Afstudeerscriptie

PCI IT

Project naam:	Afstudeeropdracht Mike Van kan		
Datum:	16-1-2022	Status:	Final
Auteur	Mike Van kan Studentnummer: 454027		
Eigenaar:	Joost Overkamp		
Client:	PCI IT Solutions		
Document versie:	3.0		

1. Voorwoord

Mijn naam is Mike Van kan en ik volg de studie HBO-ITSM aan het Saxion te Deventer. Op 30 augustus 2021 ben ik begonnen aan mijn afstuderen bij PCI IT te Haaksbergen. Voor u ligt de afstudeerscriptie die ik heb geschreven ten behoeve van dit afstuderen en waarin antwoord wordt gegeven op de volgende hoofdvraag: “Hoe kan PCI IT haar klanten een oplossing bieden die de toegang tot data in SaaS-systemen controleert en restricties op de toegang kan toepassen?”.

Ik zou via deze manier graag een aantal mensen willen bedanken voor de hulp tijdens het afstuderen. Als eerste zijn dit al mijn collega’s bij PCI IT die ik wil bedanken voor de ondersteuning die ik ontvangen heb tijdens het afstuderen. Van mijn collega’s bij PCI IT wil ik Joost Overkamp in het bijzonder bedanken voor de begeleiding, tijd en de kennis die hij beschikbaar heeft gesteld om dit afstuderen te ondersteunen.

Daarnaast zou ik Theo Lansink willen bedanken voor de hulp die ik van hem ontvangen heb en de adviezen die hij mij gegeven heeft.

Ook ben ik Niels Christenhusz zeer erkentelijk voor de inhoudelijke feedback die hij gegeven heeft.

Tot slot wil ik mijn vriendin Iris van Holsteijn bedanken voor het meerdere malen overlezen en controleren van het document, wat de leesbaarheid van het document verbeterd heeft.

Mike Van kan

Nijbroek, Januari 2022

2. Samenvatting

Dit project is opgezet omdat PCI IT ervaart dat er bij klanten geen controle is over de datastromen in SaaS-oplossingen en dat er geen zicht is op de SaaS gerelateerde schaduw IT die gebruikt wordt. Door het gebrek aan inzicht komen er in de huidige situatie geen meldingen bij oneigenlijk gebruik van de data in de SaaS-applicaties. Ook is het momenteel niet inzichtelijk als er medewerkers van een klant een niet-beheerde filesharing service gebruiken om data te delen. Dit zorgt ervoor dat PCI IT een product zoekt dat zij kunnen gebruiken om deze blinde vlek te elimineren.

In dit project zijn er een paar fases doorlopen om tot het antwoord op de hoofdvraag te komen. De hoofdvraag van dit project is, “Hoe kan PCI IT haar klanten een oplossing bieden die de toegang tot data in SaaS-systemen controleert en restricties op de toegang kan toepassen?”. Als eerste is er in dit project onderzocht wat exact de aard van het probleem is en wat PCI IT exact met dit project wil bereiken. Door gesprekken met meerdere werknemers van PCI IT is hier duidelijkheid in gekomen en zijn er requirements opgesteld. Tevens zijn er uit de gesprekken die gevoerd zijn met medewerkers randvoorwaarden ontstaan en is er achtergrondinformatie achterhaald welke benodigd is om deelvragen zoals “Van welke SaaS-applicaties maken klanten van PCI IT gebruik?” te beantwoorden.

Toen de basis van het project aanwezig was, is er onderzoek gedaan naar welk producttype het best past bij de wensen van PCI IT en is er een groot aantal producttypes met een raakvlak aan SaaS-applicaties onderzocht. Tijdens dit proces is er gekeken of het producttype aan alle requirements van PCI IT voldeed. Na veel onderzoek is hier uiteindelijk uitgekomen dat de oplossing met een correcte scope voor de problemen die PCI IT ervaart een CASB is.

Daarna zijn verschillende producten die als CASB op de markt zijn gebracht, onderzocht op feitelijke werking en toepasbaarheid bij de klanten van PCI IT. Dit is onderzocht aan de hand van bureauonderzoek, literatuuronderzoek en gesprekken met leveranciers van deze producten. De conclusie van dit onderzoek naar meerdere leveranciers is dat een CASB genaamd Microsoft Defender for Cloud Apps het best aansluit bij de wensen van PCI IT. Het product is samen met Forcepoint het meest compleet, maar onderscheidt zich van Forcepoint met enkele zaken. Het heeft bijvoorbeeld een koppeling van Microsoft Defender for Endpoint en Microsoft Defender for Cloud Apps, waardoor het mogelijk is om op en buiten het bedrijfsnetwerk inzicht te hebben in schaduw IT, zonder dat een extra agent nodig is. Daarnaast zijn er duidelijke eisen over de requirements om een nieuwe SaaS-applicatie toe te voegen en er is al een bestaande relatie met Microsoft waar PCI IT waarde aan hecht.

Revisie historie

In onderstaande tabel is genoteerd wanneer het document is aangepast en welke aanpassingen er zijn gemaakt.

Revisie datum	Laatste revisie datum	Aanpassingen
20-9-2021	-	Opzetten document.
21-9-2021	20-9-2021	Inleiding, probleemstelling, methodes, voorwoord.
22-9-2021	21-9-2021	Hoofdstuk indeling gewijzigd, basisinformatie toegevoegd aan diverse hoofdstukken.
23-9-2021	22-9-2021	Empathize fase opstellen.
27-9-2021	23-9-2021	Empathize fase, verwerken interviews, empathy maps, 6 W-vragen.
1-10-2021	30-9-2021	Feedback verwerken
8-10-2021	1-10-2021	Feedback verwerken
15-10-2021	8-10-2021	Feedback verwerken
26-10-2021	15-10-2021	Feedback verwerken
16-10-2021	15-10-2021	Requirements en visie
22-10-2021	16-10-2021	Hoofdstuk 9 ideate en onderzoek
30-11-2021	22-10-2021	Feedback verwerken en onderzoek
3-12-2021	30-11-2021	Feedback verwerken en onderzoek
10-12-2021	3-2-2021	Feedback verwerken, conclusies schrijven, long en shortlist afmaken en de laatste deelvraag invullen
17-12-2021	10-12-2021	Feedback verwerken, advies, voorwoord, reflectie en samenvatting
24-12-2021	17-12-2021	Feedback verwerken
31-12-2021	24-12-2021	Feedback verwerken
11-1-2022	31-12-2021	Feedback verwerken

Tabel 1 Revisie historie

Distributielijst

In onderstaande tabel is genoteerd wanneer het document met welke personen is gedeeld.

Naam	Datum	Versie
Joost Overkamp	30-9-2021	V0.1
Joost Overkamp	30-9-2021	V0.2
Theo Lansink	1-10-2021	V0.3
Joost Overkamp	7-10-2021	V0.4
Theo Lansink	22-10-2021	V0.5
Joost Overkamp	4-11-2021	V0.6
Joost Overkamp	11-11-2021	V0.7
Theo Lansink	12-11-2021	V0.8
Joost Overkamp	18-11-2021	V0.9
Theo Lansink	24-11-2021	V1.0
Joost Overkamp	25-11-2021	V1.1
Theo Lansink	26-11-2021	V1.2
Joost Overkamp	2-12-2021	V1.3
Theo Lansink en Joost Overkamp	7-12-2021	V1.6
Joost Overkamp	16-12-2021	V1.7
Saxion	19-12-2021	V1.8
Joost Overkamp	30-12-2021	V1.9
Bart Brevink	3-1-2022	V2.0
Joost Overkamp	6-1-2022	V2.1
Theo Lansink	7-1-2022	V2.1
Joost Overkamp	13-1-2022	V2.2
Saxion	16-1-2022	V3.0

Tabel 2 Distributie beheer

Inhoudsopgave

Tabellenlijst

Figurenlijst

Afkortingen

Tijdens het lezen van dit document zullen er veel afkortingen voorbijkomen. De meeste zullen bekend zijn voor lezers van het document, maar sommige kunnen nieuw zijn. Om het lezen van dit document eenvoudiger te maken zijn alle voorkomende afkortingen in de tabel hieronder genoemd en uitgelegd.

APA= American Psychological Association	MCAS= Microsoft Cloud App Security
AVG= Algemene Verordening Gegevensbescherming	MFA= Multi Factor Authenticatie
CASB= Cloud Access Security Broker	MSP= Managed Service Provider
CNAPP= Cloud Native Application Protection Platform	MSSP= Managed Security Service Provider
CSPM= Cloud Security Posture Management	NGF= Next Generation Firewall
CV= Curriculum Vitae	PAM= Privileged Access Management
CWPP= Cloud Workload Protection Platform	RBI= Remote Browser Isolation
DLP= Data Loss Prevention	SaaS= Software as a Service
EDLP= Enterprise Data Loss Prevention	SASE= Secure Access Service Edge
FG= Functionaris Gegevensbescherming	SPM= SaaS Management Platforms
IAM= Identity and Access Management	SWG= Secure Web Gateway
IDLP= Integrated Data Loss Prevention	USP= Unique Selling Point
IDP= Identity Provider	WAF= Web Application Firewall

Tabel 3 Afkortingen

3. Inleiding

Dit document is gecreëerd door Mike Van kan en is in samenwerking met PCI IT uitgewerkt tijdens zijn afstudeeropdracht bij PCI IT.

Het doel van dit project is dat PCI IT namens haar klanten meer grip gaat krijgen op de datastromen in SaaS-oplossingen. Om dit doel te halen, zullen er tijdens dit project meerdere fases worden doorlopen om een goed onderbouwde oplossing te presenteren. Dit zal dan als een generieke oplossing aan PCI IT gepresenteerd worden in de vorm van documentatie. De beschrijving van de implementatie zal vrij generiek zijn. Dit is het geval omdat elke klant van PCI IT verschillend is en de toepassing van de oplossing die dit project oplevert, zal dus ook in elke klantomgeving anders geconfigureerd moeten worden. In de implementatie zal hier dus rekening mee worden gehouden.

In dit document staan de bevindingen van het project en zijn zaken zoals de opbouw, het onderzoek, de interviews, de afwegingen, de conclusie, mijn reflectie en de bijlagen van dit project genoteerd.

4. Achtergrond

Dit hoofdstuk behandelt de probleemstelling en geeft achtergrondinformatie over PCI IT en haar bedrijfsvoering. De informatie in dit hoofdstuk is verkregen via diverse interviews met medewerkers van PCI IT en via bureauonderzoek. Deze informatie is vervolgens geanalyseerd.

4.1. Achtergrond PCI IT

PCI Nederland is een grote dienstverlener met een hoofdvestiging in Lijnden en andere vestigingen in Apeldoorn, Arnhem, Goes, Haaksbergen, Rotterdam en Utrecht. PCI Nederland levert diverse soorten ICT-oplossingen aan bedrijven, zoals Cloud-oplossingen, AV-oplossingen, print-oplossingen en informatiemanagement. Het bedrijf beschikt over ongeveer 500 FTE medewerkers waarvan er ongeveer 150 bij PCI IT werken. PCI IT is een business unit van PCI Nederland welke IT-gerelateerde oplossingen aanbiedt aan klanten. Dit zijn zaken zoals printeroplossingen, audiovisuele-oplossingen of, zoals relevant voor dit project, on-premise en Cloud gebaseerde klantomgevingen. De verschillende afdelingen binnen PCI IT staan genoteerd in het organogram welke als bijlage bij dit document is bijgevoegd.

4.2. Probleemstelling

Het probleem dat PCI IT ervaart, is dat er geen volledige beheersbaarheid is van de SaaS-applicaties. De doelstelling van dit afstudeerproject is dan ook om meer overzicht en controle te creëren in de beheerde en onbeheerde SaaS-oplossingen die in gebruik zijn bij de klanten van PCI IT.

4.2.1. Oorzaak probleemstelling

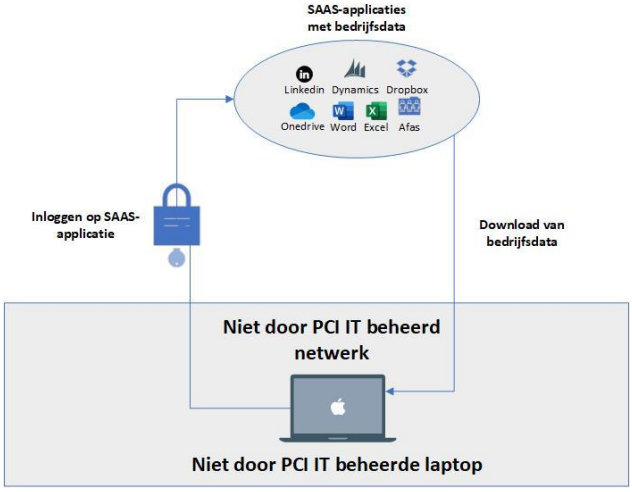
In de klantomgevingen van PCI IT haar klanten wordt in een groeiende mate gebruik gemaakt van Software As A Service (SaaS). SaaS is een alternatief voor het lokaal configureren en beheren van applicaties. Bij een SaaS-oplossing wordt de applicatie afgenomen van een bedrijf. Dit bedrijf draagt vervolgens zorg voor alle IT-infrastructuur welke de SaaS-oplossing nodig heeft om te functioneren zoals hardware, licenties en onderhoud van de software (Salesforce, z.d.). Bij de klanten van PCI IT is het gebruik van SaaS-applicaties ten koste van on-premise gehoste software ook toegenomen. Deze SaaS-applicaties zijn oplossingen zoals OneDrive of SharePoint welke een file share vervangt of Afas Online welke een lokale Afas installatie vervangt.

Deze SaaS-oplossingen van klanten hebben een grote hoeveelheid bedrijfsdata waar aan het begin van het afstuderen weinig tot geen controle op is. Mede doordat de applicaties die tegenwoordig worden gebruikt SaaS-oplossingen zijn, is een groot deel van het inzicht en de controle verdwenen. Deze SaaS-applicaties kunnen namelijk buiten dit genoemde bedrijfsnetwerk vanaf elk apparaat benaderd worden. Bij de aanvang van dit project is er enkel beperkte controle aanwezig tijdens de inlog en hierna is het onduidelijk wie er een actie onderneemt, welke actie er precies ondernomen wordt en vanaf welke locatie dat gebeurt.

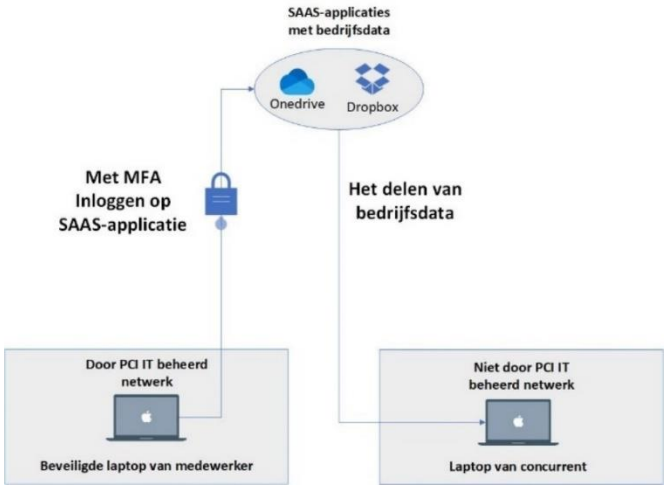
Voor de opkomst van SaaS-applicaties was er controle voordat een persoon fysiek een bedrijfsgebouw kon betreden. Hierna moest deze persoon inloggen op een workstation. Dit workstation was voorzien van een BIOS die bijvoorbeeld geen USB-opslag apparaten toeliet. Daarna opende de gebruiker dan een applicatie welke verbinding maakte met een server op het beveiligde bedrijfsnetwerk en als laatste was de server dan weer volledig in beheer van PCI IT. In de huidige situatie kan een medewerker van een klant bijvoorbeeld inloggen vanaf zijn iPhone op office365 en mails met gevoelige offertes bekijken of kan een HR-medewerker op vakantie met de familietablet inloggen op AFAS en Cv's en andere gevoelige informatie inzien. Dit is in theorie geen probleem maar als de medewerker kwade bedoelingen heeft dan is dit zeer onwenselijk, omdat het dan gebeurt op een apparaat waar geen zicht op is.

Voor alle klanten zijn er dus wel oplossingen die ervoor zorgen dat alleen de juiste gebruiker na verificatie toegang heeft tot de SaaS-applicaties, maar na de beveiligde login zijn het overzicht en de controle weg. Dit zorgt ervoor dat PCI IT zich afvraagt of er oplossingen bestaan die het mogelijk maken dat PCI IT – indien managed aangeboden – of de klant zelf – indien als project aangeboden - meer controle kunnen uitoefenen op de datastromen in de SaaS-oplossingen. Deze datastromen zijn acties van gebruikers die interactie hebben met de data die opgeslagen staan in de SaaS-applicaties. Het uitoefenen van meer controle zal uiteindelijk onderdeel van een dienst kunnen zijn die PCI IT aan haar klanten aanbiedt.

Om duidelijker te maken waar het probleem in de huidige situatie ligt, zijn er enkele tekeningen gemaakt. De eerste situatie, in figuur 1, gaat over een werknemer die met kwade bedoelingen tientallen Cv's of andere bedrijfsdata downloadt. In de huidige situatie zal PCI IT, door het gebrek aan inzichtelijkheid, het downloaden door de werknemer met slechte bedoelingen niet opmerken en daardoor kan PCI IT er dus niet op acteren. De tweede voorbeeldsituatie, getekend in figuur 2, is een werknemer die een map met bedrijfsinformatie via OneDrive deelt met een concurrent.



Figuur 1 Downloaden bedrijfsdata



Figuur 2 Delen bedrijfsinformatie

De beide problemen die worden geschetst in de voorbeeldsituaties zijn niet zichtbaar voor PCI IT of het bedrijf zelf. Aangezien het niet inzichtelijk is voor PCI IT of het bedrijf of het ongeoorloofd delen van bedrijfsdata plaats vindt, zullen er geen maatregelen worden genomen als een dergelijke situatie zich voordoet. In de toekomstige situatie zullen ongebruikelijke acties geregistreerd moeten worden en zal de gekozen oplossing automatische acties moeten kunnen ondernemen op ongewenst gedrag.

Het tweede probleem dat PCI IT ervaart, is dat er geen inzicht is in het gebruik van SaaS-applicaties die onder Schaduw IT vallen. Schaduw IT zijn alle hard- of software middelen welke gebruikt worden om werkzaamheden voor het bedrijf te verrichten, die niet door de werkgever zijn geleverd (Blanken, 2020). Doordat dit niet inzichtelijk is kunnen er diensten worden gebruikt om bedrijfsdata op te slaan waar PCI IT of haar klant geen controle over heeft.

De wens van PCI IT is dus tweedelig. Ten eerste wil PCI IT inzicht en de mogelijkheid om te sturen in de acties van de gebruikers van beheerde SaaS-applicaties en ten tweede wil PCI IT het gebruik van SaaS-applicaties die onder Schaduw IT vallen zichtbaar hebben zodat zij hierop kan acteren.

5. Hoofd- en deelvragen

Om de probleemstelling zoals in het vorige hoofdstuk beschreven is op te lossen, zijn er in samenwerking met PCI IT één hoofdvraag en enkele deelvragen bedacht. Door het beantwoorden van deze deelvragen wordt uiteindelijk de hoofdvraag beantwoord.

5.1. Hoofdvraag

De hoofdvraag van dit afstudeerproject is als volgt: “Hoe kan PCI IT haar klanten een oplossing bieden die de toegang tot data in SaaS-systemen controleert en restricties op de toegang kan toepassen?”. Deze hoofdvraag is opgebroken in enkele kleinere deelvragen die allemaal hun eigen deel van de hoofdvraag beantwoorden. Deze deelvragen werken toe naar een goed onderbouwd antwoord op de hoofdvraag. Hieronder zijn de deelvragen samen met een korte omschrijving genoteerd.

5.2. Deelvragen

De deelvragen van dit project zijn hieronder genoteerd. De deelvragen zijn grotendeels genoteerd in de volgorde waarin zij ook beantwoord gaan worden.

Van welke SaaS-applicaties maken klanten van PCI IT gebruik?

In deze deelvraag zal onderzocht worden welke SaaS-applicaties veelal gebruikt worden binnen de organisaties van klanten van PCI IT. Deze informatie kan later gebruikt worden om een oplossing te kiezen welke compatibel is met de gebruikte SaaS-applicaties. Deze informatie zal verzameld worden aan de hand van interviews met medewerkers op relevante afdelingen binnen PCI IT. Dit proces en de informatie voortkomend uit dit proces zullen genoteerd worden in het scriptieverslag.

Wat voor data staat er in de SaaS-applicaties die door klanten van PCI worden gebruikt?

In deze deelvraag zal geïnventariseerd worden wat voor data klanten voornamelijk opgeslagen hebben in de verschillende SaaS-applicaties welke zij gebruiken. Deze data en hoe deze applicaties dus worden gebruikt kan dan in de komende deelvragen worden meegenomen. Aan de hand van deze informatie zal er dan beslist worden in welke mate het gebruik van deze data gecontroleerd kan en moet worden. Dit zal te maken hebben met de vertrouwelijkheid van de data. Er zal bijvoorbeeld onderscheid gemaakt worden in financiële informatie, personeelsdata of aantekeningen.

Welke eisen heeft PCI IT met betrekking tot databeveiliging voor SaaS-applicaties?

In deze deelvraag zal door middel van interviews onderzocht worden wat de visie van PCI IT is als het gaat om de beveiliging en het inzichtelijk maken van het gebruik van SaaS-applicaties van haar klanten. In deze deelvraag zal ook genoteerd worden aan welke wetten en regelgevingen verschillende klanten moeten voldoen. Dit moet genoteerd worden om hier rekening mee te houden in het onderzoek. Op basis hiervan zullen requirements gegenereerd worden die in de komende deelvragen gebruikt worden om een oplossing te kiezen.

Wat is de mate van invloed die een klant, met of zonder dienstverlener, kan uitoefenen op een SaaS-applicatie?

In deze deelvraag zal er gekeken worden welke mogelijkheden klanten standaard hebben binnen de genoteerde SaaS-applicaties om invloed uit te oefenen op de SaaS-systemen om de datastromen te controleren of te beveiligen. Dit zal dan inhouden dat er voor de meest gebruikte SaaS-applicaties wordt gekeken wat de mogelijkheden zijn die in het pakket zitten. Het gaat in deze deelvraag dus alleen om de opties die standaard al in het pakket aanwezig zijn.

Welke oplossingen gebruikt PCI IT op dit moment om de data in door klanten gebruikte SaaS-oplossingen te beveiligen en welke functies biedt dat PCI IT en haar klanten?

In deze deelvraag zal door middel van interviews geïnventariseerd worden welke oplossingen er bij PCI IT aanwezig zijn op het gebied van SaaS-data monitoring en beveiliging. Bij elke dienst zal genoteerd worden wat deze dienst voor toegevoegde waarde heeft voor PCI IT. Aan het einde van deze deelvraag zal door het gebruik van een multicriteria-analyse voor PCI IT en voor mij duidelijk zijn welke gebieden afgedicht zijn met de bestaande oplossingen en welke gebieden nog “bloot” liggen en in de volgende deelvraag gebruikt kunnen worden.

Wat voor producttype zoekt PCI IT op basis van de reeds beantwoorde deelvragen?

Op basis van de eerder verzamelde requirements zal er een beeld geschetst worden van waar er in de datastroom geen overzicht of controle meer over de data is. Daarnaast zal er duidelijk genoteerd worden wat de visie van PCI IT voor de toekomst is. In deze deelvraag kan dan, aan de hand van literatuuronderzoek, bepaald worden wat de specifieke overkoepelende naam is voor het producttype welke PCI IT zoekt. Deze term kan in de volgende deelvraag gebruikt worden om de scope te beperken en alleen relevante oplossingen op te leveren.

Welke beveiliging en controle oplossingen zijn er op de markt die voldoen aan de eisen van PCI IT en welke past het beste bij PCI IT?

In deze deelvraag zal er door middel van literatuuronderzoek gekeken worden wat voor oplossingen er op de markt zijn die het probleem uit de hoofvraag kunnen oplossen. Hier zal dan bijvoorbeeld worden gekeken naar wat voor product het is, wat de mogelijkheden van het beheer zijn en waar deze zullen liggen. Hierbij zal rekening worden gehouden met de verzamelde requirements van de vorige deelvragen. Aan het eind van deze deelvraag is het dus duidelijk welke pakketten er bestaan, welke het best bij PCI IT past, waar het beheer zal liggen en wat de mogelijkheden binnen de software zijn.

Hoe zouden toekomstige klantsystemen gebruik kunnen maken van de gekozen oplossing en is dit met terugwerkende kracht toe te passen op bestaande systemen?

In deze deelvraag zal op basis van de gekozen oplossing een functioneel en technisch ontwerp worden gemaakt voor toekomstige systemen. Nadat dit gebeurd is, zal getracht worden om een plan te maken om bestaande omgevingen gebruik te laten maken van de gekozen oplossing, zodat het overzicht en de controle hier ook beschikbaar in zijn.

6. Gekozen methodes

In dit project wordt er gebruik gemaakt van verschillende methodes om tijdens het project gestructureerd te werk te gaan, informatie te verzamelen en informatie te verwerken. De gebruikte methodes zijn allemaal in de bijlage genoemd met een korte uitleg en een toelichting op hoe deze methodes gebruikt zijn binnen dit project. Daarnaast wordt per hoofdstuk in de tekst genoemd welke methodes er in dat hoofdstuk of onderdeel gebruikt zijn.

Tijdens dit project is er hoofdzakelijk gebruik gemaakt van design thinking. Aan de hand van enkele van de fases van design thinking is er stelselmatig gewerkt vanaf het in kaart brengen van de probleemstelling tot aan het creëren van een ontwerp. Hierna is PCI IT geadviseerd over verdere implementatie. Deze fases zijn empathize, define en ideate. De laatste twee fases van design thinking zijn niet gebruikt omdat met PCI IT afgesproken is dat er geen prototype gecreëerd wordt. Dit zou volgens de betrokken partijen namelijk niet haalbaar en dus wenselijk zijn in de tijd die voor het project staat.

7. Empathize

In dit eerste hoofdstuk van design thinking is er onderzocht hoe het probleem binnen de organisatie van PCI IT leeft en wat verschillende werknemers van het probleem meekrijgen. Dit is gedaan aan de hand van verschillende methodes zoals interviews, bureauonderzoek, de 6 W-vragen en een contextanalyse.

7.1. Stakeholderanalyse

In dit hoofdstuk is onderzocht wie de stakeholders binnen dit project zijn, wat hun professionele mening over de probleemstelling is en wat er in de organisatie en daarbuiten speelt.

7.1.1. Stakeholders

Tijdens de startup van het project is de tijd genomen om mensen binnen het bedrijf te leren kennen en bekend te worden met de bedrijfsprocessen. Deze kennis is daarna gebruikt om te bepalen wie er in dit project de stakeholders zijn en wie er bij dit project betrokken zijn. Nadat dit bepaald was, zijn er formele en informele gesprekken gevoerd met deze personen om de oorzaak van het probleem, de probleemstelling en de wensen duidelijk in beeld te krijgen. De stakeholders en hun rol zijn hieronder kort beschreven.

Joost Overkamp

Joost is de teamlead in het team Identity & Collaboration en hij is mijn aangewezen begeleider vanuit PCI IT. Hij heeft door zijn werkervaring kennis over omgevingen, securityoplossingen, vraagstukken bij klanten, vraagstukken in de organisatie en informatie over de bedrijfsvoering zelf.

Bart Brevink

Bart Brevink is Technical Field Service Manager bij PCI IT. Hij is verantwoordelijk voor de verschillende IT-gerelateerde teams in de organisatie. Zijn positie in het bedrijf zorgt ervoor dat hij op de hoogte is van de wensen van PCI IT en haar klanten. Daarnaast zal hij in zijn managementrol ook zaken over de bedrijfsdoelstellingen die in dit project van belang zijn, kunnen vertellen. Om de positie van Bart en andere personen binnen PCI IT duidelijker te maken is in de bijlage een Organigram geplaatst.

Dennis Schutten

Dennis Schutten is een networking en security expert bij PCI IT. Hij heeft kennis over de gebruikte securityproducten, leveranciers en de wensen van klanten gerelateerd aan securityoplossingen. Dit alles is belangrijke informatie om de randvoorwaarden waar het product aan moet voldoen duidelijk te krijgen.

Marc Schuurman

Marc Schuurman is een systems engineer bij PCI IT. Hij heeft ervaring met meerdere klanten en kan dus vertellen wat er speelt in de gemiddelde klantomgeving. Daarnaast kan hij verdere achtergrondinformatie verstrekken. Deze extra informatie is belangrijk om te begrijpen hoe het beschreven probleem leeft in de organisatie en bij klanten.

7.1.2. Stakeholder Matrix

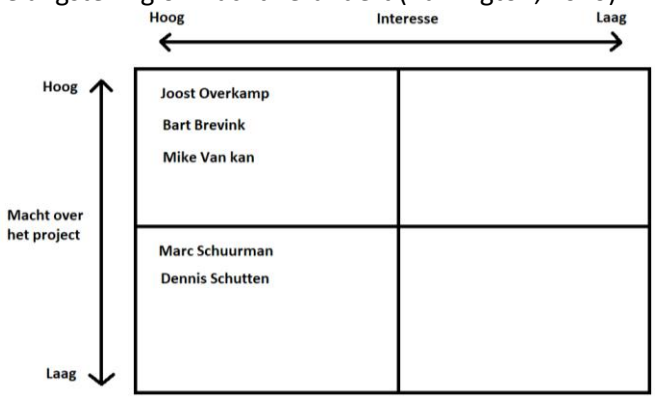
Om de interesse en de macht over het project van de genoemde stakeholders in kaart te brengen, is er gebruik gemaakt van de matrix van Mendelow. De stakeholders zijn genoteerd in één van de vier vierkanten. De vierkanten krijgen een betekenis op basis van interesse en macht. Dit is hieronder uitgelegd.

Mensen met veel macht en veel interesse (sterk in de gaten houden): het streven is deze mensen volledig bij het project te betrekken.

Mensen met veel macht en weinig interesse (tevreden houden): genoeg moeite doen om deze mensen tevreden en op de hoogte te houden, maar niet zo veel dat ze verveeld raken door het project.

Mensen met weinig macht en veel belangstelling (geïnformeerd houden): deze mensen zullen voldoende geïnformeerd worden. Deze personen kunnen ook helpen bij het aanwijzen van gebieden die voor verbetering vatbaar zijn of die over het hoofd zijn gezien.

Mensen met weinig macht en minder belangstelling (monitoren): deze personen moeten niet verveeld worden met overdadige communicatie, maar het moet wel in de gaten gehouden worden of hun belangstelling of macht verandert (Barrington, 2020).



Figuur 3 Matrix van Mendelow

7.1.2.1. Conclusie stakeholders Matrix

De stakeholders die het meest betrokken zijn bij dit project zijn Joost Overkamp, Bart Brevink en Mike Van kan. Bart Brevink heeft als Technical Field Service Manager een hoog niveau van belang en interesse in dit project omdat hij het resultaat van dit project gaat gebruiken om de positie van PCI IT in de markt te versterken. Joost Overkamp heeft een hoge interesse in dit project omdat hij de bedrijfsbegeleider in dit project is. Gezien het project door Mike Van kan wordt uitgevoerd, is zijn belang en interesse in dit project ook erg groot. De andere stakeholders, genaamd Marc Schuurman en Dennis Schutten, zijn betrokken bij het project en hebben interesse in het project aangezien zij personen zijn die na het uitvoeren van dit project in aanraking komen en moeten werken met het gekozen product.

7.1.3. Empathy maps

De stakeholders van dit project zijn formeel of informeel geïnterviewd om hun standpunten, opmerkingen en verwachtingen van het project duidelijk te krijgen. De informatie welke uit deze interviews is verkregen, is verwerkt in empathy maps welke de gedachte en gevoelens van deze personen reflecteren. Empathy maps worden gebruikt om de gedachten en gevoelens van elk van de belanghebbenden te achterhalen om een beter idee te krijgen van de problemen waar elke stakeholder mee te maken heeft. Alle stakeholders hebben een eigen empathy kaart omdat elke stakeholder die zal worden geïnterviewd zijn eigen pijnpunten en voordelen kan hebben. Deze moeten allemaal in de empathy maps worden opgenomen. Dit is het geval omdat de stakholders verschillende functies hebben binnen het bedrijf en omdat ze dingen anders ervaren. Het doel van de empathy maps is om zoveel mogelijk informatie te verzamelen en om een oplossing te bieden aan alle medewerkers die in contact staan met het probleem. Door een zo groot mogelijk aantal stakeholders tevreden te stellen, zal het project zelf een grotere kans hebben om te slagen. De volledige versies van de empathy maps zijn in de bijlage geplaatst.

7.1.3.1. Conclusie empathy maps

De conclusie welke kan worden getrokken uit de empathy maps is dat de stakeholders, welke werkzaam zijn bij PCI IT, opzoek zijn naar security gerelateerde producten voor de klanten van PCI IT en in het bijzonder een product om SaaS-gebruik te monitoren en inzicht te hebben in het gebruik van SaaS gerelateerde schaduw IT. Dit komt voort uit de vraag vanuit klanten, vanuit de behoefte te blijven groeien in verschillende sectoren, het groeiende aantal beveiligingsrisico's en de behoefte om een Managed Security Services Provider (MSSP) positie in te kunnen nemen in de toekomst. Een MSSP draagt zorg voor de gedeeltelijke of complete security bij een klant (KPN, 2020). Dit betekent dat de MSSP dan zorg draagt voor het implementeren, onderhouden en afhandelen van meldingen vanuit producten zoals een managed firewall, virusbeveiliging, Security Information and Event Management, Intrusion Detection System en andere security gerelateerde producten. In meerdere empathy maps komt ook naar voren dat de stakeholders het SaaS-gebruik bij klanten de afgelopen jaren hebben zien groeien en dat ze meer grip willen hebben op de beheerde en onbeheerde SaaS-applicaties die aanwezig zijn in klantomgevingen.

7.2. Contextanalyse

De contextanalyse wordt gebruikt om in te zien welke factoren invloed hebben op PCI IT en dit project en of er randvoorwaarden aanwezig zijn waar bij de uitvoering van dit project rekening mee moet worden gehouden. Hierbij wordt gekeken naar het macro-, meso-, en microniveau. De macro-analyse richt zich op ontwikkelingen van het bedrijfsleven en de algemene huidige markt in Nederland, de meso-analyse kijkt naar de IT-sector in Nederland en de micro-analyse onderzoekt interne ontwikkelingen binnen PCI IT. De conclusies van deze analyse staan hieronder genoteerd en de volledige analyse is terug te vinden in de bijlages.

7.2.1. Conclusie contextanalyse

De conclusie die uit de macro, meso en micro analyse kan worden genomen is dat PCI IT een goede kans heeft om de oplossing welke uit dit project komt op de markt te brengen. De voornaamste redenen waarom de slagingskans groot is, zijn dat de vraag vanuit de markt voor securityproducten erg groot is en dat er een de stijging van het gebruik van SaaS-applicaties is. Er zijn echter wel enkele zaken waar PCI IT rekening mee zal moeten houden, wil het op de markt brengen van een oplossing welke in dit project gezocht wordt, slagen. Deze punten zijn hieronder genoemd met een korte uitleg over waarom het belangrijk is om hier rekening mee te houden. Randvoorwaarden die uit de contextanalyse en andere delen van dit project zijn gekomen, zijn genoemd in "Randvoorwaarden project".

7.2.1.1. Personeel

Er zijn de afgelopen jaren wel mensen aangenomen bij PCI IT, maar er is alsnog vraag naar meer personeel. Dit wordt een belangrijk punt als er een MSSP-positie in de markt wordt aangeboden. Dit zal er namelijk in resulteren dat de bestaande werknemers tijd moeten spenderen om de aangeboden dienst te leren kennen, deze te verkopen, deze te implementeren en deze bij te houden voor de klanten. De tijd welke hieraan besteed gaat worden zal ten koste gaan van de tijd welke zij nu aan andere werkzaamheden besteden.

7.2.1.2. Concurrentie

Door de grote vraag naar security gerelateerde diensten zijn er de afgelopen jaren veel managed serviceproviders bijgekomen. Dit zorgt ervoor dat de klant een sterke positie heeft om te onderhandelen en weg te lopen naar de concurrentie. Indien PCI IT de markt als MSSP betreedt, zal het de diensten welke hij aanbiedt ofwel met een scherpe prijs moeten neerzetten ofwel een andere manier nodig hebben om zichzelf van de concurrentie te onderscheiden.

7.2.1.3. Snel bewegende markt

Dit punt is een punt dat niet enkel van toepassing is op dit project maar op elk gebied van de IT. Dit komt doordat de ontwikkelingen in de IT vrij snel zijn en de kennis welke een bedrijf vergaart dus ook snel verouderd kan zijn. Hierom moet PCI IT na de implementatie letten op trends in de markt, zodat ze mee gaat met kleine of grote veranderingen en daardoor haar verkregen positie niet verloren laat gaan.

7.3. Randvoorwaarden project

Uit het onderzoek en gesprekken met medewerkers van PCI IT zijn verschillende randvoorwaarden gekomen. Het is belangrijk om deze randvoorwaarden duidelijk te hebben, aangezien de gemaakte keuzes voor het producttype en het uiteindelijke product beïnvloed worden door de randvoorwaarden. Al deze randvoorwaarden zullen een code bevatten welke later gebruikt wordt om naar deze randvoorwaarden te refereren.

Uit de gesprekken die gevoerd zijn met Joost, Dennis, Bart, Marc en Marc is naar voren gekomen welke soorten SaaS-applicaties bij de klanten van PCI IT voorkomen. Dit zijn vrij veel verschillende soorten, aangezien het klantenbestand van PCI IT zeer divers is. Er is besproken welke SaaS-applicaties in dit project prioriteit hebben, namelijk Office365, Dynamics365, Exact Online en AFAS Online. Deze applicaties moeten gemonitord worden met de oplossing welke in dit project gekozen gaat worden. (R01)

Een andere randvoorwaarde komt voort uit het feit dat PCI IT Microsoft-producten, zoals Office365 en Defender, levert aan haar klanten. In de vorige paragraaf is al benoemd dat de nieuwe applicatie met een aantal Microsoftproducten moet werken, maar de nieuwe oplossing zal, indien mogelijk, ook gebruik kunnen maken van de reeds bestaande licenties. Daarnaast is er een bias aanwezig voor een Microsoftproduct, aangezien er veelal Microsoftdiensten aan klanten worden geleverd. (R02)

De hardware die aan klanten wordt geleverd, is ook geanalyseerd en genoteerd. Deze merken zijn hieronder genoteerd om op een later moment in dit project te kijken of de genoemde hardware leveranciers compatibel zijn en meerwaarde kunnen bieden aan de onderzochte oplossingen. Als er voor correcte werking van het gekozen product gebruik moet worden gemaakt van oplossingen van derden, dan geniet het de voorkeur om gebruik te maken van bestaande oplossingen.

- Barracuda
    - Diverse netwerkapparatuur
- Palo Alto
    - Diverse netwerkapparatuur
- HPE
    - Servers
    - Diverse netwerkapparatuur
    - Workstations
- Secureme2
    - Sam (netwerkanalyse) (R03)

De laatste technische randvoorwaarde is dat de gekozen oplossing meer voordelen aan PCI IT moet bieden dan de huidige DLP-oplossing. Op het moment van schrijven heeft PCI IT bij Microsoftdiensten een Cloud-service-provider-native DLP (nader verklaard in DLP) in gebruik. (R04)

Naast de soft- en hardware randvoorwaarden moet er ook rekening gehouden worden met een drietal minder technische randvoorwaarden. De eerste is dat de prijs van het product dat uit dit project zal komen marktconform geprijsd moet zijn. Omdat er nog geen zicht is op het type product dat gekozen gaat worden en dus de prijzen ervan is er op dit moment nog geen prijs te bepalen. De nieuwe oplossing moet zoals gezegd echter marktconform geprijsd zijn. (R05)

De op één na laatste randvoorwaarde is dat, indien er data wordt opgeslagen, deze wordt opgeslagen binnen de EU om te blijven voldoen aan de AVG. (R06)

Als laatste is er uit gesprekken gebleken dat PCI IT opzoek is naar één enkele oplossing welke alle eigenschappen heeft die PCI IT wenst. (R07)

8. Define

In dit hoofdstuk wordt de informatie uit de empathy fase gedestilleerd tot het kernprobleem van dit project. Dit zal gebeuren door het opstellen van user stories en requirements, die dan een duidelijk traceerbaar beeld geven van wat er in dit project opgelost moet worden.

8.1. User stories

In dit stuk zijn de user stories genoteerd van alle stakeholders die binnen dit project aanwezig zijn. Aangezien de gedachtes binnen PCI IT over dit probleem redelijk unaniem zijn gebleken, vindt er overlapping plaats tussen verschillende user stories en zijn sommige user stories dus gecombineerd genoteerd.

Uit de formele en informele interviews welke gevoerd zijn met de verschillende stakeholders zijn er user stories gedefinieerd. Deze user stories geven aan wat de verschillende personen voor wensen hebben in dit project. Deze user stories zijn bedoeld om traceerbaar te maken waar een requirement vandaan komt. Bij elke requirement zal de code welke bij de user story genoemd staat genoteerd worden.

8.1.1. Gedeelde user stories

- Als Technical field Service Manager, Teamlead Identity & Collaboration, ICT networking expert en ICT Systems Engineer willen wij controle over datastromen in SaaS-applicaties bij klantomgevingen. (US1)
- Als Technical field Service Manager, Teamlead Identity & Collaboration, ICT networking expert en ICT Systems Engineer willen wij inzicht in datastromen in SaaS-applicaties bij klantomgevingen. (US2)
- Als Technical field Service Manager, Teamlead Identity & Collaboration, ICT networking expert en ICT Systems Engineer willen wij voorkomen dat door meerdere oorzaken steeds meer werknemers van klanten gebruik maken van IT-middelen die niet door het bedrijf verschaft zijn. (US3)
- Als Technical field Service Manager, Teamlead Identity & Collaboration, ICT networking expert en ICT Systems Engineer willen wij in de toekomst een portfolio hebben welke het mogelijk maakt dat PCI IT als MSSP kan fungeren. (US4)
- Als Technical field Service Manager, Teamlead Identity & Collaboration, ICT networking expert en ICT Systems Engineer willen wij voorkomen dat wij klanten mislopen doordat er bij PCI IT geen portfolio aanwezig is en concurrenten dit wel aanbieden. (US5)

8.1.2. User stories van Bart Brevink

- Als Technical field Service Manager wil ik dat het gebruik van schaduw IT in relatie tot SaaS in klantomgevingen zichtbaar wordt. (US6)

8.1.3. User stories van Joost Overkamp

- Als Teamlead Identity & Collaboration wil ik dat de nieuwe oplossing meer zaken kan afvangen dan de op dit moment gebruikte DLP. (US7)
- Als Teamlead Identity & Collaboration wil ik dat de nieuwe oplossing marktconform geprijsd is. (US8)

8.1.4. User stories van Marc Schuurman

- Als ICT Systems Engineer wil ik dat de medewerkers van klanten meer inzicht hebben in de gevolgen van hun IT-gerelateerde acties. (US9)

8.2. Requirements

In het vorige stuk zijn de user stories per stakeholder gedefinieerd. Deze worden hier verwerkt tot requirements. Deze requirements hebben allemaal een code aangewezen gekregen welke gebruikt wordt om op een later moment naar de requirement te verwijzen. De code is opgebouwd uit vier onderdelen: de userstory waar deze vandaan komt, of hij functioneel of non-functioneel is, of het een business, systeem of user requirement is en als laatst zal er staan of het een must, should, could of would requirement is. Dit alles gecombineerd zal een code zoals deze geven: US1-F-S1-M.

8.2.1. Requirements:

Code:	US1-NF-S1-M	**Type:**	Systeem
MoSCoW:	Must	**(Non-) Functioneel**	Non-functioneel
Requirement	De nieuwe oplossing moet overweg kunnen met de SaaS-applicaties van de klanten van PCI IT.		

Code:	US1-F-S2-M	**Type:**	Systeem
MoSCoW:	Must	**(Non-) Functioneel**	Functioneel
Requirement	De nieuwe oplossing moet automatisch acties kunnen uitvoeren aan de hand van aangemaakte thresholds in SaaS-applicaties.		

Code:	US1-NF-S3-M	**Type:**	Systeem
MoSCoW:	Must	**(Non-) Functioneel**	Non-functioneel
Requirement	De nieuwe oplossing moet controle kunnen uitoefenen over de datastromen in beheerde SaaS-applicaties van klanten.		

Code:	US2-NF-S4-M	**Type:**	Systeem
MoSCoW:	Must	**(Non-) Functioneel**	Non-functioneel
Requirement	De nieuwe oplossing moet inzicht geven in de acties van medewerkers van klanten in beheerde SaaS-applicaties.		

Code:	US3-NF-S5-M	**Type:**	Systeem
MoSCoW:	Must	**(Non-) Functioneel**	Non-functioneel
Requirement	De nieuwe oplossing moet onderscheid kunnen maken tussen apparaten en aan de hand hiervan rechten toekennen.		

Code:	US3-NF-S6-M	**Type:**	Systeem
MoSCoW:	Must	**(Non-) Functioneel**	Non-functioneel
Requirement	De nieuwe oplossing moet onderscheid kunnen maken tussen door het bedrijf uitgegeven applicaties en schaduw IT.		

Code:	US3-NF-S7-M	**Type:**	Systeem
MoSCoW:	Must	**(Non-) Functioneel**	Non-functioneel
Requirement	De nieuwe oplossing mag niet afhankelijk zijn van de locatie van de eindgebruiker.		

Code:	US3-NF-S8-M	**Type:**	Systeem
MoSCoW:	Must	**(Non-) Functioneel**	Non-functioneel
Requirement	De nieuwe oplossing zal moeten werken met beheerde apparaten van klanten.		

Code:	US3-NF-S9-M	**Type:**	Systeem
MoSCoW:	Must	**(Non-) Functioneel**	Non-functioneel
Requirement	De nieuwe oplossing zal moeten werken met onbeheerde apparaten van klanten.		

Code:	US6-NF-S10-M	**Type:**	Systeem
MoSCoW:	Must	**(Non-) Functioneel**	Non-functioneel
Requirement	De nieuwe oplossing moet inzicht kunnen geven in het gebruik van SaaS-applicaties welke onder schaduw IT vallen bij klanten van PCI IT.		

Code:	US7-F-S11-M	**Type:**	Systeem
MoSCoW:	Must	**(Non-) Functioneel**	Functioneel
Requirement	De nieuwe oplossing moet meer mogelijkheden bieden dan wat de Data Loss Prevention oplossing aan het begin van het project biedt aan PCI IT.		

Code:	US9-NF-B1-W	**Type:**	Business
MoSCoW:	Would	**(Non-) Functioneel**	Non-functioneel
Requirement	Het zou fijn zijn als er aan het eind van het project een document met richtlijnen voor medewerkers van klanten opgeleverd wordt die richtlijnen voor veilig gebruik van bedrijf data inzichtelijk maakt.		

8.3. Visie van PCI IT

Uit de interviews, de 6 W-vragen en andere analysemethoden volgt de volgende conclusie. De algemene wens van PCI IT is om de positie van een MSSP in te nemen en hiermee bestaande en nieuwe klanten MSSP-diensten aan te kunnen bieden. Dit project zal in een deel van die behoefte kunnen voorzien, aangezien dit project gericht is op een specifiek vraagstuk dat deel uitmaakt van deze visie.

In dit project is PCI IT op zoek naar een product dat de datastromen in de beheerde SaaS-applicaties inzichtelijk kan maken en kan controleren. Deze acties in SaaS-applicaties zullen gemonitord moeten worden. Dit is nodig voor zowel beheerde systemen, zoals door PCI IT uitgegeven workstations, als voor onbeheerde systemen zoals privé laptops of smartphones die door medewerkers van klanten gebruikt worden. De wens van PCI IT is dat er op acties die van tevoren als kwaadwillig zijn gedefinieerd, automatische acties worden ondernomen in de beheerde SaaS-applicaties. Het product moet naast de eerdergenoemde inzichten in beheerde SaaS-oplossingen ook zicht creëren op de SaaS gerelateerde schaduw IT welke aanwezig is bij klanten. Het product dat in dit project gezocht wordt, zal in de toekomst deel worden van een pakket dat PCI IT (als MSSP) aan klanten wil aanbieden.

9. Ideate

In dit hoofdstuk worden de hoofd- en deelvragen beantwoord. Om de hoofdvraag later te kunnen beantwoorden zullen de eerdergenoemde deelvragen eerst beantwoord worden om een weloverwogen antwoord te kunnen formuleren.

9.1. Van welke SaaS-applicaties maken klanten van PCI IT gebruik?

Om te bepalen welk product, van welke leverancier het beste aansluit bij PCI IT en haar klanten is het belangrijk om de randvoorwaarden duidelijk te hebben. Eén van deze randvoorwaarden is het softwaregebruik van de klanten. Dit is belangrijk aangezien de oplossing in de toekomst overweg moet kunnen met bestaande software. Om duidelijk te krijgen welke software bij klanten van PCI IT gebruikt wordt, is er gesproken met Marc Schuurman. Aan de hand van dit gesprek is er een beeld ontstaan waar duidelijk uit geworden is welke software in gebruik is. Om zo volledig mogelijk te zijn, heeft Marc na dit gesprek het lijstje bijgewerkt met applicaties welke hij is tegengekomen tijdens zijn dagelijkse werkzaamheden. De softwareapplicaties welke hieronder genoteerd staan, zijn de door PCI IT beheerde software en onbeheerde SaaS-applicaties (schaduw IT) welke tijdens de uitvoering van zijn werkzaamheden toevallig gezien zijn door Marc.

9.1.1. Gebruikte SaaS-applicaties

De volgende SaaS-applicaties zijn minimaal in gebruik bij klanten van PCI IT. Deze lijst is zoals gezegd samengesteld met behulp van informatie van vooral Marc Schuurman en Marc de Vries. Het is dus geen volledige lijst maar het gros van de gebruikte SaaS-applicaties is genoteerd samen met de door Marc de Vries geverifieerde SaaS-applicaties met prioriteit. Van de applicaties in het lijstje hebben enkele prioriteit aangezien dit de SaaS-applicaties zijn die bij grote klanten van PCI IT draaien. SaaS-applicaties met prioriteit zijn:

- Office365
- Dynamics365
- AFAS online
- Exact online

De overige SaaS-applicaties zijn als volgt:

- ADP
- Ecare
- Nedap
- Topdesk
- Cobra
- Scansys
- Swift-Syntess
- NotisOne
- SAP
- King
- Unit4
- Fierit Cura

Zoals eerder benoemd, zijn er weinig of geen schaduw IT SaaS-oplossingen genoemd omdat deze bijna niet inzichtelijk zijn aan het begin van het project. Bij enkele klanten van PCI IT is SAM aanwezig. Dit is een apparaat die SaaS gerelateerde schaduw IT op een bedrijfsnetwerk inzichtelijk maakt. Op deze manier is PCI IT erachter gekomen dat Dropbox en Wetransfer gebruikt worden bij klanten. Dit is echter maar bij enkele klanten aanwezig en werkt alleen op het bedrijfsnetwerk. Daarnaast wordt SaaS gerelateerde schaduw IT soms gedetecteerd als er ondersteuning aan klanten

wordt verleend. Er zijn dan soms bij toeval voorbeelden te zien, zoals een medewerker die even snel een bestand naar zijn privéadres heeft gemaild om later te bewerken. Volgens recente onderzoeken naar het gebruik van schaduw IT in organisaties is het geen uitzondering als 80% van een organisatie gebruik maakt van schaduw IT (Haag & Eckhardt, 2017). Naast dat schaduw IT bestaat uit software, moet PCI IT ervan bewust zijn dat gebruik van hardware die niet door de organisatie uitgegeven is ook onder schaduw IT valt.

9.1.2. Wat voor data staat er in de SaaS-applicaties die door klanten van PCI worden gebruikt?

De data die in deze SaaS-applicaties opgeslagen staat, is dankzij de afwijkende use cases van de verschillende applicaties zeer divers. Als er bijvoorbeeld gekeken wordt naar AFAS Online dan gaat het vooral om (bijzondere) persoonsgegevens die beschermd zijn door de AVG-wetgeving. De SaaS-applicatie Topdesk daarentegen kan ook informatie over de bedrijfsvoering bevatten, zoals contracten en details over werkzaamheden en klanten. De applicaties bevatten dus in het geval van de klanten van PCI IT allemaal data die of door wetgeving beschermd is en niet mag uitlekken of gegevens over bedrijfsvoering welke niet naar buiten mogen komen. Hoewel de opzet van deze deelvraag aan de start van dit project opgezet was om informatie te winnen, is door het legio aan klanten en het legio aan SaaS-applicaties het antwoord helaas aardig banaal geworden. Hoewel dit jammer is voor de informatievoorziening geeft dit wel de noodzaak aan van het hebben van zicht op SaaS-applicaties en de gevoelige data welke hierin staat.

9.2. Welke eisen heeft PCI IT met betrekking tot data beveiliging voor SaaS-applicaties?

Uit interviews met verschillende werknemers bij PCI IT is duidelijk geworden wat de insteek van dit project is en wat er verwacht wordt. Deze eisen zijn uiteindelijk SMART uitgewerkt tot requirements en deze zijn verwerkt in het hoofdstuk requirements. Samengevat betekenen deze eisen dat PCI IT inzicht heeft in de datastromen vanaf beheerde en onbeheerde apparaten van werknemers en dat ze indien wenselijk in de datastromen kan sturen.

9.3. Wat is de mate van invloed die een klant, met of zonder dienstverlener, kan uitoefenen op een SaaS-applicatie?

Uit interviews met bijvoorbeeld Bart Brevink en Joost Overkamp is duidelijk geworden welke mogelijkheden er op dit moment in de meest gebruikte SaaS-applicaties van klanten aanwezig zijn om te sturen wie vanaf welk apparaat op welke locatie toegang heeft tot de data in SaaS-applicaties. Deze mogelijkheden zijn ingebouwd in de meeste SaaS-applicaties en worden ook actief gebruikt door de klanten. De exacte implementatie en het gebruik van elke mogelijkheid verschilt per applicatie en klant, maar de ingebouwde mogelijkheden welke de controle over de SaaS-applicaties vergroot zijn hieronder genoteerd.

- Authenticatie
    - Voordat de SaaS-applicatie benaderd kan worden, vindt er authenticatie plaats op basis van bijvoorbeeld de gebruiker, locatie, apparaat of MFA.
- Cloud-service-provider-native DLP (nader verklaard in DLP)
- Beleidsmanagement
    - Interne rechten in SaaS-applicaties zorgen ervoor dat niet elke gebruiker alle data in de SaaS-applicatie kan benaderen.

9.4. Welke oplossingen gebruikt PCI IT op dit moment om de data in door klanten gebruikte SaaS-oplossingen te beveiligen en welke functies biedt dat PCI IT en haar klanten?

Zoals in de vorige deelvraag al kort behandeld is, wordt er bij PCI IT gebruik gemaakt van de ingebouwde mogelijkheden bij SaaS-applicaties. Naast de ingebouwde mogelijkheden wordt er ook gebruik gemaakt van oplossingen zoals Single Sign-On (SSO), Multi Factor Authenticatie (MFA), Cloud-service-provider-native DLP of Identity Provider (IDP) om de beveiliging van de data in de SaaS-applicaties bevorderen. Deze oplossingen worden hieronder kort besproken.

Een Cloud-service-provider-native DLP is, zoals in het hoofdstuk DLP wordt uitgelegd, een oplossing welke exfiltratie van bepaalde gegevens binnen de eigen applicatie waar hij in verwerkt is, kan voorkomen (proofpoint, 2021). In het geval van Office365 wordt er bijvoorbeeld gedetecteerd wanneer er meerdere BSN-nummers in een document worden genoteerd. Als actie hierop is het daarna niet meer mogelijk om dit bestand op te slaan.

Multi Factor Authenticatie (MFA) is een oplossing met meerdere subcategorieën. Het basisprincipe van MFA is dat er meerdere methoden van authenticatie gebruikt worden om toegang te krijgen tot de dienst waarop ingelogd probeert te worden (Microsoft, z.d.-b).

Single Sign-On (SSO) is een oplossing welke ervoor zorgt dat gebruikers met een enkele inlog zich authentiseren voor verschillende diensten (Citrix, z.d.).

Identity Provider (IDP) is een centraal systeem welke gebruiker gegevens opslaat en beheert. Dit systeem wordt gebruikt om inlogpogingen van gebruikers bij diensten te toetsen (Okta, z.d.).

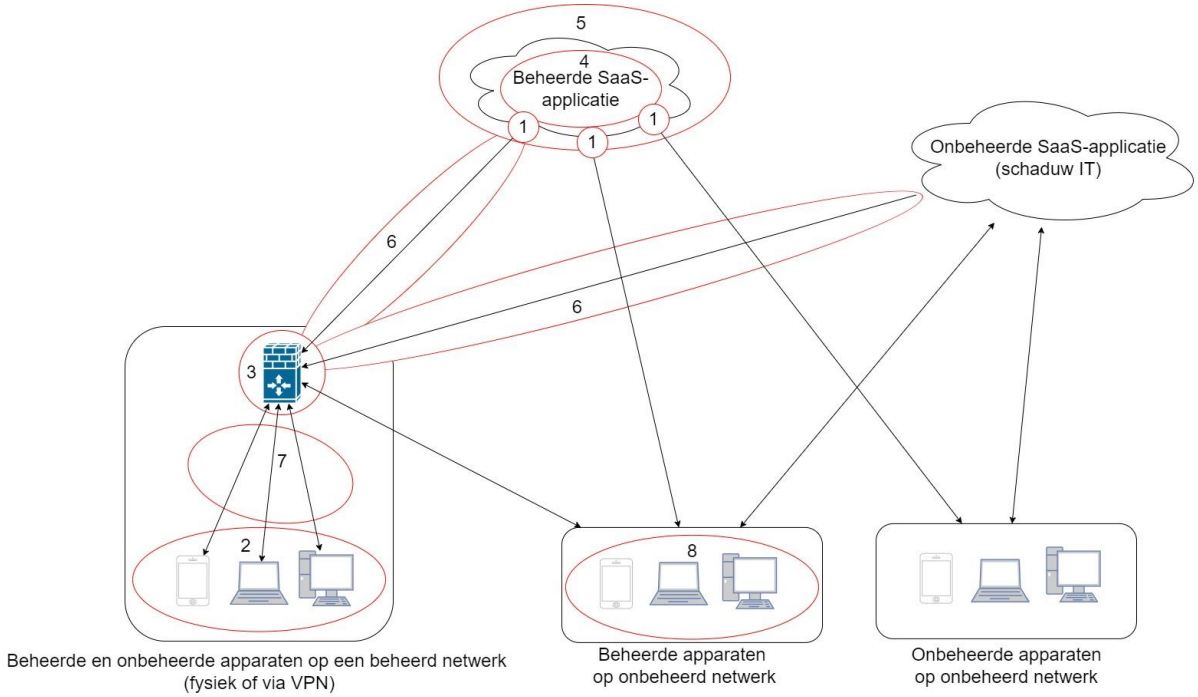
9.5. Wat voor producttype zoekt PCI IT op basis van de reeds beantwoorde deelvragen?

In het hoofdstuk genaamd define is er gekeken naar wat voor visie PCI IT heeft en wat dit project in die visie kan en gaat betekenen. Nu duidelijk is geworden wat PCI IT precies uit dit project wil bereiken, wordt er gezocht naar welk type producttype hierbij past. Dit wordt gedaan door te onderzoeken wat voor soort producttype voldoet aan de gestelde eisen. De uitkomst van dit onderzoek is ook direct het antwoord op de huidige deelvraag "**Wat voor producttype zoekt PCI IT op basis van de reeds beantwoorde deelvragen?**".

Zoals uit de interviews, user stories en requirements al duidelijk is geworden, is PCI IT op zoek naar een op zichzelf staand producttype welke het zicht en de controle over SaaS-applicaties vergroot. Als er gekeken wordt naar de requirements welke vanuit PCI IT gecommuniceerd worden, dan valt een groot aantal soorten oplossingen af. Elk van deze concepten draagt wel bij aan het beveiligen van de data in de SaaS-applicaties, maar doet dit op een onvolledige manier of op een manier welke de SaaS-beveiliging wel helpt, maar niet geheel relevant is voor dit project. Het belangrijkste punt is dat de soort oplossing het inzichtelijk maakt wie wat in de SaaS-applicaties van klanten doet. Dit zal betekenen dat de oplossing welke PCI IT zoekt inzicht in stromen verkeer van beheerde en onbeheerde apparaten zal moeten hebben, ongeacht de locatie. De belangrijkste producttypes welke tijdens de zoektocht voorbij zijn gekomen, zijn hieronder genoemd. Bij elk redelijk relevant concept is genoteerd wat deze verwezenlijkt, samen met de reden waarom deze is afgevallen. Nadat deze producttypes tekstueel behandeld zijn, zullen deze aan het eind van het hoofdstuk weergeven worden in een multicriteria-analyse welke snel overzicht geeft over de functionaliteiten van een producttype. Aangezien het hier over concepten gaat, worden er geen exacte producten van leveranciers genoemd. De informatie welke in dit hoofdstuk gebruikt wordt, is afkomstig uit

literatuuronderzoek uit bronnen zoals onafhankelijke media, bijvoorbeeld Gartner, en onderzoek naar invulling van de concepten door leveranciers.

In het onderstaande figuur 4 is een bedrijfssituatie gecreëerd met meerdere scenario's over hoe medewerkers gebruik maken van SaaS-applicaties. In de tekening zijn meerdere rode cirkels met nummers genoteerd. In het komende hoofdstuk wordt enkele keren verwezen naar deze nummers om duiding aan te brengen waar deze oplossingen precies het gebruik van de SaaS-applicatie verbeteren.



Figuur 4 Controle punten infrastructuur

9.5.1. Identity and Access Management (IAM)

Identity and Access Management (IAM) is één van de eerste en voornaamste oplossingen waaraan gedacht wordt bij het beveiligen van de data in SaaS-applicaties. IAM kan helpen om de data in de SaaS-applicaties te beveiligen door eisen te stellen aan de manier waarop er toegang tot de SaaS-oplossingen wordt gevraagd. Over het algemeen wordt dit bewerkstelligd door het gebruik van meerdere van de volgende zaken: het afdwingen van het gebruik van MFA, wachtwoordcomplexiteit eisen of andere manieren van toegangscontrole. Nadat de gebruiker is ingelogd, zal de IAM-software rechten aan de ingelogde gebruiker toewijzen (digitalguardian, 2019; Wikipedia contributors, 2021b).

Deze soort oplossing controleert dus de inlogpogingen van een persoon op een SaaS-applicatie. In figuur 4 is dit controlepunt zichtbaar als nummer 1.

De reden dat deze oplossing afvalt, is omdat de oplossing niet volledig is in het beschermen van de data in de SaaS-applicaties en enkele van de MUST requirements niet kan waarmaken. Dit soort oplossingen biedt namelijk geen inzicht in wat er na het inloggen in de SaaS-applicaties gebeurt, zoals in requirement US2-NF-S4-M beschreven. Dit betekent dan ook dat er geen mogelijkheid is om in te grijpen zodra een threshold overtreden wordt. Dus hoewel dit soort oplossingen de SaaS-oplossingen kunnen beveiligen, is het niet de oplossing welke PCI IT zoekt.

9.5.2. Cloud Security Posture Management (CSPM)

CSPM staat voor Cloud Security Posture Management (checkpoint, 2021b). Een CPSM-oplossing kijkt in de Cloud-omgevingen of er instellingen zijn welke de beveiliging van de Cloud in gevaar brengen. Dit kunnen instellingen zijn waardoor de API van een SAAS-oplossing openstaat, waardoor er misbruik gemaakt kan worden, of een instelling waardoor een online opslagdienst zoals een informatie-uitwisseling dienst, bijvoorbeeld SharePoint, openstaat naar externe gebruikers (checkpoint, 2021).

Deze oplossing controleert de beheerde SaaS-applicatie. In figuur 4 is dit controlepunt zichtbaar als nummer 5. Dankzij de aard van het product is het ook tot op zekere hoogte actief in de controle van interne rechten in de applicatie, dus nummer 4 in figuur 4.

Zoals te lezen is, zorgt ook een CSPM-oplossing dus voor een beter beveiligde SaaS-applicatie, maar is de oplossing niet relevant omdat het niet kan voldoen aan een groot aantal must requirements, zoals het inzicht geven in SaaS gerelateerde schaduw IT (US6-NF-S10-M) of het inzichtelijk maken van de gebruikers en hun acties in de SaaS-applicaties (US2-NF-S4-M).

9.5.3. Cloud Workload Protection Platform (CWPP)

CWPP staat voor Cloud Workload Protection Platform. Een CWPP gaat opzoek naar kwetsbaarheden en andere security issues in Cloud en lokale systemen. Een CWPP kan net als de eerdergenoemde CSPM-oplossing zoeken naar configuratiefouten welke de beveiliging verzwakken, maar een CWPP is, zoals de naam al aangeeft, gefocust op “workloads” zoals servers, virtuele machines of containers. Naast het controleren op de configuratie biedt deze oplossing ook zaken zoals anti-malware scanning, exploit prevention en inzicht in Cloud workloads (Supasatit, 2021; checkpoint, 2021a; MacDonald & Croll, 2021).

Deze oplossing is aanwezig in figuur 4 op de positie van cijfer 5. Aangezien een CWPP gepositioneerd is op workloads van cloud oplossingen, staat het feitelijk op nummer 5 in figuur 4.

Hoewel deze soort oplossingen dus een andere scope hebben dan de CSPM-oplossingen, voldoet ook een CWPP niet aan de requirements die in dit project geformuleerd zijn. De CWPP-oplossing is namelijk gefocust op de systemen waar software op wordt gehost en niet op de software zelf. De oplossing maakt ook SaaS gerelateerde schaduw IT nog steeds niet inzichtelijk (US6-NF-S10-M) en echte gebruikersacties in beheerde SaaS-applicaties zijn ook nog niet inzichtelijk door het gebruik van deze oplossing (US2-NF-S4-M). Hierdoor valt dus ook een CWPP af voor de doeleinden van PCI IT.

9.5.4. Cloud Native Application Protection Platform (CNAPP)

CNAPP staat voor Cloud Native Application Protection Platform. Een CNAPP is een samenvoeging van de eerdergenoemde CWPP en CSPM-oplossingen. Het heeft dus de goede eigenschappen van beide oplossingen en voegt dit samen in een enkele oplossing (Supasatit, 2021; MacDonald & Winckless, 2021).

Net als de CSPM-oplossing kan CNAPP op nummer 5 in figuur 4 de SaaS-applicatie controleren. Ook hier is de oplossing dankzij zijn aard aanwezig in de controle van interne rechten in de applicatie, dus op nummer 4 in de tekening. Dit is echter niet genoeg om de gebruikers en hun acties in de SaaS-applicaties inzichtelijk te krijgen.

Hoewel deze oplossing dus meer biedt, is de oplossing niet geschikt om het vraagstuk van PCI IT op te lossen. Deze oplossing werkt niet om dezelfde redenen die eerder bij zowel de CWPP als de CSPM zijn genoemd. Net als de CSPM-oplossing kan CNAPP op nummer 5 in figuur 4 de SaaS-applicatie

controleren. Ook hier is de oplossing dankzij zijn aard aanwezig in de controle van interne rechten in de applicatie, dus op nummer 4 in de tekening. Dit is echter niet genoeg om de gebruikers en hun acties in de SaaS-applicaties inzichtelijk te krijgen. Ook deze oplossing maakt SaaS gerelateerde schaduw IT nog steeds niet inzichtelijk (US6-NF-S10-M) en echte gebruikersacties in beheerde SaaS-applicaties zijn ook nog niet inzichtelijk door het gebruik van deze oplossing (US2-NF-S4-M).

9.5.5. Data Loss Prevention (DLP)

DLP is een afkorting welke staat voor Data Loss Prevention (Cisco, 2021). Een DLP is een oplossing welke potentiële datalekken of exfiltratie van data kan detecteren. Indien dit gedetecteerd wordt, kan een DLP-oplossing hier automatisch geconfigureerde acties op ondernemen.

Volgens een artikel van Bales & Chugh (2021) op Gartner bestaan er drie soorten DLP-oplossingen, namelijk Enterprise Data Loss Prevention (EDLP), Integrated Data Loss Prevention (IDLP) en Cloud-service-provider-native DLP-oplossingen. De eerste variant is een losstaande DLP-oplossing welke dus hoofdzakelijk als DLP in de markt is gezet. De tweede is een DLP welke deel is van een bestaande oplossing zoals een SecureWebGateway (SWG). In het laatste geval zijn de DLP-functionaliteiten ingebouwd om de data in een IaaS of SaaS-oplossing te beveiligen. Een EDLP-oplossing is meestal te vinden in een security-gerelateerd product dat zich door het toevoegen van in dit geval EDLP-functionaliteiten sterker in de markt wil zetten. In het geval van een Cloud-service-provider-native DLP is het de bedoeling dat de data in de omgeving beter wordt beveiligd door de toevoeging van DLP-functionaliteiten.

Op het moment van schrijven is er bij sommige klanten van PCI IT ook een Cloud-service-provider-native DLP aanwezig. Deze zit verwerkt in Office365 en kan hier dus de data beschermen. De toepassing van deze DLP is dus zoals eerder besproken gelimiteerd tot één enkele SaaS-applicatie, in dit geval Office365. Waar een DLP-oplossing in de infrastructuur staat, is afhankelijk van wat voor soort DLP-oplossing er wordt afgenomen. Ook de exacte mogelijkheden die een DLP kan monitoren en beveiligen verschillen per leverancier, maar een DLP-oplossing is gebaseerd op drie principes (Cisco, 2021; Proofpoint, 2021; Bales, 2021), namelijk de onderstaande:

- “Data in use”
    - Het beveiligen van data welke actief gebruikt wordt door middel van authenticatie en andere soorten van toegangscontrole.
- “Data in motion”
    - Het beveiligen van data welke over het netwerk verstuurd wordt en, indien nodig geacht, routeren of onderscheppen.
- “Data at rest”
    - Het beveiligen van data welke opgeslagen staat.

In figuur 4 betekent het dus dat deze oplossing op nummer 4 het gebruik van de data in de SaaS-applicatie door gebruikers inzichtelijk heeft, verkeer op positie 6 en 7 kan controleren, op positie 1 de inlog kan beveiligen en het data gebruik op 2 en 8 kan controleren. Dit zal niet allemaal mogelijk zijn bij iedere DLP, aangezien iedere leverancier een andere implementatie heeft en er zoals eerder beschreven een drietal soorten DLP bestaat. Een EDLP zal in tegenstelling tot een IDLP wel lokaal op een workstation data kunnen beveiligen.

Een DLP-oplossing is vrij volledig in zijn bescherming van de data en biedt ook het gewenste inzicht in acties, maar doordat een DLP geen inzicht kan verschaffen in SaaS gerelateerde schaduw IT, zoals gevraagd in US6-NF-S10-M, valt ook deze soort oplossingen af.

9.5.6. Deep Packet Inspection (DPI) / packet sniffer

Een DPI of packet sniffer is een software of hardware-matige tool welke datastromen die zich bewegen over het netwerk kan inzien en onderscheppen. Dit producttype zal dus het verkeer op locatie van de klant kunnen inzien en situaties voorkomen waarin data ongewenst het bedrijfsnetwerk verlaat. Dit gebied kan met bijvoorbeeld het gebruik van een VPN vergroot worden naar plekken buiten het bedrijfsnetwerk.

In figuur 4 betekent het dus dat deze oplossing op nummer 3 verkeer richting de SaaS-applicatie kan onderscheppen en kan controleren voordat deze verstuurd wordt, zoals weergegeven op nummer 6 in figuur 4.

Hoewel er op beheerde apparaten gebruik kan worden gemaakt van een VPN is dit niet mogelijk op niet beheerde apparaten. Dit betekent dat requirement US3-NF-S9-M niet nageleefd kan worden. Daarnaast is er met behulp van deze oplossing nog geen inzicht in de beheerde SaaS-oplossingen zelf, zoals in US2-NF-S4-M is beschreven, maar alleen het verkeer van en naar deze SaaS-applicaties is dan inzichtelijk (Brook, 2018).

9.5.7. Next generation Firewall (NGF)

NGF staat voor Next Generation Firewall. Een NGF is in de basis een traditionele firewall die, naast zijn standaard firewall functies, op basis van definities die continue geüpdatet worden andere taken op zich kan nemen, zoals deep packet inspection (DPI) of intrusion prevention systems (IPS). Leveranciers geven invulling aan wat er naast de firewall functionaliteit daadwerkelijk in een NGF aanwezig is (Securityboulevard, 2019). Deze firewall en nader te bepalen functies worden dan binnen een enkel pakket aangeboden. Door de toevoeging van meerdere diensten binnen de NGF betekent het ook dat de NGF nu werkt op meerdere niveaus van het OSI-model (Brook, 2020; Fortinet, z.d.).

In figuur 4 betekent het dus dat deze oplossing op nummer 3 verkeer richting de SaaS-applicatie kan onderscheppen en kan controleren voordat het deze verstuurt op nummer 6.

Hoewel er met deze oplossing op diverse niveaus zicht is op datastromen, heeft deze oplossing geen overzicht over het dataverkeer in de beheerde SaaS-applicaties zelf zoals beschreven in US2-NF-S4-M en is deze oplossing alleen toepasbaar op beheerde apparaten. Door het niet halen van de genoemde requirements valt deze oplossing af.

9.5.8. SaaS Management Platform (SPM)

SPM staat voor SaaS Management Platform. Een SPM is een oplossing waarmee er meerdere andere SaaS-applicaties beheerd kunnen worden. Deze soort oplossing is dus in de markt gezet om SaaS-applicaties van meerdere leveranciers op een centrale plek te beheren. In deze centrale omgeving kunnen dan meerdere SaaS-applicaties door administrators beheerd worden en kunnen de gebeurtenissen van alle applicaties inzichtelijk zijn. Deze soort oplossingen controleert, zoals beschreven, meerdere SaaS-applicaties en heeft dus controle over de SaaS-applicaties en voor een deel ook over de data welke opgeslagen is in de SaaS-applicaties.

Deze oplossing kan dus volledig invloed uitoefenen in figuur 4 op nummer 5 en gedeeltelijk op nummer 4.

Hoewel deze oplossing dus ook beveiliging van deze SaaS-applicaties kan verbeteren, mist dit type oplossingen bijvoorbeeld inzicht in gebruikersacties binnen de SaaS, wat wel gevraagd wordt in US2-NF-S4-M, en ook het zicht op SaaS gerelateerde schaduw IT is niet aanwezig (Silva et al., 2021). Door het niet halen van genoemde valt deze oplossing af.

9.5.9. Privileged Access Management (PAM)

PAM staat voor Privileged Access Management. Privileged Access Management is een producttype welke gebruikt wordt voor het definiëren van rechten voor “priveleged” gebruikers van een systeem (Gaehtgens et al., 2021). Dit zijn dan verhoogde rechten binnen een systeem.

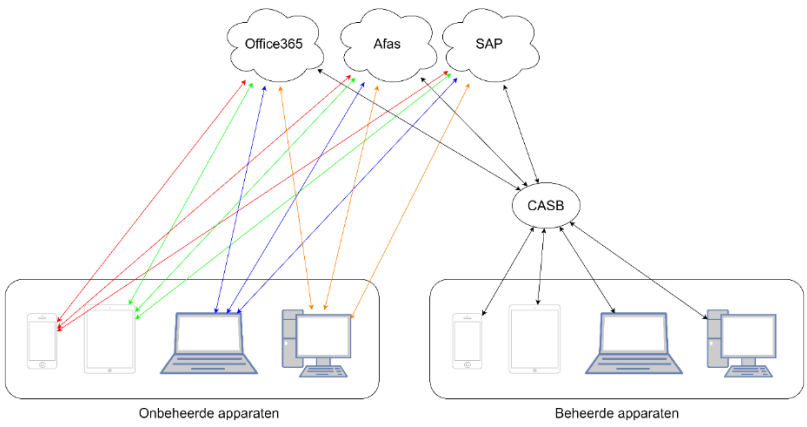
Deze soort oplossingen implementeert de hoedanigheid waarin de gebruiker toegang heeft tot resources in de applicatie en zit dus op nummer 4 van figuur 4.

Hoewel dit dus de beveiliging van SAAS-applicaties kan verhogen, is dit niet de soort oplossing waar PCI IT naar op zoek is binnen dit project. Het voldoet niet aan het gros van de requirements, zoals US3-NF-S9-M en US2-NF-S4-M.

9.5.10. Cloud Access Security Broker (CASB)

Cloud Access Security Broker, of CASB in het kort, is een vrij brede term aangezien deze net als de eerdere genoemde CNAPP bestaat uit de beginselen van meerdere zaken en omdat elke leverancier een iets andere invulling geeft aan het begrip “CASB”. Hoofdzakelijk zorgt een CASB ervoor dat het opgegeven beveiligingsbeleid wordt nageleefd in SaaS-applicaties. Een CASB-oplossing biedt echter meer mogelijkheden, zoals het inzichtelijk maken van het gebruik van SaaS gerelateerde schaduw IT door gebruik te maken van logging van bijvoorbeeld de firewall. Daarnaast biedt het de mogelijkheden om het beveiligingsbeleid in en rond de SaaS-applicatie geforceerd na te leven en de instellingen te controleren op positie 4 en 5 in figuur 4. Als laatste kan een CASB-oplossing data exfiltratie door zoals een EDLP op positie 4 voorkomen en logging informatie over het gebruik van de SaaS-applicaties op positie 4 genereren (Croll, 2020).Dit doet deze oplossing op verschillende manieren, zoals via een agent op een managed apparaat op positie 1, forward/reverse proxy op positie 3 of 6 of via een API welke verkeer van beheerde en onbeheerde apparaten kan sturen binnen de SaaS-applicatie. Doordat er meerdere manieren zijn waarop er gebruik gemaakt kan worden van de oplossing, zijn acties van zowel beheerde als onbeheerde apparaten afgevangen (Fritchen, 2020; Bhardwaj, 2020; Riley & Lawson, 2020).

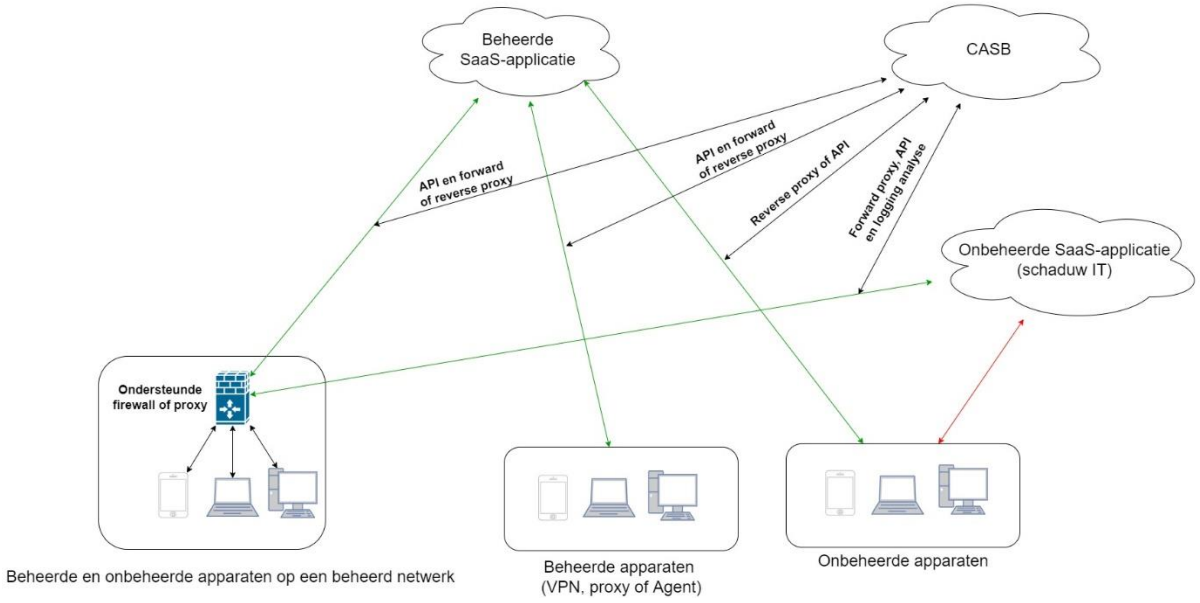
Indien een CASB op de “oude” oorspronkelijke manier wordt ingezet, dan is dit als forward proxy vanuit positie 3 in figuur 4. Dit zorgt ervoor dat apparaten die goed ingesteld zijn of die een agent geïnstalleerd hebben, via de CASB communiceren met de SaaS-applicatie. Onbeheerde apparaten buiten het bedrijfsnetwerk kunnen geen gebruik maken van deze versie van een CASB en maken dus rechtstreeks verbinding met de SaaS-applicaties. In figuur 5 is genoteerd hoe dit er in de praktijk uit zal zien. In deze variant welke door sommige leveranciers nog wordt verkocht, zal er dus geen grip zijn op de onbeheerde apparaten. Hierdoor valt deze specifieke implementatie van een CASB dus af.



Figuur 5 V1 CASB infrastructuur

In de meest ideale situatie staat de SaaS-applicatie in contact met de CASB via de ingebouwde API van de SaaS-applicatie. Hierdoor hoeft het verkeer niet langs de CASB te gaan, maar kunnen beheerde en onbeheerde apparaten rechtstreeks met de SaaS-oplossing communiceren (Kirti, 2016).

In figuur 6 is voor elke mogelijke locatie van het apparaat genoteerd op welke manier het verkeer gecontroleerd kan worden. Deze implementatie maakt gebruik van een API, een forward proxy en een reverse proxy. In het groen is genoteerd welke verbindingen met SaaS-applicaties gemonitord of verijdeld kunnen worden met deze versie van een CASB. De groene lijnen geven aan dat de CASB werkt vanaf zowel het genoteerde apparaat als vanaf de locatie en er staat dan door middel van een zwarte pijl genoteerd op welke manier dit wordt gedaan door de CASB. De meest rechter netwerkstroom vanaf onbeheerde apparaten richting de onbeheerde SaaS-applicatie is dus op geen enkele manier te controleren of tegen te houden. Dit was een tegenslag welke in de lijn van verwachtingen lag, aangezien dit technisch bijna onmogelijk op te lossen is. Uit gesprekken met Joost Overkamp is gebleken dat dit voor PCI IT geen probleem zou zijn. De requirements van dit project zullen ook te behalen zijn met deze concessie. De enige impact die dit heeft op het behalen van de requirements is op randgevallen waar lokaal opgeslagen bedrijfsdata wordt benaderd vanaf onbeheerde hardware of waar er al gebruik wordt gemaakt van een onbeheerd apparaat om SaaS gerelateerde schaduw IT te benaderen waar bedrijfsdata al opgeslagen staat.



Figuur 6 Optimale CASB implementatie

9.5.11. Multicriteria-analyse product type

In de onderstaande tabel is weergegeven of de concepten aan de requirements van PCI IT voldoen. Voor elke requirement kan een oplossing niet, gedeeltelijk of geheel zorgdragen. Aan welke van de eerdergenoemde drie niveaus een oplossing voldoet, is samen met een korte uitleg beschreven in de tabel. Zoals eerder genoemd en nu ook terug te zien is in de onderstaande tabel voldoet een CASB-oplossing aan alle gestelde requirements. Om deze reden zal er tijdens de productselectie worden ingezoomd op dit soort producten.

	IAM	CSPM	CWPP	CNAPP	DLP	DPI	NGF	SPM	PAM	CASB
US1-NF-S1-M De nieuwe oplossing moet overweg kunnen met de SaaS-applicaties van de klanten van PCI IT.	X *Compatibiliteit verschilt per leverancier	X *Compatibiliteit verschilt per leverancier	X *Compatibiliteit verschilt per leverancier	X *Compatibiliteit verschilt per leverancier	X *Compatibiliteit verschilt per leverancier	X Er is geen connectie met de SaaS-applicatie, alleen het netwerkverkeer van en naar is inzichtelijk.	X Er is geen connectie met de SaaS-applicatie, alleen het netwerkverkeer van en naar is inzichtelijk.	X *Compatibiliteit verschilt per leverancier	X *Compatibiliteit verschilt per leverancier	X *Compatibiliteit verschilt per leverancier
US1-F-S2-M De nieuwe oplossing moet automatisch acties kunnen uitvoeren aan de hand van aangemaakte thresholds in SaaS-applicaties.		X	X	X	X					X
US1-NF-S3-M De nieuwe oplossing moet controle kunnen uitoefenen over de datastromen in beheerde SaaS-applicaties van klanten.	X *Door het aanpassen van rechten kan er gestuurd worden in de SaaS-applicaties. De datastromen zelf zijn niet inzichtelijk.	X *Door het aanpassen van rechten kan er gestuurd worden in de SaaS-applicaties. De datastromen zelf zijn niet inzichtelijk.		X *Door het aanpassen van rechten kan er gestuurd worden in de SaaS-applicaties. De datastromen zelf zijn niet inzichtelijk.	X	X *Door het aanpassen van rechten kan er gestuurd worden in de SaaS-applicaties. De datastromen zelf zijn niet inzichtelijk.	X *Door het aanpassen van rechten kan er gestuurd worden in de SaaS-applicaties. De datastromen zelf zijn niet inzichtelijk.	X *Door het aanpassen van rechten kan er gestuurd worden in de SaaS-applicaties. De datastromen zelf zijn niet inzichtelijk.	X *Door het aanpassen van rechten kan er gestuurd worden in de SaaS-applicaties. De datastromen zelf zijn niet inzichtelijk.	X
US2-NF-S4-M De nieuwe oplossing moet inzicht geven in de acties van medewerkers van klanten in beheerde SaaS-applicaties.	X Details over inloggen zijn inzichtelijk.				X	X *Alleen het netwerkverkeer is inzichtelijk.	X *Alleen het netwerkverkeer is inzichtelijk.			X
US3-NF-S5-M De nieuwe oplossing moet onderscheid kunnen maken tussen apparaten en aan de hand hiervan rechten toekennen.	X Dit kan bij het inloggen afgedwongen worden.				X		X			X
US3-NF-S6-M De nieuwe oplossing moet onderscheid kunnen maken tussen door het bedrijf uitgegeven applicaties en schaduw IT.						X *Netwerkverkeer kan gestuurd worden.	X *Netwerkverkeer kan gestuurd worden.			X
US3-NF-S7-M	X	X	X	X	X	X	X	X	X	X

De nieuwe oplossing mag niet afhankelijk zijn van de locatie van de eindgebruiker.						Dit kan afgedwongen worden door het gebruik van een agent of VPN maar is niet standaard aanwezig.	*Dit kan afgedwongen worden door het gebruik van een agent of VPN maar is niet standaard aanwezig.			
US3-NF-S8-M De nieuwe oplossing zal moeten werken met beheerde apparaten van klanten.	X	X	X	X	X	X	X	X	X	X
US3-NF-S9-M De nieuwe oplossing zal moeten werken met onbeheerde apparaten van klanten.	X	X	X	X	X *Compatibiliteit en invulling verschillen per leverancier			X	X	X
US6-NF-S10-M De nieuwe oplossing moet inzicht kunnen geven in het gebruik van SaaS-applicaties welke onder schaduw IT vallen bij klanten van PCI IT.						X *Het netwerkverkeer op bedrijfslocaties van medewerkers zal inzichtelijk zijn. SaaS gerelateerde schaduw IT valt hier ook onder.	X *Het netwerkverkeer op bedrijfslocaties van medewerkers zal inzichtelijk zijn. SaaS gerelateerde schaduw IT valt hier ook onder.			X
US7-F-S11-M De nieuwe oplossing moet meer mogelijkheden bieden dan wat de Data Loss Prevention oplossing aan het begin van het project biedt aan PCI IT.					X *Er wordt al gebruik gemaakt van EDLP-oplossingen bij PCI IT. Andere leveranciers kunnen potentieel meer mogelijkheden bieden.					X

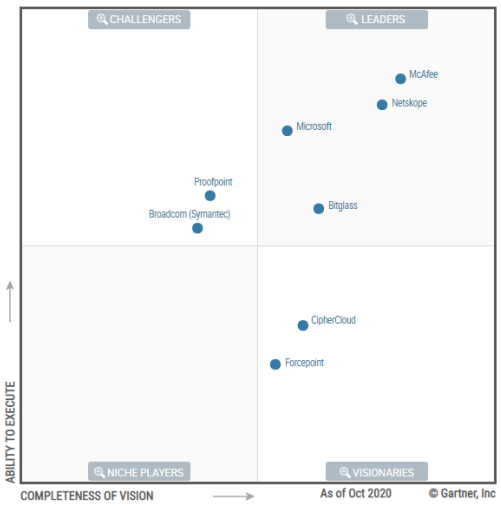
Tabel 4 Multicriteria analyse oplossingen

9.6. Welke beveiliging en controle oplossingen zijn er op de markt die voldoen aan de eisen van PCI IT en welke past het beste bij PCI IT?

In het vorige hoofdstuk is duidelijk geworden dat er in dit project gezocht wordt naar een CASB. Aan de hand van deze informatie is er in dit hoofdstuk gezocht naar oplossingen die deze titel dragen. In dit hoofdstuk wordt er gewerkt met een long- en shortlist van producten van leveranciers van CASB-oplossingen. Vanuit de grotere longlist is uiteindelijk gewerkt naar een shortlist. De producten van de longlist vallen af als er wordt afgeweken van de gestelde requirements. In de shortlist staan de voornaamste producten genoteerd. Bij alle verschillende producten op de shortlist is genoteerd wat de exacte implementatiemogelijkheden zijn van deze CASB en of er nog randvoorwaarden zijn om deze CASB te implementeren, zoals dat er een firewall van een bepaald bedrijf aanwezig moet zijn.

Tijdens dit onderzoek zijn enkele leveranciers vooraf al afgevallen en niet meegenomen in de longlist. Deze leveranciers zijn niet meegenomen omdat er geen antwoord is gekomen op contact verzoeken die wel nodig waren om een correct beeld van het product te krijgen. Deze producten hadden weinig of geen informatie openbaar staan over de toepasbaarheid van de oplossing welke zij aanbieden. Hierdoor konden deze producten dus niet geëvalueerd worden, omdat een toelichting ontbrak. Dit is het geval voor Proofpoint en Netskope. Andere leveranciers zijn in de meeste gevallen ook benaderd voor achtergrondinformatie maar ook hier is niet altijd antwoord op gekomen. Dit uit zich bijvoorbeeld in het niet kunnen tonen van prijzen voor de meeste leveranciers. Voor het onderzoek betekent dit dat er producten afvallen die volgens onafhankelijke media erg sterk gepositioneerd zijn op de markt (Lawson & Riley, 2020; Ingalls, 2020; Tolly, 2021).

De informatie in dit hoofdstuk is afkomstig van de marketinginformatie van leveranciers, meetings met leveranciers, implementatiegidsen, administratorgidsen, FAQ's, reviews en onderzoek van onafhankelijke media zoals Gartner. Om te bepalen welke leveranciers sowieso moesten terugkomen in de longlist, is gebruik gemaakt van de "Magic Quadrant 2020" van Gartner uit 2020. Dit zijn de leveranciers die in figuur 7 genoemd zijn. Daarnaast zijn er enkele leveranciers meegenomen die niet in figuur 7 genoemd zijn, omdat PCI IT bijvoorbeeld al een bestaande relatie had met deze leverancier.



Figuur 7 Magic quadrant 2020 (Lawson & Riley, 2020)

9.6.1. Multicriteria-analyse longlist

In de onderstaande tabel worden alle producten van de longlist behandeld aan de hand van de requirements. Voor elke requirement kan een oplossing niet, gedeeltelijk of geheel zorgdragen. Aan welke van de eerdergenoemde drie niveaus een oplossing voldoet, is samen met een korte uitleg beschreven in de tabel.

	MVISION	Palo Alto	Microsoft	Forcepoint	Broadcom	Lookout
US1-NF-S1-M De nieuwe oplossing moet overweg kunnen met de SaaS-applicaties van de klanten van PCI IT.	Via API wordt Office365 standaard ondersteund. Andere SaaS zal aangevraagd moeten worden, via "custom apps" aangemaakt moeten worden of met behulp van reverse proxy geïmplementeerd moeten worden (McAfee, z.d.-a; McAfee, 2021b).	Van de SaaS-applicaties met prioriteit wordt alleen Office365 ondersteund en er is geen methode om andere applicaties toe te voegen (Palo Alto, z.d.).	Office365 wordt standaard ondersteund. Andere SaaS kan worden toegevoegd indien inlog bij Microsoft door SAML 2.0 mogelijk is (Microsoft, 2021g; Soseman, 2020b).	Via API wordt Office365 standaard ondersteund. Andere SaaS moet worden aangevraagd en kan met behulp van reverse proxy geïmplementeerd worden (Forcepoint, 2021; Bitglass, z.d. ; Gee, 2020).	Van de SaaS-applicaties met prioriteit wordt alleen Office365 standaard ondersteund. Er is wel een mogelijkheid om andere SaaS-applicaties toe te voegen maar dit zal dan basale informatie geven zoals wanneer er ingelogd is (Broadcom, 2021c, 2021b, 2021a, 2021d). Reverse proxy is volgens Gartner uitgefaseerd en de vervanger "Mirror Gateway" is niet terg te vinden in de documentatie (Lawson & Riley, 2020).	Ondersteunt Office365 via API. Andere SaaS-applicaties moeten worden toegevoegd via forward of reverse proxy. De SaaS-applicaties van Exact is al vaker geïmplementeerd.
US1-F-S2-M De nieuwe oplossing moet automatisch acties kunnen uitvoeren aan de hand van aangemaakte thresholds in SaaS-applicaties.	In ondersteunde SaaS-applicaties is er een scala aan automatische acties (McAfee, 2021a; McAfee, 2021g).	In ondersteunde SaaS-applicaties is er een scala aan automatische acties (Palo Alto, z.d.-b).	In ondersteunde SaaS-applicaties is er een scala aan automatische acties (Microsoft, 2021o).	In ondersteunde SaaS-applicaties is er een scala aan automatische acties (Forcepoint, 2021).	Broadcom heeft Securlets en Gatelets. Securlets ziin volledіger dan Gatelets, Gatelets kunnen slechts upload, download, log in en log out monitoren (Broadcom, 2021c, 2021b, 2021a, 2021d).	In ondersteunde SaaS-applicaties is er een scala aan automatische acties (P. Visch meeting, 6 December 2021).
US1-NF-S3-M De nieuwe oplossing moet controle kunnen uitoefenen over de datastromen in beheerde SaaS-applicaties van klanten.	De datastromen zijn aan de hand van een ingestelde policy in te regelen (McAfee, 2021a; McAfee, 2021g.	De datastromen zijn aan de hand van een ingestelde policy in te regelen (Palo Alto, z.d.-b).	De datastromen zijn aan de hand van een ingestelde policy in te regelen (Microsoft, 2021m; Microsoft, 2021o).	De datastromen zijn aan de hand van een ingestelde policy in te regelen (Forcepoint, 2021, p. 52).	De datastromen zijn aan de hand van een ingestelde policy in te regelen (Broadcom, 2021b).	In gekoppelde SaaS-applicaties is er een scala aan mogelijkheden om controle over de datastromen uit te voeren (P. Visch meeting, 6 December 2021).
US2-NF-S4-M De nieuwe oplossing moet inzicht geven in de acties van medewerkers van klanten in beheerde SaaS-applicaties.	In ondersteunde SaaS-applicaties zijn acties inzichtelijk (McAfee, 2021h; McAfee, 2021f). Wat er zichtbaar is, ligt aan de ondersteuning van de gecontroleerde SaaS-applicatie.	In ondersteunde SaaS-applicaties zijn acties inzichtelijk (Palo Alto, z.d.-b). Wat er zichtbaar is, ligt aan de ondersteuning van de gecontroleerde SaaS-applicatie.	In ondersteunde SaaS-applicaties zijn acties inzichtelijk. Wat er zichtbaar is, ligt aan de ondersteuning van de gecontroleerde SaaS-applicatie (Microsoft, 2021f).	In ondersteunde SaaS-applicaties zijn acties inzichtelijk (Forcepoint, 2021). Wat er zichtbaar is, ligt aan de ondersteuning van de gecontroleerde SaaS-applicatie.	In ondersteunde SaaS-applicaties zijn acties inzichtelijk (Broadcom, 2021c). Wat er zichtbaar is, ligt aan de ondersteuning van de gecontroleerde SaaS-applicatie.	In gekoppelde SaaS-applicaties is er inzicht in de acties van gebruikers van de SaaS-applicaties (P. Visch meeting, 6 December 2021).
US3-NF-S5-M De nieuwe oplossing moet onderscheid kunnen maken tussen apparaten en aan de hand hiervan rechten toekennen.	Device management met toevoeging van MobileIron zit verwerkt in deze oplossing (McAfee, 2020b).	Afhankelijk van welke informatie uitgelezen kan worden.	Dit is mogelijk met toevoegingen vanuit Azure AD (Microsoft, 2021s).	Afhankelijk van welke informatie uitgelezen kan worden.	Afhankelijk van welke informatie uitgelezen kan worden.	Afhankelijk van welke informatie uitgelezen kan worden. (P. Visch meeting, 6 December 2021).
US3-NF-S6-M De nieuwe oplossing moet onderscheid kunnen maken tussen door het bedrijf uitgegeven applicaties en schaduw IT.	X	X	X	X	X	X
US3-NF-S7-M De nieuwe oplossing mag niet afhankelijk zijn van de locatie van de eindgebruiker.	De oplossing is bruikbaar voor beheerde SaaS vanaf elke locatie, maar de mogelijkheden van de CASB werken dan niet volledig.	De oplossing is bruikbaar voor beheerde SaaS vanaf elke locatie, maar de mogelijkheden van de CASB werken dan niet volledig.	De oplossing is bruikbaar vanaf elke locatie, maar de mogelijkheden verschillen indien het apparaat niet beheerd is.	De oplossing is bruikbaar voor beheerde SaaS vanaf elke locatie, maar de mogelijkheden van de CASB werken dan niet volledig.	De oplossing is bruikbaar voor beheerde SaaS vanaf elke locatie, maar de mogelijkheden van de CASB werken dan niet volledig.	De oplossing is bruikbaar voor beheerde SaaS vanaf elke locatie, maar de mogelijkheden van de CASB werken dan niet volledig.

US3-NF-S8-M De nieuwe oplossing zal moeten werken met beheerde apparaten van klanten.	**Deze oplossing werkt op beheerde apparaten indien deze aanwezig zijn in het bedrijfsnetwerk.**	**Deze oplossing werkt op beheerde apparaten indien deze aanwezig zijn in het bedrijfsnetwerk.**	**Deze oplossing is dankzij de integratie met Windows defender op beheerde apparaten van elke locatie bruikbaar. Daarnaast zijn beheerde SaaS-applicaties die ondersteund worden door deze oplossing ook overal gecontroleerd (Microsoft, 2019, 2021b; Microsoft, 2021j; Microsoft, 2021f).**	**Dit product heeft een agent voor beheerde apparaten welke verkeer ook buiten het bedrijfsnetwerk kan inzien en filteren (Forcepoint, 2020; Forcepoint, 2021, p. 266; Forcepoint, z.d.).**	**De oplossing werkt op beheerde apparaten indien deze aanwezig zijn in het bedrijfsnetwerk.**	**De oplossing werkt op beheerde apparaten indien deze aanwezig zijn in het bedrijfsnetwerk.**
US3-NF-S9-M De nieuwe oplossing zal moeten werken met onbeheerde apparaten van klanten.	**In het geval van onbeheerde apparaten werkt dit product op het bedrijfsnetwerk en met beheerde SaaS-applicaties.**	**In het geval van onbeheerde apparaten werkt dit product op het bedrijfsnetwerk en met beheerde SaaS-applicaties.**	**In het geval van onbeheerde apparaten werkt dit product op het bedrijfsnetwerk en met beheerde SaaS-applicaties.**	**In het geval van onbeheerde apparaten werkt dit product op het bedrijfsnetwerk en met beheerde SaaS-applicaties.**	**In het geval van onbeheerde apparaten werkt dit product op het bedrijfsnetwerk en met beheerde SaaS-applicaties.**	**In het geval van onbeheerde apparaten werkt dit product op het bedrijfsnetwerk en met beheerde SaaS-applicaties.**
US6-NF-S10-M De nieuwe oplossing moet inzicht kunnen geven in het gebruik van SaaS-applicaties welke onder schaduw IT vallen bij klanten van PCI IT.	**Dit is mogelijk, maar zodra er vanaf een locatie anders dan het bedrijfsnetwerk wordt gewerkt, valt het zicht op SaaS gerelateerde schaduw IT weg.**	**Dit is mogelijk, maar zodra er vanaf een locatie anders dan het bedrijfsnetwerk wordt gewerkt, valt het zicht op SaaS gerelateerde schaduw IT weg.**	**Dit is mogelijk, maar zodra er vanaf een locatie anders dan het bedrijfsnetwerk gewerkt wordt met een systeem zonder een configureerde Windows defender valt het zicht op SaaS gerelateerde schaduw IT weg.**	**Dit is mogelijk, maar zodra er vanaf een locatie anders dan het bedrijfsnetwerk gewerkt wordt met een niet beheerd apparaat valt het zicht op SaaS gerelateerde schaduw IT weg.**	**Dit is mogelijk, maar zodra er vanaf een locatie anders dan het bedrijfsnetwerk gewerkt wordt met een niet beheerd apparaat valt het zicht op SaaS gerelateerde schaduw IT weg.**	**Dit is mogelijk, maar zodra er vanaf een locatie anders dan het bedrijfsnetwerk gewerkt wordt met een niet beheerd apparaat valt het zicht op schaduw IT weg. Daarnaast is er een losse licentie voor nodig (P. Visch meeting, 6 December juli 20210).**
US7-F-S11-M De nieuwe oplossing moet meer mogelijkheden bieden dan wat de Data Loss Prevention oplossing aan het begin van het project biedt aan PCI IT.	**X**	**X**	**X**	**X**	**X**	**X**

Tabel 5 Multicriteria analyse CASB producten

9.6.2. Conclusie longlist

Bij de aanvang van dit onderzoek was de aanvankelijke veronderstelling, die gevoed werd door marketinginformatie, dat een CASB zo goed als alle SaaS-applicaties zou kunnen monitoren, vanaf alle gewenste locaties. Bij nader onderzoek blijkt dit bij veel producten niet het geval te zijn. Tijdens het onderzoek is er daarom veel onderzoek gedaan naar de exacte toepassing en compatibiliteit van de oplossing. De CASB oplossingen verschillen qua methode waarop er verbinding wordt gemaakt met de SaaS-applicaties.

Zoals ook zichtbaar is in de tabel, zijn er enkele producten die helaas niet verdergaan naar de shortlist. Dit zijn de CASB-oplossing van Palo Alto en Broadcom. Deze producten vallen beide af omdat de SaaS-applicaties die PCI IT als cruciaal heeft benoemd niet ondersteund worden. Deze SaaS-applicaties zijn eerder genoemd in "Gebruikte SaaS-applicaties".

In het geval van Palo Alto is er geen ondersteuning aanwezig voor zowel alle genoemde SaaS-applicaties die prioriteit hebben als de SaaS-applicaties welke geen prioriteit hebben. Om deze reden zal er niet worden verder gekeken naar de oplossing van Palo Alto.

In het geval van Broadcom kan er enkel basale controle worden uitgeoefend op de SaaS-applicaties met prioriteit in vergelijking met de andere leveranciers (Broadcom, 2021a, 2021c, 2021d). Deze implementatie zal een stuk minder inzichten en mogelijkheden opleveren dan andere CASB-leveranciers kunnen bieden.

Hierdoor blijven alleen MVISION Cloud van McAfee, Microsoft Defender for Cloud Apps van Microsoft, Lookout en Forcepoint over omdat zij aan alle gestelde requirements voldoen. Deze producten zijn dus verder onderzocht en vergeleken. De resultaten hiervan volgen in de volgende paragraaf. Naast de resultaten van de shortlist zal er ook vermeld worden of de CASB-oplossingen van de leveranciers voldoen aan de randvoorwaarden die vermeld zijn in "Randvoorwaarden project".

9.6.3. Shortlist

Het viertal oplossingen dat van de longlist overgebleven is en naar de shortlist verder is gegaan, is op alle voor PCI IT relevante punten verder vergeleken. In dit hoofdstuk wordt het gekozen product uitgebreid behandeld en wordt een samenvatting van elk afgevallen product genoteerd. De volledige beschrijving van de afgevallen drie producten is te vinden in de bijlage.

9.6.3.1. Randvoorwaarden

Aan het begin van dit project zijn er enkele randvoorwaarden genoteerd waar rekening mee moest worden gehouden. In dit hoofdstuk worden de randvoorwaarden besproken en wordt er genoteerd of de producten op de shortlist hieraan voldoen.

9.6.3.1.1. Ondersteuning voor de prioriteit SaaS-applicaties. (R01)

Alle oplossingen die in de shortlist zijn meegenomen, ondersteunen de vier SaaS-applicaties die prioriteit hebben. Sommige leveranciers moeten de SaaS-applicaties op aanvraag toevoegen aan de CASB en bij andere producten is er de mogelijkheid om dit zelf te doen.

9.6.3.1.2. Voordelen Microsoftproduct. (R02)

Er is maar één product op de shortlist dat voldoet aan deze randvoorwaarde en dat is de Microsoft CASB. De voordelen die deze CASB heeft, zijn verderop genoemd in de paragraaf die dieper op de CASB van Microsoft ingaat.

9.6.3.1.3. Werkt met de aanwezige netwerkapparatuur. (R03)

Alle oplossingen die op de shortlist genoteerd staan, kunnen overweg met de netwerkapparatuur bij de klanten van PCI IT. Alle oplossingen kunnen overweg met de logging formats die aangeleverd worden door Palo Alto en in het geval van McAfee is er een integratie met Palo Alto beschikbaar om actiever te sturen in het netwerkverkeer.

9.6.3.1.4. De CASB heeft meer te bieden dan de DLP die tot nu gebruikt wordt. (R04)

Dit is het geval voor alle producten die genoteerd staan op de shortlist. Alle producten bieden meer inzicht in SaaS-applicaties, ondersteunen meerdere SaaS-applicaties en voegen zaken zoals zicht op SaaS gerelateerde schaduw IT toe.

9.6.3.1.5. De CASB is marktconform geprijsd. (R05)

Tijdens dit project is meerdere keren getracht contact te krijgen met bedrijven om toelichting van beschikbare informatie of überhaupt informatie. Dit is ook het geval als er gesproken wordt over de prijzen van de oplossingen. Op Microsoft na is er van alle producten op de shortlist geen officiële prijs beschikbaar. Er zijn gesprekken, speculaties en prijzen van subcontractors te vinden maar geen exact openbaar bedrag. Hierom kan er helaas niet gelet worden op de prijs. Er kan alleen ingegaan worden op licentiestructuren waarop een product is weggezet door de leverancier.

9.6.3.1.6. Opgeslagen data locatie is AVG-compliant. (R06)

Alle oplossingen die op de shortlist genoteerd staan, kunnen binnen de EU of zelfs binnen Nederland gehost worden om te voldoen aan de eisen binnen de AVG (Forcepoint, z.d.-a; McAfee, 2021e; Microsoft, z.d.).

9.6.3.1.7. Het is een enkele oplossing en geen samenvoeging. (R07)

Alle oplossingen die op de shortlist genoteerd staan, zijn een losse CASB zonder samenvoeging van producten. De enige echte afhankelijkheid welke aanwezig is, is de aanvoer van logging. Hiernaast kan er per product nog afhankelijkheid zijn voor een verbeterde werking zoals Microsoft Defender for Endpoint bij Microsoft of Palo Alto netwerkapparatuur bij McAfee voor een actievere sturing in het netwerk.

9.6.3.2. MVISION Cloud (Skyhigh Networks Cloud Security Platform)

MVISION Cloud is een oplossing van McAfee welke op de markt is gezet als een CASB. De oplossing van Microsoft was het hoogst genoteerd in de magic quadrant van Gartner in 2020 zoals te zien in figuur 7 (Lawson & Riley, 2020).

De conclusie is dat de oplossing in theorie voldoet aan alle eisen van PCI IT. De oplossing kan SaaS gerelateerde schaduw IT zichtbaar maken op het bedrijfsnetwerk, de oplossing kan sturen in beheerde SaaS-applicaties die toegevoegd zijn aan de CASB en de oplossing kan sturen in netwerkverkeer. Het grote nadeel is echter dat de SaaS-applicaties die klanten van PCI IT gebruiken niet officieel ondersteund worden. Dit betekent dat er voor de werking van deze SaaS-applicaties minimaal acties van McAfee nodig zijn, wat betekent dat er geen gegarandeerde werking is bij de aanschaf van het product. Hoewel er altijd voor gekozen kan worden om de SaaS-applicatie toe te voegen als “Custom app”, kunnen er vraagtekens geplaatst worden bij de uitvoering van deze in theorie goede oplossing. Deze functionaliteit van McAfee is gebaseerd op het leren van gedrag op de webpagina van de SaaS-applicatie. Zodra er veranderingen worden gemaakt aan de SaaS-applicatie, kan het zijn dat de monitoring niet meer werkt.

9.6.3.3. Lookout

Lookout biedt een CASB aan welke een samenvoeging van zijn eigen product is met toevoegingen van het in 2021 overgenomen bedrijf Ciphercloud (Lookout, 2021). Lookout heeft weinig openbare informatie over de technische werking van hun CASB en daarom is zo goed als alle gebruikte informatie uit een tweetal gesprekken die ik gevoerd heb met Paul Visch (Accountmanager) en Andela Popovic (Business Development Representative).

De conclusie over de CASB van Lookout is dat de oplossing in theorie voldoet aan alle eisen van PCI IT. De oplossing kan SaaS gerelateerde schaduw IT zichtbaar maken op het bedrijfsnetwerk, de oplossing kan sturen in beheerde SaaS-applicaties mits deze door Lookout toegevoegd zijn en de oplossing kan sturen in netwerkverkeer. Daarnaast is er bij Lookout in het verleden al gewerkt met Exact Online, wat vertrouwen schept over de implementatie van de vereiste applicaties. Er is echter geen agent aanwezig, zoals Microsoft of Forcepoint wél aanbieden, die het bereik van de oplossing zou vergroten. Dit, gebundeld met de compliceerde licentiestructuur, maakt Lookout niet de beste oplossing van de shortlist.

9.6.3.4. Forcepoint

Forcepoint biedt een CASB aan welke een samenvoeging van zijn eigen product is met toevoegingen van het overgenomen Bitglass (Forcepoint, 2021b).

De conclusie is dat de oplossing voldoet aan alle eisen van PCI IT. De oplossing kan SaaS gerelateerde schaduw IT zichtbaar maken op het bedrijfsnetwerk, de oplossing kan sturen in beheerde SaaS-applicaties die toegevoegd zijn aan de CASB (en daarbuiten indien er gebruik wordt gemaakt van een beheerd apparaat met een agent), de oplossing kan een ACL opstellen om te sturen in netwerkverkeer op de bedrijfslocatie en de oplossing kan netwerkverkeer van beheerde apparaten op elk netwerk sturen.

9.6.3.5. Microsoft Defender for Cloud Apps

Microsoft biedt een CASB aan welke de naam Microsoft Defender for Cloud Apps draagt. Deze oplossing is verweven in het licentiemodel van Microsoft en de producten welke Microsoft aanbiedt. Deze integratie en andere zaken zoals OAuth monitoring, samenvoeging met Microsoft Defender for Endpoint en de mogelijkheid om niet-officieel ondersteunde SaaS-oplossingen te integreren in deze CASB maken Microsoft Defender for Cloud Apps een zeer interessante oplossing.

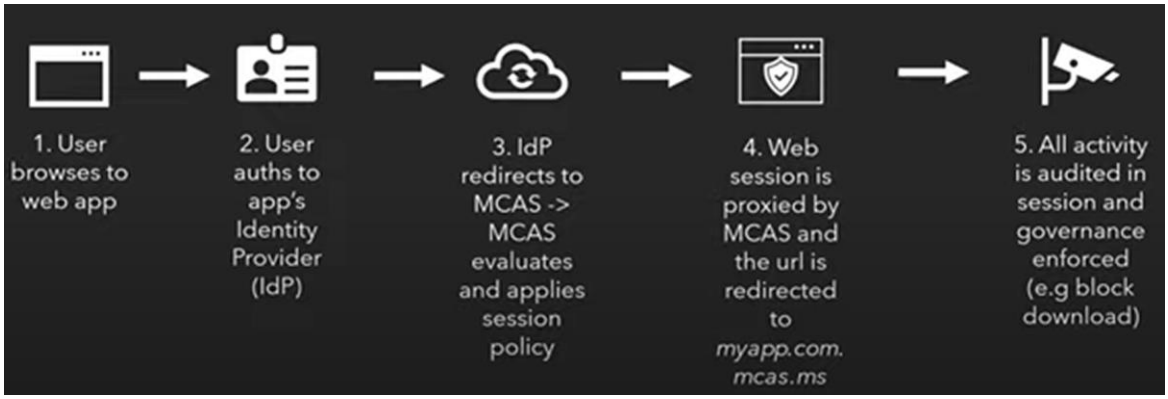
9.6.3.5.1. Ondersteuning van SaaS-applicaties

Zoals kort in de inleiding al beschreven, heeft deze oplossing naast de standaard ondersteunde SaaS-oplossingen ook de mogelijkheid om andere SaaS-applicaties toe te voegen. Deze functionaliteit heet “Conditional Access App Control” en is te gebruiken bij apps die voldoen aan de hieronder genoteerde eisen (Microsoft, 2021g):

- De volgende licenties moeten aanwezig zijn
    - Azure Active Directory Premium P1 of hoger indien Azure gebruikt wordt als IDP. Indien er gebruik wordt gemaakt van een andere IDP dan moet de licentie van de IDP-leverancier toereikend zijn.
    - Microsoft Defender for Cloud Apps, deze licentie is verwerkt in de volgende producten (Microsoft, 2021a):
        - Microsoft 365 E5
        - Microsoft 365 E5 Security
        - Microsoft 365 E5 Compliance
        - Enterprise Mobility & Security E5
        - Microsoft Cloud App Security + Enterprise Mobility & Security E3
        - Microsoft 365 Education A3
        - Microsoft 365 Education A5
        - Microsoft Cloud App Security (losse licentie)
- De apps die toegevoegd worden moeten voorzien zijn van Single Sign-On (SSO)
- De apps die toegevoegd worden moeten, indien Azure als IDP gebruikt wordt, SAML 2.0 of OpenID Connect ondersteunen. Indien een andere IDP-leverancier wordt gebruikt, dan moet de applicatie SAML 2.0 ondersteunen.

Indien alles aan de eisen voldoet en het geconfigureerd is, dan wordt er door middel van een functie die Microsoft “sessiebeheer” noemt, monitoring op die exacte situatie toegepast. Het verkeer wordt omgeleid via een reverse proxy en zal dus niet direct met een dienst zoals Exact online communiceren.

De afhandeling van een standaard inlog in bijvoorbeeld Exact online is in figuur 10 hieronder gevisualiseerd.



Figuur 8 Flow sessiebeheer (Soseman, 2020b, 2:34)

Zoals in de afbeelding al aangehaald wordt, zorgt “Conditional Access App Control” ervoor dat de CASB inzicht heeft en acties in de SaaS-applicatie kan sturen (Microsoft, 2021o). De oplossing heeft volgens Microsoft (Microsoft, 2019; Microsoft, 2021m; Microsoft, 2021o) de volgende mogelijkheden als de sessie actief is:

- **“Gegevensexfiltratie voorkomen:** u kunt het downloaden, knippen, kopiëren en afdrukken van gevoelige documenten op bijvoorbeeld onbeheerde apparaten blokkeren.
- **Verificatiecontext vereisen:** u kunt het beleid voor voorwaardelijke toegang van Azure AD opnieuw beoordelen wanneer er een gevoelige actie plaatsvindt in de sessie. Bijvoorbeeld meervoudige verificatie vereisen bij het downloaden van een uiterst vertrouwelijk bestand.
- **Beveiligen bij downloaden:** in plaats van het downloaden van gevoelige documenten te blokkeren, kunt u vereisen dat documenten worden gelabeld en beveiligd met Azure Information Protection. Deze actie zorgt ervoor dat het document wordt beveiligd en dat gebruikerstoegang wordt beperkt in een mogelijk riskante sessie.
- **Uploaden van niet-gelabelde bestanden voorkomen:** voordat een gevoelig bestand wordt geüpload, gedistribueerd en gebruikt door anderen, is het belangrijk om ervoor te zorgen dat het bestand het juiste label en de juiste beveiliging heeft. U kunt ervoor zorgen dat niet-gelabelde bestanden met gevoelige inhoud niet worden geüpload totdat de gebruiker de inhoud classificeert.
- **Mogelijke malware blokkeren:** u kunt uw omgeving beschermen tegen malware door het uploaden van mogelijk schadelijke bestanden te blokkeren. Elk bestand dat wordt geüpload of gedownload, kan worden gescand op bedreigingsinformatie van Microsoft en onmiddellijk worden geblokkeerd.
- **Gebruikerssessies controleren op naleving:** riskante gebruikers worden bewaakt wanneer ze zich aanmelden bij apps en hun acties worden vastgelegd vanuit de sessie. U kunt het gedrag van gebruikers onderzoeken en analyseren om te begrijpen waar en onder welke omstandigheden sessiebeleid in de toekomst moet worden toegepast.
- **Toegang blokkeren:** u kunt de toegang voor specifieke apps en gebruikers gedetailleerd blokkeren, afhankelijk van verschillende risicofactoren. U kunt ze bijvoorbeeld blokkeren als ze clientcertificaten gebruiken als een vorm van apparaat beheer.
- **Aangepaste activiteiten blokkeren:** sommige apps hebben unieke scenario's die risico's met zich meebrengen, bijvoorbeeld het verzenden van berichten met gevoelige inhoud in apps zoals Microsoft Teams of Slack. In dit soort scenario's kunt u berichten scannen op gevoelige inhoud en deze in realtime blokkeren.” (Microsoft, 2021m).

Dankzij de mogelijkheden van deze oplossing is het dus mogelijk om de vier genoemde SaaS-applicaties te monitoren (AFAS, z.d.; Exact, z.d.). Naast de vier genoemde SaaS-applicaties met prioriteit is de verwachting dat veel van de in de deelvraag genaamd SaaS-applicaties?” genoteerde SaaS-applicaties zullen voldoen aan de gestelde eisen om verwerkt te worden in deze CASB.

9.6.3.5.2. Locatieafhankelijkheid van de oplossing

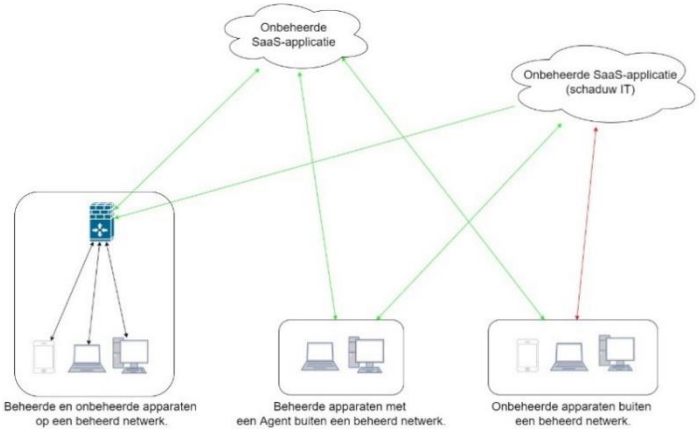
Om een beeld te vormen van de mogelijkheden van de oplossing op verschillende locaties zijn de vier situaties van gebruikers hieronder genoteerd en daarna visueel weergegeven in figuur 9.

Op het bedrijfsnetwerk

- Onbeheerde apparaten
    - Het gebruik van beheerde en onbeheerde SaaS-applicaties wordt op verschillende manieren in de gaten gehouden. Al het netwerkverkeer en de beheerde SaaS-applicaties die in de CASB geconfigureerd zijn, worden gemonitord door middel van de API of forward- en reverse proxy. Hierdoor zijn de acties in de beheerde SaaS-applicaties zichtbaar en kan hier op gestuurd worden. Daarnaast is het gebruik van SaaS gerelateerde schaduw IT zichtbaar dankzij logging afkomstig van de netwerkapparatuur op locatie welke de CASB verwerkt. Afhankelijk van de instellingen kan ook in het netwerkverkeer gestuurd worden door middel van een ACL.
- Beheerde apparaten
    - Bovenop alle eigenschappen die een onbeheerd apparaat op dit netwerk geniet, kan er in het geval van een beheerd apparaat gestuurd worden via de agent. Dit heeft hetzelfde resultaat als via een ACL.

Buiten het bedrijfsnetwerk

- Onbeheerde apparaten
    - Het gebruik van onbeheerde SaaS-applicaties wordt op verschillende manieren gemonitord. De beheerde SaaS-applicaties worden door middel van een reverse proxy of via API gemonitord. Hierdoor zijn de acties in de beheerde SaaS-applicaties zichtbaar, maar is er geen zicht op het gebruik van SaaS gerelateerde schaduw IT vanaf deze apparaten en kan er ook niet in netwerkverkeer gestuurd worden.
- Beheerde apparaten
    - Het gebruik van beheerde en onbeheerde SaaS-applicaties wordt op verschillende manieren in de gaten gehouden. Het netwerkverkeer wordt gemonitord via de Microsoft Defender Advanced Threat Protection van het apparaat en de beheerde SaaS-applicaties die in de CASB geconfigureerd zijn, worden gemonitord via de CASB. Hierdoor zijn de acties in de beheerde SaaS-applicaties zichtbaar en kan hier op gestuurd worden. Daarnaast is het gebruik van schaduw IT zichtbaar en kan ook hierin gestuurd worden.



Figuur 9 CASB-werking met agent

9.6.3.5.3. Netwerkapparatuur ondersteuning

Microsoft Defender voor Cloud Apps is compatibel met alle “edge” apparaten. Dit kan een firewall, SWG of proxy zijn, die allen logging kunnen aanleveren aan de CASB. Deze logging zal dan geanalyseerd worden om een beeld van het netwerkgebruik en dus de SaaS gerelateerde schaduw IT te genereren. Buiten deze standaard inzichten in de schaduw IT op basis van logging kan Microsoft Defender voor Cloud Apps ook geïntegreerd worden met een aantal soorten proxies of firewalls. Indien deze ondersteund worden, kan er actiever gestuurd worden in het netwerkverkeer. De oplossingen waarmee dat mogelijk is, zijn hieronder genoemd (Microsoft, 2021n).

- Zscaler
- Iboss
- Corrata
- Menlo security

Naast de hierboven genoemde producten zijn er andere mogelijkheden om in het netwerkverkeer te sturen met deze CASB. Dit wordt gedaan door middel van het creëren van een blocklist (dit is een benaming van Microsoft, in feite is het een ACL), waarna deze richting een “edge” apparaat wordt verstuurd. Deze blocklist is een product van de CASB welke dan aan het netwerkapparaat duidelijk maakt dat de websites die genoemd zijn in de blocklist niet meer bezocht mogen worden. Op het moment van schrijven worden de volgende fabrikanten ondersteund (Microsoft, 2021e).

- BlueCoat ProxySG
- Cisco ASA
- Fortinet FortiGate
- Juniper SRX
- Palo Alto
- Websense
- Zscaler

9.6.3.5.4. Unique Selling Points (USP)

De eerste USP van het product van Microsoft is de integratie met de Microsoft Defender for endpoint, doordat deze oplossing werkt met de managed variant van Windows Defender welke in basis al aanwezig is op de beheerde laptops van klanten. Dit zorgt ervoor dat er met vrij weinig configuratie een agent aanwezig is op de beheerde apparaten. Deze agent kan vanaf dat moment actief sturen in netwerkverkeer, zelfs als het apparaat niet op het bedrijfsnetwerk aanwezig is (Microsoft, 2021b). Dit zorgt ervoor dat het apparaat buiten het netwerk van het bedrijf beveiligd is en dat ook het zicht op SaaS gerelateerde schaduw IT aanwezig blijft (Soseman, 2020a). Om deze functionaliteit te gebruiken, moet er gebruik gemaakt worden van een Microsoft Defender for Endpoint license. Er zijn enkele licenties waar het gebruik van deze Microsoft Defender for Endpoint in verweven zit en dit zijn:

- Windows 11 Enterprise E5
- Windows 11 Education A5
- Windows 10 Enterprise E5
- Windows 10 Education A5
- Microsoft 365 E5
- Microsoft 365 A5
- Microsoft 365 E3 met Enterprise Mobility en Security E5 Add-on
- Microsoft 365 Business Premium (indien aangeschaft via een Microsoft Cloud Solution Provider)
- Microsoft 365 E5 Security

- Microsoft 365 A5 Security
- Microsoft Defender for Endpoint (losse licentie) (Microsoft, 2021i)

Na navraag bij PCI IT blijkt dat het gros van de klanten van PCI IT gebruik maakt van Microsoft365 E3, Microsoft 365 Business Premium, Office 365 E3 en enkele klanten op Microsoft365 E5. Zoals uit de opgevraagde licentie modellen blijkt, zal voor de complete werking van Microsoft Defender for Cloud Apps, Microsoft Defender for Endpoint en Microsoft Defender for Cloud Apps Discovery een Microsoft365 E5 licentie afdoende zijn. Gezien er ook veel gebruik wordt gemaakt van Microsoft365 E3, raad ik aan om Microsoft365 E5 Security toe te voegen aan de E3 licentie. Afhankelijk van het volume waarmee deze licenties worden ingekocht en de oorsprong zal dat ongeveer € 8,76 per gebruiker per maand kosten (dsaict, z.d.). De Microsoft 365 Business Premium licenties zouden op een soortgelijke manier uitgebreid kunnen worden (Microsoft, 2021t).

De tweede USP van Microsoft Defender for Cloud Apps is dat het inzicht kan creëren in de applicaties van derden waar OAuth rechten aan verleend zijn met een managed SaaS-account (Microsoft, 2021d). Dankzij deze toevoeging is er meer grip en zicht op de rechten die gebruikers aan derde partijen verlenen. Naast dat er staat dat er rechten zijn gegeven, zal er ook informatie staan over de dienst welke de rechten heeft ontvangen. Aan de hand van deze informatie kunnen er dan acties opgezet worden en kunnen de rechten ingetrokken worden. Daarnaast kan deze CASB hier automatisch actie op ondernemen indien dit geconfigureerd is.

De derde USP van Microsoft Defender for Cloud Apps is dat de licentie structuur anders opgezet is dan die van de concurrentie. Waar dit bij de concurrentie zoals Lookout vaak is dat er per koppeling met een SaaS-applicatie betaald wordt, is dit bij Microsoft Defender for Cloud Apps per gebruiker. Dit zorgt ervoor dat er bij Microsoft een enkele licentie kan worden afgenomen en niet naast de licentie per gebruiker gerekend wordt met licenties voor de SaaS-applicaties en gebruikers.

9.6.3.5.5. Conclusie

De conclusie is dat de oplossing voldoet aan alle eisen van PCI IT. De oplossing kan SaaS gerelateerde schaduw IT zichtbaar maken op het bedrijfsnetwerk (en daarbuiten indien er gebruik wordt gemaakt van een beheerd apparaat met Microsoft Defender for Endpoint), de oplossing kan sturen in beheerde SaaS-applicaties die toegevoegd zijn aan de CASB, de oplossing kan blocklists opstellen om te sturen in netwerkverkeer op de bedrijfslocatie en de oplossing kan netwerkverkeer van beheerde apparaten op elk netwerk sturen. Naast de technische mogelijkheden die deze oplossing biedt, zijn ook het licentiemodel en de integratie met Microsoft haar eigen producten een grote pré. De licentie is, zoals gezegd, in sommige gevallen al aanwezig en in andere zal het een uitbreiding zijn op een bestaande licentie. De integratie met andere (security) gerelateerde producten van Microsoft zoals in dit geval de Microsoft Defender for Endpoint is ook iets wat veel voordelen oplevert, zoals het overzicht en de controle.

9.6.3.6. Conclusie shortlist

Als alle oplossingen van de leveranciers op de shortlist tegenover elkaar worden gezet, dan komt Microsoft boven de andere oplossingen uit. De oplossing heeft samen met Forcepoint het grootste bereik door de inzet van een agent, maar onderscheidt zich van Forcepoint door middel van de mogelijkheid om SaaS-applicaties zelf toe te voegen met duidelijke requirements. Daarnaast onderscheidt het zich omdat er een licentievoordeel aanwezig is, aangezien er al gebruik wordt gemaakt van gerelateerde Microsoftproducten, omdat er OAuth monitoring aanwezig is en omdat deze CASB diepgaande integratie heeft binnen het Microsoft ecosysteem. Naast de voordelen die zichtbaar zijn in technische eigenschappen, is er al een bestaande relatie met Microsoft wat een pré vanuit PCI IT is en is Microsoft erg transparant in de mogelijkheden van haar CASB. Dit versterkt het gevoel dat er een werkend product aangeschaft wordt in tegenstelling tot een belofte. Waar bij andere producten de belofte wordt gedaan om een SaaS-applicatie in de CASB te integreren, wordt bij deze CASB duidelijk vermeld welke vereisten er zijn om een SaaS-applicatie werkend te krijgen.

Dit alles maakt dat ik met vertrouwen kan aanraden om Microsoft Defender for Cloud Apps in te gaan zetten bij klanten van PCI IT. Aangezien Microsoft Defender for Cloud Apps voldoet aan alle opgestelde requirements en randvoorwaarden is het antwoord op de deelvraag “Welke beveiliging en controle oplossingen zijn er op de markt die voldoen aan de eisen van PCI IT en welke past het beste bij PCI IT?” dan ook Microsoft Defender for Cloud Apps.

9.7. Hoe zouden toekomstige klantsystemen gebruik kunnen maken van de gekozen oplossing en is dit met terugwerkende kracht toe te passen op bestaande systemen?

In de laatste fase van het project is er gekeken naar hoe het gekozen product het meest effectief ingezet kan worden door PCI IT. Mijn bevindingen en zaken die ik aanraad om het product succesvol op de markt te zetten, zijn vermeld in dit hoofdstuk. In het geval van dit project is er geen toegang tot de diverse klantsystemen en is er nog geen product ingekocht om mee te werken. Het resultaat hiervan is dat er alleen implementatie advies kan worden uitgebracht over de toekomstige inrichting aan de hand van tekstuele uitleg. In dit hoofdstuk is er zoveel mogelijk beschreven wat gedaan moet worden om het maximale uit het potentieel aangekochte product te halen en hoe deze te verwerken is in nieuwe en bestaande infrastructuren. Gezien de CASB als een SaaS-dienst geleverd wordt, zal er geen implementatie nodig zijn op on-premise gehoste infrastructuur, zoals een ESXI host. Dit zorgt er ook voor dat dit detail van de implementatie niet beschreven is.

9.7.1. Licenties

Om van dit product gebruik te maken zijn er enkele licenties nodig. Zoals eerder beschreven, hebben PCI IT en haar klanten het voordeel dat sommige licenties al aanwezig zijn of dat er alleen een licentie uitbreiding nodig is. In het hoofdstuk Unique Selling Points (USP) en "Ondersteuning van SaaS-applicaties" is beschreven hoe er gecombineerd kan worden met verschillende licenties. Gezien de aanwezige licenties per klant verschillen, is er geen definitief antwoord op de vraag welke licentie het meest kosteffectief is, maar over het algemeen genomen zal dit Microsoft365 E5 Security zijn. Deze licentie bevat de mogelijkheid om gebruik te maken van Microsoft Defender for Cloud Apps en Microsoft Defender for Endpoint.

9.7.2. SaaS gerelateerde schaduw IT inzichtelijk maken

Dit project heeft twee hoofddoelen, waaronder het inzicht in SaaS gerelateerde schaduw IT verschaffen. Om inzicht te krijgen in het netwerkverkeer en dus de SaaS gerelateerde schaduw IT die aanwezig is op de bedrijfslocatie, zal er gebruik moeten worden gemaakt van de logboeken van netwerkapparatuur of de Microsoft Defender for Endpoint agent. In het geval van logboeken van netwerkapparatuur zullen deze logboeken door middel van een zogenoemde "logboekverzamelaar" aangeleverd moeten worden aan de CASB (Microsoft, 2021c Microsoft, 2021j). Er zijn verschillende manieren waarop deze logboekverzamelaar gehost wordt, maar het zal – of het nu lokaal op een Ubuntu machine draait of in Azure zelf – allemaal op basis van een Docker container zijn (Microsoft, z.d.-c).

De tweede mogelijkheid om inzicht in SaaS gerelateerde schaduw IT te genereren is om gebruik te maken van Microsoft Defender for Endpoint zoals beschreven in Microsoft Defender for Endpoint. Indien de logboekverzamelaar en Microsoft Defender for Endpoint juist geconfigureerd zijn, zal het gebruik van SaaS gerelateerde schaduw IT op en buiten het kantoornetwerk zichtbaar zijn.

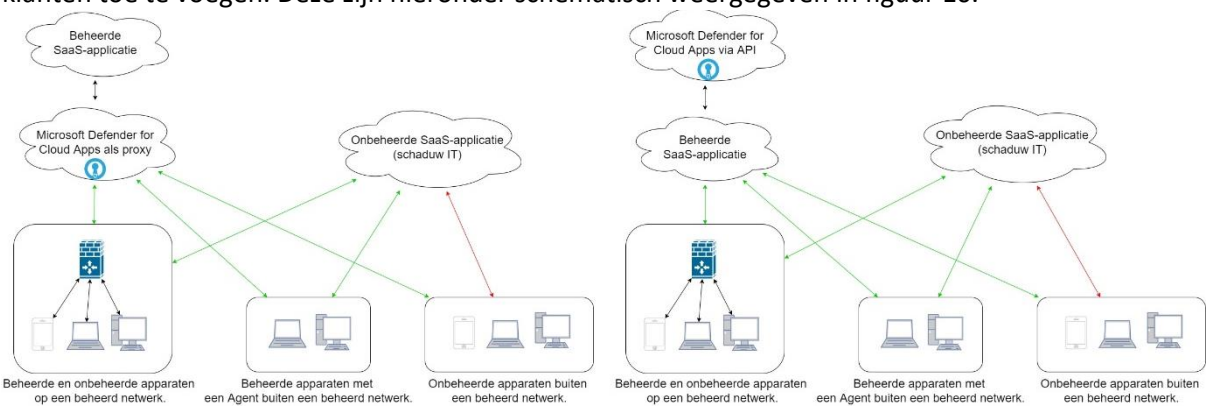
Zodra de SaaS gerelateerde schaduw IT via één van de genoemde manieren inzichtelijk is, zal er door de CASB informatie bij genoteerd worden over de locatie van de webserver, de beveiliging van de website, compliance, bedrijfsinformatie en nog veel meer. Op basis van deze gegevens zal er een risicoscore aan de gedetecteerde SaaS gerelateerde schaduw IT gekoppeld worden (M. Soseman, 2020). De genoemde punten, zoals compliance of de totaal score, kunnen gebruikt worden om automatisch SaaS-applicaties te blokkeren die niet voldoen aan de eisen van de organisatie.

9.7.3. Blokkeren van toegang tot SaaS-applicaties

In de vorige paragraaf is besproken hoe de logging van netwerkapparatuur verzonden gaat worden naar de CASB. Aan de hand van de informatie uit deze logging kan bepaald worden dat er te veel gebruik wordt gemaakt van een niet beheerde SaaS-applicatie en dat deze niet meer bereikbaar moet zijn. Om dit rond te krijgen, kan deze SaaS-applicatie op een zwarte lijst gezet worden zodat deze niet meer te bereiken is vanaf het kantoornetwerk of een beheerd apparaat. Deze lijsten kunnen op twee manier gebruikt worden. De eerste variant is dat deze lijst wordt geëxporteerd en geïmporteerd gaat worden in de netwerkapparatuur van de klant. Dit zorgt ervoor dat beheerde en onbeheerde apparaten niet meer vanaf het bedrijfsnetwerk bij de SaaS-applicaties kunnen komen. De tweede methode is dat er gebruik wordt gemaakt van Microsoft Defender for Endpoint op de beheerde apparaten. Indien dit het geval is en er geconfigureerd is zoals beschreven in Microsoft Defender for Endpoint, dan kunnen deze beheerde apparaten niet meer bij de SaaS-applicaties op de zwarte lijst, ongeacht op welk netwerk zij aanwezig zijn.

9.7.4. Acties in SaaS-applicaties inzichtelijk krijgen

Het tweede hoofddoel van dit project is het inzichtelijk krijgen van acties van gebruikers van SaaS-applicaties en hierop kunnen acteren. Zaken zoals inloggen, benaderen van data, downloaden, delen van data en meer zullen dan inzichtelijk zijn en kunnen gemonitord worden (Microsoft, 2021m). Om dit te implementeren zullen de gebruikte SaaS-applicaties toegevoegd moeten worden binnen de CASB. Er zijn twee varianten die gebruikt moeten worden om de gebruikte SaaS-applicaties van klanten toe te voegen. Deze zijn hieronder schematisch weergegeven in figuur 10.



Figuur 10 SaaS-applicaties communicatie reverse proxy en API

De eerste variant is via de “app-connector-API” van Microsoft. Deze zal gebruikt worden om de verbinding te leggen met Office 365 via een daarvoor ontworpen API. Dit is een kwestie van de stappen op de “app connector” pagina in Microsoft Defender for Cloud Apps doorlopen. Hier zal toestemming worden verleend tot de Office365 omgeving via de API (Microsoft, 2021j). Met deze variant zal er na implementatie door de CASB via API-communicatie plaatsvinden om activiteiten te controleren. Dit betekent dat de gebruikers de originele SaaS-applicatie bezoeken en op de achtergrond de CASB en de SaaS-applicatie contact hebben.

De tweede optie welke gebruikt gaat worden voor het gros van de applicaties zoals AFAS online en Exact online is “Conditional Access App Control”. Deze variant maakt gebruik van de reverse proxy implementatie van een CASB. Om gebruik te maken van deze variant moet er een aantal zaken aangemaakt worden. Eerst moet er een “Conditional Access Policy” aangemaakt worden om de scope te creëren. Hierna moet er verbinding gemaakt worden met de IDP die aan de eerdergenoemde SAML 2.0 of OpenID eisen voldoet. Zodra dit is gebeurd, kunnen er policies worden aangemaakt om het gebruik van de SaaS-applicatie te sturen, zoals het blokkeren van downloads van niet beheerde apparaten (Microsoft, 2021q). Deze variant van connectie tussen de CASB en de SaaS-

applicatie is anders dan de eerstgenoemde, want in dit geval zal de gebruiker niet meer direct communiceren met de website van de SaaS-applicatie maar zal de gebruiker worden omgeleid naar de CASB. Een URL zoals portal.office.com zal veranderen in een URL van de CASB zoals casb.portal.office.com. Zodra de aanmeldpoging via een IDP geauthentiseerd is, zal de gebruiker naar de URL van de CASB doorgestuurd worden en zal de sessie gemonitord kunnen worden. Hoe dit proces er visueel uitziet, is weergegeven in figuur 11.

Figuur 11 Microsoft Defender for Cloud Apps flow

Nadat de SaaS-applicaties toegevoegd zijn, is er inzichtelijk wat er binnen deze SaaS-applicaties wordt gedaan door de gebruikers van deze SaaS-applicaties. Acties zoals inloggen, openen van bestanden, delen van bestanden of zelfs knip-en-plak pogingen zullen dan inzichtelijk zijn (Microsoft, 2021m; Soseman, 2020b).

9.7.5. Policies creëren

In de vorige paragraaf is al kort geschreven over het aanmaken van policies om gedrag in SaaS-applicaties te beheren en notificaties te ontvangen bij ongewenst gedrag binnen de SaaS-applicaties. De policies welke aangemaakt worden zullen per klant van PCI IT verschillen, maar mijn advies is om, gezien de oorsprong van het project en de wens van PCI IT, zo veel mogelijk acties van niet beheerde apparaten te blokkeren met policies. Dit zorgt ervoor dat er geen data toegankelijk is op een apparaat waar geen controle over is en waarop dus bijvoorbeeld geen encryptie geconfigureerd is. Een voorbeeld hiervan is dat een onbeheerd apparaat wel mag inloggen in Office365 maar geen bestanden mag downloaden of inhoud van bestanden mag kopiëren.

Naast de implementatie van policies welke zaken afvangen, adviseer ik PCI IT om gebruik te maken van zichtbare waarschuwingen die de gebruiker van SaaS-applicaties ziet zodra een threshold overschreden wordt. Dit kan gebruikt worden om de medewerkers te onderwijzen en gelijktijdig de ongewenste actie tegen te houden.

9.7.6. Microsoft Defender for Endpoint

Om maximaal gebruik te maken van de CASB van Microsoft moet er gebruik worden gemaakt van Microsoft Defender for Endpoint. Dit heeft als eerste voordeel dat er op locaties buiten het bedrijfsnetwerk ook voorkomen kan worden dat SaaS-applicaties op de zwarte lijst bezocht worden en als tweede voordeel dat er buiten het bedrijfsnetwerk alsnog zicht is op het gebruik van SaaS gerelateerde schaduw IT.

Om gebruik te maken van de samenvoeging van Microsoft Defender voor Cloud Apps en Microsoft Defender for Endpoint moet er een koppeling gemaakt worden tussen deze twee Microsoftproducten, moet er voor beide zoals eerder beschreven een licentie aanwezig zijn en moeten realtime-beveiliging, cloudbeveiliging en netwerkbeveiliging geconfigureerd zijn in Microsfoft Defender Antivirus (Microsoft, 2021o). De laatste drie configuratie aanpassingen van Microsoft Defender Antivirus kunnen afgedwongen worden via een Group Policy op de beheerde apparaten en de koppeling tussen Microsoft Defender voor Cloud Apps en Microsoft Defender for Endpoint kan gemaakt worden in security.microsoft.com.

9.7.7. Personeel

Het product dat tijdens dit project gekozen is, is een product dat naast de tijd die in de verkoop en inrichting van het product zit, ook extra meldingen oplevert en dus tijd van bestaande werknemers vraagt. Uit gevoerde gesprekken met bijvoorbeeld Bart Brevink is gebleken dat er een tweetal varianten is waarin dit gekozen product ingezet gaat worden.

De eerste variant is de variant die minder tijd van het personeel van PCI IT gaat vragen. Dit is het geval omdat er alleen een traject aanwezig is waar dit product verkocht en geconfigureerd wordt aan een klant. De tweede variant is de variant die de meeste tijd van het personeel van PCI IT gaat vragen. In dit geval is het namelijk zo dat het product als service op de markt gebracht wordt. PCI IT zal dan als MSSP zal fungeren. In deze situatie zullen het onderhoud en de controle van het systeem en de melding hieruit door de medewerkers van PCI IT opgepakt moeten worden.

In beide gevallen zal er rekening moeten worden gehouden met de manuren die in dit product gestopt moeten worden om deze adequaat te ondersteunen. Uit de gesprekken die ik met Bart Brevink heb gevoerd, blijkt PCI IT hiervan op de hoogte te zijn en is hieraan gedacht. Indien dit product op de markt wordt gezet, zal er gekeken worden naar extra personeel om deze dienst te ondersteunen.

9.7.8. Veranderende markt

Zoals in de contextanalyse al kort aangehaald werd, is de IT-markt een snel bewegende markt waar niet stil gestaan kan worden. Ik raad PCI IT ook aan om, als deze CASB daadwerkelijk geïmplementeerd wordt, scherp op te letten of er nieuwe functies worden toegevoegd aan de CASB en te blijven kijken naar ontwikkelingen op de markt. Hiervoor zouden bronnen zoals de Magic Quadrants van Gartner of de hype cycles die Gartner produceert nuttig kunnen zijn.

9.7.9. Kritiek op heimelijk toezicht

Gezien een CASB een oplossing is welke zeer veel inzichten geeft in acties van gebruikers, zal niet elke organisatie gretig zijn om een CASB te implementeren. De CASB kan door sommige mensen gezien worden als een inbreuk op privacy van de werknemers. Zelfs als de IT of de IT-security de wens heeft om deze oplossing te implementeren, dan is er een goede mogelijkheid dat een ondernemingsraad niet gelijk akkoord gaat met de implementatie van een CASB. Een CASB kan namelijk voor dezelfde discussies zorgen als heimelijk cameratoezicht bij bedrijven, aangezien het doel van het bedrijf de privacy van medewerkers schendt. Voor PCI IT is het daarom aan te raden dat zij zichzelf onderwijzen over de mogelijkheden van Microsoft Defender for Cloud Apps om data te anonimiseren. Dit is bijvoorbeeld mogelijk voor inzichten in SaaS gerelateerde schaduw IT (Microsoft, 2021h).

9.7.10. Conclusie

Door de functionaliteiten van de CASB welke Microsoft op de markt heeft gebracht, is het mogelijk om deze te implementeren in bestaande klantomgevingen en omgevingen van toekomstige klanten, indien de SaaS-applicaties aan de eisen zoals genoemd in “Ondersteuning van SaaS-applicaties” voldoen. Voor de SaaS-applicaties die prioriteit hebben in dit project is dit nagekeken en alle vier deze SaaS-applicaties voldoen aan de gestelde eisen. De andere SaaS-applicaties zullen waarschijnlijk voldoen aan het eisenpakket om toegevoegd te worden gezien deze eisen redelijk marktconform zijn voor SaaS-applicaties.

10. Conclusie

In dit project is gezocht naar een antwoord op de vraag “Hoe kan PCI IT haar klanten een oplossing bieden die de toegang tot data in SaaS-systemen controleert en restricties op de toegang kan toepassen?”. Aan de hand van de deelvragen is hier gestructureerd naartoe gewerkt met in het achterhoofd wat de eisen van PCI IT zijn en welke randvoorwaarden er aanwezig zijn. Door middel van onderzoek is gebleken dat het producttype dat PCI IT wenst te gaan gebruiken een CASB is. Op basis van een long- en shortlist is uiteindelijk gebleken dat Microsoft Defender for Cloud Apps het beste bij de door PCI IT gestelde requirements past. In de voorgaande deelvragen is deze oplossing doorgelicht en is beschreven hoe de implementatie eruit zou zien en met welke randzaken rekening moet worden gehouden tijdens de implementatie. Indien het ontwerp en de gegeven adviezen ter harte worden genomen tijdens een toekomstige implementatie, is het mogelijk om toegang tot de data in SaaS-applicaties te monitoren en te beheren zoals gevraagd in de hoofdvraag en is het mogelijk om inzicht te krijgen in SaaS gerelateerde schaduw IT, zoals PCI IT in interviews als requirement heeft uitgesproken.

11. Reflectie

Vanaf het begin ben ik heel erg geïnteresseerd geweest in het onderwerp van het project aangezien dit probleem niet alleen bij PCI IT en haar klanten aanwezig is. Dit heeft gezorgd dat ik erg veel motivatie had om het project tot een goed einde te sturen. Doordat er dus oprechte interesse aanwezig is geweest sinds de start van het project, is er sinds dag 1 hard gewerkt en is er niet stil gestaan. Op het einde van het project heeft mij dit extra tijd opgeleverd die nodig bleek tijdens de communicatie met leveranciers van de CASB-oplossingen. Hoewel er dus enkele weken uitgetrokken waren voor de communicatie met leveranciers, is er ondanks herhaaldelijke pogingen niet altijd reactie gekomen. Dit heeft er op het punt van het leverancier onderzoek voor gezorgd dat sommige grote namen zoals Netskope niet meegenomen konden worden in het onderzoek. Dit was voor mij een erg demotiverend moment aangezien dit voor mij het gevoel gaf dat een groot deel van het project op dat moment teniet is gedaan. Dit is uiteindelijk besproken met Joost en Theo en hierop is een deadline gesteld waarop reacties binnen zouden moeten zijn. Als de reacties niet op tijd binnen waren, dan zou er begonnen worden met het schrijven van mijn bevindingen en de conclusie. Uit de bevindingen is een goede kandidaat gekomen en hiermee is verder gewerkt om de resterende deelvragen tijdig te beantwoorden. Op dit punt was mijn motivatie weer gegroeid. Dit heeft gezorgd dat er naar mijn mening een goed onderbouwd document is opgesteld met de antwoorden die PCI IT uit dit project wenste te krijgen.

Hoewel ik dus over het algemeen erg tevreden ben met de loop van het project en de resultaten die uit het project zijn gekomen, zijn er enkele dingen die ik bij een volgend project anders zou willen aanpakken. De grootste is een bekend punt waar ik in enkele voorgaande projecten ook tegenaan ben gelopen, namelijk het gestructureerd werken. De grootste valkuil hier is dat ik te veel zaken tegelijkertijd uit probeer te voeren, waardoor er weinig overzicht is van wat de status van verschillende zaken is. Het tweede punt wat ik de volgende keer wil aanpakken, is de structurering van het document. Doordat er sinds het begin fouten in de opmaak van het document zaten, heeft het mij in de laatste dagen voor de oplevering erg veel tijd gekost om dit aan te passen zodat de rode lijn in het document beter zichtbaar zou zijn. Als hier bij de aanvang van het project dieper over was nagedacht, zou dit veel tijd gescheeld hebben. Naast de fouten in de opmaak van het document kan ik ook erg lang van stof zijn. Dit komt de leesbaarheid niet ten goede en dit heeft er op het einde van dit project voor gezorgd dat er nog veel aan opmaak is veranderd.

12. Bronnen

Afas. (z.d.). Single sign-on (SSO) inrichten - AFAS Help Center. Help.Afas. Geraadpleegd op 15 december 2021, van https://help.afas.nl/help/NL/SE/plv2_Config_SSO.htm

American Psychological Association. (2019, oktober). About APA Style. Https://Apastyle.Apa.Org. Geraadpleegd op 3 september 2021, van https://apastyle.apa.org/about-apa-style

Auth0® Inc. (z.d.). OAuth 2.0 Authorization Framework. Auth0 Docs. Geraadpleegd op 29 november 2021, van https://auth0.com/docs/authorization/protocols/protocol-oauth2

Autoriteitpersoonsgegevens. (z.d.). Cameratoezicht op de werkplek. Geraadpleegd op 1 januari 2022, van https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/cameratoezicht/cameratoezicht-op-de-werkplek

AWS. (z.d.). AWS Marketplace: McAfee MVISION Cloud. AWS.Amazon. Geraadpleegd op 5 december 2021, van https://aws.amazon.com/marketplace/pp/prodview-jcqpukfpntzoy

Bales, A. (2021, 20 augustus). Getting DLP Right: 4 Elements of a Successful DLP Program. Gartner. Geraadpleegd op 16 november 2021, van https://www.gartner.com/account/signin?method=initialize&TARGET=http%253A%252F%252Fwww.gartner.com%252Fdocument%252F4004948%253Fref%253DsolrAll%2526refval%253D307099328

Bales, A., & Chugh, R. (2021, 28 juli). Market Guide for Data Loss Prevention. Gartner. Geraadpleegd op 12 november 2021, van https://www.gartner.com/account/signin?method=initialize&TARGET=http%253A%252F%252Fwww.gartner.com%252Fdocument%252F4002997%253Fref%253DsolrAll%2526refval%253D307099621

Barrington, R. (2020, 1 augustus). What is Mendelow's Matrix and Why Is It Useful For Marketers? Oxford College of Marketing Blog. Geraadpleegd op 12 oktober 2021, van https://blog.oxfordcollegeofmarketing.com/2018/04/23/what-is-mendelows-matrix-and-how-is-it-useful/

Bhardwaj, R. (2020, 27 oktober). What is CASB (Cloud Access Security Broker)? ». Network Interview. Geraadpleegd op 16 november 2021, van https://networkinterview.com/what-is-casb-cloud-access-security-broker/

Bitglass. (z.d.). Bitglass CASB Solution Brief. Pages.Bitglass. Geraadpleegd op 7 december 2021, van https://pages.bitglass.com/rs/418-ZAL-815/images/CDFY17SBCloudSecurityBrief.pdf?utm_source=email&utm_campaign=CDFY17SBCloudSecurityBrief&mkt_tok=NDE4LVpBTC04MTUAAAGBM_0maImlQH6amzEKWWFYcmvKGOtvZIQ0So2JUSjDbj8N2xoYweyMg34XZwrv6pIpJl4k3h9EKdON-BTWrTXr7iXuqcJ116LV2JqBqGHHZhzdyQ

Blanken, B. (2020, 19 november). Wat is schaduw-IT? Antwoord op 5 veelgestelde vragen. TOPdesk. Geraadpleegd op 28 december 2021, van https://blog2.topdesk.com/nl/wat-is-schaduw-it

Broadcom. (2021a, november 19). Custom Gatelets. Techdocs.Broadcom. Geraadpleegd op 2 december 2021, van https://techdocs.broadcom.com/us/en/symantec-security-software/information-security/symantec-cloudsoc/cloud/audit-home/opening-audit/creating-custom-gatelets-in-audit.html

Broadcom. (2021b, november 19). Responding to incidents with Protect. Techdocs.Broadcom. Geraadpleegd op 3 december 2021, van https://techdocs.broadcom.com/us/en/symantec-security-

software/information-security/symantec-cloudsoc/cloud/detect-home/responding-to-incidents-with-protect.html

Broadcom. (2021c, november 19). Securlets. Techdocs.Broadcom. Geraadpleegd op 2 december 2021, van https://techdocs.broadcom.com/us/en/symantec-security-software/information-security/symantec-cloudsoc/cloud/securlets-home.html

Broadcom. (2021d, november 19). Supported Generic Gatelets. Techdocs.Broadcom. Geraadpleegd op 2 december 2021, van https://techdocs.broadcom.com/us/en/symantec-security-software/information-security/symantec-cloudsoc/cloud/gateway-home/generic-gatelets.html

Broadcom. (2021e, november 19). Symantec CloudSOC. Techdocs.Broadcom. Geraadpleegd op 30 januari 2021, van https://techdocs.broadcom.com/us/en/symantec-security-software/information-security/symantec-cloudsoc/cloud.html

Brook, C. (2018, 5 december). What is Deep Packet Inspection? How It Works, Use Cases for DPI, and More. Digital Guardian. Geraadpleegd op 14 november 2021, van https://digitalguardian.com/blog/what-deep-packet-inspection-how-it-works-use-cases-dpi-and-more

Brook, C. (2020, 29 september). What is a Next Generation Firewall? Learn about the differences between NGFW and traditional firewalls. Digital Guardian. Geraadpleegd op 12 november 2021, van https://digitalguardian.com/blog/what-next-generation-firewall-learn-about-differences-between-ngfw-and-traditional-firewalls

Centraal Bureau voor de Statistiek. (2021, 18 augustus). Dashboard bevolking. Geraadpleegd op 1 oktober 2021, van https://www.cbs.nl/nl-nl/visualisaties/dashboard-bevolking

checkpoint. (2021a, juli 15). What is a Cloud Workload Protection Platform (CWPP)? Check Point Software. Geraadpleegd op 5 november 2021, van https://www.checkpoint.com/cyber-hub/cloud-security/what-is-a-cloud-workload-protection-platform-cwpp/

checkpoint. (2021b, oktober 18). What is Cloud Security Posture Management (CSPM). Check Point Software. Geraadpleegd op 5 november 2021, van https://www.checkpoint.com/cyber-hub/cloud-security/what-is-cspm-cloud-security-posture-management/

Cisco. (2021, 29 oktober). What Is Data Loss Prevention (DLP)? Geraadpleegd op 6 december 2021, van https://www.cisco.com/c/en/us/products/security/email-security-appliance/data-loss-prevention-dlp.html#%7Etypes-of-dlp

Citrix. (z.d.). What is Single Sign-On (SSO)? - Citrix Netherlands. Citrix.com. Geraadpleegd op 30 december 2021, van https://www.citrix.com/nl-nl/solutions/secure-access/what-is-single-sign-on-sso.html

Croll, T. (2020, 29 december). 3 Steps to Gartner's SaaS Security Framework. Gartner. Geraadpleegd op 29 oktober 2021, van https://www.gartner.com/account/signin?method=initialize&TARGET=http%253A%252F%252Fwww.gartner.com%252Fdocument%252F3994928%253Fref%253DsolrAll%2526refval%253D307256218

digitalguardian. (2019, 19 december). What is Identity and Access Management (IAM)? Geraadpleegd op 14 november 2021, van https://digitalguardian.com/blog/what-identity-and-access-management-iam

dsaict. (z.d.). Microsoft 365 E5 Security. DSA ICT Services & Software B.V. Geraadpleegd op 7 december 2021, van https://www.dsaict.nl/shop/aad-41519-microsoft-365-e5-security-1793#attr=15

Exact. (z.d.). How to activate the Single Sign On (SSO) module. Support.ExactOnline. Geraadpleegd op 15 december 2021, van https://support.exactonline.com/community/s/knowledge-base?language=en_GB#All-All-HNO-Task-general-security-general-security-gen-sec-accyssot

Fahad, F. (2020, 14 mei). De probleemanalyse van je scriptie. 24editor. Geraadpleegd op 3 september 2021, van https://24editor.com/de-probleemanalyse-van-je-scriptie/

Forcepoint. (z.d.-a). datasheet cloud infrastructure enus. Geraadpleegd op 16 december 2021, van https://www.forcepoint.com/sites/default/files/resources/files/datasheet_cloud_infrastructure_enus.pdf

Forcepoint. (z.d.-b). Forcepoint CASB Endpoint Windows deployments. Websense. Geraadpleegd op 5 december 2021, van https://www.websense.com/content/support/library/endpoint/v20/ep_upgrade/eca_deployment_2.aspx

Forcepoint. (2020, 8 december). Introducing Forcepoint One Endpoint. Websense. http://www.websense.com/content/support/library/endpoint/v20/installation.pdf

Forcepoint. (2021a, juni 6). Forcepoint CASB Administration Guide. Websense. Geraadpleegd op 1 december 2021, van https://www.websense.com/content/support/library/casb/admin_guide/casb_admin_guide.pdf

Forcepoint. (2021b, oktober 25). Forcepoint Completes Acquisition of Bitglass. Geraadpleegd op 7 december 2021, van https://www.forcepoint.com/newsroom/2021/forcepoint-completes-acquisition-bitglass

Fortinet. (z.d.-a). FortiCASB 2.0 Handbook. Help.fortinet. Geraadpleegd op 4 december 2021, van https://help.fortinet.com/fcasb/2-0-0/olh/index.html#FortiCASB/User%20Guide/GettingStartedNew.htm#Install

Fortinet. (z.d.-b). WAF vs. Firewall: Web Application & Network Firewalls. Geraadpleegd op 17 november 2021, van https://www.fortinet.com/resources/cyberglossary/waf-vs-firewall

Fortinet. (2020, 30 december). FortiCASB - Admin Guide. Fortinet.com. Geraadpleegd op 1 december 2021, van https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/f0da2f64-5080-11eb-b9ad-00505692583a/forticasb-20.4.0-admin_guide.pdf

Friis Dam, R. (2021, 2 januari). 5 Stages in the Design Thinking Process. The Interaction Design Foundation. Geraadpleegd op 27 september 2021, van https://www.interaction-design.org/literature/article/5-stages-in-the-design-thinking-process

Fritchen, K. (2020, 5 februari). API vs Proxy CASB: Which Is Right For You? ManagedMethods. Geraadpleegd op 17 november 2021, van https://managedmethods.com/blog/api-vs-proxy-casb-which-is-right-for-you/

Gaehtgens, F., Data, A., Kelley, M., & Rakheja, S. (2021, 19 juli). Magic Quadrant for Privileged Access Management. Gartner. Geraadpleegd op 15 november 2021, van

https://www.gartner.com/account/signin?method=initialize&TARGET=http%253A%252F%252Fwww.gartner.com%252Fdocument%252F4003658%253Fref%253Dddisp%2526refval%253D4003666

Gartner. (2021, 21 april). Gartner Forecasts Worldwide Public Cloud End-User Spending to Grow 23%. Geraadpleegd op 29 december 2022, van https://www.gartner.com/en/newsroom/press-releases/2021-04-21-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-grow-23-percent-in-2021

Gee, K. (2020, 18 juni). The Importance of a Robust Reverse Proxy. Bitglass. Geraadpleegd op 14 december 2021, van https://www.bitglass.com/blog/the-importance-of-a-robust-reverse-proxy

Geers, J. (2021, 25 februari). SWOT-analyse maken. KVK. Geraadpleegd op 3 september 2021, van https://www.kvk.nl/advies-en-informatie/marketing/swot-analyse-maken/

Guermellou, M. [TrustmarqueTV]. (2020, 20 juli). McAfee | Unified Cloud Edge [Video]. YouTube. https://www.youtube.com/watch?v=kEJsskzglF8&list=FLNgL-NGA0q61ZVIJumQUzyQ

Haag, S., & Eckhardt, A. (2017). Shadow IT. Business & Information Systems Engineering, 59(6), 461–473. https://doi.org/10.1007/s12599-017-0497-x

Hardt, D. (2012, oktober). rfc6749. The OAuth 2.0 Authorization Framework. Geraadpleegd op 3 december 2021, van https://datatracker.ietf.org/doc/html/rfc6749

Henderson, T. (2016, 8 augustus). Cloud access security brokers deliver must-have protection for your SaaS apps. CSO Online. Geraadpleegd op 5 december 2021, van https://www.csoonline.com/article/3105266/casb-delivers-must-have-protection-for-your-saas-apps.html#:%7E:text=Starts%20at%20%248%20per%20user,Malware%20Protection%20are%20priced%20separately.

Hoogenraad, W. (2021, 15 augustus). Gap-analyse in 4 stappen. IT Knowledge. Geraadpleegd op 3 september 2021, van https://www.itpedia.nl/2020/01/10/gap-analyse-in-4-stappen/

Ingalls, S. (2020, 15 december). 12 Best CASB Security Vendors of 2021. Esecurityplanet. Geraadpleegd op 29 november 2021, van https://www.esecurityplanet.com/products/casb-security-vendors/

Irwin, L. (2021, 22 juli). ISO 27001 vs. ISO 27002: What's the difference? IT Governance UK Blog. Geraadpleegd op 6 oktober 2021, van https://www.itgovernance.co.uk/blog/understanding-the-differences-between-iso-27001-and-iso-27002

Kepinski, K. (2020, 17 december). Corona pandemie zorgt voor meer uitgaven aan cloud services | Dutch IT-channel. Dutchitchannel. Geraadpleegd op 27 december 2021, van https://dutchitchannel.nl/663992/corona-pandemie-zorgt-voor-meer-uitgaven-aan-cloud-services.html

Kirti, G. (2016, 23 juni). Why APIs beat proxies for cloud security. InfoWorld. Geraadpleegd op 21 november 2021, van https://www.infoworld.com/article/3087361/why-apis-beat-proxies-for-cloud-security.html#:%7E:text=The%20API's%20greatest%20advantage%20is,PaaS%20as%20well%20as%20SaaS.

KPN. (2020, 6 augustus). Zo beschermt een MSSP bedrijven tegen cybercrime. KPN.com. Geraadpleegd op 29 december 2021, van https://www.kpn.com/zakelijk/blog/zo-beschermt-een-mssp-bedrijven-tegen-cybercrime.htm

Krul, A. (2021, 27 augustus). Hoe voer je deskresearch uit? Scribbr. Geraadpleegd op 3 september 2021, van https://www.scribbr.nl/onderzoeksmethoden/deskresearch/

Latesen, E. (2021, 17 maart). What's the difference between a Next Generation Firewall and a Web Application Firewall? VCG. Geraadpleegd op 9 november 2021, van https://vcg.group/news/whats-the-difference-between-a-next-generation-firewall-and-a-web-application-firewall/

Lawson, C., & Riley, S. (2020, 28 oktober). Magic Quadrant for Cloud Access Security Brokers. Gartner. Geraadpleegd op 23 november 2021, van https://www.gartner.com/account/signin?method=initialize&TARGET=http%253A%252F%252Fwww.gartner.com%252Fdocument%252F3992205%253Fref%253Dlib

Lookout. (2021, 15 maart). Lookout Acquires CipherCloud to Deliver Security from Endpoint to Cloud. Prnewswire. Geraadpleegd op 7 december 2021, van https://www.prnewswire.com/news-releases/lookout-acquires-ciphercloud-to-deliver-security-from-endpoint-to-cloud-301246849.html

MacDonald, N., & Croll, T. (2021, 12 juli). Market Guide for Cloud Workload Protection Platforms. Gartner. Geraadpleegd op 8 november 2021, van https://www.gartner.com/document/4003465?ref=solrAll&refval=307093150

MacDonald, N., & Winckless, C. (2021, 25 augustus). Innovation Insight for Cloud-Native Application Protection Platforms. Gartner. Geraadpleegd op 10 november 2021, van https://www.gartner.com/document/4005115?ref=solrAll&refval=307095969

Managementmodellensite. (2019, 7 mei). Vijfkrachtenmodel van Porter. Geraadpleegd op 24 september 2021, van https://managementmodellensite.nl/krachtenmodel-porter/

MARQIT. (z.d.). Wat is een Access Control List (ACL) | IT Woordenboek | Marqit.be. Geraadpleegd op 8 december 2021, van https://www.marqit.be/access-control-list

McAfee. (z.d.-a). McAfee CASB Connect Catalog | McAfee MVISION Cloud. Geraadpleegd op 1 december 2021, van https://www.mcafee.com/enterprise/en-us/products/mvision-cloud/casb-connect.html

McAfee. (z.d.-b). Remote Browser Isolation | McAfee Products. Geraadpleegd op 7 december 2021, van https://www.mcafee.com/enterprise/en-us/products/remote-browser-isolation.html

McAfee. (z.d.-c). What is a Cloud Workload Protection Platform (CWPP)? | McAfee. Geraadpleegd op 25 november 2021, van https://www.mcafee.com/enterprise/en-us/security-awareness/cloud/what-is-a-cwpp.html

McAfee. (2020a, mei 15). Cloud Access Security Broker (CASB) Deployment Modes Best Practices. McAfee Blogs. Geraadpleegd op 1 december 2021, van https://www.mcafee.com/blogs/enterprise/cloud-security/casb-cloud-access-security-brokers-deployment-modes-best-practices/

McAfee. (2020b, juli 28). Allow List Devices with MobileIron. McAfee Enterprise MVISION Cloud. Geraadpleegd op 5 december 2021, van https://success.myshn.net/Policy/Device_Management/Allow_List_Devices_with_MobileIron

McAfee. (2021a, januari 27). Edit an Activity. McAfee Enterprise MVISION Cloud. Geraadpleegd op 5 december 2021, van https://success.myshn.net/Custom_Apps/Edit_Apps_and_Activities/Edit_an_Activity

McAfee. (2021b, juli 13). About CASB Connect. McAfee Enterprise MVISION Cloud. Geraadpleegd op 3 december 2021, van https://success.myshn.net/CASB_Connect/About_CASB_Connect/About_CASB_Connect

McAfee. (2021c, juli 27). About Custom Apps. McAfee Enterprise MVISION Cloud. Geraadpleegd op 1 december 2021, van https://success.myshn.net/Custom_Apps/About_Custom_Applications/About_Custom_Apps

McAfee. (2021d, juli 28). Integrating an Edge Device. McAfee Enterprise MVISION Cloud. Geraadpleegd op 25 november 2021, van https://success.myshn.net/Settings/Firewall_and_Proxy_Integration/02_Integrating_an_Edge_Device

McAfee. (2021e, augustus 24). MVISION Cloud Data Centers. McAfee Enterprise MVISION Cloud. Geraadpleegd op 3 december 2021, van https://success.myshn.net/Start_Here_with_MVISION_Cloud/MVISION_Cloud_Overview/MVISION_Cloud_Data_Centers

McAfee. (2021f, augustus 26). About MVISION Cloud for Office 365. McAfee Enterprise MVISION Cloud. Geraadpleegd op 5 december 2021, van https://success.myshn.net/Skyhigh_for_Sanctioned_IT/MVISION_Cloud_for_Office_365/About_MVISION_Cloud_for_Office_365

McAfee. (2021g, augustus 27). About Connected Apps. McAfee Enterprise MVISION Cloud. Geraadpleegd op 6 december 2021, van https://success.myshn.net/Analytics/Connected_Apps/About_Connected_Apps

McAfee. (2021h, september 2). About Cloud Connector. McAfee Enterprise MVISION Cloud. Geraadpleegd op 2 december 2021, van https://success.myshn.net/MVISION_Cloud_Connector_(GroundLink)/About_MVISION_Cloud_Connector/About_Cloud_Connector

McAfee. (2021i, september 23). Sanctioned DLP Policy Response Actions. McAfee Enterprise MVISION Cloud. Geraadpleegd op 5 december 2021, van https://success.myshn.net/Policy/Sanctioned_DLP_Policies/Sanctioned_DLP_Policy_Response_Actions#API_Actions

McAfee. (2021j, oktober 22). About Users. McAfee Enterprise MVISION Cloud. Geraadpleegd op 5 december 2021, van https://success.myshn.net/Analytics/Users/01_Users_Overview

McAfee Cloud BU. (2020, 9 december). Protecting Against Shadow IT: 5 Key CASB Use Cases. McAfee Blogs. Geraadpleegd op 28 november 2021, van https://www.mcafee.com/blogs/enterprise/cloud-security/protecting-against-shadow-it-5-key-casb-use-cases/

Microsoft. (z.d.-a). Kies de juiste Azure-regio voor u. Microsoft Azure. Geraadpleegd op 16 december 2021, van https://azure.microsoft.com/nl-nl/global-infrastructure/geographies/#overview

Microsoft. (z.d.-b). MFA (meervoudige verificatie) - Microsoft-beveiliging. Geraadpleegd op 30 december 2021, van https://www.microsoft.com/nl-nl/security/business/identity-access-management/mfa-multi-factor-authentication

Microsoft. (z.d.-c). Roll out continuous reports for Defender for Cloud Apps using a Docker on Windows. Microsoft Docs. Geraadpleegd op 10 januari 2022, van https://docs.microsoft.com/en-us/defender-cloud-apps/discovery-docker-windows

Microsoft. (2019, 9 april). Microsoft Cloud App Security Webinar Series [Video]. Microsoft videoplayer. https://www.microsoft.com/videoplayer/embed/RE4GriX

Microsoft. (2021a, november). Microsoft Cloud App Security Licensing Datasheet. Geraadpleegd op 28 november 2021, van https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE2NXYO

Microsoft. (2021b, november 10). Integrate Microsoft Defender for Endpoint with Defender for Cloud Apps. Microsoft Docs. Geraadpleegd op 3 december 2021, van https://docs.microsoft.com/en-us/defender-cloud-apps/mde-integration

Microsoft. (2021c, november 24). Automatisch uploaden van logboeken configureren met behulp van on-premises Docker. Microsoft Docs. Geraadpleegd op 17 december 2021, van https://docs.microsoft.com/nl-nl/defender-cloud-apps/discovery-docker-ubuntu?tabs=centos

Microsoft. (2021d, november 24). Bepalen welke cloud-OAuth-apps van derden machtigingen krijgen. Microsoft Docs. Geraadpleegd op 3 december 2021, van https://docs.microsoft.com/nl-nl/defender-cloud-apps/manage-app-permissions

Microsoft. (2021e, november 24). Blokkeerscript genereren - Cloud Discovery API. Microsoft Docs. Geraadpleegd op 3 december 2021, van https://docs.microsoft.com/nl-nl/defender-cloud-apps/api-discovery-script

Microsoft. (2021f, november 24). Cloud Discovery implementeren. Microsoft Docs. Geraadpleegd op 26 november 2021, van https://docs.microsoft.com/nl-nl/cloud-app-security/set-up-cloud-discovery

Microsoft. (2021g, november 24). Defender for Cloud Apps App-beheer voor voorwaardelijke toegang voor Azure AD-apps implementeren. Microsoft Docs. Geraadpleegd op 5 december 2021, van https://docs.microsoft.com/nl-nl/defender-cloud-apps/proxy-deployment-aad

Microsoft. (2021h, november 24). Gebruikersgegevens anoniem maken in Defender for Cloud Apps. Microsoft Docs. Geraadpleegd op 18 december 2021, van https://docs.microsoft.com/nl-nl/defender-cloud-apps/cloud-discovery-anonymizer

Microsoft. (2021i, november 24). Minimum requirements for Microsoft Defender for Endpoint. Microsoft Docs. Geraadpleegd op 7 december 2021, van https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/minimum-requirements?view=o365-worldwide

Microsoft. (2021j, november 24). Verbinding maken Office 365 maken met Defender for Cloud Apps. Microsoft Docs. Geraadpleegd op 17 december 2021, van https://docs.microsoft.com/nl-nl/defender-cloud-apps/connect-office-365

Microsoft. (2021k, november 28). Automatisch uploaden van logboeken configureren voor doorlopende rapporten in Defender for Cloud Apps. Microsoft Docs. Geraadpleegd op 17 december 2021, van https://docs.microsoft.com/nl-nl/defender-cloud-apps/discovery-docker

Microsoft. (2021l, november 28). Beleid maken om activiteiten in Defender for Cloud Apps te beheren. Microsoft Docs. Geraadpleegd op 5 december 2021, van https://docs.microsoft.com/nl-nl/defender-cloud-apps/user-activity-policies

Microsoft. (2021m, november 28). Beveiligen met Microsoft Defender voor Cloud Apps App-beheer voor voorwaardelijke toegang. Microsoft Docs. Geraadpleegd op 4 december 2021, van https://docs.microsoft.com/nl-nl/defender-cloud-apps/proxy-intro-aad

Microsoft. (2021n, november 28). Cloud Discovery implementeren. Microsoft Docs. Geraadpleegd op 3 december 2021, van https://docs.microsoft.com/nl-nl/defender-cloud-apps/set-up-cloud-discovery

Microsoft. (2021o, november 28). Het gebruik van cloud-apps controleren door beleid te maken. Microsoft Docs. Geraadpleegd op 5 december 2021, van https://docs.microsoft.com/nl-nl/defender-cloud-apps/control-cloud-apps-with-policies

Microsoft. (2021p, november 28). Microsoft Defender for Endpoint integreren met Defender for Cloud Apps. Microsoft Docs. Geraadpleegd op 17 december 2021, van https://docs.microsoft.com/nl-nl/defender-cloud-apps/mde-integration

Microsoft. (2021q, november 28). Sessiebeleid maken in Defender for Cloud Apps. Microsoft Docs. Geraadpleegd op 24 december 2022, van https://docs.microsoft.com/nl-nl/defender-cloud-apps/session-policy-aad

Microsoft. (2021r, december 1). Defender for Cloud Apps: gegevensbeveiliging en privacyprocedures. Microsoft Docs. Geraadpleegd op 5 december 2021, van https://docs.microsoft.com/nl-nl/defender-cloud-apps/cas-compliance-trust

Microsoft. (2021s, december 11). Beleid maken om activiteiten in Defender for Cloud Apps te beheren. Microsoft Docs. Geraadpleegd op 3 januari 2022, van https://docs.microsoft.com/nl-nl/defender-cloud-apps/user-activity-policies

Microsoft. (2021t, december 29). Microsoft 365 and Office 365 service descriptions - Service Descriptions. Microsoft Docs. Geraadpleegd op 3 januari 2022, van https://docs.microsoft.com/nl-nl/office365/servicedescriptions/office-365-service-descriptions-technet-library

Netskope. (z.d.-a). API Data Protection Policy Actions per Cloud App. Docs.Netskope. Geraadpleegd op 5 december 2021, van https://docs.netskope.com/en/api-data-protection-policy-actions-per-cloud-app.html

Netskope. (z.d.-b). Risk Insights. Docs.Netskope. Geraadpleegd op 5 december 2021, van https://docs.netskope.com/en/risk-insights.html

Okta. (z.d.). Identity providers (IdP's): wat zijn dat en waarom heeft u ze nodig | Okta. Okta, Inc. Geraadpleegd op 23 november 2021, van https://www.okta.com/nl/identity-101/why-your-company-needs-an-identity-provider/

Palo Alto. (z.d.-a). Add Cloud Apps to SaaS Security API. Docs.Paloaltonetworks. Geraadpleegd op 1 december 2021, van https://docs.paloaltonetworks.com/saas-security/saas-security-admin/saas-security-api/secure-cloud-apps/add-cloud-apps-to-saas-security-api.html

Palo Alto. (z.d.-b). Monitor and Investigate User Activity. Docs.PaloAltonetworks. Geraadpleegd op 5 december 2021, van https://docs.paloaltonetworks.com/saas-security/saas-security-admin/saas-security-api/monitor-saas-security-api-issues/monitor-user-activity.html#ide55344f5-010e-400c-99a9-bf787aaa9752

Palo Alto. (z.d.-c). Remediate Risks of Sanctioned SaaS Apps. Docs.PaloAltonetworks. Geraadpleegd op 5 december 2021, van https://docs.paloaltonetworks.com/saas-security/saas-security-admin/saas-security-api/remediate-risks-saas-security-api.html

Pol, F. H. (2021, 4 oktober). 'Aantal Nederlandse cybersecuritybedrijven in vijf jaar verdubbeld'. Techzine.nl. Geraadpleegd op 1 januari 2022, van https://www.techzine.nl/nieuws/security/467654/aantal-nederlandse-cybersecuritybedrijven-in-vijf-jaar-verdubbeld/

proofpoint. (2021, 27 oktober). What Is Data Loss Prevention? - DLP Meaning | Proofpoint US. Geraadpleegd op 13 november 2021, van https://www.proofpoint.com/us/threat-reference/dlp

Riley, S., & Lawson, C. (2020, 2 november). Critical Capabilities for Cloud Access Security Brokers. Gartner. Geraadpleegd op 13 november 2021, van https://www.gartner.com/account/signin?method=initialize&TARGET=http%253A%252F%252Fwww.gartner.com%252Fdocument%252F3992364%253Fref%253DsolrAll%2526refval%253D307256088

Salesforce. (z.d.). Wat is SaaS? Software as a Service uitgelegd. Salesforce.com. Geraadpleegd op 24 oktober 2021, van https://www.salesforce.com/nl/learning-centre/tech/saas/

secureme2. (z.d.). SAM voor Enterprise – SecureMe2. Geraadpleegd op 20 oktober 2021, van https://www.secureme2.eu/sam-voor-enterprise/

Securityboulevard. (2019, 6 juni). Next-generation firewall (NGFW) vs. traditional firewall. Geraadpleegd op 27 november 2021, van https://securityboulevard.com/2019/06/next-generation-firewall-ngfw-vs-traditional-firewall/

Silva, C., Bhat, M., Wilson, D., & Stefani, R. (2021, 10 februari). Market Guide for SaaS Management Platforms. Gartner. Geraadpleegd op 14 november 2021, van https://www.gartner.com/account/signin?method=initialize&TARGET=http%253A%252F%252Fwww.gartner.com%252Fdocument%252F3996830%253Fref%253DsolrAll%2526refval%253D307249038

Soseman, M. (2020, 24 juni). App Risk Scoring in Microsoft Cloud App Security. YouTube. Geraadpleegd op 8 januari 2022, van https://www.youtube.com/watch?v=vMFyBZh7pyI&list=PLhTS5hnNCfqdxyqr9JOMifwk_cZmBBz9Z&index=5

Soseman, M. [Matt Soseman]. (2020a, juni 22). Discover (and Block) Shadow IT w/ Microsoft Cloud App Security & Microsoft Defender ATP [Video]. YouTube. https://www.youtube.com/watch?app=desktop&v=MsHkTOoqSQo

Soseman, M. [Matt Soseman]. (2020b, juni 29). What is Conditional Access App Control in Microsoft Cloud App Security? [Video]. YouTube. https://www.youtube.com/watch?v=CvsjM8TX81c

Supasatit, T. (2021, 23 maart). What's the difference between CASB, CWPP, CSPM, and CNAPP? Uptycs. Geraadpleegd op 7 november 2021, van https://www.uptycs.com/blog/whats-the-difference-between-casb-cwpp-cspm-and-cnapp

Tinner, N. (2021, 23 oktober). A tour through Cloud App Security. Oceanleaf. Geraadpleegd op 4 december 2021, van https://oceanleaf.ch/a-tour-through-cloud-app-security/

Tolly, K. (2021, 11 januari). Review these 7 CASB vendors to best secure cloud access. SearchCloudSecurity. Geraadpleegd op 5 december 2021, van

https://searchcloudsecurity.techtarget.com/tip/Review-these-7-CASB-vendors-to-best-secure-cloud-access

Wikipedia contributors. (2021a, augustus 23). MoSCoW method. Wikipedia. Geraadpleegd op 3 september 2021, van https://en.wikipedia.org/wiki/MoSCoW_method

Wikipedia contributors. (2021b, oktober 22). Identity management. Wikipedia. Geraadpleegd op 2 november 2021, van https://en.wikipedia.org/wiki/Identity_management

Wikipedia contributors. (2021c, november 7). Application firewall. Wikipedia. Geraadpleegd op 8 november 2021, van https://en.wikipedia.org/wiki/Application_firewall

Wikipedia-bijdragers. (2019, 3 februari). Multicriteria-analyse. Wikipedia. Geraadpleegd op 3 september 2021, van https://nl.wikipedia.org/wiki/Multicriteria-analyse

13. Bijlages

13.1. Probleemanalyse

In dit deel van de afstudeerscriptie is er gekeken naar de eerdergenoemde probleemstelling. In dit hoofdstuk wordt deze probleemstelling verder geanalyseerd aan de hand van de verkregen informatie uit de interviews, empathy maps en de 6 W-vragen.

13.1.1. Probleemanalyse aan de hand van de interviews

Door het afnemen van de interviews is er een beter beeld gecreëerd over hoe het vastgestelde probleem in de organisatie leeft en wat de wensen van verschillende lagen in de organisatie zijn. Hieronder is beschreven wat verschillende mensen als probleem hebben aangewezen. De individuele pijnpunten van de huidige situatie voor elke stakeholder zijn apart genoteerd.

13.1.1.1. Gedeelde pijnpunten

- Geen controle over datastromen in SaaS-applicaties bij klantomgevingen.
- Geen inzicht in datastromen in SaaS-applicaties bij klantomgevingen.
- Door meerdere oorzaken maken steeds meer werknemers van klanten gebruik van IT-middelen die niet door het bedrijf zijn verschaft.
- Het gebrek aan een portfolio waardoor PCI IT als MSSP zou kunnen fungeren.
- Het mislopen van klanten doordat er bij PCI IT geen portfolio aanwezig is en concurrenten dit wel aanbieden.

13.1.1.2. Pijnpunten van Bart Brevink

- Geen inzicht in SaaS gerelateerde schaduw IT in klantomgevingen.

13.1.1.3. Pijnpunten van Joost Overkamp

- De DLP-oplossing welke wij gebruiken kan niet alle situaties afvangen.

13.1.1.4. Pijnpunten van Dennis Schutten

- Niet genoeg personeel hebben om sommige oplossingen aan te bieden.

13.1.1.5. Pijnpunten van Marc Schuurman

- Sommige klanten hebben weinig zicht op gevolgen van acties in de IT.

13.1.2. 6 W-vragen

De 6 W-vragen zorgen ervoor dat er nagedacht wordt over verschillende aspecten van het probleem. Deze methode zorgt ervoor dat het probleem volledig gedefinieerd wordt. Zoals de naam al doet vermoeden bestaat de 6 W-methode uit 6 vragen welke beginnen met de letter ‘w’. Hieronder is er kort beschreven wat er beantwoord wordt bij iedere vraag.

- Bij ‘wat’ wordt er omschreven wat het probleem is.
- Bij ‘wie’ wordt er omgeschreven wie het probleem heeft.
- Bij ‘wanneer’ wordt er beantwoord wanneer dit probleem ontstaan is.
- Bij ‘waarom’ wordt beantwoord waarom het nu een probleem is.
- Bij ‘waar’ wordt beantwoord waar het probleem zich voordoet.
- Bij de tweede ‘wat’ wordt beantwoord wat de aanleiding van dit probleem is.

13.1.2.1. Wat?

Het probleem in dit project is dat men datastromen in SaaS-applicaties in klantomgevingen niet kan inzien of sturen. Dit betreft dan de acties welke werknemers van klanten uitvoeren in SaaS-applicaties die PCI IT zou willen controleren of inzien.

13.1.2.2. Wie?

In dit project is degene die het probleem ervaart hoofdzakelijk PCI IT. Naast PCI IT zou er het argument gemaakt kunnen worden dat klanten van PCI IT hier ook onder vallen. Dit argument is echter niet geheel waar, aangezien het een extra service is die wel gevraagd wordt maar nog niet geleverd is.

13.1.2.3. Wanneer?

Het probleem is voor een groot deel ontstaan toen er gemigreerd is naar SaaS-applicaties. Vóór deze migratie waren er bijvoorbeeld beveiligde workstations in een beveiligd netwerk op locatie bij de klant en de applicatie was in beheer van het bedrijf zelf.

13.1.2.4. Waarom?

Er zijn meerdere redenen waarom het gebrek aan inzicht en controle op datastromen in SaaS-applicaties op dit moment een probleem is bij PCI IT. De voornaamste reden is dat de markt aan het verschuiven is naar SaaS-applicaties. Dit betekent dat de blinde vlek bij klanten groter wordt. De tweede reden is dat andere bedrijven de diensten die PCI IT wil gaan aanbieden al aanbieden aan klanten. Dit resulteert erin dat PCI IT haar bestaande klanten geen oplossing kan bieden en deze de dienst dan afnemen bij de concurrent.

13.1.2.5. Waar?

In dit project doet het probleem zich voor in de SaaS-applicaties bij klanten. Dit zijn dan niet alleen de diensten waar gelijk aan wordt gedacht, zoals Office365 of AFAS, maar ook diensten zoals LinkedIn, waar bijvoorbeeld Cv's in worden gedeeld met bedrijven. Hier mist de transparantie die door klanten wordt gezocht.

13.1.2.6. Wat?

Het probleem is ontstaan toen de markt is verschoven naar SaaS-applicaties. Dit is het startpunt geweest van het probleem. Doordat nu een overgroot percentage van bedrijfsdata in SaaS-applicaties staat, ligt de focus er nu op om deze blinde vlek aan gebruikersacties te elimineren. Bedrijfsmatig ligt het probleem er dat er niet actief gehandeld is om een positie als MSSP in de markt in te nemen. Dit is een bedrijfsmatig probleem gezien er klanten zijn die wel andere diensten van PCI IT afnemen, maar nu ook diensten afnemen van andere leveranciers om de door PCI IT geleverde SaaS-applicaties te beveiligen.

13.1.3. Conclusie probleemanalyse

Uit de verschillende methodes die in dit hoofdstuk gebruikt zijn om vollediger bekend te worden met het probleem, de oorzaak van het probleem en de wensen van PCI IT blijkt het volgende. De afgelopen paar jaar is in de gehele markt, en dus ook bij de klanten van PCI IT, het gebruik van SaaS-applicaties explosief gegroeid. PCI IT vindt dat er te weinig controle is op deze vorm van applicaties en wil meer zicht op hoe deze SaaS-applicaties door werknemers gebruikt worden. Dit willen zij, zodat ze kunnen acteren zodra er oneigenlijk gebruik wordt gemaakt van data die in deze SaaS-applicaties aanwezig is. Daarnaast is PCI IT van mening dat er een blinde vlek aanwezig is, namelijk de SaaS gerelateerde schaduw IT. Deze blinde vlek wil PCI IT elimineren en zodoende inzicht in het gebruik van SaaS gerelateerde schaduw IT creëren voor haar klanten.

De wens van PCI IT is dus tweedelig. Ten eerste wil PCI IT inzicht en de mogelijkheid om te sturen in de acties van de gebruikers van beheerde SaaS-applicaties en ten tweede wil PCI IT het gebruik van SaaS gerelateerde Schaduw IT zichtbaar hebben zodat zij hierop kan acteren.

13.2. Methodes

13.2.1. Design thinking

Design thinking is een oplossingsgerichte, probleemoplossing methodologie. De methodologie is gebaseerd op 5 fases. Deze 5 fases staan hieronder met een korte uitleg van het doel van elke fase.

- Emphatize
  - Het inleven in het bedrijf en de medewerkers.
- Define
  - Het definiëren van de problemen welke relevant zijn voor het project.
- Ideate
  - Het bedenken van oplossingen om de genoteerde problemen op te lossen.
- Prototype
  - Het implementeren van de bedachte oplossingen.
- Test
  - Het testen of het voldoet aan de eisen die gesteld zijn.

Design thinking is in tegenstelling tot veel andere methodologieën non-lineair. Dit houdt in dat er vanuit fases teruggegaan kan worden naar een vorige fase om aanpassingen te maken (Friis Dam, 2021).

13.2.2. 6 W-vragen

Hoofdzakelijk tijdens de analyse van de probleemstelling zal er gebruik gemaakt worden van de 6 W-vragen. De methode bestaat, zoals de naam al aangeeft, uit een zestal vragen welke beginnen met de w (Fahad, 2020). Deze methode zal de volgende vragen beantwoorden:

- Wat is het probleem?
- Wat is de aanleiding van het probleem?
- Wie heeft het probleem?
- Wanneer doet het probleem zich voor?
- Waar doet het probleem zich voor?
- Waarom is het een probleem?

13.2.3. APA

APA is een van de meest gebruikte methodes om naar bronnen te verwijzen in een document. APA is bedacht door de American Psychological Association. Sinds het creëren van de richtlijnen in 1929 zijn er enkele versies van uitgebracht door American Psychological Association en zijn er door verschillende partijen eigen versies op uitgebracht (American Psychological Association, 2019). Binnen dit project zal het gebruikt worden om de geraadpleegde bronnen weer te geven.

13.2.4. Stakeholderanalyse

Tijdens de analysefase zal er gekeken worden wie er in dit project stakeholders zijn en wat hun belang in het project is. Dit zal zorgen dat het duidelijk is wat de visie op het project is en wat er door welke belanghebbende verwacht wordt van dit project. Deze analyse zal uitgevoerd worden aan de hand van de matrix van Mendelow. In deze matrix zal per belanghebbende bepaald worden hoeveel interesse en macht deze stakeholder heeft.

13.2.5. Interviews

Tijdens dit project zullen er meerdere interviews plaats vinden met medewerkers van PCI IT en leveranciers van producten. Deze gesprekken zullen in het geval van medewerkers van PCI IT plaats vinden om bijvoorbeeld de stakeholders en belanghebbenden in kaart te brengen, requirements te verzamelen en om snel van gedachte te wisselen met iemand over een idee voor het project. Deze gesprekken zullen indien mogelijk op het kantoor in Haaksbergen plaatsvinden. In het geval van leveranciers zullen deze gesprekken gevoerd worden om meer duidelijkheid te krijgen over het product dat aangeboden wordt door de leverancier.

13.2.6. MoSCoW

MoSCoW is een methode om duidelijk te noteren wat de prioriteiten binnen een project zijn. MoSCoW staat voor Must, Should, Could en Would (Wikipedia contributors, 2021). De requirements van dit project zullen met behulp van MoSCoW gecategoriseerd worden en hierdoor zal zichtbaar worden welke van deze requirements de meeste prioriteit hebben.

13.2.7. Bureauonderzoek

Tijdens dit project zal er ook gebruik gemaakt worden van bureauonderzoek. Bureauonderzoek is een methode van onderzoek welke gebruik maakt van reeds verzamelde informatie (Krul, 2021). Tijdens dit onderzoek zal er dus bestaande data worden gezocht om de onderzoeksvraag te beantwoorden. Deze gevonden data zal dan geanalyseerd worden en indien mogelijk vergeleken en toegepast worden. Deze bestaande data zullen bijvoorbeeld afkomstig zijn van organisaties zoals dat van het grote onderzoeksbureau Gartner.

13.2.8. Multicriteria-analyse

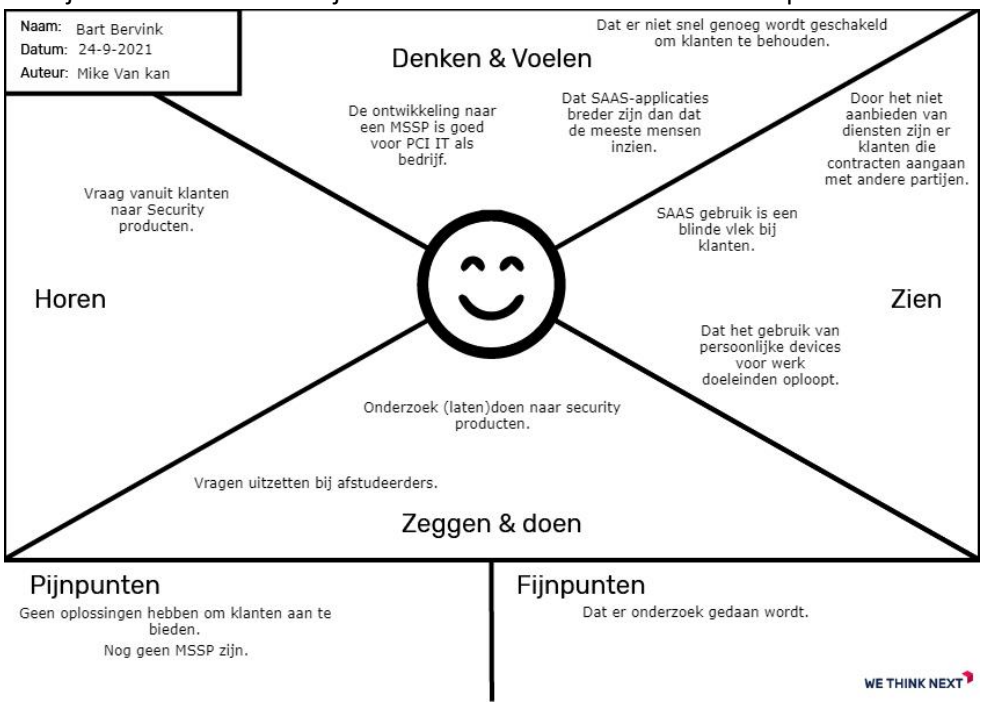
Een multicriteria-analyse is een evaluatiemethode welke gebruikt wordt om een keuze te maken tussen meerdere alternatieven. Dit gebeurt door alle voor- en nadelen te benoemen en er een waarde aan te verbinden. Aan het einde van deze methode zal er dan duidelijk onderbouwt zijn welk alternatief de beste keuze is en aan welke eisen deze voldoet (Wikipedia-bijdragers, 2019). In het geval van dit project zal het gebruikt worden om een keuze voor een concept en een leverancier te maken aan de hand van requirements.

13.3. Empathy maps

13.3.1. Bart Brevink

Het interview met Bart Brevink is gehouden om een beter beeld te krijgen over de wensen van PCI IT als organisatie en om de visie inzage dit project vanuit de hogere lagen in de organisatie duidelijk te krijgen. Daarnaast weet Bart dankzij zijn positie veel van klantomgevingen, wat relevant is als achtergrondkennis.

Uit het interview kwam naar voren dat er vraag is naar het aanbieden van securityproducten als Managed Security Service Provider of MSSP. Bart kon vertellen dat PCI IT deze positie op de markt op dit moment nog niet ingenomen heeft. Hierdoor gaan sommige klanten van PCI IT al naar andere bedrijven omdat deze bedrijven wel al diensten vanuit een MSSP-positie kunnen aanbieden.

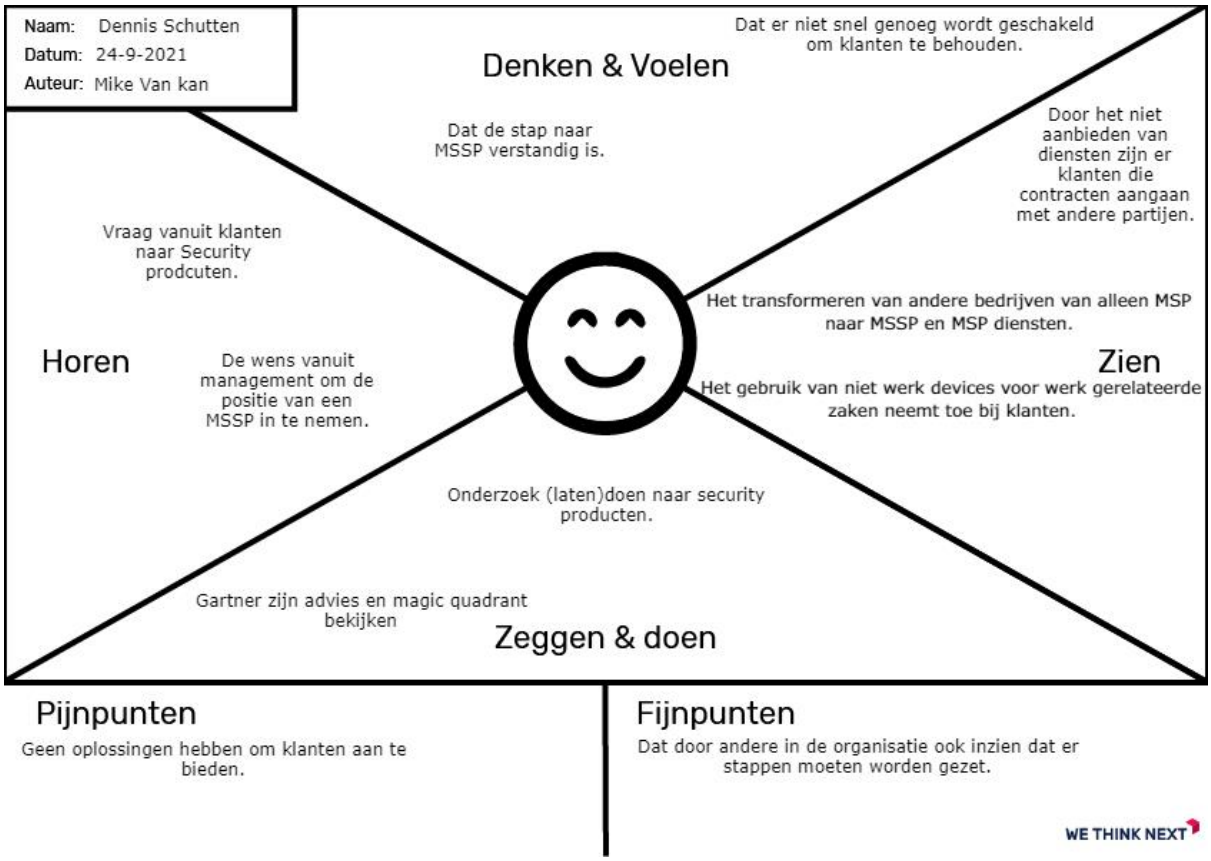


Figuur 12 Empathy map Bart Brevink

13.3.2. Dennis Schutten

Dennis Schutten is een networking en security expert bij PCI IT. Het gesprek met Dennis is gevoerd om meer informatie te verzamelen over de security gerelateerde zaken bij PCI IT. Voor het project is het belangrijk om te weten wat er al voor security gerelateerd zaken aanwezig zijn en wat de visie van het personeel is.

Tijdens dit interview werd al snel duidelijk dat het onderwerp van mijn afstuderen erg relevant is en dat het leeft in de organisatie. Er is een wens om PCI IT te positioneren als een MSSP maar doordat dit op het moment van schrijven nog niet gebeurt zijn er klanten die de oplossing elders zoeken terwijl andere producten wel nog bij PCI IT worden afgenomen. Daarnaast merkte Dennis op dat het onderwerp van het afstuderen een door meerdere klanten aangehaald onderwerp is.

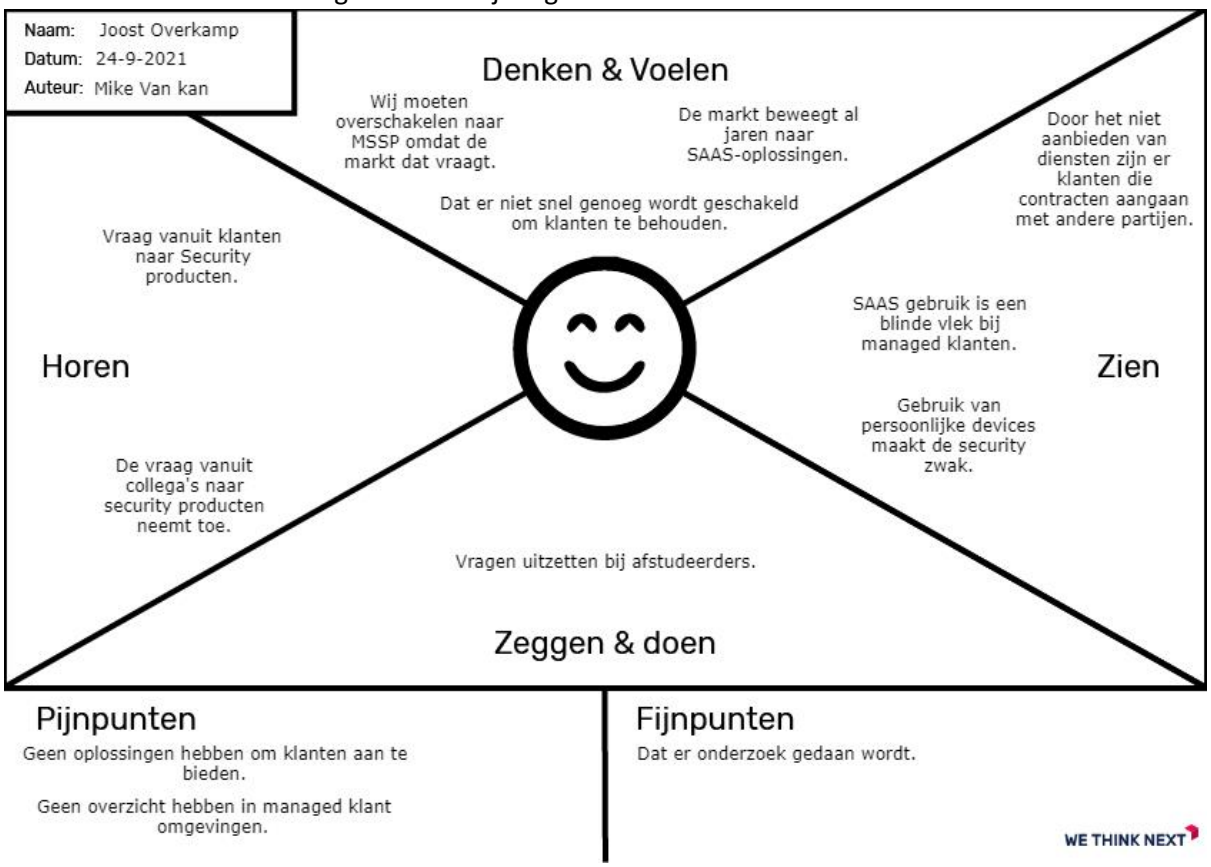


Figuur 13 Empathy map Dennis Schutten

13.3.3. Joost Overkamp

Joost Overkamp is mijn begeleider vanuit PCI IT en hij is dus bekend met de probleemstelling en waar deze vandaan komt. Er is een interview met hem gehouden om meer te weten te komen over de beweegredenen van de organisatie en om antwoord te krijgen op vragen zoals waarom dit een probleem is, of dit een nieuw probleem is, waar het dan uit voortkomt en of er al aan gewerkt is in het verleden.

Aangezien er minimaal elke week gesproken werd met Joost was zijn visie over de probleemstelling al redelijk bekend maar dankzij dit gesprek is er vooral inzichtelijk geworden hoe de organisatie functioneert en is de achtergrond duidelijker geworden.

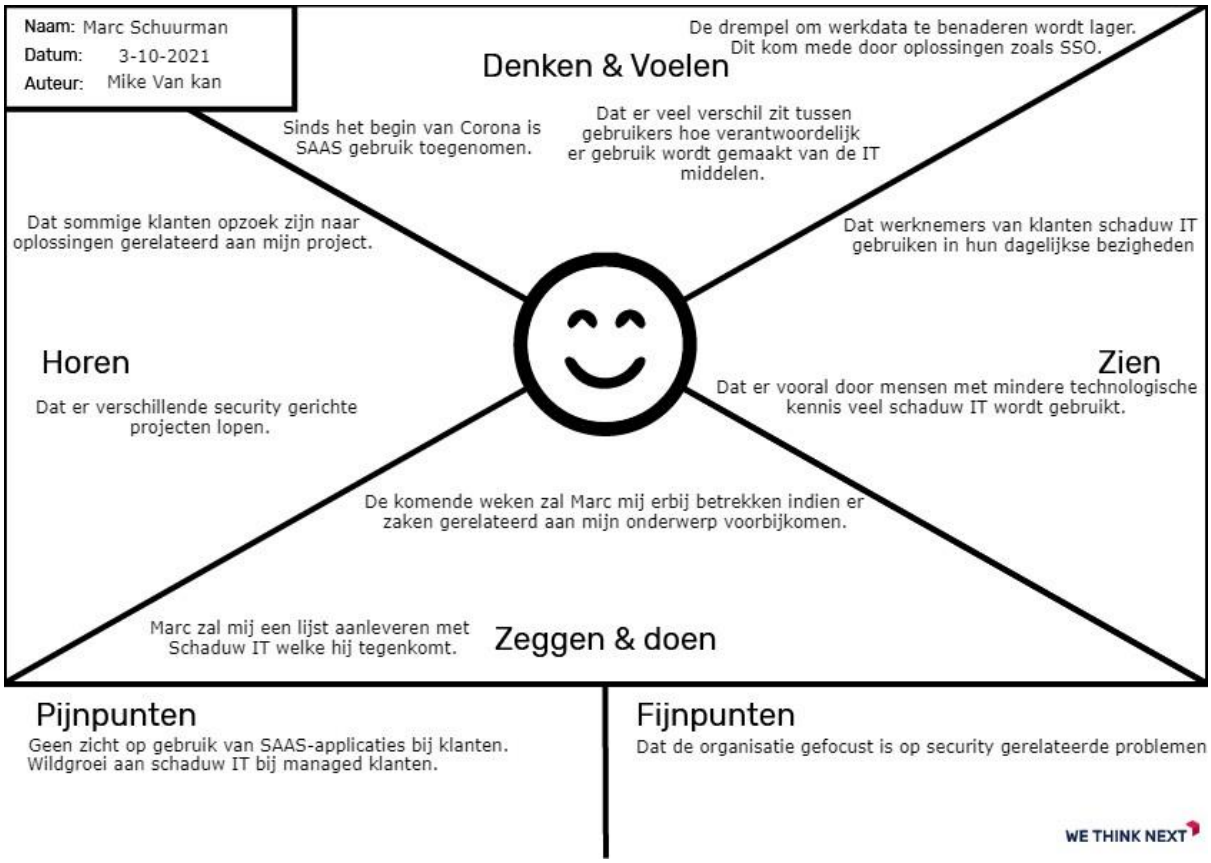


Figuur 14 Empathy map Joost Overkamp

13.3.4. Marc Schuurman

Het interview met Marc Schuurman is gevoerd omdat Marc Schuurman volgens meerdere personen binnen PCI IT een brede kennis zou hebben van klantomgevingen en hoe deze door de klanten van PCI IT worden gebruikt. De informatie uit dit interview zorgt ervoor dat er een goed beeld gevormd wordt over de omgevingen waar het product dat in dit project gezocht wordt in zou moeten functioneren.

Door dit gesprek is er inzicht ontstaan over hoe de klanten van PCI IT daadwerkelijk gebruik maken van de aangeleverde omgevingen. Dit is dan bijvoorbeeld hoe SaaS-applicaties in de klantorganisaties worden gebruikt en wat voor SaaS gerelateerde schaduw IT er bij deze klanten aanwezig is. Naast de nieuwe inzichten is er ook informatie verkregen over wat er volgens derdelijns medewerkers mist in de klantomgevingen. Dankzij het gesprek met Marc is er ook informatie verkregen over het gebruik van SaaS gerelateerde schaduw IT in de omgevingen van klanten. Schaduw IT is het gebruik van hardware of software welke niet van de werkgever afkomstig is maar wel gebruikt wordt voor het uitvoeren van werk voor de werkgever. Dit kan een privé tablet zijn waarop mail wordt gelezen of een privé account op Dropbox welke gebruikt wordt om een offerte te delen met de klant.



Figuur 15 Empathy map Marc Schuurman

13.4. Contextanalyse

Hieronder zijn de uitgebreide macro, meso en micro analyse genoteerd. De conclusie hiervan is genoteerd in het document zelf.

13.4.1. Macro

De macroanalyse houdt rekening met krachten die de markt en omgeving rond PCI IT beïnvloeden. Het is erg belangrijk om hiermee rekening te houden binnen dit project aangezien PCI IT een dienstverlener is en dus afhankelijk is van de wensen en veranderingen van de markt.

Door Corona is de markt opgeschud en is de overgang van het IT-landschap naar SaaS-oplossingen in een stroomversnelling geraakt (Kepinski, 2020). Alle medewerkers die vroeger op het kantoor werkzaam waren, moesten aan het begin van de lockdown thuis werken. Hoewel dit een tijdelijke oplossing was, is vanuit veel bedrijven gecommuniceerd dat er in de toekomst meer thuis gewerkt zal worden dan eerder het geval was. Het thuiswerken heeft ervoor gezorgd dat er nu applicaties beschikbaar gemaakt zijn die vanaf andere locaties dan het bedrijfsnetwerk te bereiken zijn. Wegens de aard van de oplossingen zijn de SaaS-applicaties dan ook beschikbaar vanaf andere apparaten dan de door het bedrijf uitgegeven laptop.

Naast Corona is de beweging richting SaaS-applicaties al langer gaande en groeit het gebruik van SaaS-applicaties al jaren (Gartner, 2021). Veel bedrijven zijn tegenwoordig afhankelijk van SaaS-applicaties voor de dagelijkse werkzaamheden. Dit kan gaan om HR-oplossingen, mailservers of zelfs zorgsystemen. Al deze systemen zijn tegenwoordig, al dan niet afgeschermd, via het internet bereikbaar. Dit kan een risico zijn voor een bedrijf dat de toegangscontrole niet op orde heeft.

Een ander fenomeen waar Nederlandse bedrijven de laatste jaren mee bezig zijn, is beveiliging rondom IT-diensten. De laatste jaren zijn er veel redenen geweest waardoor de Nederlandse bedrijven gepusht zijn om IT-beveiliging serieuzer te nemen dan voorheen. Voorbeelden hiervan zijn ransomware aanvallen, malware aanvallen, spoofing en natuurlijk de aangescherpte wet- en regelgeving. Door deze toegenomen vraag zijn er exponentieel meer bedrijven de IT-security markt toegetreden (Pol, 2021).

Als laatste moet er rekening mee worden gehouden dat PCI IT en haar klanten gevestigd zijn in Nederland en zich dus aan de AVG en GDPR moeten houden. Bij het kiezen van een oplossing zal hierop moeten worden gelet.

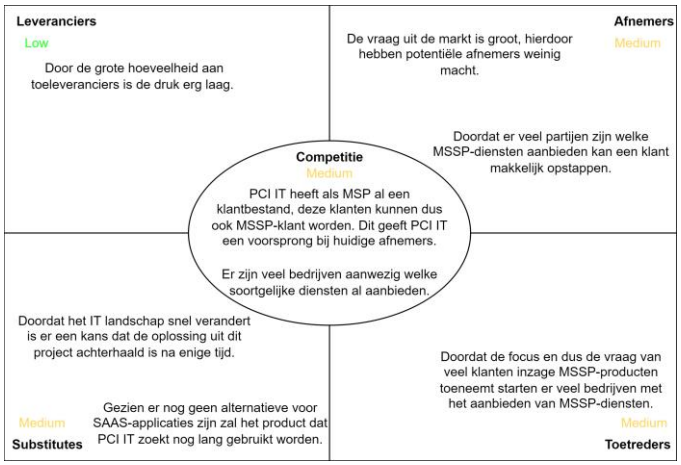
13.4.2. Meso

De meso analyse brengt de directe omgeving van PCI IT in kaart en laat zien of en waar er gevaren aanwezig zijn in de directe omgeving van PCI IT. Dankzij het uitvoeren van een meso analyse is inzichtelijk waar rekening mee moet worden gehouden om het succes van het project te bewerkstelligen. Deze analyse wordt uitgevoerd aan de hand van het vijfkrachtenmodel van Porter.

Het vijfkrachtenmodel van Porter heeft zoals de naam al doet vermoeden vijf krachten die volgens dit model de bedrijfsvoering beïnvloeden. Doordat er zoveel diensten zijn welke PCI IT aanbiedt aan haar klanten kijkt deze analyse alleen naar de zaken die voor dit project relevant zijn. In het geval van dit project zal dat de oplossing welke in dit project gekozen gaat worden aanbieden aan PCI IT haar klanten. De vijf krachten zijn als volgt (Managementmodellensite, 2019).:

- De macht van leveranciers
- De macht van afnemers
- De dreiging van toetreders
- De mate waarin substituten en complementaire goederen verkrijgbaar zijn
- Concurrentiekracht

Deze krachten zijn ingevuld in de onderstaande afbeelding samen met de zaken welke in de vijf categorieën vallen.



Figuur 16 Porter

Zoals in de afbeelding hierboven te zien is, zijn er enkele tegenwerkende krachten aanwezig die het toetreden tot de MSSP markt als nieuwe speler bemoeilijken. De grootste punten zijn “er zijn veel bedrijven aanwezig welke soortgelijke diensten al aanbieden” en “doordat er veel partijen zijn welke MSSP-diensten aanbieden kan een klant makkelijk opstappen”. Deze punten zijn sterk van invloed op het bedrijfsmatig slagen van het project. Deze punten worden gemitigeerd doordat PCI IT al een klantenbinding heeft met aanwezige klanten die andere producten afnemen. Punten waar PCI IT voordeel door heeft zijn het grote aantal toeleveranciers waar zij gebruik van kunnen maken en de grote vraag vanuit de markt naar security-gerelateerde producten.

13.4.2.1. Conclusie Meso analyse

De conclusie welke getrokken kan worden uit de meso analyse is dat, als alle voor- en nadelen tegenover elkaar worden gezet, PCI IT een hoge kans van slagen heeft om de oplossing welke uit dit project komt straks succesvol aan te bieden. De hoofdredenen die de implementatie zullen bevoorlijken, zijn het grote aantal toeleveranciers in security producten, de vraag vanuit de markt en de binding welke PCI IT al heeft met bestaande klanten.

13.4.3. Micro

In de micro analyse wordt gekeken naar de interne krachten die invloed hebben op PCI IT.

PCI Nederland heeft in juli 2019 ICT spirit overgenomen. Dit is gebeurd nadat oud-eigenaar van ICT Spirit, Mark Leferink, zich niet meer geschikt vond om ICT Spirit als bedrijf verder te laten groeien. Naar zijn mening had hij onvoldoende kennis van de IT-markt. Voordat PCI Nederland ICT Spirit heeft overgenomen heeft Mark Leferink Office Works al verkocht aan PCI Nederland.

Bij de verkoop van ICT Spirit aan PCI Nederland werd de afspraak gemaakt dat de inkoop, administratie en personeelszaken van ICT Spirit behouden zou blijven en ICT Spirit een zelfstandige organisatie zou worden binnen de organisatie PCI Nederland, zodoende ook de naam PCI IT Solutions. Door de bestaande opdrachten vanuit het klantenbestand van PCI Nederland heeft ICT Spirit de mogelijkheid gekregen verder te kunnen groeien. Door de overname is het personeelsbestand van PCI IT ook toegenomen. Medewerkers die vroeger in eerder door PCI Nederland overgenomen bedrijven werkten zijn in sommige gevallen nu werkzaam onder PCI IT. De specialiteit van deze medewerkers kunnen nu dus ook ingezet worden in de naam van PCI IT waardoor PCI IT meer diensten kan aanbieden dan eerder het geval was.

Hoewel er dus meer mensen en kennis beschikbaar zijn, groeit het klantenbestand ook gestaag en is er alsnog vraag naar extra personeel. Uit gesprekken met Bart komt voort dat PCI IT hiervan op de hoogte is en dat er specifiek voor dit project plannen aanwezig zijn om nieuwe medewerkers aan te nemen.

De hard- en softwareproducten die in gebruik zijn bij de klanten van PCI IT zijn vaak van dezelfde leverancier. De hard- en softwareproducten die veelal ingezet worden zijn hieronder genoemd met het soort product dat gebruikt wordt.

- Barracuda
    - Diverse netwerkapparatuur
- Palo Alto
    - Diverse netwerkapparatuur
- HPE
    - Servers
    - Diverse netwerkapparatuur
    - Workstations
    - Monitoren
- Microsoft
    - Azure
    - Office365
    - Dynamics365
- Aruba
    - Diverse netwerkapparatuur
- Secureme2
    - Sam (netwerkanalyse)

13.5. Shortlist

13.5.1.1. MVISION Cloud (Skyhigh Networks Cloud Security Platform)

MVISION Cloud is een oplossing van McAfee welke op de markt is gezet als een CASB. De invulling aan het producttype CASB is vrij volledig en het grootste nadeel aan deze oplossing is het missen van API-ondersteuning van grote applicaties die de klanten van PCI IT gebruiken, zoals AFAS of Exact. De CASB zelf zal in een datacenter van McAfee draaien, die vanwege de wetgeving binnen de EU moet zijn. Er zijn enkele datacenter locaties beschikbaar in de EU (McAfee, 2021e).

13.5.1.1.1. Ondersteuning van SaaS-applicaties

Zoals in de inleiding van dit hoofdstuk al kort aangehaald is, biedt deze oplossing geen native ondersteuning voor SaaS-applicaties zoals Exact online of AFAS. Om deze SaaS-applicaties alsnog werkend te krijgen in deze oplossing is er een tweetal mogelijkheden. In het eerste geval zouden deze en andere SaaS-applicaties (indien compatible) na aanvraag bij McAfee toegevoegd kunnen worden in de CASB door middel van reverse proxy. Indien een SaaS-applicatie nog niet toegevoegd is, kan er via een support ticket gevraagd worden om deze SaaS-applicatie in de toekomst te ondersteunen. Naast dat McAfee dus SaaS-applicaties reactief kan toevoegen, is het ook mogelijk om zelf applicaties toe te voegen die niet officieel ondersteund worden, zoals “Custom App”. Het gedrag van de SaaS-applicatie zal eerst via enkele stappen geleerd moeten worden en hierna zal de CASB het gedrag monitoren aan de hand van de ingestelde thresholds. Deze oplossing kan het gedrag in de SaaS-applicaties monitoren door middel van het monitoren van remote function calls (McAfee, 2021c).

13.5.1.1.2. Locatie afhankelijkheid van de oplossing

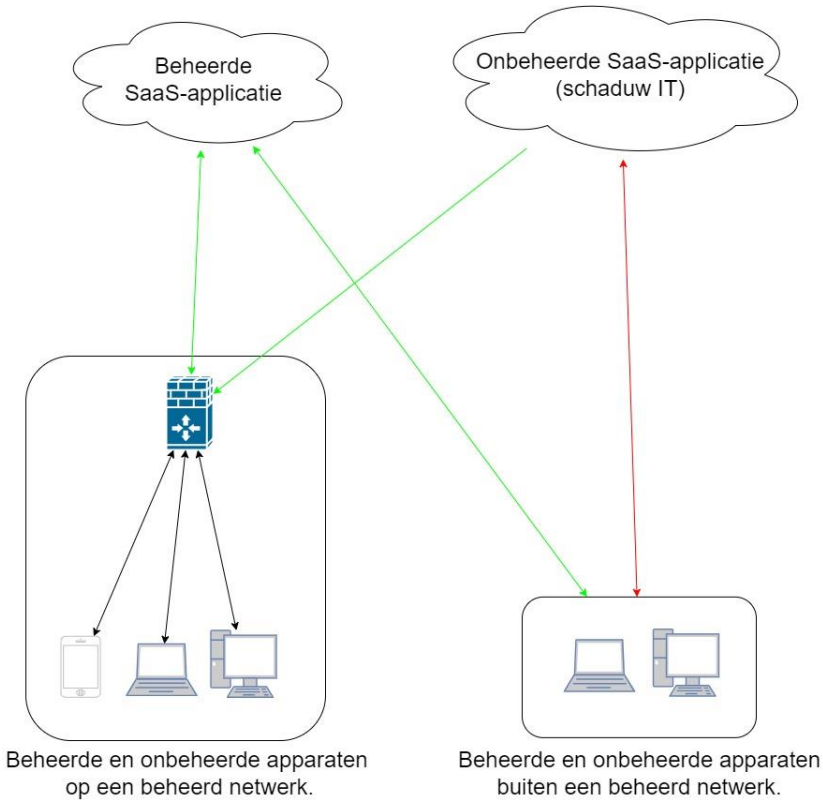
Om een beeld te vormen van de mogelijkheden van de oplossing van McAfee zijn de vier situaties van gebruikers hieronder genoteerd en daarna visueel weergegeven in figuur 17. De werking van de MVISION Cloud oplossing is als volgt:

Op het bedrijfsnetwerk

- Beheerde en onbeheerde apparaten
    - Het gebruik van beheerde en onbeheerde SaaS-applicaties wordt op verschillende manieren in de gaten gehouden. Al het netwerkverkeer en de beheerde SaaS-applicaties die in de CASB geconfigureerd zijn, worden gemonitord door middel van de API of forward- en reverse proxy. Hierdoor zijn de acties in de beheerde SaaS-applicaties zichtbaar en kan hier op gestuurd worden. Daarnaast is het gebruik van SaaS gerelateerde schaduw IT zichtbaar dankzij logging die afkomstig is van de netwerkapparatuur op locatie, welke de CASB verwerkt. Afhankelijk van de instellingen kan ook in het netwerkverkeer gestuurd worden door middel van een ACL. Een ACL is een lijst met regels die de rechten bepalen (MARQIT, z.d.). In dit geval is de ACL aanwezig op bijvoorbeeld een firewall welke netwerkverkeer kan sturen. De CASB kan opgeven welke adressen bereikbaar zijn vanaf het netwerk waar de firewall zich in bevindt en welke geblokkeerd moeten worden. Dit zorgt ervoor dat er gestuurd kan worden in welke SaaS-applicaties er bereikbaar zijn. Dit zal echter, tenzij het vooraf geconfigureerd is, een reactieve blokkering van diensten opleveren aangezien er pas na de detectie van het gebruik van deze SaaS-applicaties een ACL opgesteld en gedistribueerd wordt.

Buiten het bedrijfsnetwerk

- Beheerde en onbeheerde apparaten
    - Deze gebruikers worden gemonitord via de beheerde SaaS-applicaties die in de CASB geconfigureerd zijn. Dit gebeurt via een reverse proxy of met een geconfigureerde API. Hierdoor is er inzicht in de acties in de SaaS-applicaties en kan er geacteerd worden op oneigenlijk gedrag. Er is bij deze variant echter geen zicht op het gebruik van SaaS gerelateerde schaduw IT.



Figuur 17 CASB werking zonder agent

13.5.1.1.3. Netwerkapparatuur ondersteuning

McAfee Cloud is compatible met alle “edge” apparaten. Dit kan een firewall, SWG of proxy zijn, die allen logging kunnen aanleveren aan de CASB. Deze logging zal dan geanalyseerd worden om een beeld van het netwerkgebruik en dus de SaaS gerelateerde schaduw IT te genereren. Buiten deze standaardinzichten in de SaaS gerelateerde schaduw IT op basis van logging, kan McAfee Cloud ook geïntegreerd worden met een aantal soorten proxy of firewalls. Indien deze ondersteund worden, kan er actiever gestuurd worden in het netwerkverkeer. Doordat er directe communicatie is tussen de CASB en de netwerkapparatuur kan de CASB de netwerkapparatuur opdragen welk netwerkverkeer toegestaan is en welk netwerkverkeer geblokkeerd moet worden. De oplossingen waarmee dat mogelijk is, zijn hieronder genoemd (McAfee, 2021d).

- Blue Coat
- Fortigate
- McAfee Enterprise Web Gateway
- Palo Alto Networks Panorama
- Zscaler

13.5.1.1.4. Unique Selling Points (USP)

Deze oplossing onderscheidt zichzelf van andere CASB-oplossingen met de mogelijkheden welke MVISION Cloud biedt om niet ondersteunde SaaS-applicaties alsnog toe te voegen aan de CASB. Hoe dit precies werkt is eerder in dit hoofdstuk uitgelegd.

Een andere functie welke niet altijd aanwezig is bij producten van andere leveranciers is de mogelijkheid om in te zien met welke applicaties van derde partijen er via OAuth is ingelogd. OAuth is een autorisatie framework welke bedoeld is om beperkte toegang te krijgen tot gebruikersaccounts. Het werkt door de authenticatie van gebruikers te delegeren naar de dienst die een gebruikersaccount beheerd en door applicaties van derden partijen toestemming te geven om het al bestaande gebruikersaccount te benaderen. Dit zorgt ervoor dat de derde partij wel toegang heeft, maar geen inzicht in wachtwoorden of andere zaken heeft. Het opvragen van de data zal dan plaats vinden door middel van het gebruik van een token (Auth0® Inc, z.d.; Hardt, 2012). Aan de hand van de informatie welke er over de verleende OAuth rechten aanwezig is, kan er dan gecontroleerd worden welke diensten van derden er verbonden zijn en welke impact dit heeft en kunnen er acties op worden ondernemen. De controle op OAuth is te integreren met Google Drive en Microsoft 365 (McAfee, 2021g).

Naast deze twee punten is McAfee door Gartner aangewezen als leader in haar laatste Magic Quadrant inzage CASB-oplossingen (Lawson & Riley, 2020). Hierbij moet wel vermeld worden dat er in de magic quadrant van Gartner daterend uit October 2020 functies als grote voordelen worden benoemd zoals Remote Browser Isolation welke inmiddels niet meer in de CASB-oplossing aanwezig lijken te zijn. Bij nader onderzoek is deze functionaliteit niet terug te vinden in documentatie voor de CASB-oplossing en lijkt deze functionaliteit te zijn verplaatst naar de Secure Access Service Edge (SASE) oplossing van McAfee, genaamd MVISION Unified Cloud Edge (McAfee, z.d.-b).

13.5.1.1.5. Conclusie

De conclusie is dat de oplossing in theorie voldoet aan alle eisen van PCI IT. De oplossing kan SaaS gerelateerde schaduw IT zichtbaar maken op het bedrijfsnetwerk, de oplossing kan sturen in beheerde SaaS-applicaties die toegevoegd zijn aan de CASB en de oplossing kan sturen in netwerkverkeer. Het grote nadeel is echter dat de SaaS-applicaties welke klanten van PCI IT gebruiken niet officieel ondersteund worden. Dit betekent dat er voor de werking van deze SaaS-applicaties minimaal acties van McAfee nodig zijn, wat betekent dat er geen gegarandeerde werking is bij de aanschaf van het product. Hoewel er altijd voor gekozen kan worden om de SaaS-applicatie toe te voegen als “Custom app” kunnen er vraagtekens geplaatst worden bij de uitvoering van deze in theorie goede oplossing. Deze functionaliteit van McAfee is gebaseerd op het leren van gedrag op de webpagina van de SaaS-applicatie. Zodra er veranderingen worden gemaakt aan de SaaS-applicatie, kan het zijn dat de monitoring niet meer werkt.

13.5.1.2. Lookout

Lookout biedt een CASB aan welke een samenvoeging van zijn eigen product is met toevoegingen van het in 2021 overgenomen Ciphercloud (Lookout, 2021). Lookout heeft weinig openbare informatie over de technische werking van hun CASB en daarom is zo goed als alle informatie die genoemd staat in dit hoofdstuk afkomstig uit een tweetal gesprekken die ik gevoerd heb met Paul Visch (Accountmanager) en Andela Popovic (Business Development Representative).

13.5.1.2.1. Ondersteuning van SaaS-applicaties

Lookout heeft net als de eerdergenoemde CASB's meerdere manieren om gebruik van beheerde SaaS-applicaties te monitoren. Dit zijn wederom forward-, reverse proxy en API. Qua toegang, gebaseerd op API, ondersteunt Lookout net als de concurrentie Office365. Daarnaast ondersteunt het andere SaaS-applicaties, maar die zijn niet in gebruik bij klanten van PCI IT en dus niet relevant voor dit onderzoek. Als het gaat om SaaS-applicaties zoals Exact of AFAS dan zullen deze dus met een reverse proxy geïmplementeerd moeten worden. Volgens Paul Visch is dit in het verleden met Exact bijvoorbeeld al gedaan voor klanten in de Benelux en moet dit geen probleem zijn. Na aanlevering van informatie zal Lookout dit configureren en werkend opleveren. Bij Lookout is men dan wel verplicht om een duurdere licentie af te nemen gezien de "Essentials" licentie geen reverse proxy ondersteunt.

13.5.1.2.2. Locatieafhankelijkheid van de oplossing

Om een beeld te vormen van de mogelijkheden van Lookout zijn de vier situaties van gebruikers hieronder genoteerd en visueel weergegeven in de eerdergenoemde figuur 17.

Op het bedrijfsnetwerk

- Beheerde en onbeheerde apparaten
    - Het gebruik van beheerde en onbeheerde SaaS-applicaties wordt op verschillende manieren in de gaten gehouden. Al het netwerkverkeer en de beheerde SaaS-applicaties die in de CASB geconfigureerd zijn, worden gemonitord door middel van de API of forward- en reverse proxy. Hierdoor zijn de acties in de beheerde SaaS-applicaties zichtbaar en kan hier op gestuurd worden. Daarnaast is het gebruik van SaaS gerelateerde schaduw IT zichtbaar dankzij logging afkomstig van de netwerkapparatuur op locatie, welke de CASB verwerkt. Afhankelijk van de instellingen kan ook in het netwerkverkeer gestuurd worden door middel van een ACL.

Buiten het bedrijfsnetwerk

- Beheerde en onbeheerde apparaten
    - Deze gebruikers worden gemonitord via de beheerde SaaS-applicaties die in de CASB geconfigureerd zijn. Dit zal gebeuren via een reverse proxy of met een geconfigureerde API. Hierdoor is er inzicht in de acties in de SaaS-applicaties en kan er geacteerd worden op oneigenlijk gedrag. Er is bij deze variant echter geen zicht op het gebruik van SaaS gerelateerde schaduw IT.

13.5.1.2.3. Netwerkapparatuur ondersteuning

De CASB van Lookout biedt volgens Paul Visch ondersteuning voor alle grote merken, waaronder Palo Alto, welke veel in gebruik zijn bij de klanten van PCI IT. De ondersteuning is aanwezig om de logbestanden van deze apparaten uit te lezen en daardoor een beeld te vormen van de aanwezige

SaaS gerelateerde schaduw IT. Het is in deze oplossing gedeeltelijk mogelijk om te sturen in de netwerkstromen door middel het gebruik van een Access Control List (ACL).

13.5.1.2.4. Unique Selling Points (USP)

Als er gekeken wordt naar het licentiemodel van Lookout dan is dit vrij modulair. Dit is zowel een voor- als nadeel. Als er gesproken wordt van een CASB dan is één van de hoofdzaken waar een CASB-oplossing voor gemaakt is, inzicht creëren in het gebruik van SaaS gerelateerde schaduw IT (Riley & Lawson, 2020). Hoewel dit mogelijk is in deze oplossing, is hier een aparte licentie voor benodigd. Dit komt ook terug als er wordt gekeken naar de onderstaande tabel voor UEBA, proxy gebruik, het licenseren van SaaS-applicaties en andere zaken. Of dit een voor- of nadeel is ligt aan de prijs welke er aan verbonden zit. Aangezien het op dit moment nog een onderzoek is en er geen klant bekend is, kan Lookout geen prijzen delen.

	Essentials	Advanced	Premium
App Bundles	1, 3, 5, Unlimited	1, 3, 5, Unlimited	1, 3, 5, Unlimited
Deployment Modes Included	API Only	API, Inline (forward, reverse proxy) and Inline Email gateway	API, Inline (forward, reverse proxy) and Inline Email gateway
Key Features Included	User Activity Monitoring Cloud Activity Audit Log DLP	**Essentials plus:** Login Access Control Real time Inline Adaptive Access Control Collaboration Sharing Controls Anti-Virus / Anti Malware UEBA & Anomaly Detection, Insights Investigate Continuous risk-based access control	**Advanced plus:** Advanced DLP (Structured Data, Exact Data Match, OCR). Data Classification Integration (Microsoft / Titus). EDRM (Encryption / Download Protection). Connected Apps Visibility. SaaS Security Posture Management (SSPM – Office365, Salesforce)
Add-on or Standalone	Shadow IT, Cloud Security Posture Management (CSPM)		
Add On	CDD – (historical data scanning – API mode only – OneDrive, Sharepoint Online, Box, Slack, GDrive, Salesforce, ServiceNow) - One time service based on (TB)		
Add On			Field Level Encryption - ServiceNow and SAP SuccessFactors
Enterprise Integrations	SSO & Lookout MES (no services required) SIEM, MDM/EMM, MFA, Managed Endpoint Detection (services required)		SSO & Lookout MES (no services required) SIEM, MDM/EMM, MFA, Managed Endpoint Detection, Microsoft Azure Information Protection & TITUS, EDLP, Key Management (hybrid), ATP/Sandboxing (services required).

Tabel 6 Licentiemodel Lookout

13.5.1.2.5. Conclusie

De conclusie over de CASB van Lookout is dat de oplossing in theorie voldoet aan alle eisen van PCI IT. De oplossing kan SaaS gerelateerde schaduw IT zichtbaar maken op het bedrijfsnetwerk, de oplossing kan sturen in beheerde SaaS-applicaties mits deze door Lookout toegevoegd zijn en de oplossing kan sturen in netwerkverkeer. Daarnaast is er bij Lookout in het verleden al gewerkt met Exact Online, wat vertrouwen schept over de implementatie van de vereiste applicaties. Er is echter geen agent aanwezig, zoals Microsoft of Forcepoint wél aanbieden, die het bereik van de oplossing zou vergroten. Dit, gebundeld met de compliceerde licentiestructuur, maakt Lookout niet de beste oplossing van de shortlist.

13.5.1.3. Forcepoint

Forcepoint biedt een CASB aan welke een samenvoeging van zijn eigen product is met toevoegingen van het overgenomen Bitglass (Forcepoint, 2021b).

13.5.1.3.1. Ondersteuning van SaaS-applicaties

De CASB-oplossing van Forcepoint heeft net als de eerdergenoemde CASB's meerdere manieren om gebruik van beheerde SaaS-applicaties te monitoren. Dit zijn forward-, reverse proxy, een agent en API. Qua API-toegang ondersteund Forcepoint, net als de concurrentie, Office365. Daarnaast ondersteunt het andere SaaS-applicaties die niet in gebruik zijn bij klanten van PCI IT en dus voor dit onderzoek niet relevant zijn. Als het gaat om SaaS-applicaties zoals Exact of AFAS dan zullen deze dus met een reverse proxy geïmplementeerd moeten worden.

13.5.1.3.2. Locatie afhankelijkheid van de oplossing

Om een beeld te vormen van de mogelijkheden van de oplossing op verschillende locaties zijn de vier situaties van gebruikers hieronder genoteerd en visueel weergegeven in de figuur 19.

Op het bedrijfsnetwerk

- Onbeheerde apparaten
    - Het gebruik van beheerde en onbeheerde SaaS-applicaties wordt op verschillende manieren in de gaten gehouden. Al het netwerkverkeer en de beheerde SaaS-applicaties die in de CASB geconfigureerd zijn, worden gemonitord door middel van de API of forward- en reverse proxy. Hierdoor zijn de acties in de beheerde SaaS-applicaties zichtbaar en kan hier op gestuurd worden. Daarnaast is het gebruik van SaaS gerelateerde schaduw IT zichtbaar dankzij logging afkomstig van de netwerkapparatuur op locatie, welke de CASB verwerkt. Afhankelijk van de instellingen kan ook in het netwerkverkeer gestuurd worden door middel van een ACL.
- Beheerde apparaten
    - Bovenop alle eigenschappen die een onbeheerd apparaat op dit netwerk geniet, kan er in het geval van een beheerd apparaat gestuurd worden via de agent. Dit heeft hetzelfde resultaat als via een ACL.

Buiten het bedrijfsnetwerk

- Onbeheerde apparaten
    - Het gebruik van onbeheerde SaaS-applicaties wordt op verschillende manieren gemonitord. De beheerde SaaS-applicaties worden door middel van een reverse proxy of via de API gemonitord. Hierdoor zijn de acties in de beheerde SaaS-applicaties zichtbaar, maar is er geen zicht op het gebruik van SaaS gerelateerde schaduw IT vanaf deze apparaten en kan er ook niet in netwerkverkeer gestuurd worden.
- Beheerde apparaten
    - Het gebruik van beheerde en onbeheerde SaaS-applicaties wordt op verschillende manieren in de gaten gehouden. Het netwerkverkeer wordt gemonitord via de "Forcepoint CASB Security Service" van het apparaat en de beheerde SaaS-applicaties die in de CASB geconfigureerd zijn, worden gemonitord via de CASB. Hierdoor zijn de acties in de beheerde SaaS-applicaties zichtbaar en kan hier op gestuurd worden. Daarnaast is het gebruik van SaaS gerelateerde schaduw IT zichtbaar en kan ook hierin gestuurd worden.

13.5.1.3.3. Netwerkapparatuur ondersteuning

Qua ondersteuning van netwerkondersteuning is weinig terug te vinden bij Forcepoint en Bitglass. De gevonden documentatie beschrijft wel het implementeren van een “Log collector”. Dit is een machine welke in het netwerk van de klant aanwezig is om de logging te benaderen en deze aan de CASB aan te leveren. Om dit werkend te krijgen, zal er op de netwerkapparatuur geconfigureerd moeten worden dat de logging benaderbaar is voor de machine die de logging doorstuurt of dat de logging geëxporteerd wordt naar een plek waar deze te benaderen is voor de machine.

Deze oplossing heeft ook de mogelijkheid om een ACL aan te leveren welke handmatig gekopieerd moet worden naar de netwerpapparatuur. Naast deze mogelijkheid is het ook een optie om verkeer te sturen via de “Forcepoint CASB Security Service” op beheerde apparaten. Deze zal dan verkeer richting de geconfigureerde domeinen tegenhouden.

13.5.1.3.4. Unique Selling Points (USP)

De USP van deze oplossing is dat deze CASB gebruik kan maken van een agent op beheerde systemen. Net als bij de oplossing van Microsoft vergroot dit de locaties waarvandaan deze CASB werkzaam kan zijn. Zoals eerder uitgelegd, zorgt dit er namelijk voor dat er gestuurd kan worden in het netwerkverkeer richting ongewenste SaaS-applicaties en dat er zicht is op het gebruik van SaaS gerelateerde schaduw IT.

13.5.1.3.5. Conclusie

De conclusie is dat de oplossing voldoet aan alle eisen van PCI IT. De oplossing kan SaaS gerelateerde schaduw IT zichtbaar maken op het bedrijfsnetwerk (en daarbuiten indien er gebruik wordt gemaakt van een beheerd apparaat met een agent), de oplossing kan sturen in beheerde SaaS-applicaties die toegevoegd zijn aan de CASB, de oplossing kan een ACL opstellen om te sturen in netwerkverkeer op de bedrijfslocatie en de oplossing kan netwerkverkeer van beheerde apparaten op elk netwerk sturen.

13.5.1.4. Microsoft Defender for Cloud Apps

Microsoft biedt een CASB aan welke de naam Microsoft Defender for Cloud Apps draagt. Deze oplossing is verweven in het licentiemodel van Microsoft en de producten welke Microsoft aanbiedt. Deze integratie en andere zaken zoals OAuth monitoring, samenvoeging met Microsoft Defender for Endpoint en de mogelijkheid om niet-officieel ondersteunde SaaS-oplossingen te integreren in deze CASB maken Microsoft Defender for Cloud Apps een zeer interessante oplossing.

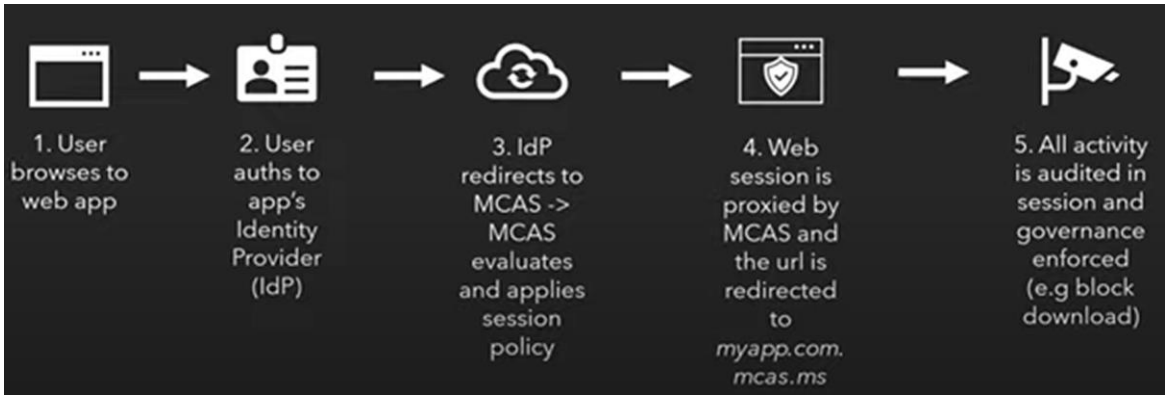
13.5.1.4.1. Ondersteuning van SaaS-applicaties

Zoals kort in de inleiding al beschreven, heeft deze oplossing naast de standaard ondersteunde SaaS-oplossingen ook de mogelijkheid om andere SaaS-applicaties toe te voegen. Deze functionaliteit heet “Conditional Access App Control” en is te gebruiken bij apps die voldoen aan de hieronder genoteerde eisen (Microsoft, 2021g):

- De volgende licenties moeten aanwezig zijn
    - Azure Active Directory Premium P1 of hoger indien er gebruikt wordt van Azure als IDP. Indien er gebruik wordt gemaakt van een andere IDP, dan moet de licentie van de IDP-leverancier toereikend zijn.
    - Microsoft Defender for Cloud Apps, deze licentie is verwerkt in de volgende producten (Microsoft, 2021a):
        - Microsoft 365 E5
        - Microsoft 365 E5 Security
        - Microsoft 365 E5 Compliance
        - Enterprise Mobility & Security E5
        - Microsoft Cloud App Security + Enterprise Mobility & Security E3
        - Microsoft 365 Education A3
        - Microsoft 365 Education A5
        - Microsoft Cloud App Security (losse licentie)
- De apps die toegevoegd worden, moeten voorzien zijn van Single Sign-On (SSO)
- De apps die toegevoegd worden moeten, indien Azure als IDP gebruikt wordt, SAML 2.0 of OpenID Connect ondersteunen. Indien een andere IDP-leverancier wordt gebruikt, moet de applicatie SAML 2.0 ondersteunen.

Indien alles aan de eisen voldoet en het geconfigureerd is, wordt er door middel van een functie die Microsoft “sessiebeheer” noemt, monitoring op die exacte situatie toegepast. Het verkeer wordt omgeleid via een reverse proxy en zal dus niet direct met een dienst zoals Exact online communiceren.

De afhandeling van een standaard inlog in bijvoorbeeld Exact online is in figuur 18 hieronder gevisualiseerd.



Figuur 18 Flow sessiebeheer (Soseman, 2020b, 2:34)

Zoals in de afbeelding al aangehaald wordt, zorgt “Conditional Access App Control” ervoor dat de CASB inzicht heeft en acties in de SaaS-applicatie kan sturen (Microsoft, 2021o). De oplossing heeft volgens Microsoft (Microsoft, 2019; Microsoft, 2021m; Microsoft, 2021o) de volgende mogelijkheden als de sessie actief is:

- **“Gegevensexfiltratie voorkomen:** u kunt het downloaden, knippen, kopiëren en afdrukken van gevoelige documenten op bijvoorbeeld onbeheerde apparaten blokkeren.
- **Verificatiecontext vereisen:** u kunt het beleid voor voorwaardelijke toegang van Azure AD opnieuw beoordelen wanneer er een gevoelige actie plaatsvindt in de sessie. Bijvoorbeeld meervoudige verificatie vereisen bij het downloaden van een uiterst vertrouwelijk bestand.
- **Beveiligen bij downloaden:** in plaats van het downloaden van gevoelige documenten te blokkeren, kunt u vereisen dat documenten worden gelabeld en beveiligd met Azure Information Protection. Deze actie zorgt ervoor dat het document wordt beveiligd en dat gebruikerstoegang wordt beperkt in een mogelijk riskante sessie.
- **Uploaden van niet-gelabelde bestanden voorkomen:** voordat een gevoelig bestand wordt geüpload, gedistribueerd en gebruikt door anderen, is het belangrijk om ervoor te zorgen dat het bestand het juiste label en de juiste beveiliging heeft. U kunt ervoor zorgen dat niet-gelabelde bestanden met gevoelige inhoud niet worden geüpload totdat de gebruiker de inhoud classificeert.
- **Mogelijke malware blokkeren:** u kunt uw omgeving beschermen tegen malware door het uploaden van mogelijk schadelijke bestanden te blokkeren. Elk bestand dat wordt geüpload of gedownload, kan worden gescand op bedreigingsinformatie van Microsoft en onmiddellijk worden geblokkeerd.
- **Gebruikerssessies controleren op naleving:** riskante gebruikers worden bewaakt wanneer ze zich aanmelden bij apps en hun acties worden vastgelegd vanuit de sessie. U kunt het gedrag van gebruikers onderzoeken en analyseren om te begrijpen waar en onder welke omstandigheden sessiebeleid in de toekomst moet worden toegepast.
- **Toegang blokkeren:** u kunt de toegang voor specifieke apps en gebruikers gedetailleerd blokkeren, afhankelijk van verschillende risicofactoren. U kunt ze bijvoorbeeld blokkeren als ze clientcertificaten gebruiken als een vorm van apparaat beheer.
- **Aangepaste activiteiten blokkeren:** sommige apps hebben unieke scenario's die risico's met zich meebrengen, bijvoorbeeld het verzenden van berichten met gevoelige inhoud in apps zoals Microsoft Teams of Slack. In dit soort scenario's kunt u berichten scannen op gevoelige inhoud en deze in realtime blokkeren.” (Microsoft, 2021m).

Dankzij de mogelijkheden van deze oplossing is het dus mogelijk om de vier genoemde SaaS-applicaties te monitoren (AFAS, z.d.; Exact, z.d.). Naast de vier genoemde SaaS-applicaties met prioriteit is de verwachting dat veel van de in de deelvraag genaamd “Van welke SaaS-applicaties maken klanten van PCI IT gebruik?” genoteerde SaaS-applicaties zullen voldoen aan de gestelde eisen om verwerkt te worden in deze CASB.

13.5.1.4.2. Locatieafhankelijkheid van de oplossing

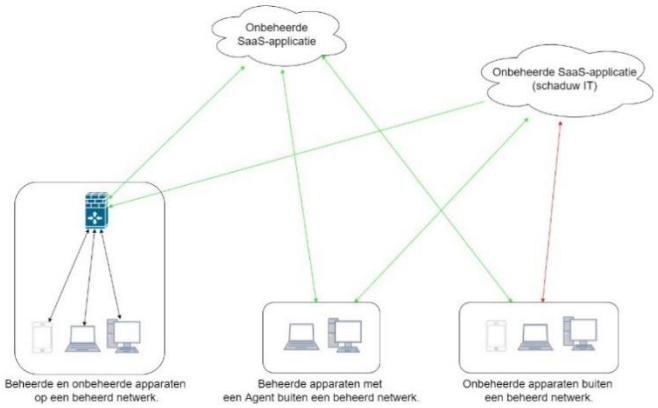
Om een beeld te vormen van de mogelijkheden van de oplossing op verschillende locaties zijn de vier situaties van gebruikers hieronder genoteerd en daarna visueel weergegeven in figuur 19.

Op het bedrijfsnetwerk

- Onbeheerde apparaten
    - Het gebruik van beheerde en onbeheerde SaaS-applicaties wordt op verschillende manieren gemonitord. Al het netwerkverkeer en de beheerde SaaS-applicaties die in de CASB geconfigureerd zijn, worden gemonitord door middel van de API of forward- en reverse proxy. Hierdoor zijn de acties in de beheerde SaaS-applicaties zichtbaar en kan hier op gestuurd worden. Daarnaast is het gebruik van SaaS gerelateerde schaduw IT zichtbaar dankzij logging afkomstig van de netwerkapparatuur op locatie welke de CASB verwerkt. Afhankelijk van de instellingen kan ook in het netwerkverkeer gestuurd worden door middel van ACL.
- Beheerde apparaten
    - Bovenop alle eigenschappen die een onbeheerd apparaat op dit netwerk geniet, kan er in het geval van een beheerd apparaat gestuurd worden via de agent. Dit heeft hetzelfde resultaat als via een ACL.

Buiten het bedrijfsnetwerk

- Onbeheerde apparaten
    - Het gebruik van onbeheerde SaaS-applicaties wordt op verschillende manieren gemonitord. De beheerde SaaS-applicaties worden door middel van een reverse proxy of via de API gemonitord. Hierdoor zijn de acties in de beheerde SaaS-applicaties zichtbaar, maar is er geen zicht op het gebruik van SaaS gerelateerde schaduw IT vanaf deze apparaten en kan er ook niet in netwerkverkeer gestuurd worden.
- Beheerde apparaten
    - Het gebruik van beheerde en onbeheerde SaaS-applicaties wordt op verschillende manieren in de gaten gehouden. Het netwerkverkeer wordt gemonitord via de Microsoft Defender Advanced Threat Protection van het apparaat en de beheerde SaaS-applicaties die in de CASB geconfigureerd zijn, worden gemonitord via de CASB. Hierdoor zijn de acties in de beheerde SaaS-applicaties zichtbaar en kan hier op gestuurd worden. Daarnaast is het gebruik van SaaS gerelateerde schaduw IT zichtbaar en kan ook hierin gestuurd worden.



Figuur 19 CASB-werking met agent

13.5.1.4.3. Netwerkapparatuur ondersteuning

Microsoft Defender voor Cloud Apps is compatible met alle “edge” apparaten. Dit kan een firewall, SWG of proxy zijn, die allen logging kunnen aanleveren aan de CASB. Deze logging zal dan geanalyseerd worden om een beeld van het netwerkgebruik en dus de SaaS gerelateerde schaduw IT te genereren. Buiten deze standaard inzichten in de SaaS gerelateerde schaduw IT op basis van logging kan Microsoft Defender voor Cloud Apps ook geïntegreerd worden met een aantal soorten proxies of firewalls. Indien deze ondersteund worden, kan er actiever gestuurd worden in het netwerkverkeer. De oplossingen waarmee dat mogelijk is, zijn hieronder genoemd (Microsoft, 2021n).

- Zscaler
- Iboss
- Corrata
- Menlo security

Naast de hierboven genoemde producten zijn er andere mogelijkheden om in het netwerkverkeer te sturen met deze CASB. Dit wordt gedaan door middel van het creëren van een blocklist (dit is een benaming van Microsoft, in feite is het een ACL), waarna deze richting een “edge” apparaat wordt verstuurd. Deze blocklist is een product van de CASB welke dan aan het netwerkapparaat duidelijk maakt dat de websites die genoemd zijn in de blocklist niet meer bezocht mogen worden. Op het moment van schrijven worden de volgende fabrikanten ondersteund (Microsoft, 2021e).

- BlueCoat ProxySG
- Cisco ASA
- Fortinet FortiGate
- Juniper SRX
- Palo Alto
- Websense
- Zscaler

13.5.1.4.4. Unique Selling Points (USP)

Een uniek onderdeel van het product van Microsoft is de integratie met de Microsoft Defender for Endpoint, doordat deze oplossing werkt met de managed variant van Windows Defender welke in basis al aanwezig is op de beheerde laptops van klanten. Dit zorgt ervoor dat er met vrij weinig configuratie een agent aanwezig is op de beheerde apparaten. Deze agent kan vanaf dat moment actief sturen in netwerkverkeer, zelfs als het apparaat niet op het bedrijfsnetwerk aanwezig is (Microsoft, 2021b). Dit zorgt ervoor dat het apparaat buiten het netwerk van het bedrijf beveiligd is en dat ook het zicht op SaaS gerelateerde schaduw IT aanwezig blijft (Soseman, 2020a). Om deze functionaliteit te gebruiken, moet er gebruik gemaakt worden van een Microsoft Defender for Endpoint license. Er zijn enkele licenties waar het gebruik van deze Microsoft Defender for Endpoint in verweven zit en dit zijn:

- Windows 11 Enterprise E5
- Windows 11 Education A5
- Windows 10 Enterprise E5
- Windows 10 Education A5
- Microsoft 365 E5
- Microsoft 365 A5
- Microsoft 365 E3 met Enterprise Mobility en Security E5 Add-on
- Microsoft 365 Business Premium (indien aangeschaft via een Microsoft Cloud Solution Provider)

- Microsoft 365 E5 Security
- Microsoft 365 A5 Security
- Microsoft Defender for Endpoint (losse licentie) (Microsoft, 2021i)

Na navraag bij PCI IT blijkt dat het gros van de klanten van PCI IT gebruik maakt van Microsoft365 E3, Microsoft 365 Business Premium, Office 365 E3 en enkele klanten op Microsoft365 E5. Zoals uit de opgevraagde licentie modellen blijkt, zal er voor de complete werking van Microsoft Defender for Cloud Apps, Microsoft Defender for Endpoint en Microsoft Defender for Cloud Apps Discovery een Microsoft365 E5 licentie afdoende zijn. Gezien er ook veel gebruik wordt gemaakt van Microsoft365 E3, raad ik aan om Microsoft365 E5 Security toe te voegen aan de E3 licentie. Afhankelijk van het volume waarmee deze licenties worden ingekocht en de oorsprong zal dat ongeveer € 8,76 per gebruiker per maand kosten (dsaict, z.d.). De Microsoft 365 Business Premium licenties zouden op een soortgelijke manier uitgebreid kunnen worden (Microsoft, 2021t).

Een andere USP van Microsoft Defender for Cloud Apps is dat het inzicht kan creëren in de applicaties van derden waar OAuth rechten aan verleend zijn met een managed SaaS-account (Microsoft, 2021d). Dankzij deze toevoeging is er meer grip en zicht op de rechten die gebruikers aan derde partijen verlenen. Naast dat er staat dat er rechten zijn gegeven, zal er ook informatie staan over de dienst welke de rechten heeft ontvangen. Aan de hand van deze informatie kunnen er dan acties opgezet worden en kunnen de rechten ingetrokken worden. Daarnaast kan deze CASB hier automatisch actie op ondernemen indien dit geconfigureerd is.

Het derde USP van Microsoft Defender for Cloud Apps is dat de licentie structuur anders opgezet is dan die van de concurrentie. Waar dit bij de concurrentie zoals Lookout vaak is dat er per koppeling met een SaaS-applicatie betaald wordt, is dit bij Microsoft Defender for Cloud Apps per gebruiker. Dit zorgt ervoor dat er bij Microsoft een enkele licentie kan worden afgenomen en niet naast de licentie per gebruiker gerekend wordt met licenties voor de SaaS-applicaties en gebruikers.

13.5.1.4.5. Conclusie

De conclusie is dat de oplossing voldoet aan alle eisen van PCI IT. De oplossing kan SaaS gerelateerde schaduw IT zichtbaar maken op het bedrijfsnetwerk (en daarbuiten indien er gebruik wordt gemaakt van een beheerd apparaat met Microsoft Defender for Endpoint), de oplossing kan sturen in beheerde SaaS-applicaties die toegevoegd zijn aan de CASB, de oplossing kan blocklists opstellen om te sturen in netwerkverkeer op de bedrijfslocatie en de oplossing kan netwerkverkeer van beheerde apparaten op elk netwerk sturen. Naast de technische mogelijkheden die deze oplossing biedt, zijn ook het licentiemodel en de integratie met Microsoft haar eigen producten een grote pré. De licentie is, zoals gezegd, in sommige gevallen al aanwezig en in andere gevallen zal het een uitbreiding zijn op een bestaande licentie. De integratie met andere (security) gerelateerde producten van Microsoft, zoals in dit geval de Microsoft Defender for Endpoint, is ook iets wat veel voordelen oplevert, zoals het overzicht en de controle.

13.5.1.5. Conclusie shortlist

Als alle oplossingen van de leveranciers op de shortlist tegenover elkaar worden gezet, dan komt Microsoft boven de andere oplossingen uit. De oplossing heeft samen met Forcepoint het grootste bereik door de inzet van een agent, maar onderscheidt zich van Forcepoint door middel van de mogelijkheid om SaaS-applicaties zelf toe te voegen met duidelijke requirements. Daarnaast onderscheidt het zich omdat er een licentie voordeel aanwezig is, aangezien er al gebruik wordt gemaakt van gerelateerde Microsoftproducten, omdat er OAuth monitoring aanwezig is en omdat deze CASB diepgaande integratie heeft binnen het Microsoft ecosysteem. Naast de voordelen die zichtbaar zijn in technische eigenschappen, is er al een bestaande relatie met Microsoft wat een pré vanuit PCI IT is en is Microsoft erg transparant in de mogelijkheden van haar CASB. Dit versterkt het gevoel dat er een werkend product aangeschaft wordt in tegenstelling tot een belofte. Waar bij andere producten de belofte wordt gedaan om een SaaS-applicatie in de CASB te integreren, wordt bij deze CASB duidelijk vermeld welke vereisten er zijn om een SaaS-applicatie werkend te krijgen.

Dit alles maakt dat ik met vertrouwen kan aanraden om Microsoft Defender for Cloud Apps in te gaan zetten bij klanten van PCI IT. Gezien Microsoft Defender for Cloud Apps voldoet aan alle opgestelde requirements en randvoorwaarden is het antwoord op de deelvraag “Welke beveiliging en controle oplossingen zijn er op de markt die voldoen aan de eisen van PCI IT en welke past het beste bij PCI IT?” dan ook Microsoft Defender for Cloud Apps.

13.6. Organogram