen nog niet over na. Vaak zie je dat dat in de waan van de dag steeds wat vooruitgeschoven wordt. En daar lig ik soms weleens wakker van. Dat komt er allemaal aan en daar moeten we wel wat mee. En daar moet je als organisatie goed op voorbereid zijn."***
>
> **- Jordan van den Akker, CISO.**
>
> Meer lezen? Lees dit *interview* met Jordan.

2 Het perspectief van de koper

Uitdagingen bij het evalueren van oplossingen

De realiteit waarmee CISO's worden geconfronteerd is complex: de security markt ziet een stortvloed aan oplossingen, waarbij iedere leverancier claimt de meest innovatieve en beste te zijn. Het wordt voor CISO's steeds uitdagender om door de marketingretoriek heen te prikken en de daadwerkelijke toegevoegde waarde van deze oplossingen te bepalen.

Uit de gemiddelde frustratiecijfers (afbeelding 4) komen vijf hoofdpunten naar voren. De hoogste gemiddelde score gaat naar de agressieve verkoopbenadering waarbij leveranciers hun oplossing pushen zonder te luisteren naar specifieke behoeften. Daarna volgen praktische bezwaren: gebrekkige integratie met bestaande systemen, onduidelijke prijsstructuren en een algemeen gebrek aan transparantie. Het risico op vendor lock-in sluit de top vijf af - CISO's vrezen dat een keuze voor een specifieke oplossing hen voor jaren vastlegt op één leverancier.

Afbeelding 4. Resultaten uit de Security Innovation Stories Survey

> ***"Hoe toon je nu aan dat jij of een leverancier secure is? Dat vind ik een heel moeilijk onderwerp om mee om te gaan. Het kan bijna niet anders dan dat je mensen maar op hun blauwe ogen moet geloven. Uiteraard kan je pentesten doen, volwassenheidsmetingen doen of compliance certificeringen halen, maar deze metingen zijn vaak arbitrair of een momentopname of tonen de effectiviteit niet aan. Ik denk vaak: hoe laat je zien dat wat je doet effectief is? Dat geldt zowel voor mijn eigen rol, maar ook als leverancier-zijnde."***
>
> **- Martijn Eikelenboom, CISO.**
> Meer lezen? Lees het *interview met Martijn.*

Risicomijding vs. innovatie

Hoewel CISO's aangeven innovatie 'zeer belangrijk' of 'belangrijk' te vinden bij de selectie van leveranciers, ervaren nieuwe spelers grote moeite om voet aan de grond te krijgen.
De realiteit is dat er vaak voor gevestigde namen wordt gekozen. Dit is begrijpelijk: security draait immers om het gecontroleerd nemen van risico's, en een volledig nieuwe oplossing vertegenwoordigt inherent een risico. Het opbouwen van vertrouwen is daarom essentieel.

Het gebrek aan vertrouwen in nieuwe leveranciers wordt treffend geïllustreerd door de frustratie van een CISO: "Heel vaak wil ik weten 'kan je X' en moet ik 20 minuten luisteren naar alles behalve X." Deze uitspraak onderstreept een structureel probleem: veel leveranciers slagen er niet in om vanuit de klantbehoefte te denken en te communiceren.

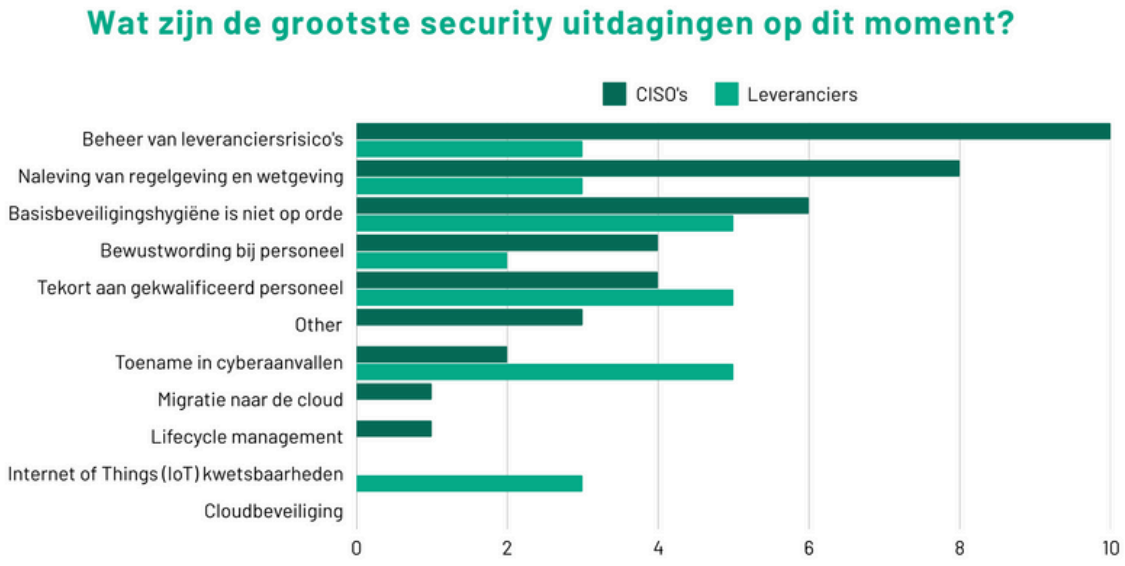
Uit onze survey blijkt dat CISO's wel degelijk actief nieuwe oplossingen evalueren, zij het in verschillende frequenties. Een kwart doet dit doorlopend, 20% evalueert elk kwartaal, en 40% heeft een jaarlijkse evaluatiecyclus. Bij deze evaluaties hanteren CISO's een praktische aanpak: 60% voert intern trials uit en 55% raadpleegt andere CISO's voor hun ervaringen.

Deze cijfers tonen aan dat het opbouwen van vertrouwen niet per se een complexe uitdaging hoeft te zijn. Leveranciers die zich richten op de daadwerkelijke behoeften van CISO's, bereid zijn hun oplossing te bewijzen via trials, en kunnen bouwen op positieve ervaringen van andere CISO's, hebben een reële kans om het vertrouwen te winnen.

> ***Je moet niet denken dat je een goed product hebt. Het moet een oplossing zijn van een vraag bij een klant. Bij bijna alle succesvolle startups zie je een sterk team zitten dat snapt waar hun kracht ligt."***
>
> **- Joris den Bruinen, directeur van Security Delta (HSD)**
>
> Meer lezen? Lees het hele *interview met Joris.*

De discrepantie tussen wat leveranciers en CISO's als prioriteiten zien, illustreert het fundamentele communicatieprobleem in de sector (zie afbeelding 5). Waar CISO's het beheer van leveranciersrisico's (10%) en compliance (8%) als grootste uitdagingen ervaren, blijken leveranciers deze zorgen significant te onderschatten (beiden 3%). In plaats daarvan focussen leveranciers zich onevenredig veel op zaken als cyberaanvallen (5%) en IoT-kwetsbaarheden (3%), die voor CISO's juist minder urgent zijn.

Deze mismatch verklaart waarom veel verkoopgesprekken vastlopen: leveranciers presenteren oplossingen voor problemen die niet bovenaan de prioriteitenlijst van hun potentiële klanten staan. Dit onderstreept het belang van een luisterende houding - wanneer leveranciers beter zouden afstemmen op de daadwerkelijke zorgen van CISO's, zou dit niet alleen de kwaliteit van de gesprekken verbeteren, maar ook hun kansen op het winnen van vertrouwen significant vergroten.



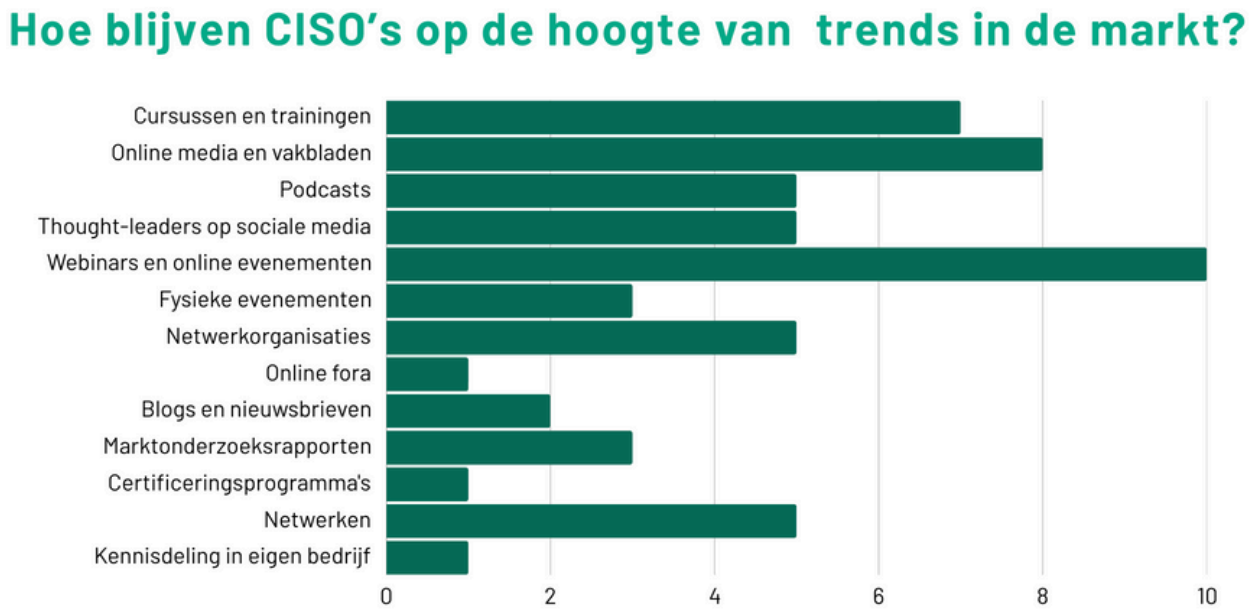
Afbeelding 5: Resultaten uit de Security Innovation Stories Survey

Innovatie-appetijt en barrières

Het is duidelijk dat de wil er is, maar wat is de weg? Een fundamenteel probleem blijkt het bij elkaar brengen van vraag en aanbod. Het opbouwen van vertrouwen vereist een andere aanpak dan de huidige verkoopgedreven benadering. Leveranciers moeten eerlijk zijn over zowel de mogelijkheden als beperkingen van hun oplossingen. Dit betekent concreet dat ze direct duidelijk moeten zijn over potentiële false positives, integratie-uitdagingen of prijsstructuren, in plaats van deze informatie te verhullen achter marketingretoriek.

> ***"Je kunt je geld maar één keer uitgeven, dus je moet op de lange termijn denken."*** *Een belangrijke boodschap voor leveranciers die soms vergeten dat hun product niet het enige is dat aandacht vraagt. Elke security-investering moet worden afgewogen tegen andere prioriteiten binnen een beperkt budget.*
>
> **- Marianne Schinkel, CISO**
> Meer lezen? Lees het hele interview met Marianne.

De sleutel tot succes ligt in het opbouwen van persoonlijke relaties via het informele CISO-netwerk. CISO's vertrouwen sterk op aanbevelingen van collega's en ervaringen die worden gedeeld tijdens netwerkevenementen. Voor leveranciers betekent dit dat ze moeten investeren in betekenisvolle aanwezigheid op deze events, het delen van inhoudelijke kennis, en het opbouwen van langetermijnrelaties - ook als dit niet direct tot verkoop leidt.



Afbeelding 6. Resultaten uit de Security Innovation Stories Survey

Deze relationele benadering moet echter wel rekening houden met de praktische uitdagingen waar CISO's mee worstelen. Met beperkte budgetten, tijd en personeel kunnen ze niet elke innovatieve oplossing uitgebreid evalueren. Leveranciers die succesvol willen zijn moeten daarom niet alleen transparant zijn over hun product, maar ook begrip tonen voor deze beperkingen en meedenken over hoe hun oplossing efficiënt kan worden geïntegreerd binnen de bestaande constraints van de organisatie.

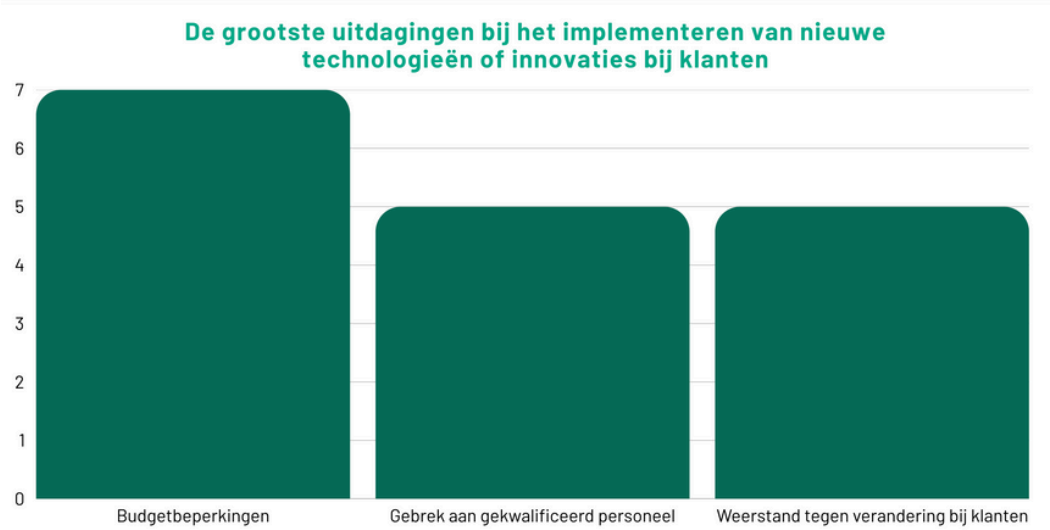
> ***"Het idee van veel regelgeving is: je moet wendbaar en weerbaar zijn en exit strategieën hebben. Maar als je daar elke keer invulling aan moet geven, dan krijg je geen tijd om het echt uit te voeren."***
>
> **- Sanne Rog, CISO**
>
> Meer lezen? Lees het hele interview met Sanne.

3 Het perspectief van de leverancier

Verkoop- en implementatie-uitdagingen

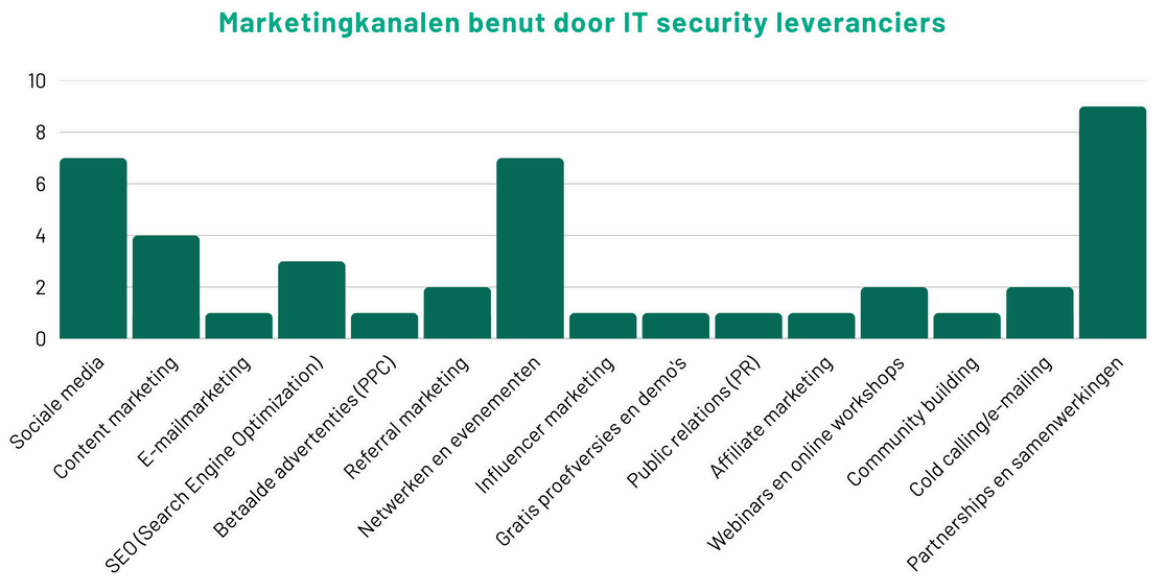
De security markt maakt een explosieve groei door, maar voor leveranciers blijft het een uitdaging om innovatieve oplossingen succesvol in de markt te zetten. Dit wordt onderstreept door het feit dat 85% van de leveranciers aangeeft dat zowel de verkoop als implementatie een grote uitdaging vormen.

De obstakels die leveranciers ervaren zijn divers maar duidelijk. Bovenaan staat het chronische gebrek aan gekwalificeerd personeel, wat zowel de verkoop als implementatie bemoeilijkt. Daarnaast stuiten ze vaak op weerstand tegen verandering binnen organisaties. Maar de meest genoemde barrière blijft toch het budget: ondanks groeiende security-budgetten blijft het voor veel organisaties moeilijk om in nieuwe oplossingen te investeren.



Afbeelding 7. Resultaten uit de Security Innovation Stories Survey

Hoe kom je als leverancier toch in gesprek met CISO's, zonder pusherig gevonden te worden? Op het gebied van marketing kiezen leveranciers overwegend voor beproefde B2B-kanalen - een strategie die zijn vruchten blijkt af te werpen. Vooral evenementen spelen een grote rol: het blijkt nog steeds de meest effectieve manier voor CISO's om zich te oriënteren op nieuwe ontwikkelingen en oplossingen. Dit persoonlijke contact, waarbij directe interactie mogelijk is en vertrouwen kan worden opgebouwd, blijft ondanks alle digitale innovaties belangrijk.



Afbeelding 8. Resultaten uit de Security Innovation Stories Survey

Begrip van klantwensen

De technische competentie van sales professionals blijkt een genuanceerd vraagstuk. Een CISO verzuchtte tijdens een interview: "Hij komt even vertellen hoe het moet" - doelend op sales professionals zonder technische achtergrond. Hoewel 'niet kundig genoeg' vaak als grote frustratie wordt genoemd, laat het gemiddelde frustratieniveau zien dat andere aspecten, zoals luisteren naar de klant en begrip van de context, als belangrijker worden ervaren. Technische kennis is relevant, maar uiteindelijk gaat het meer om het vermogen om de brug te slaan tussen technische mogelijkheden en de behoeften van de CISO.

> ***"Onze grootste uitdaging is het opvallen tussen de concurrentie en de mogelijkheid krijgen om uit te leggen waar we beter in zijn."***
>
> *– Respons van leverancier uit de survey*

Afbeelding 9. Resultaten uit de Security Innovation Stories Survey.

Het kernprobleem zit in de verschillende snelheden waarmee leveranciers en CISO's opereren. Waar leveranciers vaak streven naar snelle implementatie, onderschatten ze de complexiteit van change management binnen organisaties. Deze spanning tussen ambitie en praktische realiteit zorgt voor wederzijdse frustratie.

Een terugkerend probleem is de terughoudendheid van leveranciers met productinformatie. De veelgehoorde zorg over concurrentiegevoelige informatie staat haaks op de behoefte aan transparantie die CISO's uitspreken. Deze defensieve houding belemmert het opbouwen van wederzijds vertrouwen en effectieve samenwerking.

Afbeelding 10. Resultaten uit de Security Innovation Stories Survey

Wat kunnen leveranciers hiervan leren? Ken de business voordat je een oplossing aanbiedt, denk in langetermijnrelaties, blijf klantgericht, en focus op de risk tolerantie van bedrijven. CISO's vragen om bruikbare innovatie in plaats van marketingtermen, met specifieke kritiek op het ongefundeerd gebruik van AI-labels voor bestaande producten.

> ***"Luister naar de klant en beoordeel dan of producten werkelijk aansluiten binnen context waar de klant zich in beweegt"***
>
> – Respons van CISO uit de survey

De marktbenadering van leveranciers vraagt om een fundamentele heroriëntatie. Niet meer marketing of intensievere sales zijn de oplossing, maar een beter begrip van de CISO-realiteit. Deze reset in denken en handelen is essentieel voor het overbruggen van de huidige kloof tussen aanbieder en afnemer.

4 De regelgevende omgeving

Uitdagingen bij aanbestedingen

In de publieke sector botsen innovatieambities vaak hard met de realiteit van strikte regelgeving. Leveranciers noemen aanbestedingsregels vaak als belangrijk obstakel bij het werken met overheidsorganisaties.

Voor overheids-CISO's is deze situatie dagelijkse praktijk. Naleving van regelgeving en wetgeving staat hoog op hun prioriteitenlijst, wat voortdurend wringt met de wens om te innoveren.

> ***"Overheidsinstellingen zitten vast in logge processen die ze verhinderen echt te innoveren. Alles wordt geblokkeerd door aanbestedingen en juridische hindernissen. Het gevolg? Aanbestedingen worden een doel in plaats van een middel. Ze gaan doorgaans voor de grote, bekende namen, omdat dat makkelijker lijkt. Maar dat betekent niet dat ze de beste oplossing hebben."***
>
> **- Gemma Jansen, CISO**
>
> Meer lezen? Lees het hele interview met Gemma.

Compliance en innovatie

De uitdaging reikt verder dan alleen de publieke sector. Uit onze CISO survey blijkt dat veel organisaties worstelen met een dubbele opgave: het op orde krijgen van de security basis, terwijl er tegelijkertijd nieuwe regelgeving blijft komen die extra eisen stelt. Deze stapeling van verplichtingen zet de beschikbare capaciteit voor innovatie onder druk.

> ***"Het certificeringstraject heeft natuurlijk wel waarde, omdat je het certificaat met klanten kunt delen, het geeft de klanten vertrouwen en dat maakt het salesproces makkelijker. Maar helaas biedt een certificaat nog geen garantie dat security echt goed op orde is."***
>
> **- Ben Krutzen, Director IT and Security Advisory**
>
> Meer lezen? Lees het hele interview met Ben.

Deze complexe wisselwerking tussen compliance en innovatie vraagt om een nieuwe aanpak. Waar certificering en regelgeving belangrijk zijn voor het creëren van vertrouwen, moet dit niet ten koste gaan van de ruimte voor echte security verbeteringen. De kunst is om beide doelen te verenigen, zonder dat het een het ander verdringt.

5 Toekomstperspectief

Het overbruggen van de kloof

Zowel CISO's als leveranciers zien de urgentie van innovatie en komen met concrete suggesties voor verbetering. Het moment voor verandering is nu.

Uit het onderzoek blijkt dat succesvolle samenwerkingen een aantal overeenkomsten hebben. Het begint vaak klein, met gerichte tests en proof-of-concepts waarbij leverancier en klant samen optrekken. De focus ligt op concrete use cases en heldere, transparante communicatie over mogelijkheden én beperkingen.

> ***"Kijk verder dan zogenaamde 'proven technology' in het magic quadrant van Gartner. Het 'proven' deel gaat alleen maar over het verleden - en biedt zeker geen garantie naar vandaag en al helemaal niet naar de toekomst. Denk holistisch en niet in punt oplossingen."***
>
> – Respons van CISO uit de survey

Investeringen in innovatie

Het Nederlandse cybersecurity landschap heeft dringend behoefte aan gerichte investeringen. Waar andere landen miljarden pompen in innovatieve security-oplossingen, blijft Nederland achter. Dit is niet alleen een kwestie van middelen, maar ook van mindset: we moeten af van de risicomijdende benadering die innovatie in de weg staat.

De huidige financieringsstructuren sluiten onvoldoende aan bij de behoeften van innovatieve security-bedrijven. Startups worstelen met lange aanbestedingstrajecten en stroperige besluitvorming, terwijl ze juist behoefte hebben aan snelle, flexibele financiering om hun oplossingen door te ontwikkelen. Dit creëert een mismatch tussen innovatief potentieel en beschikbaar kapitaal.

> ***"Het innovatieklimaat in Nederland is niet altijd even best. Het is moeilijk om investeringen aan te trekken voor technologische projecten. Er zijn enkele voorbeelden van succesvolle startups, maar het merendeel heeft moeite om financiering te verkrijgen. En dat is zonde, want zoals ik eerder aangaf zijn high-tech oplossingen juist zó hard nodig om cybercrime tegen te gaan."***
>
> **- Eward Driehuis, CISO**
>
> Meer lezen? Lees het hele interview met Eward.

De oplossing ligt in een nieuwe benadering van security-investeringen. Dit vraagt om een combinatie van publieke en private middelen, gekoppeld aan snellere beoordelingsprocedures. Succesvolle voorbeelden uit het buitenland laten zien dat gerichte investeringsprogramma's, waarbij overheid en private sector samenwerken, kunnen leiden tot een bloeiend security-innovatie ecosysteem.

6 Samenvatting

- **De Nederlandse security sector worstelt met innovatie-adoptie, niet met een gebrek aan ideeën.** Ons onderzoek onder meer dan dertig security professionals laat zien dat er een kloof bestaat tussen het ontwikkelen en het implementeren van vernieuwende oplossingen. Deze kloof manifesteert zich op verschillende niveaus (H1).
- **Op macro-niveau verliest Europa terrein in de wereldwijde security-wedloop (H1).** De cijfers zijn onverbiddelijk: Europa investeert 2,5 keer minder in cybersecurity dan de VS en zelfs 6 keer minder in AI. Het contrast met Israël is nog scherper: met minder dan 2% van Europa's bevolking genereerde het 38 vroege-fase security investeringen in 2023, tegen 59 in heel Europa. Deze achterstand komt op een gevaarlijk moment, nu cyberaanvallen complexer worden en geopolitieke spanningen toenemen.
- **Op micro-niveau zien we een fundamentele mismatch tussen vraag en aanbod (H2, H3).** Waar leveranciers hun innovatievermogen beoordelen met een 8,2, geven CISO's hen slechts een 6,9. Deze kloof weerspiegelt een dieper probleem: leveranciers en CISO's spreken verschillende talen. CISO's worstelen met het evalueren van oplossingen en krijgen te maken met agressieve verkoopbenaderingen die niet aansluiten bij hun behoeften. Voor leveranciers is de uitdaging niet minder groot: 85% geeft aan dat zowel verkoop als implementatie een significante hindernis vormt (H3).
- **De grootste barrière voor innovatie blijkt systemisch van aard (H4).** Een risicomijdende cultuur, verstikkende compliance-eisen en rigide aanbestedingsregels creëren samen een klimaat waarin vernieuwing moeilijk gedijt. Dit wordt versterkt door een gebrek aan flexibele financieringsstructuren voor startups en beperkte experimenteerruimte voor security teams. Het resultaat is een sector die wel wíl innoveren, maar vastloopt in processen die vernieuwing paradoxaal genoeg blokkeren. De oplossingen voor deze uitdagingen vragen om een gezamenlijke aanpak van alle betrokkenen (H5).

7 Aanbevelingen

Het versterken van security innovatie in Nederland vraagt om een gezamenlijke inspanning. Geen enkele partij kan dit alleen - het vereist een samenspel tussen kopers, leveranciers en beleidsmakers. Onze aanbevelingen richten zich daarom op alle stakeholders in het security landschap.

Voor CISO's

- **Maak tijd voor innovatie.** Innovaties komen niet uit de lucht vallen. Het vereist een bewuste keuze om tijd vrij te maken voor het verkennen en evalueren van nieuwe oplossingen. Door dit structureel in te plannen, voorkom je dat innovatie het onderspit delft in de waan van de dag.
- **Begin klein, denk groot.** Start met gerichte pilots in een gecontroleerde omgeving waar falen mogelijk is. Deze gecontroleerde experimenten vormen de basis voor bredere implementatie bij succes.
- **Wees duidelijk over wat de markt nodig heeft.** CISO's hebben waardevolle inzichten in wat wel en niet werkt, maar zijn vaak te bescheiden in het delen hiervan. Leveranciers hebben deze directe feedback nodig om hun oplossingen te verbeteren. Deel daarom actief je ervaringen - zowel positief als negatief - en wees concreet in wat je zoekt in nieuwe oplossingen. Deze openheid helpt de hele sector vooruit.
- **Zoek de balans tussen compliance en innovatie.** Compliance is belangrijk maar mag niet verlammend werken. Onderzoek actief de ruimte binnen regelgeving voor experimenten en vernieuwing.

Voor security leveranciers

- **Luister écht naar de CISO.** Security-expertise betekent niet automatisch dat je de markt door-en-door kent. Te vaak starten verkoopgesprekken met een uitgebreide productpresentatie, terwijl de werkelijke behoefte nog niet eens bekend is. Begin in plaats daarvan met vragen stellen. Laat het slide deck achterwege en focus op het begrijpen van de specifieke uitdagingen waar deze CISO voor staat. Alleen door écht te luisteren kun je bepalen of en hoe jouw oplossing van waarde kan zijn.
- **Wees realistisch over implementatie.** De belofte van 'plug-and-play' is verleidelijk, maar zelden waar. Wees daarom transparant over wat er nodig is voor succesvolle adoptie. Schets een eerlijk beeld van integratie-uitdagingen, benodigde resources en potentiële obstakels. Door vooraf duidelijk te zijn over wat wel en niet kan, voorkom je teleurstellingen en bouw je aan duurzame klantrelaties.

- **Accepteer dat groei tijd kost.** In de security industrie bestaat geen snelle route naar succes. Elke oplossing moet grondig getest en bewezen worden - dat is geen bug maar een feature. Wees daarom realistisch in je doelstellingen en eerlijk naar investeerders. Bouw vertrouwen door transparant te zijn over zowel de mogelijkheden als beperkingen van je oplossing. Het is deze eerlijkheid die leidt tot duurzame partnerships.
- **Spreek de taal van je doelgroep.** CISO's zijn allergisch voor marketinghype en buzzwords. Ze willen concrete voorbeelden zien van hoe jouw oplossing echte problemen oplost. Deel praktijkcases van vergelijkbare organisaties, bied trials aan, en werk samen met gerespecteerde thought leaders in de industrie. Authentieke verhalen en bewijsbare resultaten overtuigen meer dan glanzende marketingpresentaties.

Voor beleidsmakers

- **Versterk bestaande innovatiefondsen.** De huidige financieringsregelingen voor security innovatie schieten tekort in vergelijking met andere landen. Waar de VS en Israël miljarden investeren, blijven Nederlandse fondsen beperkt in omvang en impact. Schaal bestaande programma's op en maak ze toegankelijker voor security bedrijven. Zonder substantiële verhoging van deze investeringen verliest Nederland verder terrein in de wereldwijde security-wedloop.
- **Moderniseer het inkoopproces.** Ontwikkel speciale procedures voor innovatieve security-oplossingen die snelle evaluatie en implementatie mogelijk maken. De huidige aanbestedingsregels zijn niet geschikt voor het innovatietempo dat we nodig hebben.
- **Creëer veilige experimenteerruimte.** Ontwikkel 'regulatory sandboxes' waar organisaties kunnen innoveren zonder direct alle compliance-eisen te hoeven meetellen. Dit stimuleert vernieuwing zonder onverantwoorde risico's.
- **Stimuleer publiek-private samenwerking.** Breng kopers en innovators samen in gerichte programma's. De overheid moet een actieve rol spelen in het verbinden van partijen en het delen van kennis en expertise.

Nederland heeft alle ingrediënten om een leidende rol te spelen in security innovatie - maar dan moeten we wel nu handelen. Door gerichte samenwerking tussen alle partijen kunnen we een ecosysteem bouwen waarin security innovatie floreert.

Methodologie van dit rapport

Voor dit onderzoek hebben we beide kanten van de security markt in kaart gebracht: de eindgebruikers (CISO's) én leveranciers. We voerden meer dan 70 diepte-interviews in het afgelopen jaar, en combineerden dit met een survey onder 40 security professionals.

Deze gesprekken leverden niet alleen artikelen op, maar gaven ook waardevolle inzichten in de dynamiek tussen kopers en verkopers in de security markt. Door deze combinatie van kwalitatieve en kwantitatieve data ontstaat een rijk beeld van de uitdagingen in security innovatie.

CISO survey

- Aantal respondenten: 20
- Functies: CISO's, Security Managers en security executives
- Organisatiegrootte: Voornamelijk 201-500 medewerkers (60%)
- Sectoren:
- Overheid/Gemeente (40%)
- Consultancy (25%)
- Security bedrijven (10%)
- Overig (25%)

Innovator survey

- Aantal respondenten: 20
- Type: Cybersecurity leveranciers en startups
- Bedrijfsgrootte: Mix van klein (1-50 medewerkers, 50%) tot groot (>200 medewerkers, 50%)
- Ervaring: Mix van scale-ups (4-6 jaar, 33%) en gevestigde spelers (>10 jaar, 67%)

Analysemethode

- Kwantitatieve analyse van gesloten vragen over innovatie-uitdagingen, budgetten en tevredenheid
- Kwalitatieve analyse van open antwoorden voor diepere inzichten

Beperkingen

- Beperkte steekproefgrootte (n=40 totaal)
- Focus op Nederlandse markt

Wil jij bijdragen aan het rapport van volgend jaar? Dat kan! Ga naar de survey.

Liever je mening delen in een persoonlijk interview? Neem contact met ons op met Marloes.

SECURITY

INNOVATION STORIES

HÉT PLATFORM VOOR PIONEER CISO'S, CIO'S EN INNOVATORS