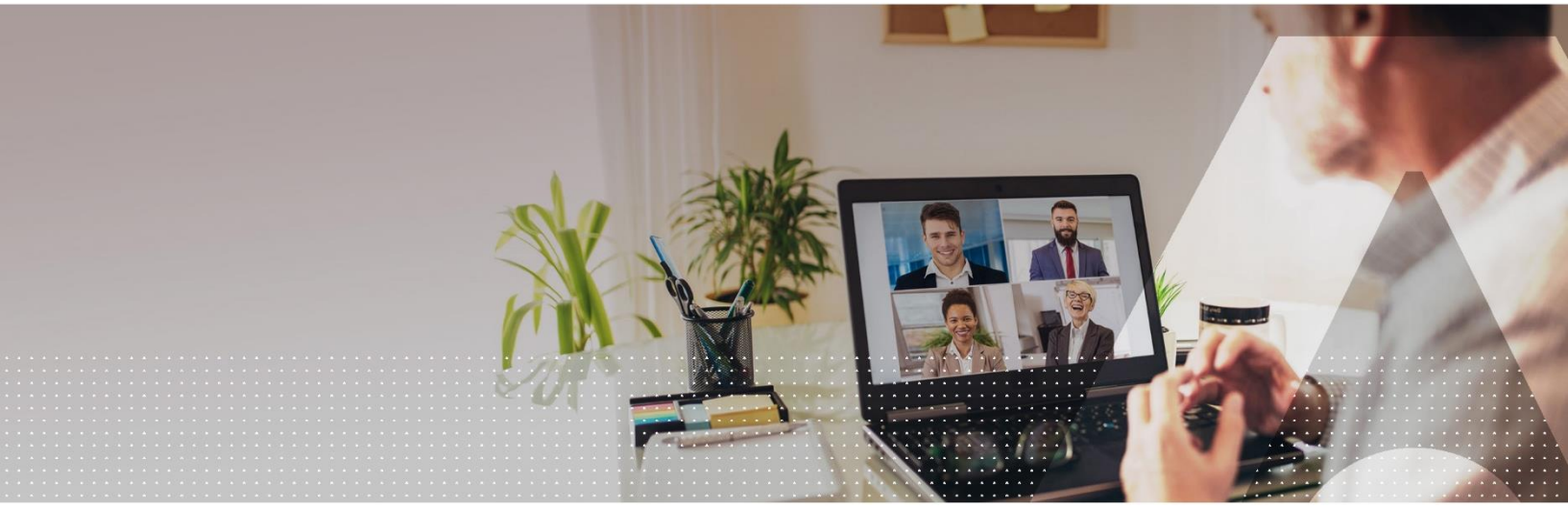
cpl.thalesgroup.com

THALES
Building a future we can all trust

Gedeelde beveiliging

Voor een sterke cloudbeveiliging en het voorkomen van vendor lock-in



Whitepaper

Inhoudsopgave

Samenvatting

De meest recente cyberaanvallen op (overheids)instellingen en bedrijven wereldwijd – organisaties die veel hebben geïnvesteerd in digitale en cloudinitiatieven – tonen aan dat een andere kijk op beveiliging noodzakelijk is. Gedeelde beveiliging in cloudomgevingen houdt in dat bedrijven hun beveiligingstaken gescheiden houden van die van hun cloudproviders en eigen beveiligingsmiddelen inzetten om cyberaanvallen en laterale beweging op hun netwerken te voorkomen.

Zo'n scheiding van beveiligingstaken helpt organisaties ook om te voldoen aan het uitdijende aantal wetten en regels, zoals de Schrems II-uitspraak heef aangetoond. Het doel van dit whitepaper is om de voordelen van een leveranciersonafhankelijke beveiligingsoplossing voor het aanpakken van nieuwe beveiligingsrisico's en privacyvereisten in cloudomgevingen aan te tonen.

Wat gedeelde beveiliging inhoudt

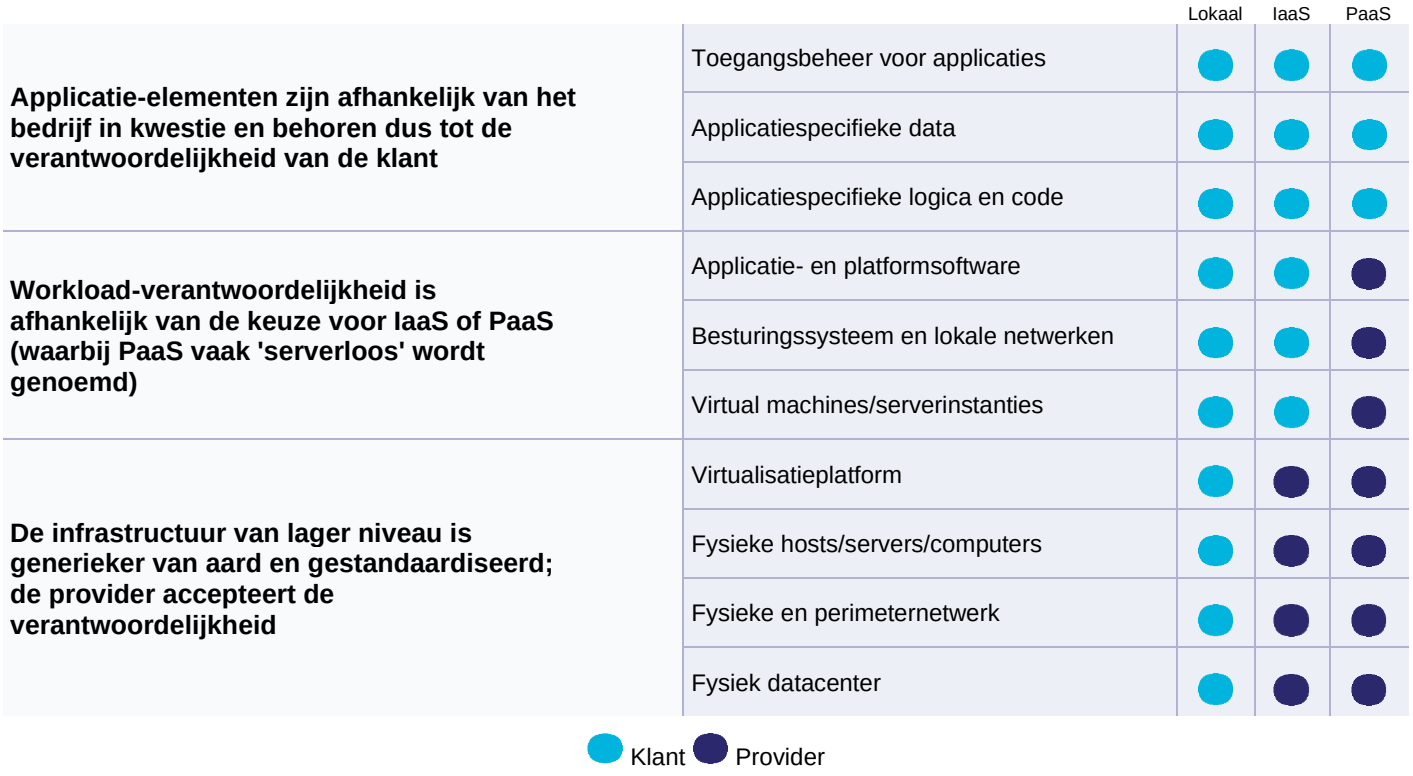
Met een conventioneel, lokaal beheerd datacenter bent u zelf verantwoordelijk voor de beveiliging van uw gehele operationele en digitale omgeving, inclusief applicaties, servers, besturingselementen voor gebruikers en zelfs fysieke beveiliging.

Als u uw services, applicaties, workload en data naar de cloud gaat migreren, moet u er rekening mee houden dat cloudserviceproviders een gedeeld beveiligingsmodel hanteren. Dat betekent dat uw eigen beveiligingsteam enige verantwoordelijkheid blijft behouden voor beveiliging, terwijl de rest door de provider wordt verzorgd. De sleutel tot effectieve cloudbeveiliging is weten waar de verantwoordelijkheid van uw provider ophoudt en die van u begint.

- In het AWS Shared Security Model[1] stelt AWS verantwoordelijk te zijn voor "het beschermen van de hardware, software, netwerken en faciliteiten waarop de cloudservices van AWS worden uitgevoerd."
- Microsoft Azure[2] stelt verantwoordelijk te zijn voor "fysieke hosts, netwerken en datacenters."
- Zowel AWS als Azure stelt dat uw eigen beveiligingsverantwoordelijkheden afhangen van de gekozen services.

1 Amazon Web Services, Shared Responsibility Model, https://aws.amazon.com/compliance/shared-responsibility-model/
2 Microsoft Azure, Shared responsibility in the cloud, https://docs.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility

In het volgende diagram vindt u een algemeen (en leveranciersonafhankelijk) conceptueel overzicht van gedeelde beveiliging:



Figuur 1: Een leveranciersonafhankelijk overzicht van verantwoordelijkheden bij gedeelde beveiliging Bron: Cloud Security Alliance[1].

Hoe uw IT-omgeving er ook uitziet (lokaal beheerd, openbare cloud, privécloud of hybride), u bent te allen tijde verantwoordelijk voor het beveiligen van waar u controle over heeft, zoals:

- **Data**: Door de controle te houden over uw data behoudt u ook de controle over hoe en wanneer data worden gebruikt. De cloudserviceprovider heeft nul inzicht in uw data en u behoudt alle toegang.
- **Applicaties**: Het is aan u om bedrijfsapplicaties te beveiligen en te beheren gedurende de gehele levenscyclus, van ontwikkeling en tests tot ingebruikname.
- **Identiteit en toegang**: U bent verantwoordelijk voor alle aspecten van Identity and Access Management (IAM), inclusief authenticatie en autorisatie, single sign-on (SSO), multi-factor-authenticatie (MFA), toegangssleutels en inloggegevens.
- **Platformconfiguratie**: Als u een cloud wilt implementeren, beheert u de configuratie van de onderliggende besturingsomgeving. De vereisten voor platformconfiguratie verschillen, afhankelijk van of uw instanties wel of niet servergebaseerd zijn.

1 Cloud Security Alliance, Shared Responsibility Model Explained, https://doudsecurityalliance.org/blog/2020/08/26/shared-responsibility-model-explained/

Risico's en nadelen van het hebben van een enkele serviceprovider

Cloudproviders hebben hun eigen tools om bedrijven te helpen met het beveiligen van hun cloudinstanties en -activa. Als u voor de beveiligingsoplossing van een specifieke leverancier kiest, betekent dat dat u de beveiliging van al uw data, applicaties, encryptiesleutels en inloggegevens aan die leverancier toevertrouwt. Dat klinkt aanlokkelijk, maar is het wel verstandig?

Wet- en regelgeving op het gebied van beveiliging en privacy verbetert de betrouwbaarheid van uw cloudomgeving. Maar juist als er sprake is van minder vertrouwen, wordt het gemakkelijker om vertrouwen te krijgen.[1] Hoewel u de technologieën achter cloudimplementaties zeker kunt vertrouwen, is het beter om voorzichtig te zijn met de beveiligingsoplossingen van cloudproviders.

Dit is erg belangrijk, aangezien risico's, kwetsbaarheden en dreigingen aan het adres van de serviceprovider kunnen overslaan op de klant, waarna kwaadwillende partijen zich lateraal kunnen bewegen op het bedrijfsnetwerk. Dit zijn drie dreigingsvectoren waarmee u rekening dien te houden wanneer u uw cloud moet beveiligen:

1. Menselijke fouten

Een hoog percentage beveiligingsincidenten is te wijten aan menselijke fouten en onachtzaamheid. Volgens het Cloud Security Report uit 2020[2] vormt verkeerde configuratie van het cloudplatform (68%) de grootste bedreiging voor cloudimplementaties. Configuratiefouten, fouten van ontwikkelaars, gebrekkige entropiebronnen en het verlies van sleutels kunnen beveiligingsincidenten tot gevolg hebben, zoals de ongeautoriseerde verspreiding van (inlog)gegevens en verlies van privacy.

2. Externe aanvallers

Externe aanvallers zijn altijd alert op de hierboven genoemde menselijke fouten en maken gebruik van deze kwetsbaarheden om gerichte aanvallen te plaatsen. Kwaadwillende partijen hebben zich in het verleden gericht op cruciale managementsystemen en zwakke authenticatiemethoden om toegang te krijgen tot grote hoeveelheden data. Tijdens de supply-chain-aanval op SolarWinds maakten hackers gebruik van 'systemische kwetsbaarheden'[3] in de systeemeigen authenticatiemethode van een cloudserviceprovider om zich toegang te verschaffen tot de netwerken van klanten. Al snel bleek dat de inzet van de systeemeigen beveiligingsoplossing van de leverancier de aanval niet alleen niet had weten te voorkomen, maar dat de aanvallers zelfs meer mogelijkheden kregen om extra schade aan te richten.

3. Dreiging van insiders

Een kwaadwillende of ontevreden werknemer met toegang tot sleutels en/of inloggegevens kan zijn of haar toegangsrechten misbruiken om vertrouwelijke data te stelen of cloudservices te verstoren.

1 Anton Chuvakin, Il-Sung Lee, The cloud trust paradox: To trust cloud computing more, you need the ability to trust it less, https://cloud.google.com/blog/products/identity-security/trust-a-cloud-provider-that-enables-you-to-trust-them-less
2 Cybersecurity Insiders, 2020 Cloud Security Report, https://www.cybersecurity-insiders.com/portfolio/2019-cloud-security-report-isc2/
3 https://www.infosecurity-magazine.com/news/crowdstrike-slams-microsoft-over/

Leveranciersonafhankelijke cloudbeveiliging en naleving

Behalve aan de hierboven beschreven dreigingen moet u aandacht besteden aan de ontwikkelingen op het vlak van privacywetgeving, en met name de concepten van overdraagbaarheid en soevereiniteit. Regionale vereisten spelen een grote rol in hoe organisaties naar de cloud migreren en hun workloads naar de openbare cloud verplaatsen. Regelgevende instanties in Europa, Japan, India, Brazilië en andere landen overwegen nieuwe of extra regels voor de opslag van niet-versleutelde gegevens en/of encryptiesleutels binnen hun grenzen.

Daarnaast kwam het Europese Hof van Justitie op 16 juli 2020 tot een uitspraak in de zaak-Schrems II. Het bleek een historische uitspraak waarmee het EU-VS-privacyschild ongeldig werd verklaard. Tot dan toe werd het Privacyschild gezien als afdoende middel om de grensoverschrijdende uitwisseling van persoonsgegevens tussen de Europese Unie en de Verenigde Staten onder de Algemene verordening gegevensbescherming (AVG) te beschermen. Meer dan 5000 organisaties doen mee aan het Privacyschild en duizenden bedrijven in de EU vertrouwen op de regeling als ze data naar deze organisaties moeten verzenden. Volgens de Schrems II-uitspraak zijn de condities voor het rechtmatig delen van deze data niet langer van toepassing.[1]

Gezien het feit dat de grote cloudserviceproviders (Amazon, Microsoft en Google) niet in de Europese Economische Ruimte (EER) gevestigd zijn, werpt dit bepaalde vraagtekens op wat betreft de toegang tot persoonsgegevens uit de EU. Het Europees Comité voor gegevensbescherming (EDPB) heeft twee gevallen van onrechtmatig gebruik vastgesteld:

- Unlawful Use Case 6: de transfer van data naar cloudserviceproviders of andere verwerkers die data niet-versleuteld verwerken.
- Unlawful Use Case 7: datatoegang op afstand voor zakelijke doeleinden.

Het bestaan van Unlawful Use Cases 6 en 7 wijst erop dat directeuren en bestuursleden van cloudserviceproviders vaak aansprakelijk kunnen worden gesteld in het geval van onrechtmatige toegang tot gegevens.[2]

Om aan de nieuwe soevereiniteitsvereisten te kunnen voldoen hebben cloudserviceproviders hun modelcontractbepalingen[3] aangepast, zodat hun dienstverlening nu geheel binnen de jurisdictie van de EU valt. Organisaties kunnen het risico van onrechtmatige datatoegang beperken door een eigen leveranciersonafhankelijke beveiligingsoplossing te gebruiken, met pseudonimisering van data en beheer van inloggegevens. Op die manier kunnen ze aan de EDPB-vereisten voor de rechtmatige uitwisseling van gepseudonimiseerde data binnen de EU voldoen.

Een laatste argument voor het kiezen van een leveranciersonafhankelijke beveiligingsoplossing is wetshandhavingsinstanties die cloudserviceproviders dwingen hun toegang te verlenen tot klantgegevens. Als u zelf uw eigen beveiliging regelt, heeft de provider geen toegang tot sleutels of inloggegevens aan de hand waarvan zulke instanties toegang tot uw data kunnen krijgen.

Het concept van Bringing-Your-Own-Security (BYOS) in de cloud is cruciaal als we rekening houden met de plannen van bepaalde landen om 'backdoors' in te bouwen in end-to-end-versleuteling, het beschermen van privacy/vertrouwelijkheid en de algemene voorwaarden die door cloudleveranciers en -platformen worden gehanteerd.

Zo valt het volgende te lezen in de contractuele bepalingen van AWS:[4]

> "Bekendmaking van wat minimaal vereist is: als we, niettegenstaande al onze bezwaren, ooit

1 Brian Hengesbaugh, CIPP/US, What Privacy Shield organizations should do in the wake of 'Schrems II', https://iapp.org/news/a/what-privacy-shield-organizations-should-do-in-the-wake-of-schrems-ii/
2 Gary LaFever, Magali Feys, 'Schrems II': How to protect against liability when using non-EEA vendors, https://iapp.org/news/a/schrems-ii-how-to-protect-against-liability-when-using-non-eea-equivalency-country-vendors/
3 Amazons modelcontractbepalingen: https://aws.amazon.com/blogs/security/aws-and-eu-data-transfers-strengthened-commitments-to-protect-customer-data/, Google Cloud: https://services.google.com/fh/files/misc/gsuite_foredu_whitepaper_gdpr_schremsii.pdf, Microsoft Azure: https://blogs.microsoft.com/eupolicy/2020/07/16/assuring-customers-about-cross-border-data-flows/
4 Stephen Schmidt, AWS and EU data transfers: strengthened commitments to protect customer data, https://aws.amazon.com/blogs/security/aws-and-eu-data-transfers-strengthened-commitments-to-protect-customer-data/

na een valide en rechtmatig verzoek verplicht worden om klantgegevens bekend te maken, zullen we alleen de minimale hoeveelheid gegevens delen die nodig is om aan het verzoek te voldoen."

4 De tastbare voordelen van gedeelde beveiliging

Gedeelde cloudbeveiliging kan bedrijven en organisaties helpen met het ontwikkelen van best practices voor het gescheiden houden van de beveiliging van clouddata en andere services. Sterker nog: hoe groter de segmentatie van taken, hoe beter u uw data kunt beveiligen.

Segmentatie van taken door middel van een leveranciersonafhankelijke oplossing is van toepassing op zowel encryptiesleutels als de authenticatiemethode die gebruikt wordt voor toegang tot opgeslagen data. Cloudbeveiliging gescheiden houden van de serviceprovider zelf biedt enkele duidelijke voordelen.

Onafhankelijkheid beperkt de impact

Tijdens de hoorzittingen van het Amerikaanse Congres over de SolarWinds-hack zeiden veel gedaagden dat het gebruiken van eigen methoden of technologieën naast die van de serviceprovider een aanzienlijke dreigingsvector kan elimineren en meer barrières kan opwerpen voor kwaadwillende partijen. Gezien het feit dat hackers zich op kwetsbaarheden richten om zich toegang tot het netwerk te verschaffen en zich vervolgens onopgemerkt lateraal te verplaatsen, werkt het opwerpen van extra barrières als afschrikmiddel. Cloudserviceproviders bieden een uitstekende infrastructuur, services, resources en apps, maar BYOS als extra laag wordt in deze wereld vol dreigingen gezien als best practice op het vlak van beveiliging.

Tip 1

Gebruik een gespecialiseerde Identity and Access Management-oplossing (IAM) met ondersteuning van verschillende authenticatiemethoden om een extra barrière voor uw netwerken en data op te werpen in het geval de cloudserviceprovider wordt gehackt.

Kies de oplossing waarmee naleving gegarandeerd is en blijft.

Vanwege de vele regels op het vlak van privacy en databescherming moeten bedrijven oplossingen kiezen waarmee ze in verschillende rechtsgebieden uit de voeten kunnen. Taken gescheiden houden en kiezen voor authenticatie- en sleutelbeheeroplossingen die aan de specifieke operationele en nalevingsvereisten voldoen is de beste manier om onrechtmatige verwerking van persoonsgegevens te voorkomen.

Tip 2

Kies een onafhankelijke IAM-oplossing en een Hardware Security Module-platform (HSM) die aan uw zakelijke benodigdheden en de lokaal geldende regelgeving voldoen. Let daarbij met name op datasoevereiniteit en de contractuele bepalingen met betrekking tot databescherming.

Neem uw beveiliging in eigen hand.

Door uw eigen, onafhankelijke oplossing te implementeren behoudt u gecentraliseerde, flexibele controle over toegang, sleutels en data. Door uw afhankelijkheid te beperken en minder te vertrouwen op uw cloudserviceprovider beperkt u de dreigingsrisico's en voorkomt u laterale netwerkbewegingen door de hacker.

Tip 3

Kies voor een authenticatie- en sleutelbeheeroplossing waarmee u uw eigen beveiliging centraal en op flexibele wijze kunt regelen.

Voorkom dat u vast komt te zitten aan een enkele leverancier.

De keuze voor een systeemeigen beveiligingsoplossing vergroot de kans op vendor lock-in. Vendor lock-in gaat gepaard met risico's op het vlak van commercie, naleving en beveiliging, wat de algehele risico's vergroot. Nu steeds meer bedrijven het ondernemersrisico willen beperken en hun veerkracht willen vergroten, is scheiding van taken de beste oplossing voor het verbeteren van de beveiliging en het beschermen van de privacy.

Tip 4

Houd uw beveiliging gescheiden van uw cloudserviceprovider en kies voor gespecialiseerde IAM- en HSM-oplossingen om de algehele veerkracht van uw bedrijf te vergroten.

De voordelen van agnostische beveiliging van Thales

Thales is wereldmarktleider op het gebied van leveranciersonafhankelijke beveiligingsoplossingen waarmee u uw activa en data overal kunt beschermen: on-premises of in de cloud. Met Thales SafeNet Trusted Access behoudt u de controle over uw toegangsbeveiliging en voorkomt u de risico's van vendor lock-in.

- **Behoud van flexibiliteit**: IT-managers beschikken over de nodige flexibiliteit doordat ze met verschillende gebruikerslijsten kunnen werken en de bedrijfscontinuïteit kunnen waarborgen door middel van interoperabiliteit in multi-cloud-implementaties.
- **Beperk het aantal kwetsbaarheden**: De CISO kan het aantal kwetsbaarheden verminderen en de bedrijfsbeveiliging verbeteren door toegangsbeheer gescheiden te houden van apps en data. Dit vermindert de kans op laterale beweging op het bedrijfsnetwerk.
- **Klaar voor nieuwe wet- en regelgeving**: De wet- en regelgeving verandert voortdurend, en snel. Door zelf de controle te behouden over toegang bent u goed voorbereid op toekomstige regels op het vlak van dataprivacy en -soevereiniteit en verkleint u de kans dat derden toegang krijgen tot vertrouwelijke bedrijfsgegevens.
- **Commerciële slagkracht**: CFO's krijgen met een multi-vendor-strategie meer mogelijkheden en zijn beter gepositioneerd in de onderhandelingen over het aanschaffen of verlengen van licenties.

Over Thales

De mensen op wie u vertrouwt om uw privacy te beschermen vertrouwen weer op Thales om hun gegevens te beveiligen. Wat gegevensbescherming betreft, krijgen organisaties te maken met steeds meer beslissende momenten. Of u nu een encryptiestrategie wilt opstellen, naar de cloud wilt verhuizen of alleen aan de wet- en regelgeving wilt voldoen, u kunt erop vertrouwen dat Thales uw digitale transformatie goed zal beveiligen.

Decisive technology for decisive moments.

THALES

Building a future we can all trust

Neem contact met ons op

Ga voor onze kantoren en contactgegevens naar
cpl.thalesgroup.com/contact-us

> cpl.thalesgroup.com <