Solvinity
Secure Managed IT Services

# PUBLIC CLOUD SECURITY

## Strategische keuzes voor **een veilige IT-omgeving**

## Inhoud



# Introductie

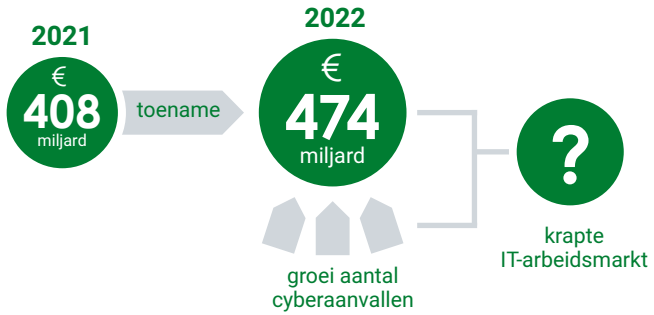
In het 2e kwartaal van 2022 nam het gemiddelde aantal wekelijkse cyberaanvallen in Nederland toe met 40%, vergeleken met hetzelfde kwartaal vorig jaar.

Of je nu CEO, CISO of CTO bent, de vraag is hetzelfde: hoe maak je optimaal gebruik van de zakelijke voordelen van de cloud? Steeds vaker worden bedrijfsprocessen en dienstverlening op de cloud gebaseerd. En met reden: overstappen naar public cloud kan tal van voordelen opleveren, zoals meer flexibiliteit, grotere efficiëntie, betere prestaties, een groter potentieel voor innovatie en door-ontwikkeling én minder beheer. De omzet uit cloud-activiteiten groeit dan ook flink. Zo schat Gartner dat de wereldwijde inkomsten uit cloud in 2022 474 miljard dollar zullen bedragen, tegenover 408 miljard dollar in 2021. Bovendien verwachten de Gartner-analisten dat de inkomsten uit cloud-activiteiten de komende jaren de niet-cloudomzet zullen overtreffen in IT-markten.

Tegelijkertijd kennen organisaties forse uitdagingen. Zo neemt het dreigingsniveau toe. Het aantal cyberaanvallen groeit al jaren. In het 2e kwartaal van 2022 nam het gemiddelde aantal wekelijkse cyberaanvallen in Nederland toe met 40%, vergeleken met hetzelfde kwartaal vorig jaar. Daarnaast nam, volgens diezelfde bron, het aantal ransomware-aanvallen toe met 59% ten opzichte van vorig jaar. En de aanvallen worden steeds geavanceerder. De tijd van de eenzame hacker is voorbij - je neemt het voortaan op tegen goed gefinancierde kartels.

Dit wordt belemmerd door een gebrek aan kennis. Er is flinke krapte op de IT-arbeidsmarkt, waardoor we logischerwijs concluderen dat het aantal securityspecialisten dat opgewassen is tegen moderne cyberdreigingen niet toereikend is om iedere organisatie van in-house kennis te voorzien. De noodzaak van een gedegen securitystrategie wordt dan ook alsmaar duidelijker - een strategie die verder gaat dan alleen IT en die doorlopend moet worden bijgestuurd naarmate marktomstandigheden veranderen.

Binnen dit spanningsveld moet je je weg naar de cloud vinden. Hoe integreer je security, ondanks deze uitdagingen, gedegen in je digitale transformatie richting public cloud? Dit whitepaper behandelt de belangrijkste aandachtspunten en valkuilen voor een veilig ingerichte public cloud-omgeving.



# **Public cloud:** een andere mentaliteit

Als je voor het eerst de public cloud betreedt, kom je in een nieuwe wereld terecht. De traditionele IT-omgeving is naar binnen gericht, afgeschermd van de buitenwereld en ontworpen voor interne toegang. In tegenstelling tot private omgevingen zijn public cloud endpoints erop gericht om vanuit de buitenwereld te worden benaderd.

Een public cloud-omgeving wordt anders opgebouwd. Private omgevingen vereisen voorwerk wanneer bijvoorbeeld de infrastructuur moet worden aangeschaft of opgeschaald, terwijl je in public cloud iets aan of uit kan zetten met een aantal regels code. Die flexibiliteit is een van de grote voordelen van public cloud. Maar mét die flexibiliteit komt meer complexiteit door de vele beschikbare functionaliteiten. Een fout in de instellingen is gauw gemaakt, waardoor een omgeving per abuis voor de buitenwereld wordt geopend, of features worden geactiveerd met hoge kosten als gevolg.

Om op een veilige manier de flexibiliteit van public cloud te benutten, is het de kunst om kaders, ook wel guardrails genoemd, te definiëren waarbinnen je wendbaar blijft. Dat is een grote mentaliteitsverschuiving als je vanuit een traditionele private cloud-omgeving komt. Het is een verschuiving die veel verder gaat dan technologie en alle aspecten van de organisatie raakt, van strategische besluitvorming en HR tot IT-beheer.

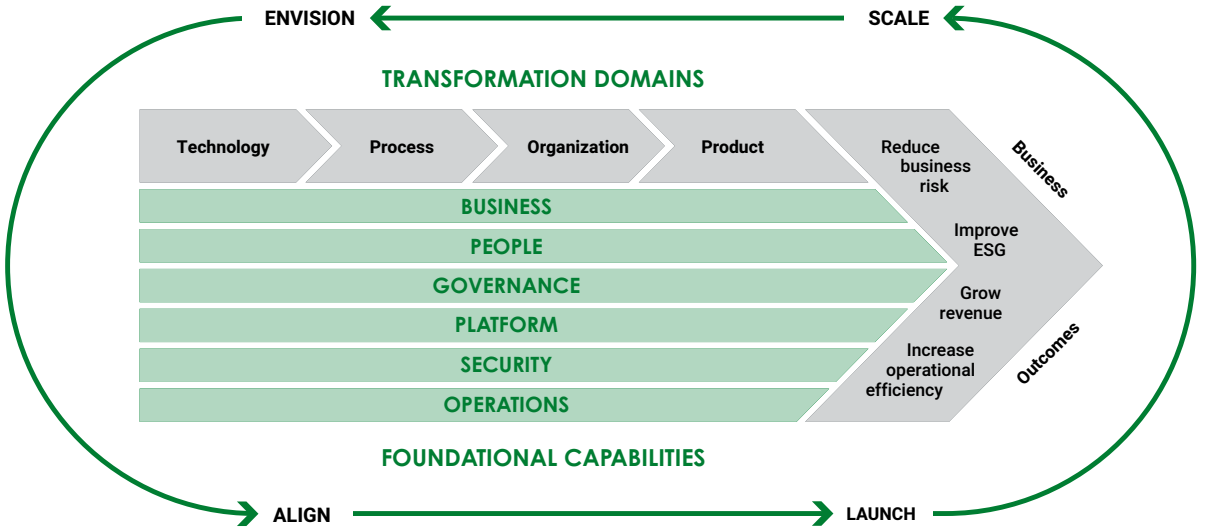
Om op een veilige manier de flexibiliteit van public cloud te benutten, is het de kunst om kaders, ook wel guardrails genoemd, te definiëren waarbinnen je wendbaar blijft.

## **Security voorop** met een Cloud Adoption Framework

Om je in deze verschuiving te helpen, ontwikkelden de grootste cloud-providers van dit moment (Amazon, Google en Microsoft) een Cloud Adoption Framework (CAF), zoals deze van Amazon.
Het CAF is een model waarbinnen alle onderwerpen aan bod komen die onderdeel kunnen zijn van een transformatie naar public cloud. Deze bevatten veel bruikbare adviezen en richtlijnen om de strategieën van een organisatie te helpen veranderen.

Security vormt een kritieke stroom binnen dit raamwerk, die verschillende lagen van de organisatie raakt. Hoe geef je security een plek? Waar moet je op letten? Kortom: wat komt er kijken bij en succesvolle en veilige transformatie richting public cloud?
In de volgende hoofdstukken gaan we laag voor laag in op de belangrijkste aandachtspunten om deze vragen te beantwoorden.

Security vormt een kritieke stroom binnen dit raamwerk, die verschillende lagen van de organisatie raakt.





# Fundamentele keuzes

Hoewel public cloud veel flexibiliteit biedt, moet je een aantal grote beslissingen van tevoren weldoordacht nemen; om veiligheidsredenen, en omdat correctie achteraf hoge kosten met zich meebrengt. In dit beginstadium heeft het bijvoorbeeld geen zin om over gedetailleerde firewall-regels te discussiëren, omdat je dit in public cloud juist wél gemakkelijk later kunt aanpassen.

## Redeneer vanuit de business

Besluitvorming begint wat ons betreft altijd vanuit zakelijke doelstellingen, niet vanuit technologie. Vanuit die doelen wordt de IT-omgeving vormgegeven. Dat geldt ook voor de security-eisen. Wat zijn de veiligheidseisen waaraan het bedrijf moet voldoen? Voor banken en verzekeraars, die aan strikte compliance-richtlijnen moeten voldoen, gelden andere regels dan voor bijvoorbeeld productiebedrijven. Helder krijgen wat je wilt bereiken met de public cloud moet dus altijd de eerste stap zijn.

"Beginnen bij de business" betekent dat er meer gevraagd wordt van het kennisniveau van business managers. De keuzes die zij maken hebben invloed op het IT-vlak, maar ze beschikken daarbij niet altijd over voldoende kennis om de gevolgen van die keuzes te overzien. Vooral in complexe omgevingen, waarin datastromen via verschillende interne en externe netwerken lopen om bepaalde applicaties van data te voorzien, hebben IT-keuzes al snel consequenties voor de werkwijze en weerbaarheid van de gehele organisatie. Blijvend investeren in dit kennisniveau is daarom essentieel.

"Beginnen bij de business" betekent dat er meer gevraagd wordt van het kennisniveau van business managers.

Het afsluiten van bepaalde regio's bij een cloudprovider is een maatregel voor kostenbeheer én tegelijkertijd een security-oplossing.

## Een stabiele basis

Een aantal zaken is lastig en kostbaar om te veranderen in een later stadium van je cloudmigratie. Dit kan afhankelijk van je organisatie op diverse manieren gebeuren, maar een tweetal daarvan willen we graag voor je uitlichten, omdat hier in de praktijk nog regelmatig aan voorbij wordt gegaan.

### Actieve geografische regio's

Public cloud-omgevingen kun je overal ter wereld opzetten. Dat doe je bijvoorbeeld om dichter bij je klanten te zitten en latency te verminderen. Of je implementeert een omgeving in een bepaalde regio vanwege hoge lokale compliance-eisen. Daarbij is het net zo belangrijk om te bepalen welke regio's je wel of niet gebruikt. Het afsluiten van bepaalde regio's bij een cloudprovider is een maatregel voor kostenbeheer én tegelijkertijd een security-oplossing. In afgesloten regio's kan niets gebeuren - en gebeurt er wél iets, dan is het meteen een signaal dat er iets niet klopt.

### Organisatiestructuur van de Cloud

We raden het af om slechts één cloud-account aan te maken voor de gehele omgeving. Daarmee leg je in feite al je eieren in één mandje - en als het binnen dat account fout gaat, ben je in een klap alles kwijt. Het is dus verstandig om na te denken over je structuur. Deze kan verschillende vormen aannemen, naargelang je specifieke behoeften: per afdeling, per applicatie en zelfs per businessmodel. Een projectorganisatie behoeft een andere accountstructuur dan een technologieleverancier.

Deze zaken zijn onder meer te regelen in de op maat gemaakte **Cloud Landing Zones** van Solvinity, die alle beschikbare diensten en talloze functies en mogelijkheden terugdringen tot één beheersbaar geheel.

## Aandachtspunten

- Zorg dat je de zakelijke en strategische doelstellingen die je met public cloud wilt bereiken helder hebt.
- Breng in kaart over welke kennis je organisatie intern beschikt en bekijk vervolgens of je een externe partner moet aanhaken voor advies, opleiding of outsourcing.
- Krijg helder of je leidinggevenden over de juiste kennis beschikken om onder andere security- en compliance-beslissingen te maken voor de nieuwe public cloud-omgeving.
- Evalueer in welke regio's de organisatie actief is en wat de ambities zijn rond internationale expansie.
- Deel op basis van de bedrijfsvoering en zakelijke doelstellingen de gewenste cloud-activiteiten in en leg op basis daarvan de accountstructuur vast.



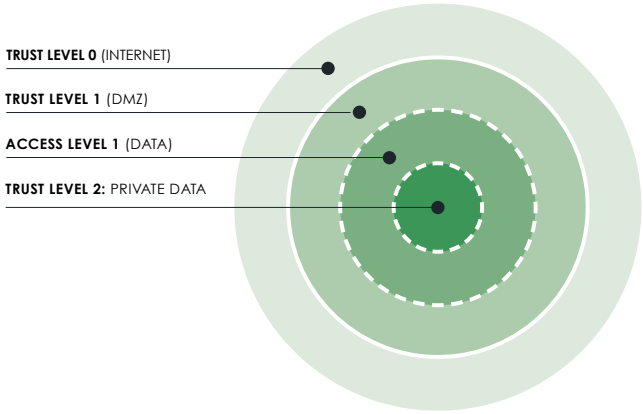
# Afkadering in netwerken

Nadat fundamentele keuzes zijn vastgelegd, kun je bovenop die fundering je netwerk bouwen. Solvinity adviseert gebruik te maken van Zero Trust-principes. Dit betekent dat niemand van binnen of buiten het netwerk standaard wordt vertrouwd en dat altijd verificatie is vereist van iedereen die toegang probeert te krijgen tot netwerkonderdelen

## Cruciale hulpmiddelen voor netwerksecurity

**"Security by Design"**-principes zijn belangrijk voor de inrichting. Dat betekent bij Solvinity dat alle processen, applicaties en systemen in beheer vanaf de ontwerpfase continu worden gecontroleerd op mogelijke zwakheden. Denk aan segmentatie en hardening.
Bij **segmentatie** scheid je netwerken van elkaar. Welke delen hebben werkelijk koppelingen nodig en waar kan het zonder? Door verschillende onderdelen van de infrastructuur zo veel mogelijk te scheiden, hebben indringers die door de eerste verdediging breken niet direct toegang tot het hele netwerk. Richt netwerken niet in als zijnde 'vertrouwd', maar als 'niet vertrouwd tenzij'.

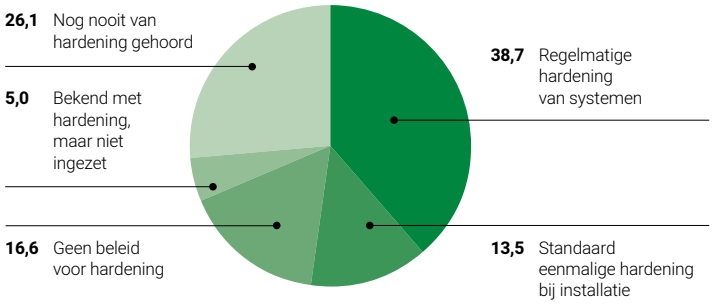
> Richt netwerken niet in als zijnde 'vertrouwd', maar als 'niet vertrouwd tenzij'.




Pas segmentering zeker toe op je dataopslag met behulp van **Identity & Access Management**: zorg je voor een toegangspolicy tot de data voor iedereen, of zet je gevoelige data (denk aan juridische stukken of intellectueel eigendom) in een streng afgescheiden segment waar niet zomaar iedere gebruiker bij kan? Pas je op elk bestand of map geautomatiseerde toegangsrechten toe? Door de antwoorden op deze vragen vooraf te formuleren, beperk je de impact van onverhoopte datalekken.

In public cloud zijn de implementaties niet het meeste werk, maar het vaststellen van beleid en het maken van keuzes daarachter.

**Hardening** is een proces waarbij alle mogelijke instellingen binnen een IT-omgeving worden gecontroleerd om de juiste balans tussen functionaliteit en veiligheid te behouden. En die balans luistert nauw: een verkeerde keuze in één netwerksegment kan ongemerkt elders gevolgen hebben. Vaak gebeurt dit eenmalig bij de opbouw van de infrastructuur. Of helemaal niet: volgens ons eigen onderzoek is 40% van IT-verantwoordelijken niet bekend met het concept. Een ernstige constatering, want wij zien hardening als een cruciaal en doorlopend proces. Iedere wijziging kan immers de gehele infrastructuur beïnvloeden. Bij elke upgrade en wijziging bekijken we daarom de mogelijke impact op de infrastructuur om de weerbaarheid te borgen. We spreken dan ook van **continuous hardening**.




## Haastige spoed is zelden goed

In public cloud zijn de implementaties niet het meeste werk, maar het vaststellen van beleid en het maken van keuzes daarachter. Dit is een voorbeeld van de benodigde mentaliteitsverandering. Neem niet snel een beslissing omdat je verwacht dat het implementatieproces lang duurt - in public cloud is dat niet zo. Richt je eerst op de beleidskeuzes en laat je op voorhand goed informeren. Kader de omgeving goed af, maar zorg wel voor flexibiliteit om te experimenteren - zelfs met nieuwe security-features. Cloud-features zijn eenvoudig te activeren, en wanneer ze niet blijken te passen bij je organisatie zijn ze even gemakkelijk weer uit te schakelen.

## Aandachtspunten

- Creëer volledig zicht op de toegang tot applicaties en omgevingen voor zowel interne als externe doelgroepen en beveilig deze volgens bewezen principes als Security-by-Design.
- Specificeer onder welke voorwaarden toegang tot applicaties of gegevens mag worden verkregen en ga daarbij zoveel mogelijk uit van ‘Zero Trust’.
- Identificeer je ‘kroonjuwelen’ en kijk voor die kritieke onderdelen extra kritisch naar toegangsrechten en -redenen en het beleid voor (tijdelijke) toegang. Denk daarbij ook aan service accounts.
- Breng in kaart welke kaders je wilt toepassen om je transformatie maximale slagkracht te bieden zonder zomaar iedereen volledige bewegingsvrijheid te geven.

LAAG 3

# Veiligheid op applicatieniveau

Met een goed ingerichte netwerkinfrastructuur en Cloud Landing Zones beschik je over een solide fundering om daadwerkelijke applicaties en diensten op te bouwen. Dit is waar de concepten ('Stretched') DevSecOps, shift-left security en Agile Security ten tonele verschijnen en een belangrijke rol spelen om public cloud-omgevingen veilig te houden.

## Shift-left security

DevOps is een stroming binnen applicatieontwikkeling die een brug slaat tussen softwareontwikkeling en IT-beheer, zodat je veel sneller updates van producten kunt uitrollen, die vervolgens beter beheersbaar zijn. Maar security is niet altijd een prioriteit als snelheid van updates wordt nagestreefd. Daarom is een beweging opgekomen genaamd **DevSecOps** met als doel security gedurende alle fasen, van concept tot beheer, als vast onderdeel in het ontwikkelproces op te nemen. In dit model zorgen ontwikkelaars dat het systeem werkt zoals het hoort, beheerders verzorgen betrouwbaarheid en onderhoud van het systeem en security toetst het product aan veiligheidsstandaarden. Het gevolg is **shift-left security**, waarin applicatiebeveiliging al aan het begin (de 'linkerkant' van een timeline) onderdeel van het ontwikkelproces wordt.

## Stretched DevSecOps

Solvinity heeft mede op basis van deze principes een samenwerkingsmodel ontwikkeld dat outsourcing combineert met snelle software releases. **Stretched DevSecOps** heeft als doel voorspelbaar, veilig en vlot nieuwe functionaliteit op te leveren, óók wanneer IT-beheer is uitbesteed.

Stretched DevSecOps heeft als doel voorspelbaar, veilig en vlot nieuwe functionaliteit op te leveren, óók wanneer IT-beheer is uitbesteed.

Agile security brengt veiligheidstests in lijn met de ontwikkelsnelheid door pentests uit te smeren over het hele jaar.

Dit stelt teams in staat veel vroeger in het proces te bepalen of nieuwe releases kwetsbaarheden in het leven roepen en of de betrouwbaarheid van de dienstverlening in het geding komt. Het “Stretched”-gedeelte houdt in dat de experts van Solvinity worden ingebed in de teams van onze klanten, zodat de lijntjes zo kort mogelijk blijven en de gewenste ontwikkelsnelheid niet in het geding komt. Er is hierdoor geen sprake meer van bedrijfsmuren tussen onze organisatie en die van de klant, wat resulteert in ontwikkelsnelheid, betere communicatie en kennisoverdracht. Maar ‘Stretched’ betekent meer dan samenwerken ‘over de bedrijfsmuren heen’. Stretched DevSecOps betekent continu samenwerken, leren en evalueren.

## Pentesting en Agile Security

Tot slot moet je ook ná het ontwikkel- en releasestadium er zeker van zijn dat de productieomgevingen beveiligd zijn. In dat stadium is het zinvol om **pentesting** in te zetten, gesimuleerde cyberaanvallen op een systeem om de security te evalueren. Maar doorgaans is de frequentie van pentests te laag. Pentests worden misschien één of twee keer per jaar uitgevoerd, terwijl maandelijks of misschien zelfs wekelijks nieuwe software-updates worden uitgerold. **Agile Security** brengt veiligheidstests in lijn met de ontwikkelsnelheid, door pentests uit te smeren over het hele jaar en te testen waar en wanneer veranderingen worden aangebracht. Zo blijft security top-of-mind én integraal onderdeel van het proces zonder al te veel in te boeten op flexibiliteit of snelheid én voorkom je imagoschade en onverwachte kosten achteraf.

## Aandachtspunten

- Evalueer de geschiktheid van je huidige testmodel voor de beoordeling en beveiliging van applicaties en identificeer verbeterpunten.
- Breng het ontwerp- en ontwikkelproces en de structurering van applicaties in kaart.
- Evalueer de organisatie en mate van optimalisatie tussen verschillende teams en disciplines.
- Krijg helder hoe, waarop en (belangrijk!) waarom audits plaatsvinden en bereid je hier tijdig op voor.
- Zorg voor een volledig beeld van de communicatie met en tussen applicaties.

LAAG 4

# Bescherming tegen externe dreigingen

De hiervoor besproken lagen verzorgen een vanaf binnenuit opgebouwde beveiliging. Vervolgens dienen aanvullende maatregelen te worden toegevoegd, die zich expliciet richten op dreigingen van buitenaf.

## Protect, Detect, Respond

Solvinity volgt hierin het bewezen principe “Protect, Detect, Respond” (Bescherm, Detecteer, Reageer), dat je terugziet in bijvoorbeeld het NIST framework:

- Het **Protect**-aspect is in eerdere lagen al deels besproken. Met Identity & Access Management kun je bepalen welke gebruikers toegang hebben tot specifieke data en applicaties. Voeg aanvullend een beveiligingslaag toe op hardwareniveau, door te bepalen welke apparaten welke toegangsniveaus krijgen. Implementeer tot slot ook technologieën zoals anti-DDoS- en anti-ransomware-oplossingen.

- **Detect** betekent kort gezegd het gericht loggen en monitoren van alle componenten en configuraties om veranderingen of afwijkingen te ontdekken. Het is immers niet de bedoeling dat je er na een half jaar pas achter komt dat iemand je netwerk is binnengedrongen. En hoewel je met gedegen netwerksegmentering een diepteverdediging kunt voeren, is het wenselijk om ook te monitoren op aanvallen vóórdat ze slagen. Denk aan het centraal en beveiligd opslaan van alle logs op een totaal afgeschermde locatie - sowieso nodig voor compliance en vergemakkelijking van audits- en het gebruik van monitoringoplossingen als Advanced Threat Detection. Met name ‘sandboxing’ is daarin een krachtig hulpmiddel. Dit is een methode om programma’s in een volledig afgeschermde omgeving (de ‘sandbox’) te activeren, zodat ze daar veilig kunnen worden gecontroleerd.

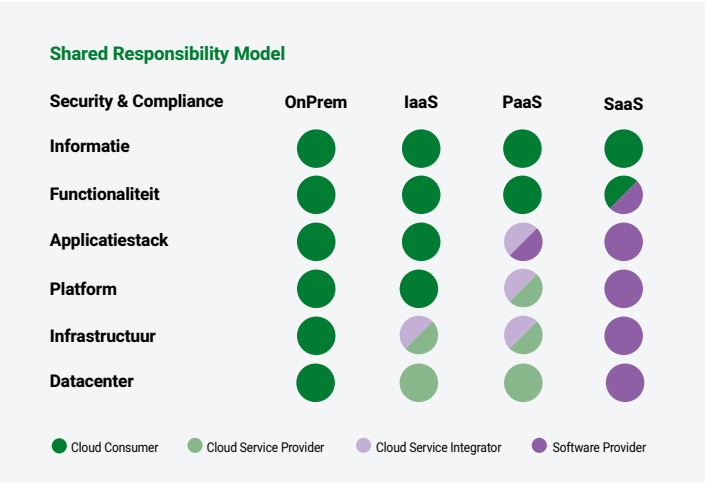
- Tot slot vraagt de **Respond**-fase om snelheid en daarmee om voorbereiding. Zorg dat playbooks klaarliggen: een lijst van voorbereide, bij voorkeur geautomatiseerde stappen als reactie op dreigingen. Zo’n stap kan een simpele notificatie zijn, maar ook het automatisch dichtzetten van een netwerk. Hoe dan ook, playbooks laten je teams efficiënt en effectief reageren zonder onnodig overleg. Zorg daarbij ook voor schadebeperkende oplossingen in het kader van Disaster Recovery wanneer zich onverhoopt toch een calamiteit voordoet en je IT-omgeving in het gedrang komt.

Het is juist de kracht van public cloud dat je security per applicatie of omgeving kunt regelen.

## Voorkom one-size-fits-all security

Een belangrijke kanttekening is dat, hoewel het Protect-Detect-Respond-principe een holistische benadering promoot, je binnen public cloud-omgevingen alle mogelijkheden moet benutten om flexibiliteit en granulariteit te behouden. Het is juist de kracht van public cloud dat je security per applicatie of omgeving kunt regelen. Je maakt vaart door gebruik te maken van de beheerde diensten van de Cloud Service Provider. Zo hoef je niet alle applicaties in één model te proppen en kun je je beleid uitstippelen per type applicatie en/of omgeving.

Hierbij komt een goed begrip van het **Shared Responsibility-model** van pas. Dit schetst de verantwoordelijkheid van security in public cloud en hoe deze verdeeld is tussen gebruiker en cloud-provider. Kortgezegd zijn gebruikers verantwoordelijk voor de veiligheid in de cloud (inclusief hun data), terwijl cloud-providers verantwoordelijk zijn voor de veiligheid van de cloud-, compute- en opslagsystemen en de netwerken die public cloud ondersteunen. Met andere woorden: de infrastructuur kan wel veilig en compliant zijn, maar dat betekent niet meteen dat de applicaties die erop draaien dat óók zijn.




## Aandachtspunten

- Weet waar en op welke wijze het ‘Shared Responsibility Model’ impact heeft op de security- en compliance-status van je omgeving.
- Bepaal hoe en op en welke dreigingen wordt gereageerd.
- Maak inzichtelijk welke calamiteitenplannen binnen je organisatie bestaan en stel ze op als deze nog niet bestaan.
- Ga na hoe en hoe vaak deze plannen worden getest.
- Evalueer welke technische maatregelen al zijn genomen tegen externe bedreigingen en vul ze aan waar nodig.

LAAG 5

# De menselijke factor

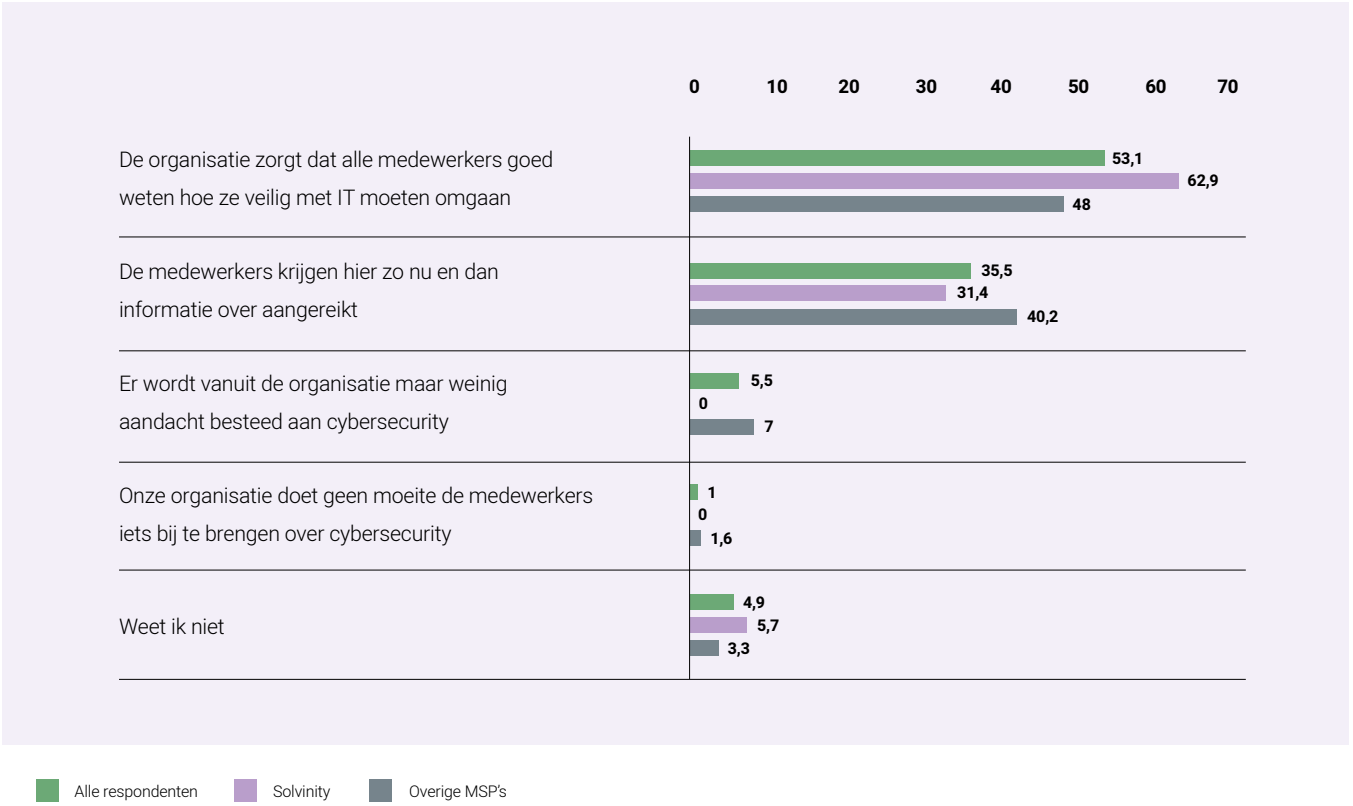
Tot nu toe zijn we dicht bij de techniek gebleven. Maar security heeft ook te maken met de menselijke factor. Dit verdient binnen iedere organisatie speciale aandacht, want een groot deel van geslaagde cyberaanvallen wordt veroorzaakt door menselijk handelen.

## Bewustzijn creëren

Allereerst is security awareness onder alle medewerkers een cruciaal onderdeel van ieder securityprogramma.
48% van de organisaties met IT in eigen beheer besteedt hier onvoldoende aandacht aan, terwijl álle medewerkers horen te weten hoe ze veilig kunnen werken in public cloud. Dat betekent dat ze zich bewust moeten zijn van de risico's én weten wat ze moeten doen wanneer er toch iets misgaat. Investeer daarom in het opleiden en bewust maken van je medewerkers middels **trainingssessies**. Toets ook periodiek de kennis en 'staat van paraatheid' binnen de organisatie met bijvoorbeeld **phishingtests**, waarbij je via de mail persoonsgegevens probeert te ontfutselen.
Er zijn tal van security awareness-programma's beschikbaar waarbij medewerkers continu op creatieve wijze scherp worden gehouden. Solvinity biedt **op maat gemaakte programma's** aan die zijn opgebouwd uit diverse video-trainingen, games, quizzen en testmodules.

48% van de organisaties met IT in eigen beheer besteedt hier onvoldoende aandacht aan, terwijl álle medewerkers horen te weten hoe ze veilig kunnen werken in public cloud.

Iedere innovatie binnen public cloud kan betekenen dat je geld kunt besparen óf dat je ineens duurder uit bent met de eerder gekozen middelen.




## Kennisdeling

Ten tweede is het belangrijk om via doorlopende **training** de securitykennis van je IT-medewerkers op peil te houden.
De public cloud-wereld verandert snel, maar het dreigingslandschap nog sneller. De kennis up-to-date houden is essentieel vanuit securityperspectief, maar ook vanuit kostenoogpunt: iedere innovatie binnen public cloud kan betekenen dat je geld kunt besparen óf dat je ineens duurder uit bent met de eerder gekozen middelen. Zorg daarom voor een continue investering in kennis, zodat je strategisch kunt nadenken over de te maken keuzes.
Dit raakt ook het onderwerp compliance: de juiste kennis en kunde is nodig om te voldoen aan de strenge standaarden van compliance-certificeringen.

Natuurlijk is het gezien de complexiteit van public cloud lang niet altijd nodig of zelfs mogelijk alle benodigde expertise in huis te hebben. Het benodigde kennisniveau kan in dat geval betekenen dat je IT-teams in staat zijn mogelijke dreigingen tijdig te identificeren, zodat ze snel externe expertise kunnen inschakelen. Bij Solvinity zien we compliance bijvoorbeeld als kritiek onderdeel van onze dienstverlening en zorgen we ervoor dat standaarden altijd worden geborgd. Door deze aandacht voor compliance leveren we als enige partij in Nederland SOC 1 en 2-rapporten voor niet alleen onze gehele private cloud-omgeving maar óók de beheeromgeving van de Azure public cloud.

## Aandachtspunten

- Evalueer of de organisatiecultuur klaar is voor de transformatie naar public cloud.
- Weet welke nieuwe services welke medewerkers en afdelingen gaan gebruiken.
- Bepaal of je wil dat mensen een bepaalde certificering dienen te behalen voordat zij een leidende rol binnen een transformatie krijgen.
- Breng in kaart wat je als organisatie moet doen en leren om de informatiebeveiliging goed te beheren - en of daarvoor de nodige trainingen beschikbaar zijn.
- Ga na of alle interne processen, monitoring, et cetera, adequaat en up-to-date zijn voor public cloud.

# Voortdurende borging

Iedere security-evaluatie is per definitie een momentopname en moet dus periodiek en bij voorkeur geautomatiseerd uitgevoerd.

Een public cloud-omgeving beveiligen is geen eenmalige taak. Public cloud leent zich bij uitstek voor innovatie. Niet alleen de applicaties van je organisatie worden constant doorontwikkeld; de onderliggende cloud-technologieën worden eveneens doorlopend verbeterd. Daarnaast zitten cybercriminelen ook niet stil. Hun aanvalsmethoden worden steeds geraffineerder. Dit alles betekent dat iedere security-evaluatie per definitie een momentopname is, en deze dus periodiek en bij voorkeur geautomatiseerd moet worden uitgevoerd.

## Het belang van periodieke evaluatie

Belangrijke hulpmiddelen in je arsenaal zijn de **'Well-Architected Frameworks'** die zowel Google, Microsoft en Amazon hebben ontwikkeld voor hun respectievelijke cloud-diensten. Deze beschrijven de belangrijkste best practices in concept, ontwerp en architectuur van public cloud-omgevingen, en helpen je de voor- en nadelen van bepaalde keuzes te doorgronden. Daarmee is zo'n framework een handig hulpmiddel om je cloud-omgeving te evalueren op basis van de huidige standaarden en best practices. Door periodiek een assessment te voltooien aan de hand van een Well-Architected Framework, kun je effectiever nieuwe security-risico's identificeren en deze efficiënter mitigeren.

Het kan moeilijk zijn om je eigen keuzes te beoordelen. Solvinity kan hierin ondersteunen met het Cloud Architecture Assessment. In dit evaluatietraject helpen we je in de spiegel te kijken en je te begeleiden in de beoordeling van je cloud-architectuur. Wij stellen daarbij vragen die tot nadenken aanzetten, die je helpen je cloud-architectuur te versterken.

## De beste lessen leer je in de praktijk

Zelfs een **Cloud Architecture Assessment** blijft tot op zekere hoogte een theoretisch verhaal. Wil je écht weten of je veilig bent, dan kan Red Teaming inzicht bieden. Waar securityteams tijdens een pentest weten dat deze plaatsvindt en zich er op voor kunnen bereiden, worden ze bij **Red Teaming** verrast. Hierdoor zullen ze de test als een echte aanval behandelen, wat een volledig beeld van de security kan opleveren, met name omtrent detectie- en respons-capaciteit. De experts van onze strategische partner Securify zullen daarbij alle mogelijke aanvalsvectoren verkennen, zelfs de (toegangs)beveiliging van je fysieke kantoor.

Door periodiek verscheidene evaluatiemethoden in te zetten, ben je vaker en beter geïnformeerd over de staat van security van je cloud-omgeving, en ben je sneller in staat gaten in de beveiliging te identificeren en te verhelpen.

De beste partner voor een veilige public cloud-omgeving is er een met ervaring en een achtergrond in security, privacy en compliance

# Conclusie

Een goed beveiligde public cloud-omgeving inrichten is makkelijker gezegd dan gedaan. Het vergt strategische keuzes, goede voorbereiding en een gestructureerde aanpak. Gebruik daarbij alle hulpmiddelen die tot je beschikking staan. Door vanaf de grond af aan met behulp van een Cloud Architecture Framework een gedegen fundament neer te leggen, ben je vervolgens goed in staat om met Protect-Detect-Response-methoden je organisatie te beschermen tegen dreigingen. Iedere organisatie zou daarbij geen enkele methode of hulpmiddel moeten schuwen dat logischerwijs binnen de behoeften en beschikbare capaciteiten past. Daarmee is de cirkel rond.

Zoals we aan het begin van dit whitepaper vaststelden, is het niet altijd mogelijk (of wenselijk) om alle benodigde expertise in huis te halen. In dat geval is een Trusted Cloud Provider de weg voorwaarts. Een partner die je in het gehele traject van conceptualisering tot periodieke evaluatie en bij alle in dit whitepaper besproken lagen kan ondersteunen.

Nu zijn niet alle partners gelijk. De beste partner voor een veilige public cloud-omgeving is er een met ervaring en een achtergrond in security, privacy en compliance. Maar even zo belangrijk is dat deze partner transparant met je samenwerkt, zodat je optimaal kunt profiteren van de kennis die deze inbrengt. En tot slot een cultuurfit - het is immers beter samenwerken met een groep professionals waar je een klik mee hebt.

Solvinity biedt in Nederland een uniek portfolio aan securitydiensten, niet alleen voor de inrichting en het beheer van je cloud-omgeving, maar ook voor doorlopende toetsing achteraf en security awareness-programma's.
Ben je na het lezen van dit whitepaper benieuwd of je een klik met Solvinity kunt vinden? We zetten het gesprek graag voort!

## Lees ook:

**Whitepaper**

- Integrated Delivery
- Security by Design

**Multimedia**

- Grip op public cloud security
- Cloud native applicatieontwikkeling

**Blogs**

- Strategische keuzes met een cloud architecture assessment
- Landingzones, het vertrekpunt richting public cloud
- Van account tot applicatie veilig in de cloud
- 7 kritische succesfactoren voor je cloud first strategie
- Veilig naar de public cloud, waar let je op?
- Snelheid, veiligheid en een soepele samenwerking met Stretched DevSecOps
- Shift-left security met Stretched DevSecOps

Solvinity
Secure Managed IT Services

Solvinity B.V.
Postbus 23673
1100 ED Amsterdam

T +31(0)20 364 3600
E info@solvinity.com
**www.solvinity.com**

**Met secure managed IT services ondersteunt en adviseert Solvinity organisaties met hoge beveiligingseisen in hun digitale transformatie.**

| | | | |
|---|---|---|---|
| | Managed Cloud<br>Outsourcing | Security & Compliance<br>Lango Workspace | Service Integration<br>Application Services |
| | Solvinity onderscheidt zich op het gebied van cybersecurity met een uitgebreid portfolio aan securitydiensten en oplossingen en biedt, met een meerderheidsbelang in Securify, aanvullende diensten op het gebied van pentesting, red teaming en agile security. | | |
| | Certificeringen volgens (inter)nationale normen als ISO 27001, ISO 14001, ISO 9001 en PCI DSS. Als eerste Managed Service Provider in Nederland SOC 1 & 2 compliance rapporten voor de gehele beheeromgeving van niet alleen de private, maar ook de Azure cloud. | | |
| | Solvinity levert aan de (rijks-)overheid, gemeenten en toonaangevende organisaties in de financiële en zakelijke dienstverlening, zoals het ministerie van Justitie en Veiligheid, Politie Nederland, Translink (OV-chipkaart), ING en ONVZ. | | |
| | 350<br>medewerkers | 2021:<br>omzet 59 mln | Amsterdam, Assen<br>Amersfoort, Den Bosch |
| | | | |