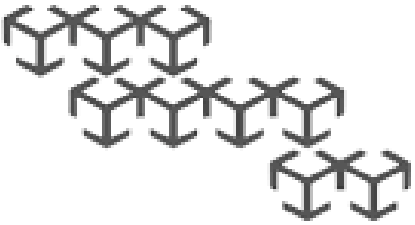
Afstudeerscriptie

Endpoint protection



BRADON

Puts IT through!

Auteur:

Sem Vreeman
476521

Bedrijfsbegeleiders:

Ernst Bakker
Ronald Letema

Afstudeerdocent:

Steven van der Linden

Opdrachtgever:

Bradon B.V.

Versie:

Definitieve versie

Datum:

21-01-2024

Voorwoord

Voor u ligt de afstudeerscriptie “Endpoint protection” welke is geschreven in opdracht van Bradon B.V. In dit document zal Bradon B.V. als Bradon worden weergegeven om het document overzichtelijk te houden. Deze scriptie is geschreven als afstudeeropdracht voor de opleiding HBO-ICT infrastructuur aan de hogeschool Saxion te Deventer.

Deze afstudeeropdracht is uitgevoerd van september 2023 tot en met februari 2024 bij Bradon. Er is onderzoek gedaan naar endpoint protection en wat voor Bradon de beste optie is, om in de toekomst als dienst aan te bieden aan klanten.

Ik wil graag Ernst Bakker bedanken voor het begeleiden vanuit Bradon en het advies en feedback op mijn scriptie. Ook wil ik Niels Simmelink bedanken voor het beantwoorden van de technische vraagstukken als ik deze had. Tenslotte wil ik mijn begeleider Steven van der Linden vanuit Saxion bedanken, voor de feedback en advies die hij mij heeft gegeven voor het maken van mijn scriptie.

Samenvatting

Deze scriptie bevat het afstudeerverslag van Sem Vreeman bij Bradon. Bradon levert IT-diensten aan een groot aantal klanten. De ambitie van Bradon is om de IT-zaken, beter, slimmer en sneller te laten verlopen.

Bradon levert momenteel geen dienst betreffende endpoint protection, wel heeft Bradon verschillende klanten waar laptops beheerd worden. Bradon is echter opzoek naar een endpoint oplossing die het mogelijk maakt om een nieuwe dienst aan te bieden bij haar klanten. In dit onderzoek wordt er antwoord gegeven op de hoofdvraag: **Hoe kan Bradon endpoint protection inrichten voor de endpoints bij haar klanten, zodat endpoint beheer als dienst kan worden aangeboden aan klanten en hoe kan Bradon de endpoint protection laten aansluiten op de NIS2?** Deze hoofdvraag wordt onderbouwd door de volgende deelvragen te beantwoorden.

In het hoofdstuk "Projectopdracht & Initiële probleemstelling" wordt er antwoord gegeven op deelvraag één**: "Wat is de huidige situatie bij Bradon?".** Momenteel levert Bradon verschillende IT-diensten aan haar klanten, maar levert Bradon geen endpoint protection. Bradon wil deze dienst gaan leveren aan huidige en toekomstige klanten.

In de behoefte analyse wordt er antwoord gegeven op deelvraag twee**: "Welke eisen en wensen zijn er vanuit Bradon?".** Hieruit is gebleken dat Bradon op zoek is naar een endpoint oplossing waarmee de endpoints efficiënt en effectief beheerd kunnen worden. Verder moet de oplossing een optie hebben om informatie te kunnen exporteren.

Om een beeld te krijgen in welke context het project afspeelt is er een contextanalyse uitgevoerd. Hieruit is een interne analyse en een externe analyse gekomen waaruit de randvoorwaarden zijn ontstaan. De endpoint oplossing dient door Bradon als dienst te worden aangeboden, de oplossing dient cloudbased te zijn, Bradon heeft als voorkeur om de oplossing af te nemen bij een van haar huidige leveranciers en de oplossing moet maandelijks te betalen zijn.

De NIS2 brengt verschillende eisen met zich mee. Om deelvraag drie: "**: Welke eisen brengt de NIS2 mee**" te kunnen beantwoorden is onderzoek gedaan. De NIS2 neemt de volgende eisen mee: zorgplicht, meldplicht en toezicht. Om deelvraag vier: "**Welke vormen van endpoint protection zijn er?**" te beantwoorden, is er gekeken naar de verschillende vormen van endpoint protection (Network access control, Data loss prevention, Insider threat protection, Data clasification, URL filtering, Browser isolation, cloud peremiter security en endpoint encryption). Verder is hier gekeken naar Security information and event management, Managed detection & response, Extended detection and response en endpoint detection end response. Ten slot zijn de best practices onderzocht die te realiseren zijn in de toekomstige oplossing.

Om een beeld te krijgen van de mogelijke opties is er eerst een conceptueel ontwerp gemaakt, er is gekeken naar de functies die eindgebruikers moeten kunnen uitvoeren en de uitwerking van de best practices. Hierna is er antwoord gegeven op deelvraag vijf: **"Welke producten zijn er voor de endpoint protection en wat zijn hier de voor- en nadelen van?"**. De verschillende mogelijke oplossingen zijn te zien in een longlist met de requirements waaraan deze voldoen. Uit deze longlist is een shortlist gekomen met hierin staan de drie oplossing die bij Bradon passen. De keuze is Datto EDR geworden, hiermee is deelvraag zes: **"Welke vorm van endpoint protection past bij Bradon?"** beantwoord. Na het kiezen van Datto EDR is deelvraag zeven: "**Hoe gaat het product worden geconfigureerd?**" beantwoord. In het technische ontwerp zijn de mogelijkheden van installatie en het dashboard te zien. Ook zijn hier de best practices uitgewerkt en is Datto getest. Hiervan zijn de resultaten te zien in het testrapport.

In het advies is antwoord gegeven op deelvraag acht: “**Hoe kan endpoint protection aansluiten op de NIS2?”** en de hoofdvraag: **“Hoe kan Bradon endpoint protection inrichten voor de endpoints bij haar klanten, zodat endpoint beheer als dienst kan worden aangeboden aan klanten en hoe kan Bradon de endpoint protection laten aansluiten op de NIS2?”.** Datto voldoet aan de NIS2 gestelde eisen die momenteel bekend zijn (zorgplicht en meldplicht), de informatie is in een overzichtelijk dashboard beschikbaar voor Bradon. Als er een ransomware attack speelt die effect heeft op de essentiële diensten in Nederland kan dit direct gemeld worden. Bradon zal doormiddel van Datto een nieuwe dienst kunnen verlenen aan haar klanten. Datto maakt het makkelijk om endpoints te managen en om over het gehele netwerk de agent te installeren. Hierdoor kan Bradon efficiënt en effectief endpoint management uitrollen bij nieuwe en huidige klanten.

Inhoud

Tabellenlijst

Figurenlijst

Begrippenlijst

Cloud Based

Cloud based houdt in dat de software via internet (de cloud) wordt aangeboden. Hierdoor is het mogelijk om snellere innovatie te krijgen, flexibele recources en schaalvoordelen (Wat is cloud computing?, z.d.).

Endpoint protection

Met endpoint protection worden apparaten van eindgebruikers zoals desktops, laptops en mobiele apparaten beveiligd tegen mensen die misbruik willen maken.
Eindpuntbeveiligingssystemen beschermen de endpoints die binnen een netwerk aanwezig zijn tegen cyberdreigingen (What is Endpoint Security? how it works & its importance | Trellix, z.d.).

Endpoints

Endpoints zijn fysieke apparaten die verbinding maken met een netwerk en hierop informatie uitwisselen. Denk hierbij een desktops, laptops, servers en mobiele apparaten.
https://www.microsoft.com/nl-nl/security/business/security-101/what-is-an-endpoint

Multi Factor Authentication

Multi Factor Authenitaction is een methode om toegang tot accounts veiliger te maken. Doormiddel van een extra code na het inloggen op het account in te moeten voeren, zorg je ervoor dat er een extra laag beveiliging is (Wat is tweefactorauthenticatie?, z.d.).

Manage service provider (MSP)

Een manage service provider is een extern bedrijf dat IT-behoeften van andere bedrijven voorziet. Deze diensten kunnen monitoring zijn, het beheren van applicaties, de IT-infrastructuur leveren, patches en updates uitvoeren en nog veel meer (Richter, 2022).

NIS2

De NIS2 is een richtlijn vanuit de Europese unie. Deze richtlijn dient de digitale en economische weerbaarheid van Europese lidstaten te versterken. NIS2 richt zich op de digitale risico's voor netwerk- en informatie systemen (Nationaal Cyber Security Centrum, 2023a).

RMM

Remote monitoring and management (RMM) wordt gebruikt voor het verzamelen van informatie over endpoints en deze weer te geven. Denk hierbij een Real-time monitoring en alerts weergeven, onderdelen zoals updates automatiseren en script kunnen uitvoeren op endpoints (Ninja, 2023).

Inleiding

Het afstudeerproject zal worden uitgevoerd voor Bradon. Bij het eerste gesprek met Bradon was duidelijk dat zij op zoek waren naar een endpoint protection oplossing en dat de NIS2 er aan komt. Bradon zag dit als een mooi afstudeerproject waar kennis kan worden opgedaan voor de afstudeerder en het bedrijf. Bradon is een managed service provider en levert verschillende diensten aan haar klanten en zij wil endpoint protection hieraan toevoegen.

In deze scriptie zal er gekeken worden naar het probleem en de huidige situatie, vervolgens zal er gekeken worden naar de eisen en wensen vanuit Bradon. Om duidelijk te krijgen in welke context dit project zich afspeelt zal deze geanalyseerd worden en zal er een literatuuronderzoek worden gedaan om zo aan de benodigde informatie te komen. Om de verkregen informatie te gebruiken zal dit worden omgezet in ontwerpen. Deze ontwerpen zullen gerealiseerd in een proof of concept die doormiddel van en testplan en testrapport zal worden getest. Hiermee wordt er voldaan aan de beroepsactiviteiten analyseren, ontwerpen en realiseren.

1. Projectopdracht & Initiële probleemstelling

In dit hoofdstuk wordt deelvraag 1 beantwoord: Wat is de huidige situatie van Bradon?

Bedrijven stappen steeds meer af van desktops en thin clients en gaan over op laptops om thuiswerken (beter) mogelijk te maken. Steeds meer bedrijven staan het concept “bring your own device” toe. Hierdoor wordt online thuiswerken aantrekkelijker voor zowel werkgevers als werknemers. Doordat er meer gebruik gemaakt wordt van laptops en er meer thuis wordt gewerkt is het belangrijk dat de endpoint protection goed in orde is. Het beheren en beheersen van de endpoint protection is ook zeer belangrijk. Vanuit de overheid worden er steeds meer eisen gesteld waaraan bedrijven moeten voldoen zoals de NIS2.

De opdracht houdt het onderzoeken en adviseren van de verschillende mogelijkheden van endpoint protection in en hieruit een endpoint protection oplossing adviseren. Tevens dient de endpoint oplossing te voldoen aan de gestelde eisen van de NIS2 die momenteel bekend zijn. Om het vraagstuk vanuit Bradon vast te stellen is een probleemanalyse uitgevoerd. Onderstaand wordt de methodiek besproken die gebruikt is bij het vaststellen van het vraagstuk. Het doel van de projectopdracht en probleemanalyse is door middel van de verschillende perspectieven de hoofd - en deelvragen te bepalen.

1.1 Methodiek

Om een goed beeld te krijgen van de opdracht en de probleemstelling is er eerst gekeken naar wie de stakeholders zijn. Hieruit is een lijst ontstaan die door middel van de Mendelow methodiek geprioriteerd wordt. De Mendelow methodiek prioriteer stakeholders door middel van macht en belang (Barrington, R. 2020, 1 augustus). Hieruit is de shortlist van stakeholders opgesteld. De prioritering van de stakeholders is te vinden in bijlage A.

Het is belangrijk om een duidelijk beeld te hebben van wat de stakeholders voor verschillende perspectieven hebben. Om de perspectieven duidelijk te krijgen zijn de stakeholders geïnterviewd. Dit is gedaan in de vorm van een semigestructureerd interview. Dit betekent dat er vooraf bedachte open vragen zijn opgesteld. Hierdoor ontstaat de mogelijkheid om door te vragen op eventuele antwoorden. Door deze manier van interviewen is de betrouwbaarheid van de antwoorden hoog. (Dingemanse, K. 2021, 12 november)

Naast het interviewen van de stakeholders is er ook gebruik gemaakt van literatuuronderzoek om een overheidsperspectief op de NIS2 te bepalen. Hiervoor zijn bronnen afkomstig van de Nederlands overheid en andere instellingen gebruikt.

1.2 Projectopdracht

Het is belangrijk om te kijken welke mogelijkheden er zijn betreffende endpoint protection. Door de mogelijkheden met elkaar te vergelijken en de voor- en nadelen van de verschillende opties tegen elkaar af te wegen, ontstaat er een beeld van de soorten endpoint protection en welke het meest geschikt is op basis van de opgestelde requirements voor Bradon. Om deze vervolgens te gaan gebruiken en als dienst aan te bieden aan haar klanten.

Bring your own device en NIS2 worden meegenomen in het analyseren van de verschillende mogelijkheden, zodat er een keuze gemaakt kan worden betreffende endpoint protection die voldoet aan de eisen van Bradon en de NIS2, om zo tot een uniform beleid te komen.

1.3 Huidige situatie

Bradon levert verschillende diensten aan haar klanten, momenteel is endpoint protection geen onderdeel van de aangeboden diensten. Er zijn wel verschillende platformen aanwezig waarop endpoint protection mogelijk is. Dit zijn Intune en Datto. Deze platformen worden momenteel gebruikt voor andere doeleinden en hierop is endpoint protection ook niet ingericht. Met deze platformen worden momenteel bij verschillende klanten de laptops beheerd.

1.4 Initiële probleemstelling

Dit hoofdstuk bevat de verschillende perspectieven van de initiële probleemstelling

1.4.1 Literatuur perspectief

Allereerst is er gekeken wat endpoint protection is en wat de NIS2 inhoudt. Endpoint protection is het beveiligen van de apparaten van eindgebruikers, zoals desktops, laptops en mobiele apparaten. (Trellix, z.d.)

Data is een van de meest kostbare bezittingen van een bedrijf. Het verliezen van data, of de toegang tot deze data, of het beschadigen van de data, kan grote gevolgen voor een bedrijf hebben. Bedrijven krijgen te maken met steeds meer endpoints en dit is tevens ook een van de zwakste schakels binnen elk bedrijf. Het is daarom van belang om de beveiliging van deze endpoints serieus aan te pakken. (Felton B.V., 2021)

De NIS2 richtlijn is opgesteld door de Europese unie na de diverse ontwikkelingen die de veiligheid van de maatschappij en de economie onder druk hebben gezet. De richtlijn is gericht op het verbeteren van de digitale en economische weerbaarheid van de Europese lidstaten (Nationaal Cyber Security Centrum, 2023) verdere uitleg volgt in het overheid perspectief.

1.4.2 Perspectief onderzoeker

Na de initiële probleemstelling is het perspectief van de onderzoeker zeer van belang. Bradon maakt momenteel al gebruik van verschillende soorten software waarmee zij klanten helpen en bij sommige klanten endpoints beheren, echter is hier geen centrale optie voor aanwezig waarin alle klanten beheerd kunnen worden. Voor Bradon is dit van belang om op orde te hebben, zodat zij een nieuwe dienst aan klanten kan verlenen en de kansen op cyberdreigingen bij klanten kunnen verkleinen of snel kunnen verhelpen.

Bradon zal moeten gaan voldoen aan de NIS2, deze regelgeving is momenteel nog in uitwerkende fase en zal kwartaal 1 van 2024 gedeeld worden met de bedrijven in Nederland en een feedback periode in gaan. Bradon kan voorbereidende stappen nemen om al aan bepaalde eisen die gesteld zijn vanuit andere normen te voldoen en mijn advies is dan ook om hieraan te beginnen.

Door deze stappen uit te voeren zal Bradon als bedrijf meer kunnen bieden aan haar klanten en ook voldoen aan de NIS2 die eind 2024 van toepassing zal zijn.

1.5 Aspecten

Uit de gesprekken met de stakeholders zijn hun perspectieven gekomen. Deze zijn te vinden in bijlage B. Uit de verschillende perspectieven zijn aspecten gekomen waar de stakeholders tegenaanlopen binnen dit onderzoek.

Senior engineer:

- Er is geen endpoint protection aanwezig
- Er is geen beleid aanwezig

Backoffice:

- Geen extra dienst die verkocht kan worden (endpoint protection)
- Geen beleid

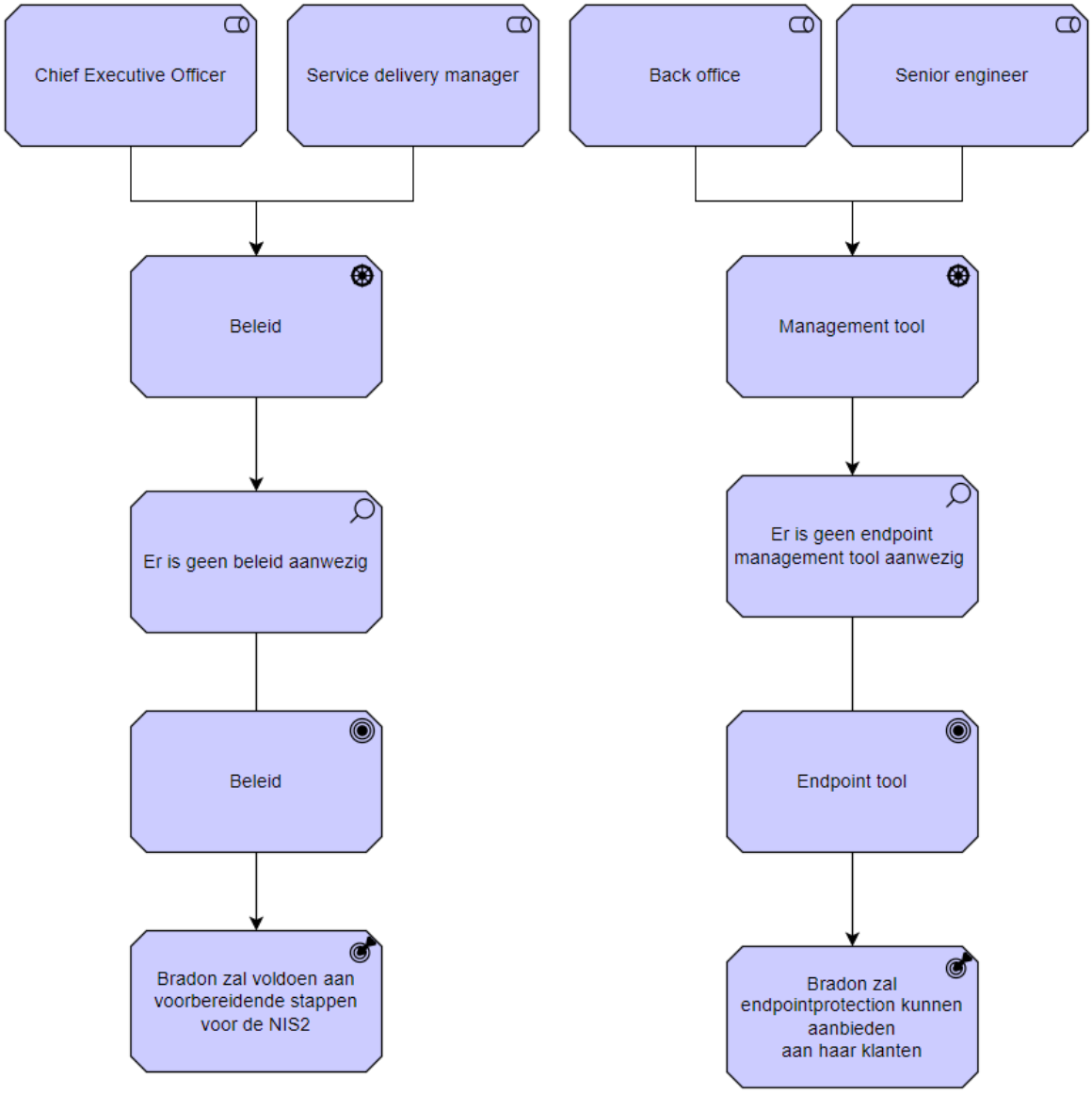
Chief executive officer

- Bradon voldoet niet aan de NIS2
- Geen beleid dat voorbereidt op de NIS2
- Bradon kan geen extra dienst leveren zonder de endpoint protection

Service delivery manager

- Er is geen beleid aanwezig die Bradon kan volgen
- Er is geen mogelijkheid om overzicht te hebben van alle werkstations en hun licentie
- Behoefte aan beleid
- NIS2

Om een duidelijk beeld te krijgen wat belangrijk is voor de stakeholders zijn de aspecten vergeleken met elkaar en zijn er afwegingen gemaakt. Hieruit zijn een aantal aspecten gekomen die voor elke stakeholder belangrijk zijn. Deze zijn in figuur 1 verwerkt. Hiervoor is gebruik gemaakt van de archimate motivation concepts model (Opengroup, z.d.). Uit de aspecten komen verschillende doelen waaruit de business requirements ontstaan. Deze business requirements zijn opgesteld om het doel te behalen. In tabel 1 zijn deze requirements te zien.



Figuur 1 Archimate Motivatie Model

1.5.1 Business requirements

Onderstaand is de tabel te zien met de business requirements die zijn voortgekomen uit het archimate motivation model.

Nr.	Beschrijving
B01	Bradon zal voldoen aan voorbereidende stappen voor de NIS2
B02	Bradon zal endpoint protection kunnen aanbieden aan haar klanten

Tabel 1 Business requirements

1.6 Conclusie

Op basis van de verschillende gesprekken met de stakeholders is er een lijst met aspecten ontstaan. Uit deze lijst van aspecten is een hoofdvraag voor dit onderzoek opgesteld. Om de hoofdvraag goed onderbouwd te beantwoorden zijn er meerdere deelvragen opgesteld. Deze worden in het onderzoeksrapport behandeld.

1.6.1 Hoofdvraag

Hoe kan Bradon endpoint protection inrichten voor de endpoints bij haar klanten, zodat endpoint beheer als dienst kan worden aangeboden aan klanten en hoe kan Bradon de endpoint protection laten aansluiten op de NIS2?

Het probleem waar onderzoek naar gedaan moet worden is het achterhalen welke vorm van endpoint protection voor Bradon het meest effectief te beheren en beheersen is, zodat deze aangeboden kan worden als dienst bij Bradon haar klanten. Ook zal er gekeken worden hoe het product zal aansluiten op de NIS2.

1.6.2 Deelvragen

Om de hoofdvraag te kunnen beantwoorden zijn er deelvragen opgesteld. Deze deelvragen komen voort uit de perspectieven van de stakeholders en zullen ook het antwoord op de hoofdvraag onderbouwen. In tabel 1 zijn de hoofd -en deelvragen te zien met de onderzoeksmethode en in welke fase van het onderzoek de vraag beantwoord wordt.

Deelvraag één: Wat is de huidige situatie bij Bradon? (Deze deelvraag wordt beantwoord in hoofdstuk 1)

Om een duidelijk beeld te krijgen wat er bij Bradon aanwezig is en wat eventueel gebruikt kan worden in het onderzoek, moet de huidige situatie beschreven worden van Bradon. Hieruit ontstaat een duidelijk beeld van de huidige situatie bij Bradon.

Deelvraag twee: Welke eisen en wensen zijn er vanuit Bradon? (Deze deelvraag wordt beantwoord in hoofdstuk 2)

Om uiteindelijk een goede keuze te maken voor de beste endpoint protection, zullen de eisen en wensen vanuit Bradon worden besproken en in de requirements analyse worden verwerkt. Deze requirements zullen worden meegenomen bij het bepalen van de beste endpoint protection en bij het bepalen van de mogelijke baseline die aan klanten aangeboden kan worden.

Deelvraag drie: Welke eisen brengt de NIS2 mee? (Deze deelvraag wordt beantwoord in hoofdstuk 4)

Vanaf 1 Juli 2024 moeten bedrijven voldoen aan de NIS2. Het is daarom van belang dat in dit onderzoek gekeken wordt welke eisen er gesteld worden vanuit de NIS2, om dit mee te nemen in de keuze van de endpoint protection.

Deelvraag vier: Welke vormen van endpoint protection zijn er? (Deze deelvraag wordt beantwoord in hoofdstuk 4)

Er zal gekeken worden naar welke vormen van endpoint protection er zijn. Deze worden uitgewerkt en met elkaar vergeleken. Op deze manier kan een duidelijk beeld verkregen worden van de verschillende vormen van endpoint protection.

Deelvraag vijf: Welke producten zijn er voor de endpoint protection en wat zijn hier de voor- en nadelen van? (Deze deelvraag wordt beantwoord in hoofdstuk 5)

Er zijn verschillende producten om het beheren en het beheersen van endpoint protection efficiënter te maken, deze zullen vergeleken worden met elkaar. Ook zullen de voor- en nadelen van de verschillende producten met elkaar vergeleken worden om hieruit de beste software te kunnen bepalen.

Deelvraag zes: Welke vorm van endpoint protection past bij Bradon? (Deze deelvraag wordt beantwoord in hoofdstuk 5)

De verschillende soorten endpoint protection zullen vergeleken worden, om zo tot de beste oplossing voor Bradon te komen.

Deelvraag zeven: Hoe gaat het product worden geconfigureerd? (Deze deelvraag wordt beantwoord in hoofdstuk 5)

Het product dient geconfigureerd te worden, hier wordt onderzoek naar gedaan. Hierdoor wordt het duidelijk wat de mogelijkheden zijn voor het dashboard en de onderliggende verbindingen van deze onderdelen.

Deelvraag acht: Hoe kan endpoint protection aansluiten op de NIS2? (Deze deelvraag wordt beantwoord in hoofdstuk 6)

De endpoint protection oplossing zal moeten aansluiten op de NIS2. Hiermee wordt bedoeld dat de gekozen oplossing zal aansluiten op de bekende onderdelen van de NIS2 (zorg- en meldplicht).

1.6.3 Onderzoeksopzet

Hieronder zijn de verschillende deelvragen te zien en hoe deze uitgewerkt worden, in welke fase en welke output deze geven. Tijdens de interviews zal er gebruik gemaakt gaan worden van verschillende interview vormen (gestructureerd, semi gestructureerd en open). Voor de literatuur onderzoeken zal vooral gebruik gemaakt gaan worden van de databanken van google, hier staat het grootste deel van de informatie in die nodig zal zijn voor het onderzoek.

Deelvraag	Hoe	Fase	Output
1. Wat is de huidige situatie bij Bradon?	Interview	Huidige situatie	Duidelijk beeld van de huidige situatie
2. Welke eisen en wensen zijn er vanuit Bradon?	Interview	Behoefte analyse/ Context analyse	Requirements van de stakeholders
3. Welke eisen brengt de NIS2 mee?	Literatuuronderzoek, Google	Behoefte analyse/ Context analyse	Eisen vanuit de NIS2
4. Welke vormen van endpoint protection zijn er?	Literatuuronderzoek, Google	Literatuuronderzoek	Overzicht van de soorten endpoint protection
5. Welke producten zijn er voor de endpoint protection en wat zijn hier de voor- en nadelen van?	Literatuuronderzoek, Google	Conceptueel ontwerp	Duidelijk beeld van de verschillende producten en wat hier de voor- en nadelen van zijn
6. Welke vorm van endpoint protection past bij Bradon?	Literatuuronderzoek, Google	Conceptueel ontwerp	Een uiteindelijke keuze voor een endpoint protection oplossing en uitleg waarom deze gekozen is
7. Hoe gaat het product worden geconfigureerd?	Literatuuronderzoek, Google	Technisch ontwerp en verificatie	Technische uitwerking van de oplossing en hier uitleg over
8. Hoe kan endpoint protection aansluiten op de NIS2?	Literatuuronderzoek, Google	Advies	Advies over hoe de endpoint protection oplossing aansluit op de NIS2
Hoofdvraag: Hoe kan Bradon endpoint protection inrichten voor de endpoints bij haar klanten, zodat endpoint beheer als dienst kan worden aangeboden aan klanten en hoe kan Bradon de endpoint protection laten aansluiten op de NIS2?	Deskresearch	Advies	Advies voor het beleid en de softwaremogelijkheid

Tabel 2 Hoofd en deelvragen

2. Behoefteanalyse

In dit hoofdstuk wordt deelvraag twee beantwoord: Welke eisen en wensen zijn er vanuit Bradon? De behoefte van de stakeholder wordt hier in kaart gebracht. Op basis van de behoefte van de stakeholders zijn de requirements opgesteld.

2.1 Methodiek

In bijlage B zijn de perspectieven van de stakeholders te vinden. Deze perspectieven zijn meegenomen in het opstellen van de requirements in combinatie met verdere gesprekken die met de stakeholders zijn geweest. De requirements zijn gecategoriseerd en geprioriteerd volgens de methodieken die beschreven staan in bijlage B.

Voor het opstellen van de requirements is er gesproken met:

- Chief Executive Officer
- Senior engineer
- Backoffice
- Service delivery manager

Deze stakeholders zijn geïnterviewd door middel van een semigestructureerd interview. Dit houdt in dat er voorafgaand aan de interviews vragen zijn bedacht en deze gesteld zijn tijdens het interview. Hierbij ontstaat de mogelijkheid om door te vragen op de antwoorden van de stakeholders (Genau, 2023). Uit deze gesprekken is de eerste opzet van de requirements gekomen, deze is besproken met de stakeholders om ze te valideren en verdere aanpassingen door te voeren.

2.1.1 Business requirements

Nr.	Beschrijving	Prioriteit	Functioneel/ Niet-Functioneel	Genereert	Realiseert
B01	Bradon zal voldoen aan voorbereidende stappen voor de NIS2	M	Niet-functioneel	U08	X
B02	Bradon zal endpoint protection kunnen aanbieden aan haar klanten	M	Functioneel	U01 t/m U07, U09 t/m U13	X

Tabel 3 Business requirements

2.1.2 User Requirements

Nr.	Beschrijving	Prioriteit	Functioneel/ Niet-Functioneel	Genereert	Realiseert
U01	Senior engineer zal endpoints kunnen toevoegen	M	Functioneel	S04, S05,S08	B02
U02	Senior engineer zal werkstations kunnen overnemen	M	Functioneel	S04, S05,S08	B02
U03	Senior engineer zal endpoints kunnen verwijderen	M	Functioneel	S04, S05,S08	B02
U04	Senior engineer zal endpoints kunnen vergrendelen op afstand	M	Functioneel	S04, S05,S08	B02
U05	Senior engineer zal endpoints en/of files in quarantaine kunnen zetten	S	Functioneel	S04, S05,S08	B02
U06	Senior engineer zal endpoints realtime en on demand kunnen scannen op malware	S	Functioneel	S11	B02
U07	Senior engineer zal versies van back-ups kunnen beheren	C	Functioneel	S13	B02
U08	Senior engineer zal het toekomstige beleid kunnen uitvoeren	M	Functioneel	S10	B01
U09	Backoffice en Service delivery manager zullen een licentie overzicht hebben	S	Functioneel	S12	B02
U10	Senior engineer zal door middel van één inlog alle klanten in het portaal kunnen zien	M	Functioneel	S01, S02, S09	B02
U11	Beheerders zal veilig kunnen inloggen	M	Functioneel	S03,	B02
U12	Senior engineer zal updates kunnen testen in een veilige omgeving	S	Functioneel	S07	B02
U13	Beheerders zullen mails ontvangen	M	Functioneel	S06	B02

Tabel 4 User Requirements

2.1.3 System requirements

Nr.	Beschrijving	Prioriteit	Functioneel/ Niet-Functioneel	Genereert	Realiseert
S01	Het systeem zal benaderbaar zijn via de webbrowser	M	Functioneel	X	U10
S02	Het systeem zal een uptime van 99.9% hebben	S	Functioneel	X	U10
S03	Het systeem zal gebruik maken van Multi Factor Authentication	M	Functioneel	X	U11
S04	Het systeem zal toepasbaar zijn op de volgende operating systemen: Windows, MacOS en Linux	S	Functioneel	X	U01, U02, U03, U04, U05
S05	Het systeem zal toepasbaar zijn op de volgende mobiele operating systemen: IOS en Android	S	Functioneel	X	U01, U02, U03, U04, U05
S06	Het systeem zal mails kunnen genereren	S	Functioneel	X	U13
S07	Het system zal een sandbox hebben voor het testen van zero days	C	Functioneel	X	U12
S08	Het systeem zal werkstations kunnen beheren	M	Functioneel	X	U01, U02, U03, U04, U05
S09	Het systeem zal multi tenant ingericht zijn	S	Functioneel	X	U10
S10	Het systeem zal aan het nieuwe beleid voldoen	S	Functioneel	X	U08
S11	Het systeem zal scans kunnen uitvoeren	M	Functioneel	X	U06
S12	Het systeem zal overzichten kunnen genereren	M	Functioneel	X	U09
S13	Het systeem zal back-ups kunnen maken	C	Functioneel	X	U07

Tabel 5 System Requirements

3. Context analyse

In dit hoofdstuk is de contextanalyse uitgevoerd om randvoorwaarden op te stellen en om ervoor te zorgen dat de resultaten uit het onderzoek bruikbaar zijn voor Bradon en de klanten van Bradon.

3.1 Methodiek

Voor het opstellen van de randvoorwaarden is een contextanalyse uitgevoerd. Hierin is gekeken naar de omgeving waarin het resultaat van het onderzoek gebruikt gaan worden. Om de interne analyse van Bradon uit te voeren is het 7-S model van McKinsey (Benders, 2023) gebruikt. Het 7-S model is te vinden bij bijlage C. Er is gekozen voor het 7-S model van McKinsey, omdat hieruit een duidelijk beeld ontstaat van de diensten die Bradon levert en welke leveranciers Bradon heeft. Ook is er gekeken naar de externe factoren. Dit is gedaan om een totaalbeeld te krijgen van de omgeving.

3.2 Resultaten

Onderstaand zijn de resultaten van het 7-S model te zien.

3.2.1 Interne organisatie Bradon

Bradon levert verschillende diensten aan haar klanten. Deze diensten worden onderhouden door de 2e lijn medewerkers (senior engineers) binnen Bradon zelf en de 1e lijn medewerkers die Bradon inhuurt. De inkoop wordt gedaan door de backoffice medewerker en er worden maandelijks facturen aan de klanten verstuurd en betaald aan Bradon, zodat er een overzichtelijk beeld is van de uitgaven en inkomsten van Bradon. Het contact met de klanten wordt onderhouden door de CEO en de service delivery manager. Alle medewerkers binnen Bradon worden gelijk behandeld om zo geen verdeling binnen het bedrijf te krijgen (Bradon B.V., 2021).

Bradon maakt gebruik van een cloud-first strategie. Er zal onderzocht moeten worden welke oplossing voor endpoint protection binnen dit beleid zal vallen en gebruikt kan worden. Deze oplossing zal daarna aangeboden gaan worden aan Bradon haar klanten als een nieuwe dienst.

3.2.2 Externe organisatie Bradon

Klanten Bradon

Bradon haar klanten nemen diensten of producten af. Bradon heeft een groot aantal klanten die in verschillende branches werkzaam zijn. Bepaalde klanten hebben intern ICT-personeel in dienst. De klanten maken gebruik van diensten die Bradon aanbiedt. Andere klanten maken gebruik van de totale IT-dienstverlening die Bradon aanbiedt.

Leveranciers Bradon

Bradon levert verschillende soorten IT-dienstverleningen en heeft hier producten en diensten voor nodig. Deze koopt Bradon in bij verschillende leveranciers in Nederland. Bradon maakt gebruik van producten en diensten die haar leveranciers aanbieden en zullen hier eerst kijken als er iets nieuws aangeschaft moet worden. De leveranciers van Bradon zijn:

- TD synnex
- Microsoft
- Kaseya
- Liquit
- Synigo pulse
- Integra

Concurrenten Bradon

Bedrijven die in hetzelfde werkgebied zitten als Bradon, zijn concurrenten van Bradon. Het gaat om Managed Service Providers die tussen de 5 en 100 werkplekken aanbieden aan hun klanten en de andere bijhorende zaken.

3.2.3 NIS2

Een externe factor waaraan Bradon zal moeten voldoen is de NIS2. Dit is een regelgeving die eind 2024 in gaat. Bradon kan hiervoor al voorbereiden stappen nemen. De endpoint protection zal moeten aansluiten op de eisen van de NIS2.

3.3 Conclusie

Na het opstellen van de context analyse is er gekeken naar de randvoorwaarden. Deze geven aan waaraan de oplossing zal moeten voldoen om ingezet te kunnen worden bij Bradon. Door deze randvoorwaarden is er een duidelijk beeld van de absolute vereisten.

Code	Randvoorwaarden
R1	De oplossing dient als dienst aangeboden te kunnen worden
R2	De oplossing dient cloudbased te zijn
R3	Bradon heeft voorkeur om de oplossing af te nemen bij een van haar leveranciers
R4	De oplossing dient maandelijks te kunnen worden betaald

Tabel 6 Randvoorwaarden

4. Literatuuronderzoek

In dit hoofdstuk zal ik antwoord geven op deelvragen drie en vier: Welke eisen brengt de NIS2? En welke vormen van endpoint protection zijn er?

4.1 Methodes

In dit hoofdstuk zal er gebruik gemaakt worden van de sneeuwbal methode in combinatie met deskresearch om aan relevante literatuur te komen die een bijdrage zal leveren aan het beantwoorden van de onderzoeksvragen. Om de validiteit van verschillende onderdelen te waarborgen, worden hier bronnen bij vermeld.

4.2 Eisen NIS2

De Network and Information Security directive, ook wel de NIS2-richtlijn genoemd, is de opvolger van de NIS-richtlijn. Deze richtlijn is vastgesteld door de Europese Unie om de cyberbeveiliging van essentiële diensten binnen de EU-lidstaten te verbeteren.

De NIS2-richtlijn richt zich op verschillende sectoren en stuurt hier op risico's die netwerken en informatiesystemen bedreigen. De NIS2-richtlijn richt zich op nieuwe sectoren die bij de NIS-richtlijn nog niet van toepassing waren. De sector overheid valt nu ook onder de richtlijn en bevat een toelichting over welke specifieke overheidsinstanties hieronder vallen.

De NIS2-richtlijn schrijf de volgende verplichtingen voor:

- **Zorgplicht-** Een entiteit dient zelf een risicobeoordeling te doen. Hieruit dienen zij passende maatregelen te nemen om diensten zoveel mogelijk te waarborgen en de gebruikte informatie te beschermen
- **Meldplicht-** Een entiteit dient binnen 24 uur incidenten te melden bij een toezichthouder. Incidenten die de verlening van essentiële diensten kunnen verstoren dienen dan gemeld te worden. Als er een cyberincident is geweest dient deze ook gemeld te worden bij het Computer Security Incident Response Team (CSIRT). Dit team kan hulp en bijstand leveren indien dit nodig is. Er zijn verschillende factoren die een incident meldingswaardig maken, zoals het aantal personen wat geraakt is door het incident, de tijdsduur van het incident en de eventuele financiële gevolgen van het incident.
- **Toezicht-** Organisaties die onder de NIS2-richtlijn vallen zullen onder toezicht komen te staan. NIS2 schrijft dat een onafhankelijke toezichthouder geplaatst wordt op een bedrijf.

Organisaties dienen al te voldoen aan de bestaande kaders voor informatiebeveiliging van de overheid, zoals de Baseline Informatiebeveiliging Overheid (BIO). Dit is van belang ter voorbereideng op de NIS2-richtlijn.

4.3 Vormen van endpoint protection

Er zijn verschillende soorten beveiliging die je op de endpoints kan implementeren. Hieronder worden de elf meest effectieve mogelijkheden beschreven voor endpoint security.

4.3.1 Network Access Control

Met netwerktoegangscontrole wordt er geprobeerd ongeautoriseerde gebruikers en apparaten uit een netwerk te houden. Organisaties kunnen apparaten en gebruikers van buiten de organisatie toegang verlenen indien dit nodig is en deze weer weghalen. Apparaten kunnen gecontroleerd worden op naleving van beveiligingsregels die zijn opgesteld door een bedrijf.

Steeds meer bedrijven maken gebruiken van het toelaten van niet-zakelijke apparaten tot het bedrijfsnetwerk. Dit vergt dat deze bedrijven speciale aandacht besteden aan de netwerkbeveiliging en wie er toegang krijgt tot het netwerk. Hiervoor zijn verschillende tools beschikbaar (VMware Glossary, 2023).

4.3.2 Data Loss Prevention

Data Loss Prevention is het detecteren en voorkomen van datalekken of het vernietigen van gevoelige gegevens. Organisaties maken gebruik van Data Loss Prevention om hun gegevens te beveiligen, beschermen en om te voldoen aan regelgeving. Er zijn verschillende onderdelen voor een oplossing, endpoint protection is hier één van. Endpoint software kan informatieoverdracht tussen gebruikers, groepen gebruikers en externe partijen controleren. Het is ook mogelijk bij sommige endpoint software om gebruikers direct feedback te geven en hun verkeer te blokkeren (Murray, 2023).

4.3.3 Insider Threat Protection

Binnen een organisatie is er altijd het risico dat een huidige of voormalige werknemer kwaadwillende acties wil uitvoeren. Dit kan opzettelijk of onopzettelijk gebeuren en er kan gevaar ontstaan op de vertrouwelijkheid, beschikbaarheid en/of integriteit van bedrijfssystemen en gegevens (OpenText, z.d.). Daarom is het van belang om de endpoint protection goed in te richten, zodat de kans hierop verkleind wordt door apparaten te kunnen vergrendelen. Ook is het van belang om ervoor te zorgen dat de gevoelige data van het bedrijf niet te benaderen is door onbevoegden en duidelijk is wie hier wel toegang tot heeft.

4.3.4 Data Classification

Met data Classification wordt er gezorgd dat de gegevens die aanwezig zijn binnen een bedrijf gescheiden en georganiseerd worden. Deze worden onderverdeeld in relevante groepen op basis van hun kenmerken zoals gevoeligheidsniveau, de risico's die ze meebrengen en de regels die ze beschermen. Hierna moet het bedrijf juist omgaan met de rechten die worden gegeven over deze gegevens (Spirion, 2023).

4.3.5 URL Filtering

Met Uniform Resource Locator filtering kan er bepaald worden welke websites medewerkers van een bedrijf kunnen benaderen. Gebruikers hebben hierdoor geen toegang tot specifieke sites en kunnen ook geen gebruikmaken van bedrijfsbronnen die negatieve effecten hebben op het bedrijf (Fortinet, z.d.).

4.3.6 Browser Isolation

Met browserisolatie worden de surfactiviteiten van gebruikers op het internet gescheiden van het proces van het lokaal laden en weergeven van de webpagina's. Hierdoor worden gebruikers beschermd van gevaarlijke websites die malware en andere bedreigingen bevatten en isoleert het de gebruikers (Cloudflare, z.d.).

4.3.7 Cloud Perimeter Security

Cloud Perimeter Security binnen endpoints beschermt de cloud bronnen tegen apparaten en gebruikers die hier geen toegang tot hebben of horen te hebben. Er kan gebruik gemaakt worden van een cloud firewall om te bepalen welke mensen of apparaten toegang krijgen tot de cloud bronnen (Fortinet, 2021).

4.3.8 Endpoint Encryption

Endpoint encryption is een beveiligingsoplossing die zich op verschillende eindpunten van een bedrijf bevindt. Er wordt gebruik gemaakt van complexe versleutelingsalgoritmen om gegevens op verschillende eindpunten te beschermen.

Medewerkers maken tegenwoordig gebruik van meerdere apparaten en hebben hier toegang toe met hun befrijfsaccount. Het versleutelen van de gegevens op deze apparaten is een prioriteit (Spiceworks, 2022).

4.3.9 Sandboxing

Door middel van sandboxing gebruik je een geïsoleerde omgeving, ook wel de sandbox genoemd, om te testen. Binnen deze sandbox kan code uitgevoerd en geanalyseerd worden. Dit gebeurt in een geïsoleerde omgeving en hierdoor ontstaan er geen problemen voor de applicatie, het systeem en het platform waarop alles draaiende is. Met behulp van sandboxing kan een verdediging opgebouwd worden tegen een zero-day-bedreiging (Fortinet, z.d.).

4.3.10 Secure Email Gateways

Secure Email Gateways maakt gebruik van een handtekeninganalyse en machine learning om zo kwaadaardige e-mails te identificeren en te blokkeren voordat deze in de inbox van medewerkers kunnen belanden. Secure Email Gateways zijn van belang binnen een organisatie, omdat phishing een van de grootste cyberdreigingen is waarmee elke organisatie te maken kan krijgen (Cloudflare2, z.d.).

4.4 Siem

Security **I**nformation and **E**vent **M**anagement is een beveiligingsbeheersysteem waarmee bedrijven real-time gegevens over de beveiliging kunnen verzamelen, bewaren, analyseren en hierop reageren. Dit met als doel om potentiële cyberaanvallen inzichtelijk te maken en om de kans op schade te verkleinen.

SIEM systemen zijn ontwikkeld om een volledig beeld te geven van de beveiligingsstatus van een bedrijf of organisatie. Hierdoor kunnen dreigingen snel worden geïdentificeerd en kan er snel worden gereageerd. SIEM heeft drie kernfuncties: Logboekbeheer, gebeurteniscorrelatie en incidentbewaking en reactie.

- Logboekbeheer: SIEM tools verzamelen gegevens van diverse bronnen (Servers, Firewalls, Applicaties en Netwerkapparaten). Deze worden geanalyseerd om potentiële dreigingen te identificeren
- Gebeurteniscorrelatie: SIEM maakt gebruik van verschillende regels en algoritmen om de verzamelde gegevens te analyseren en hierin patronen te herkennen. De tool kan indien deze een patroon gevonden heeft automatische stappen uitvoeren indien deze nodig zijn
- Incidentbewaking en reactie: Het is natuurlijk ook belangrijk dat er een dashboard gegenereerd kan worden. Hierdoor hebben beveiligingsteams die de impact bepalen van een incident een overzicht (Networking4all, z.d.)

4.5 MDR

Managed **D**etection & **R**esponse houdt het detecteren van beveiligingsincidenten door een externe partij in. Hiervoor wordt specifieke software gebruikt door de externe partij, bijvoorbeeld Endpoint Detection & Response software. Hiermee worden de activiteiten op het bedrijfsnetwerk gemonitord en geanalyseerd, om zo op zoek te gaan naar aanwijzingen van mogelijke dreigingen. Indien er dreigingen zijn zullen er direct stappen worden ondernomen om incidenten te stoppen en te voorkomen voordat deze schade kunnen aanrichten. Door gebruik te maken van MDR kan een ondernemer zich richten op belangrijke onderdelen binnen zijn organisatie, zonder zich druk te moeten maken over de beveiliging van het netwerk (Eset, 2023, 4 juli).

4.6 XDR

Extended **D**etection and **R**esponse zorgt ervoor dat bedrijven inzicht krijgen in hun gegevens. Dit gaat om de gegevens van alle netwerken, clouds, endpoints en toepassingen terwijl analyses en automation worden toegepast. Hierdoor kunnen dreigingen geanalyseerd, geprioriteerd, opgespoord en hersteld worden. Hierdoor wordt er geprobeerd dataverlies en beveiligingslekken te voorkomen (Cisco, 2023, 13 februari).

4.7 EDR

Endpoint **D**etection and **R**esponse is een endpoint beveiliging oplossing die realtime monitoring doet en gegevens verzamelt van endpoints. EDR maakt gebruik van regels en geautomatiseerde response- en analysemogelijkheden. De primaire functies van EDR zijn:

- Het bewaken en verzamelen van activiteit gegevens van endpoints
- Het analyseren van deze gegevens om dreigingspatronen te identificeren
- Het automatisch kunnen reageren op bedreigingen en meldingen sturen naar de beheerders
- Analyse hulpmiddelen aanbieden om te zoeken naar verdachte activiteiten

4.8 Best Practices

Locate & Monitor all devices on a network

Om een goed beschermde IT omgeving te hebben, moeten bedrijven in kaart hebben hoeveel endpoints zij gebruiken. De eerste stap die ervoor zorgt dat de endpoint security goed op orde is, is het identificeren van alle apparaten op het netwerk. Hiermee kan een netwerk kaart gemaakt worden met alle endpoints die hierop aanwezig zijn, om zo een duidelijk beeld te hebben voor het IT-beheer team (Endpoint Security: 8 Best Practices |NinjaOne, 2023).

Secure endpoint access

Geautoriseerde gebruikers zijn de enige mensen die toegang moeten hebben tot de endpoints. Bedrijven kunnen hier twee stappen voor uitvoeren om te zorgen dat deze toegang veiliger gebeurt. De eerste stap is het gebruiken van wachtwoorden, verificatiecodes en andere authenticatiemethoden om ervoor te zorgen dat alleen de gewenste partijen met de juiste rechten toegang hebben tot de endpoints. De tweede stap is het bieden van trainingen aan medewerkers van het bedrijf, omdat een groot aantal datalekken komen door menselijke fouten (Endpoint Security: 8 Best Practices |NinjaOne, 2023).

Scan endpoints often using EDR

Endpoint detection en response is software die endpoints scant en informatie van deze endpoints verzamelt. Endpoint detection en response levert alerts, controleert gebruiker gedrag en reageert op aanvallen of bedreigingen (Endpoint Security: 8 Best Practices |NinjaOne, 2023).

Install all updates, patches and software

Endpoints die draaien op verouderdere versies van software, zijn kwetsbaar voor een aanval. Het is daarom van belang dat alle updates en patches zo snel mogelijk geïnstalleerd worden en dat er indien nodig nieuwe software geïnstalleerd wordt.

Veel bedrijven slagen er niet in om regelmatig updates te installeren of patchen. Dit omdat het veel tijd inneemt en vervelend werk is. Doormiddel van een geautomatiseerde patchtool kunnen deze problemen opgelost worden en zijn hierdoor de endpoints in de organisatie up-to-date en veilig (Endpoint Security: 8 Best Practices |NinjaOne, 2023).

Combine endpoint security with SIEM

Endpoints genereren logboeken met daarin verschillende data zoals user data, operating systems en security application events. Deze data zijn niet nuttig als deze maar blijft staan. Organisaties kunnen deze gegevens verwerken tot waardevolle en bruikbare informatie doormiddel van een security information en event management oplossing (SIEM) (Complete Guide to Endpoint Security: Solutions and best practices, 2023).

Agent IP adress restriction

Om ervoor te zorgen dat niet zomaar iedereen toegang heeft tot de agent browser, kan er een agent IP-adres restrictie worden toegevoegd. Dit houdt in dat dat het IP-adres van het huidige werkstation van de beheerder toegevoegd wordt aan de restricted IP list (Security best practices, z.d.).

Malware protection

Endpoint management tools werken met verschillende antivirusoplossingen om in één oogopslag een overzicht beschikbaar te stellen van de malwarebeschermingsstatus. De endpoint tool werkt samen met het besturingssysteem van de endpoints om zo gegevens te verzamelen waar dit niet mogelijk is. Het gaat om de gegevens “is het product actief” en “is het product up-to-date”. Hiermee kan een diagram van de antivirusstatus van de endpoints beschikbaar gesteld worden (Security best practices, z.d.).

Ransomware detections

Ransomware detection controleert de endpoints en de bestanden die hierop aanwezig zijn op ransomware met behulp van een gedragsanalyse. Indien het apparaat geïnfecteerd is, zal dit een waarschuwing genereren. Als er ransomware wordt gedetecteerd op een endpoint kan deze geïsoleerd worden en hierna kunnen eventuele ransomware processen gestopt worden om te voorkomen dat deze zich verspreiden over andere endpoints op het netwerk (Security best practices, z.d.).

Monitoring and Alerts

Doormiddel van monitoring en alerts worden er meldingen gemaakt indien er problemen zijn. Dit kunnen performance issues zijn, security threats of andere informatie over de endpoints (Sophos, z.d.).

Multi-Factor Authentication (MFA)

Multi-Factor Authentication zorgt ervoor dat de portal van het beheer van de endpoints beter beveiligd wordt. Hierdoor is de kans dat een persoon die geen toegang hoort te hebben maar dit wel probeert te krijgen lager (Sophos, z.d.).

Lost Device security

Het kan zijn dat een medewerker een endpoint ergens vergeet of dat deze gesloten wordt. Het is daarom van belang dat er een manier is om de informatie op de endpoints te kunnen wissen. Doormiddel van lost device security is dit mogelijk. Met lost device security is het ook mogelijk om data te vergrendelen, om deze indien de endpoint gevonden is te kunnen vrijgeven (Best practices for lost Device Security, z.d.).

5. Ontwerp

In dit hoofdstuk wordt antwoord gegeven op deelvragen vijf, zes en zeven: Welke producten zijn er voor de endpoint protection en wat zijn hier de voor- en nadelen van? Welke vorm van endpoints protection past bij Bradon? En Hoe gaat het product geconfigureerd worden?

5.1 Conceptueel ontwerp

In de onderstaande kopjes is het conceptueel ontwerp uitgewerkt.

5.1.1 Methodiek

Voor het opstellen van de use-case diagrammen is er gebruik gemaakt van de Unified Modeling Language (UML) modeleertaal (Lucidchart, z.d.). Er is gekozen voor deze modeleertaal, omdat hierdoor een duidelijk beeld ontstaat over de activiteiten waar de oplossing aan moet voldoen.

Stakeholders staan aan de linker kant en deze voeren verschillende activiteiten uit. Uit deze activiteiten kunnen doelen komen.

Best practices voor endpoint security zullen worden bekeken en er zal worden beschreven hoe deze best practices uitgewerkt zullen worden. De uitwerking van de best practices zijn in het technische ontwerp te vinden.

Om een beeld te krijgen wat de verschillende applicaties te bieden hebben zal er gebruik gemaakt worden van een longlist. Hierin worden de verschillende applicaties met elkaar vergeleken en beoordeeld door middel van de opgestelde eisen en wensen van de stakeholders.

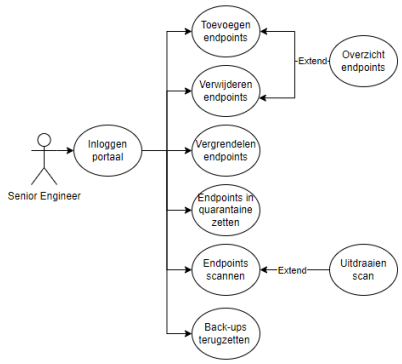
5.1.2 Use-case diagram

Om een goed beeld te krijgen van welke functies de actoren zullen uitvoeren, zijn deze in kaart gebracht door middel van een use-case diagram (Lucidchart, z.d.). Er zijn gesprekken gevoerd met de stakeholders waaruit requirements zijn ontstaan. De oplossing zal moeten voldoen aan deze requirements. Elke actor die functies zal gaan uitwerken in de nieuwe applicatie zal hier worden uitgewerkt.

5.1.2.1 Resultaten

Use-case diagram Senior engineer

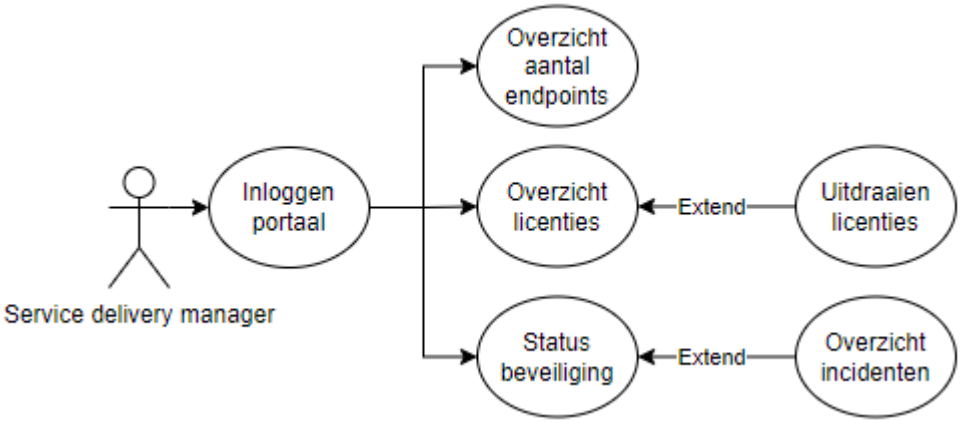
In figuur 2 is het use-case diagram te zien die de stappen van een senior engineer laat zien in de toekomstige oplossing. De activiteiten die de senior engineer zijn duidelijk en kort beschreven. Aan deze activiteiten zijn goals gekoppeld. Deze kunnen ontstaan uit de uitgevoerde stappen van de senior engineer.



Figuur 2 Use-case diagram Senior Engineer

Use-case diagram Service delivery manager

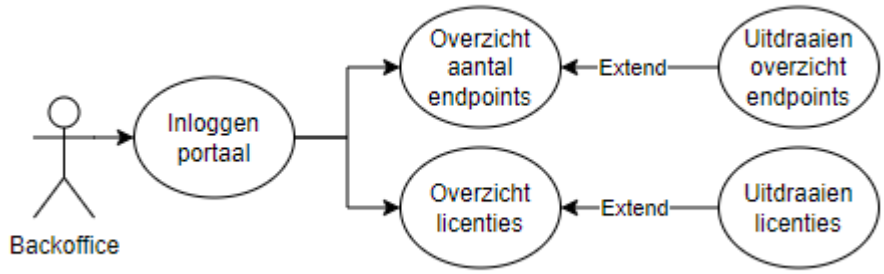
In figuur 3 is het use-case diagram te zien van de service delivery level manager. De service delivery level manager zal geen beheer taken doen met de toekomstige oplossing, maar zal overzichten willen inzien. Dit zijn overzichten zoals het aantal endpoints, de licenties op de endpoints, de status van deze endpoints en of er bedreigingen zijn gevonden bij een endpoint. Voor het bewust maken van klanten over eventuele problemen kunnen deze overzichten gebruikt worden. Er kan hierdoor een advies worden opgesteld en gegeven aan een klant indien er veel meldingen zijn om een training te volgen.



Figuur 3 Use-case diagram Service delivery manager

Use-case diagram Backoffice

In figuur 4 is het use-case diagram te zien van de backoffice. Net zoals de service delivery manager is het niet de bedoeling dat de backoffice beheer taken zal uitvoeren. Echter heeft de backoffice wel aangegeven dat er een overzicht aanwezig dient te zijn van de licenties, om dit door te kunnen communiceren met de klanten en om licenties voortijdig te kunnen bestellen indien nodig. Ook is het van belang om een overzicht te hebben van het aantal endpoints om deze te kunnen vergelijken met de licenties die in gebruik zijn.



Figuur 4 Use-case diagram Backoffice

5.1.3 Best Practices Endpoint Security

Er zijn verschillende best practices die gelden voor endpoint security. Deze zijn in het literatuuronderzoek onderzocht, om te kijken welke best practices Bradon kan gebruiken voor haarzelf en haar klanten. In de onderstaande tabel zijn deze best practices te zien en hoe deze gerealiseerd kunnen worden. Dit zal in het technisch ontwerp uitgewerkt worden.

Best practice	Hoe
Locate & Monitor all devices on a network	Doormiddel van een netwerk tekening op te stellen, wordt het mogelijk om alle endpoints binnen het netwerk in kaart te brengen
Secure endpoint access	De endpoint oplossing dient niet toegankelijk te zijn voor elke gebruiker, deze dient alleen benaderbaar te zijn door de senior engineers, de backoffice en de service delivery manager
Scan endpoints often using EDR	Het scannen van de endpoints levert informatie op over deze endpoints, deze moet zichtbaar zijn in een overzichtelijk dashboard
Install all updates, patches and software	Endpoints dienen up to date gehouden te worden. Doormiddel van automatisch updates en patches uit te voeren
Combine endpoint security with SIEM	Doormiddel van endpoints te koppelen met SIEM, krijg je een dashboard waarin alle informatie staat die anders niet gebruikt wordt
Agent IP adress restriction	Het is niet de bedoeling dat de endpoint oplossing overal ter wereld te benaderen is. Het is daarom van belang dat er een lijst komt met devices en IP-adressen waarvan de oplossing te benaderen is
Malware protection	Er dient in het dashboard van de endpoint oplossing een diagram zichtbaar te zijn waarin de status van de malware protectie beschikbaar is
Ransomware detections	Als er ransomware wordt gevonden op een endpoint moet deze in isolatie geplaatst worden. De endpoint oplossing moet hier de mogelijkheid voor bieden
Monitoring and Alerts	De endpoint oplossing dient meldingen weer te geven over onderdelen van een endpoint dat deze monitort zoals de status, update status en een diagram van de antivirus status
Multi-Factor Authentication (MFA)	De portal van de endpoint oplossing moet niet zonder extra beveiliging te benaderen zijn. Het is daarom van belang dat er gebruik gemaakt wordt van Multi-Factor Authentication
Lost Device security	Het kan gebeuren dat een endpoint verloren raakt of gestolen wordt. De endpoint oplossing moet een mogelijkheid bieden om deze te kunnen wissen of de data veilig te kunnen stellen indien het terug gevonden kan worden

Tabel 7 Best practice uitwerking

5.2 Multicriteria analyse

Om uiteindelijk tot een advies te komen voor een softwaremogelijkheid is er gebruikt gemaakt van een longlist en een shortlist. Hierin worden verschillende mogelijkheden met elkaar vergeleken op basis van de requirements. Allereerst zal er gebruik gemaakt gaan worden van een longlist, hierin worden meerdere mogelijkheden met elkaar afgewogen. Hierna zal er gebruik gemaakt gaan worden van een shortlist. Met behulp van deze shortlist zal er een endpoint software gekozen worden die het beste bij Bradon past. De “X” wordt gebruikt voor onderdelen die wel aanwezig zijn en de “/” voor onderdelen die niet aanwezig zijn.

5.2.1 Longlist User requirements

In tabel 8 worden de mogelijke opties voor de Endpoint protection software afgewogen tegenover de user requirements om zo tot een duidelijk beeld te komen waaraan deze opties voldoen.

Nr.	Beschrijving	Datto	Intune	Eset	Symantec	Heimdal	Bitdefender	Trellix	Trend Micro	Sentinal One
U01	Senior engineer zal endpoints kunnen toevoegen	X	X	X	X	X	X	X	X	X
U02	Senior engineer zal werkstations kunnen overnemen	X	X	X	X	X	X	X	X	X
U03	Senior engineer zal endpoints kunnen verwijderen	X	X	X	X	X	X	X	X	X
U04	Senior engineer zal endpoints kunnen vergrendelen op afstand	X	X	X	X	X	X	X	X	X
U05	Senior engineer zal endpoints en/of files in quarantaine kunnen zetten	X	X	X	X	X	X	X	X	X
U06	Senior engineer zal endpoints realtime en on demand kunnen scannen op malware	X	X	X	X	X	X	X	X	X
U07	Senior engineer zal versies van back-ups kunnen beheren	X	X	X	X	X	X	X	X	X

U09	Backoffice en Service delivery manager zullen een licentie overzicht hebben	X	X	X	X	X	X	X	X	X
U10	Senior engineer zal door middel van één inlog alle klanten in het portaal kunnen zien	X	X	X	X	X	X	X	X	X
U11	Beheerders zal veilig kunnen inloggen	X	X	X	X	X	X	X	X	X
U12	Senior engineer zal updates kunnen testen in een veilige omgeving	/	/	X	X	X	X	X	X	/
U13	Beheerders zullen mails ontvangen	X	X	X	X	X	X	X	X	X

Tabel 8 Longlist user requirements

5.2.2 Longlist System requirements

In tabel 9 worden de mogelijke opties voor de Endpoint protection software afgewogen tegenover de system requirements om zo tot een duidelijk beeld te komen waaraan deze opties voldoen.

Nr.	Beschrijving	Datto	Intune	Eset	Symantec	Heimdal	Bitdefender	Trellix	Trend Micro	Sentinal One
S01	Het systeem zal benaderbaar zijn via de webbrowser	X	X	X	X	X	X	X	X	X
S02	Het systeem zal een uptime van 99.9% hebben	X	X	X	X	/	/	/	/	X
S03	Het systeem zal gebruik maken van Multi Factor Authentication	X	X	X	X	X	X	X	X	X

S04	Het systeem zal toepasbaar zijn op de volgende operating systemen: Windows, MacOS en Linux	X	X	X	X	X	X	X	X	X
S05	Het systeem zal toepasbaar zijn op de volgende mobiele operating systemen: IOS en Android	/	X	X	X	X	X	X	X	X
S06	Het systeem zal mails kunnen genereren	X	X	X	X	X	X	X	X	X
S07	Het system zal een sandbox hebben voor het testen van zero days	/	/	X	X	X	X	X	X	/
S08	Het systeem zal werkstations kunnen beheren	X	X	X	X	X	X	X	X	X
S09	Het systeem zal multi tenant ingericht zijn	X	X	X	X	X	X	X	X	X
S10	Het systeem zal aan het nieuwe beleid voldoen	X	X	X	X	X	X	X	X	X
S11	Het systeem zal scans kunnen uitvoeren	X	X	X	X	X	X	X	X	X
S12	Het systeem zal overzichten kunnen genereren	X	X	X	X	X	X	X	X	X
S13	Het systeem zal back-ups kunnen maken	X	X	X	X	X	X	X	X	X

Tabel 9 Longlist System Requirements

5.2.3 Welke optie past bij Bradon?

Om de beste oplossing voor Bradon te vinden zullen er drie mogelijke oplossingen met elkaar vergeleken worden. Deze oplossingen zijn onderstaand te zien in de shortlist tabellen. Deze zullen met elkaar afgewogen worden om zo tot de beste oplossing voor Bradon te komen. Er is gekozen voor Datto, Intune en Trend micro. Dit is gedaan omdat Bradon al ervaring heeft met Datto en Intune en hier al kennis voor aanwezig is. Trend Micro is gekozen omdat dit een grote speler is en veel ervaring heeft.

5.2.3.1 Shortlist user requirements

Nr.	Beschrijving	Datto	Intune	Trend Micro
U01	Senior engineer zal endpoints kunnen toevoegen	X	X	X
U02	Senior engineer zal werkstations kunnen overnemen	X	X	X
U03	Senior engineer zal endpoints kunnen verwijderen	X	X	X
U04	Senior engineer zal endpoints kunnen vergrendelen op afstand	X	X	X
U05	Senior engineer zal endpoints en/of files in quarantaine kunnen zetten	X	X	X
U06	Senior engineer zal endpoints realtime en on demand kunnen scannen op malware	X	X	X
U07	Senior engineer zal versies van back-ups kunnen beheren	X	X	X
U09	Backoffice en Service delivery manager zullen een licentie overzicht hebben	X	X	X
U10	Senior engineer zal door middel van één inlog alle klanten in het portaal kunnen zien	X	X	X
U11	Beheerders zal veilig kunnen inloggen	X	X	X
U12	Senior engineer zal updates kunnen testen in een veilige omgeving	/	/	X
U13	Beheerders zullen mails ontvangen	X	X	X

Tabel 10 Shortlist user requirements

5.2.3.2 Shortlist system requirements

Nr.	Beschrijving	Datto	Intune	Eset
S01	Het systeem zal benaderbaar zijn via de webbrowser	X	X	X
S02	Het systeem zal een uptime van 99.9% hebben	X	X	/
S03	Het systeem zal gebruik maken van Multi Factor Authentication	X	X	X
S04	Het systeem zal toepasbaar zijn op de volgende operating systemen: Windows, MacOS en Linux	X	X	X
S05	Het systeem zal toepasbaar zijn op de volgende mobiele operating systemen: IOS en Android	/	X	X
S06	Het systeem zal mails kunnen genereren	X	X	X
S07	Het system zal een sandbox hebben voor het testen van zero days	/	/	X
S08	Het systeem zal werkstations kunnen beheren	X	X	X
S09	Het systeem zal multi tenant ingericht zijn	X	X	X
S10	Het systeem zal aan het nieuwe beleid voldoen	X	X	X
S11	Het systeem zal scans kunnen uitvoeren	X	X	X
S12	Het systeem zal overzichten kunnen genereren	X	X	X
S13	Het systeem zal back-ups kunnen maken	X	X	X

Tabel 11 Shortlist system requirements

5.2.4 Gekozen optie

Er zal uiteindelijk één mogelijkheid geadviseerd en getest worden. Dit zal Datto EDR zijn. Bradon maakt momenteel al gebruik van Datto RMM bij sommige klanten. Hierdoor is er kennis aanwezig over Datto. Verdere beredenering van de keuze voor Datto EDR is hieronder te lezen. In het adviesrapport zal verder advies worden gegeven over de keuze.

Bradon maakt gebruik van Autotask. Dit is een ticketsysteem waarin de tickets van klanten komen te staan en oudere tickets zichtbaar zijn. Datto en Autotask zijn van dezelfde developer (Kaseya). Datto en Autotask zijn hierdoor te integreren. De integratie van Autotask en Datto introduceert een uniform beheerdersplatform dat een goede oplossing is voor MSP's.

Door de integratie is het mogelijk om door middel van een "one-click workflow" te schakelen tussen Autotask en Datto RMM. Je kan via één klik van een ticket naar remote control, device agent browser en andere beheertools gaan. Verder kunnen gedetailleerde activiteitnotities worden toegevoegd aan het ticket na een ondersteuning op afstand sessie.

Eindgebruikers kunnen ondersteuning aanvragen via de agent die geïnstalleerd wordt. Hierdoor wordt er automatisch een ticket ingeschoten in Autotask. Waarschuwingen worden vervolgens toegewezen aan de juiste wachtrij. Waarschuwingen en activiteit informatie die gebruikt worden in tickets wordt dagelijks geüpdatet.

Door middel van de dashboards binnen Autotask zijn meldingen overzichtelijk te zien voor iedereen binnen Bradon. Hierdoor kunnen medewerkers sneller reageren op eventuele dreigingen dankzij de analyses van de endpoints.

5.3 Technisch Ontwerp

In de onderstaande kopjes worden de technische aspecten uitgewerkt.

5.3.1 Methodiek

Het technische ontwerp is opgesteld op basis van de gekozen endpoint protection oplossing. Dit hoofdstuk zal de oplossing beschrijven, de onderdelen die binnen Datto aanwezig zijn voor endpoint protection laten zien en de inrichting van het dashboard en hoe de onderliggende verbindingen zijn. Ook zal er gekeken worden naar het uitwerken van de best practices die in het conceptuele ontwerp zijn besproken.

5.3.2 System requirements

Onderstaande zijn nogmaals de system requirements te zien waaraan Datto zal moeten voldoen.

Nr.	Beschrijving
S01	Het systeem zal benaderbaar zijn via de webbrowser
S02	Het systeem zal een uptime van 99.9% hebben
S03	Het systeem zal gebruik maken van Multi Factor Authentication
S04	Het systeem zal toepasbaar zijn op de volgende operating systemen: Windows, MacOS en Linux
S05	Het systeem zal toepasbaar zijn op de volgende mobiele operating systemen: IOS en Android
S06	Het systeem zal mails kunnen genereren
S07	Het system zal een sandbox hebben voor het testen van zero days
S08	Het systeem zal werkstations kunnen beheren
S09	Het systeem zal multi tenant ingericht zijn
S11	Het systeem zal scans kunnen uitvoeren
S12	Het systeem zal overzichten kunnen genereren
S13	Het systeem zal back-ups kunnen maken

Tabel 12 System requirements

5.3.3 Keuze Datto RMM

Datto RMM is een EDR platform, dit houdt in dat er zonder dat de gebruiker hier iets van merkt de endpoints in de gaten worden gehouden. Beheerders kunnen op de achtergrond taken uitvoeren zonder dat de gebruikers van de endpoints dit merken.

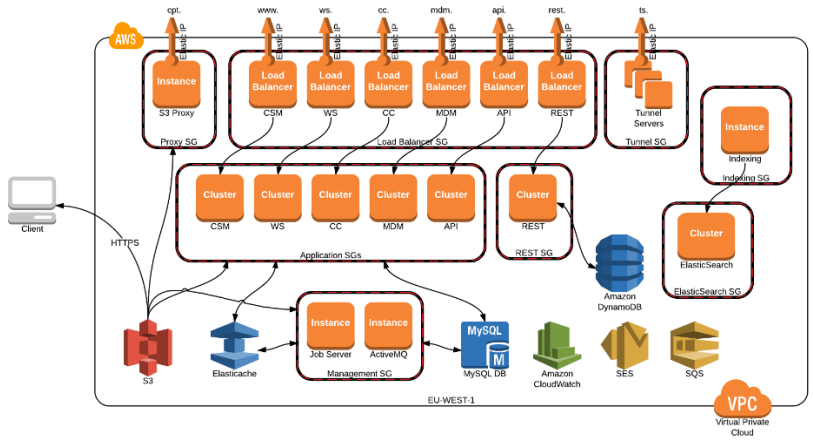
5.3.4 Technische uitwerking Datto endpoint protection

Datto wil als bedrijf ervoor zorgen dat Datto RMM de hoogste uptime **(S02)** heeft en heeft hier verschillende stappen voor genomen. Om het gewenste niveau van veerkracht en schaalbaarheid te halen verspreid Datto hun servers in vijf partnergerichte services. Deze services zijn:

1. Web interface
2. Control Channel
3. Web Service
4. Monitor Service
5. API

Verder maakt Datto gebruik van een aantal andere manieren om de kans op downtime te verminder. Zo wordt er gebruik gemaakt van verschillende availability zones, om indien er een failure is in een datacenter de beschikbaarheid van Datto RMM niet beïnvloed wordt. De services die bovenstaand zijn aangegeven worden loadbalanced, om er zo voor te zorgen dat er geen problemen ontstaan. Datto maakt gebruik van nog veel meer opties zoals firewalls, auto scaling en platform monitoring (Infrastructure and security, z.d.). Om ervoor te zorgen dat kwaadwillende niet zomaar binnen komen maakt Datto ook gebruik van Two-factor authentication **(S03).**

In figuur 5 is de Datto RMM AWS architectuur te zien. Hierin is te zien hoe Datto hun RMM-applicatie heeft draaien en wat de onderlinge connecties zijn (Infrastructure and security, z.d.).



Figuur 5 Datto RMM AWS architectuur

5.3.4.1 Installeren agents op de endpoints

Datto heeft verschillende manieren van het deployen van de agent. In tabel 13 zijn de verschillende manieren te zien. Per bedrijf kan het verschillen hoe de agent geïnstalleerd zal moeten worden.

Agent Deployment Method	Description
Vervangen van een andere RMM-software	Doormiddel van third-party tools kan de Datto agent gedeployed worden
Microsoft Azure AD Intune of Microsoft 365 endpoint manager	Agents kunnen door middel van Intune geïnstalleerd worden op endpoints met behulp van script
Active Directory GPO	De agent kan geïnstalleerd worden via Immediate scheduled task van Windows Active Directory domain.
Er is een endpoint binnen het netwerk met de endpoint geïnstalleerd	Als er op het netwerk een endpoint bevindt met de agent geïnstalleerd en de correcte rechten aanwezig zijn op het netwerk. Dan kan over het netwerk deze agent geïmplementeerd worden op endpoints die deze nog niet hebben
Er is geen endpoint binnen het netwerk met de endpoint geïnstalleerd	Indien er geen endpoint aanwezig is op het netwerk met hierop de agent geïnstalleerd, is het mogelijk om de agent via een e-mail te sturen als een file. Deze dient geïnstalleerd te worden op minimaal één endpoint binnen het netwerk.

Tabel 13 Agent installatie mogelijkheden

5.3.4.2 Dashboard inrichting

Datto heeft de mogelijkheid om meerdere soorten dashboards in te richten. De eerste optie is een leeg dashboard, deze kan ingedeeld worden met de beschikbare widgets uit de library. De tweede optie is het “default dashboard”, dit dashboard geeft informatie over de endpoints. De derde optie is het Datto EDR & Security dashboard, deze is alleen beschikbaar als de Datto EDR ingeschakeld is op het beheer account. In de onderstaande tabel zijn de verschillende dashboards informatief uitgewerkt (Dashboards, z.d.).

Type dashboard	Beschrijving	**Beschikbaarheid**	**Widgets**
Blank Dashboard	Begin met een leeg dashboard en voeg widgets toe vanuit de widgets bibliotheek voor toegang tot de gewenste data	Generaal	Geen
Default Dashboard	Een dashboard dat inzicht biedt in de endpoints	Generaal	• Offline Devices by Device type • Antivirus status • Windows Patch Status • Recent alerts • Alerts by priority
Datto EDR & Security Dashboard	Een beveiligingsdashboard dat waarschuwingen weergeeft zodat deze snel afgehandeld kunnen worden	Alleen beschikbaar als Datto EDR ingeschakeld is op het account	• Alerts by Category • Alerts Over Time • Security Threats • Datto EDR • Managed Windows Defender Status • Ransomware Status • Antivirus Status

Tabel 14 Dashboard mogelijkheden

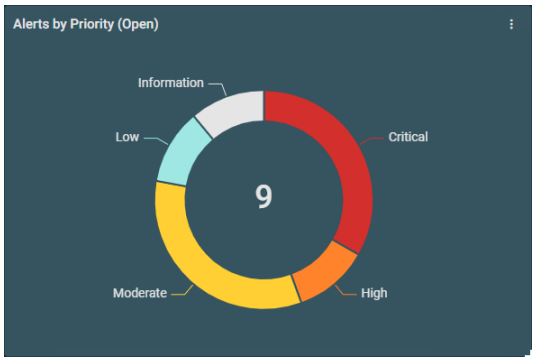
5.3.4.3 Dashboard uiterlijk en mogelijkheden

In figuur 6 is een voorbeeld dashboard te zien van Datto RMM. Hierin zijn verschillende widgets te zien die voor Bradon van pas komen, zoals de patch status van endpoints en de alerts over time. Het dashboard valt volledig zelf in te richten met de widgets die worden aangeboden door Datto.

Figuur 6 Dashboard Datto RMM

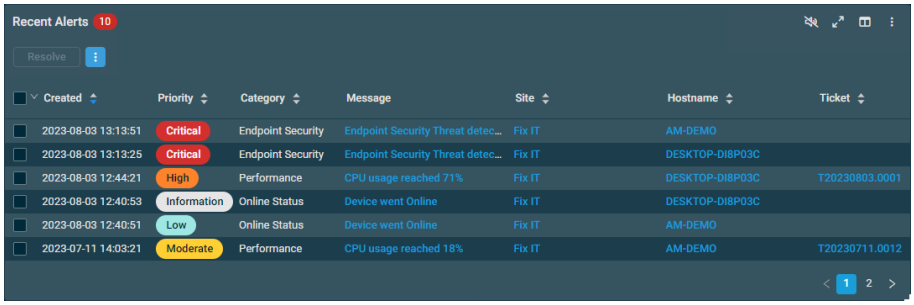
Zoals aangegeven levert Datto verschillende widgets die voor Bradon van toepassing kunnen zijn. Onderstaand zijn deze widgets te zien en wordt er beschreven wat deze widgets doen.

In figuur 7 is de widget “Alerts by priority” te zien. Hier worden alerts weergegeven van de laatste tijdperiode. Deze kan worden ingesteld door de beheerder.



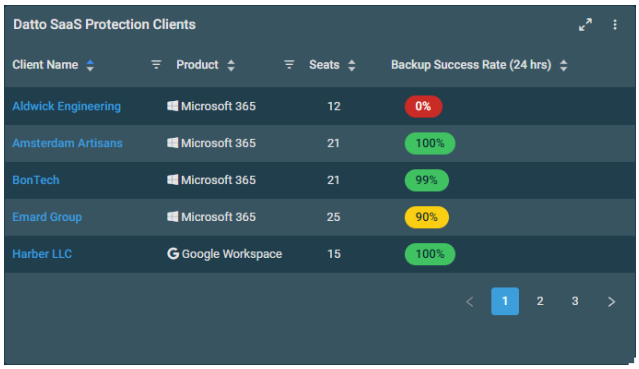
Figuur 7 Alerts by priority

In figuur 8 is de widget “Recent Alerts” te zien. Hier worden de alerts van de laatste 30 dagen weergegeven. Deze alerts kunnen geëxporteerd worden **(S12)**.



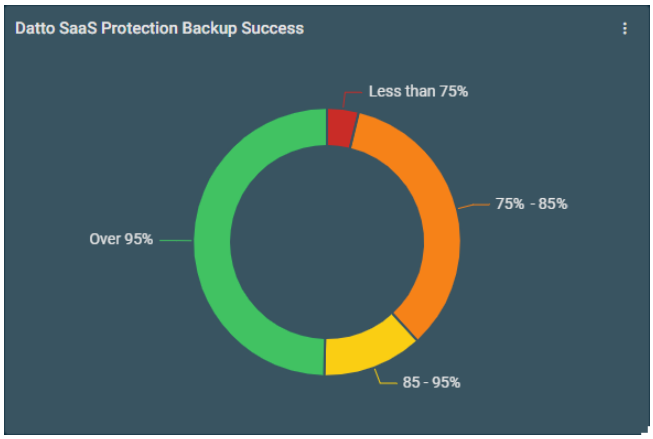
Figuur 8 Recent alerts

In figuur 9 is de widget “Datto SaaS Protection Clients” te zien. Hier is te zien van welke klanten en wat het back-up succespercentage is. **(S09 & S13)**



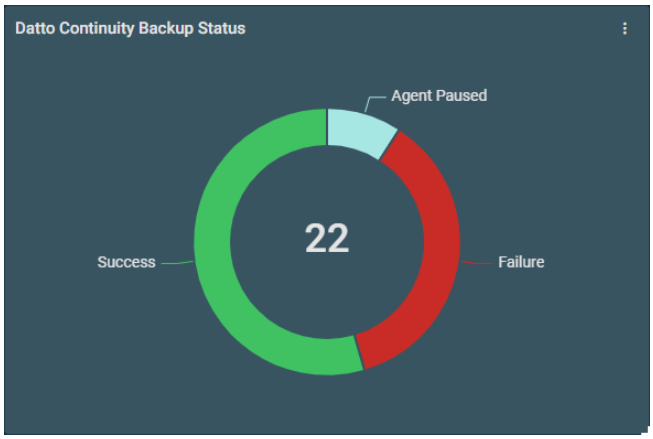
Figuur 9 Datto SaaS Protection Clients

In figuur 10 is de widget “Datto SaaS Protection Back-up Success” te zien. Hierin wordt net zoals in figuur 9 het succespercentage van de back-ups weergegeven. (**S13)**



Figuur 10 Datto SaaS Protection Back-up Success

In figuur 11 is de widget “Datto Continuity Back-up Status” te zien. Hierin worden alle endpoints weergegeven en hier de back-up status van. **(S13)**

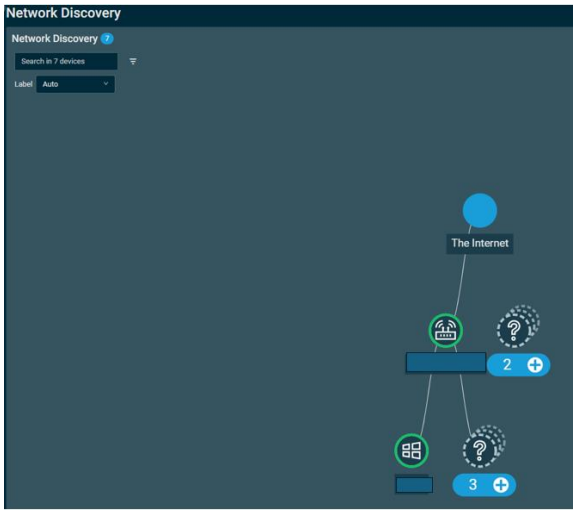


Figuur 11 Datto Continuity Back-Up Status

5.4 Best pracitces

Locate & Monitor all devices on a network

Binnen Datto is het mogelijk om een netwerk tekening te maken van de endpoints die hierop aanwezig zijn. Dit wordt gedaan door de network discovery tool. Hiermee worden allen endpoints die op dat moment aanwezig zijn op het netwerk in kaart gebracht. Hierdoor is het makkelijk om een overzicht te krijgen van de endpoints binnen een organisatie.



Figuur 12 Network discovery

Secure endpoint access

Doormiddel van accounts die worden aangemaakt door de administrator binnen Bradon, kunnen de senior engineer, backoffice en de service delivery manager toegang krijgen tot Datto. Hier kunnen zij met de rechten die zijn toegevoegd op hun account taken uitvoeren die bij hun titel horen.

Scan endpoints often using EDR

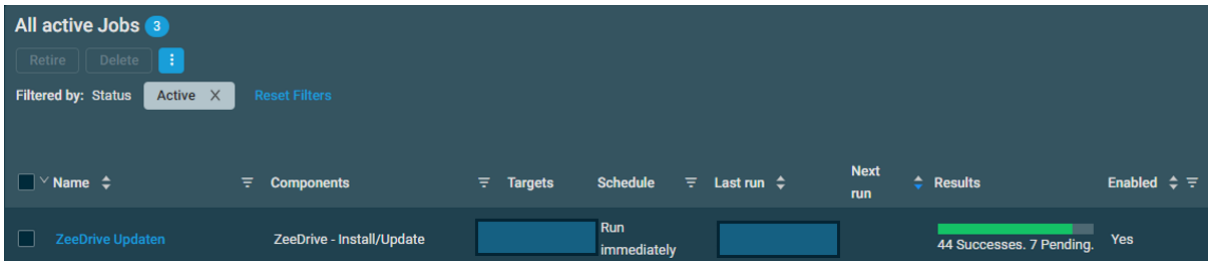
De endpoints moeten gescand kunnen worden om zo informatie te geven indien er problemen mee zijn. Het is mogelijk om een endpoint handmatig te scannen, deze zullen ook automatisch gemonitord worden op problemen.

Figuur 13 Antivirus scan

Figuur 14 Resultaat scan

Install all updates, patches and software

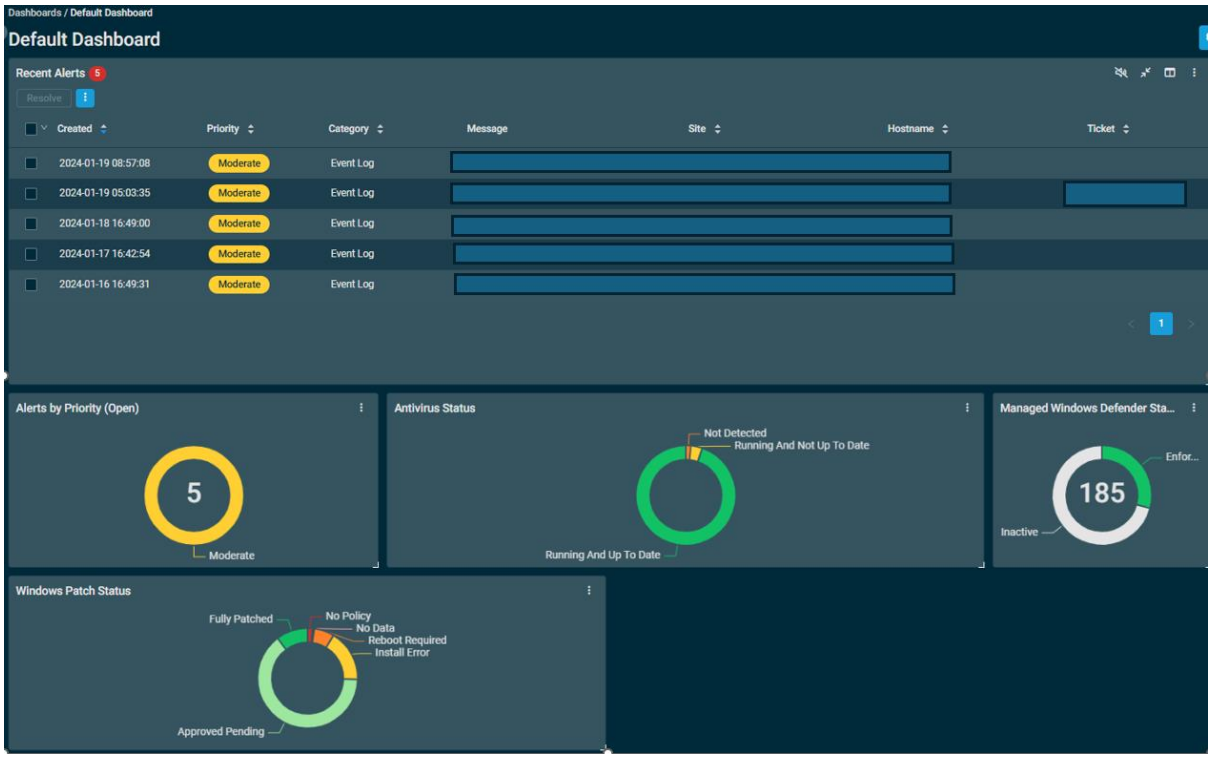
Om ervoor te zorgen dat endpoints up to date blijven met de laatste patches, kan er binnen Datto een policy worden gemaakt. Ook is het mogelijk om als software een patch heeft hier een job van te maken die op alle endpoints kan worden uitgerold, zoals hieronder te zien in figuur 15.



Figuur 15 Automatisch updaten van applicatie job

Combine endpoint security with SIEM

Endpoints leveren data aan Datto, doormiddel van een dashboard is deze data overzichtelijk te zien. Bradon beschikt hierdoor over alle data die van belang is en voorkom je dat er data niet gebruikt wordt die wel daadwerkelijk nuttig is voor Bradon. Vrijwel alle informatie van een endpoint is in het dashboard te configureren.



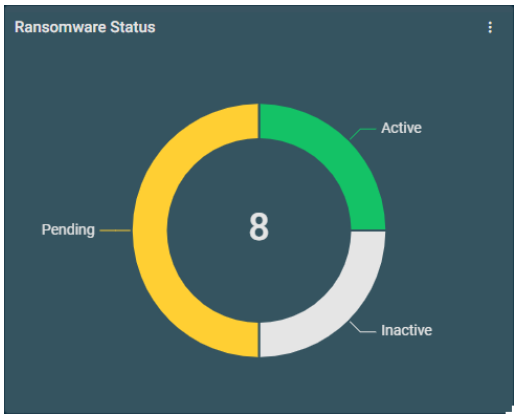
Figuur 16 Dashboard

Agent IP adress restriction

Binnen Datto is een functie om bepaalde IP-adressen toe te voegen aan een lijst, zodat deze toegang hebben tot de portal. Als je niet op deze lijst staat is het niet mogelijk om bij de portal te komen. Hierdoor kan je de portal beter beveiligen (Security best practices, z.d.).

Malware protection

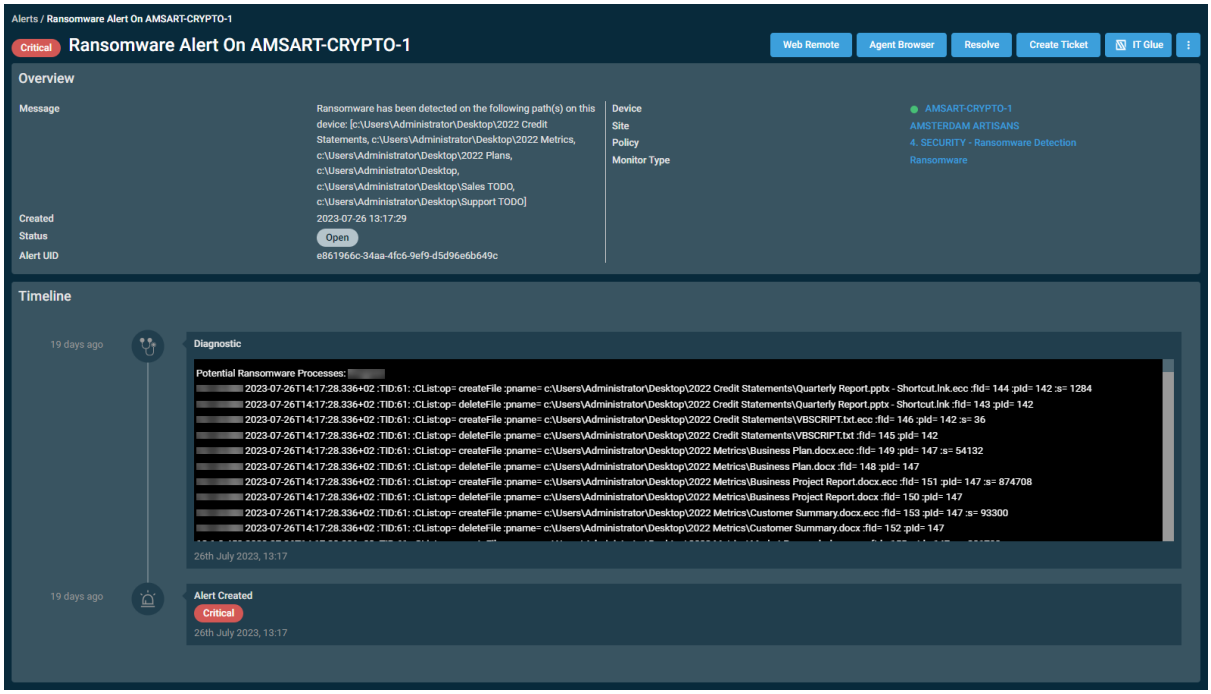
Datto maakt gebruik van verschillende antivirusoplossingen. Hierdoor is het mogelijk om op het dashboard een overzicht te krijgen van verschillende punten. Een hiervan is de ransomware status. Deze heeft verschillende mogelijkheden. Dit zijn active, inactive en pending. Active betekend dat er op de endpoint een monitor staat die data terugstuurt, inactive betekend dat er geen monitor op de endpoint staat en met pending is er een monitor aanwezig maar deze wacht op data van de agent op de endpoint.



Figuur 17 Overzicht met protected devices

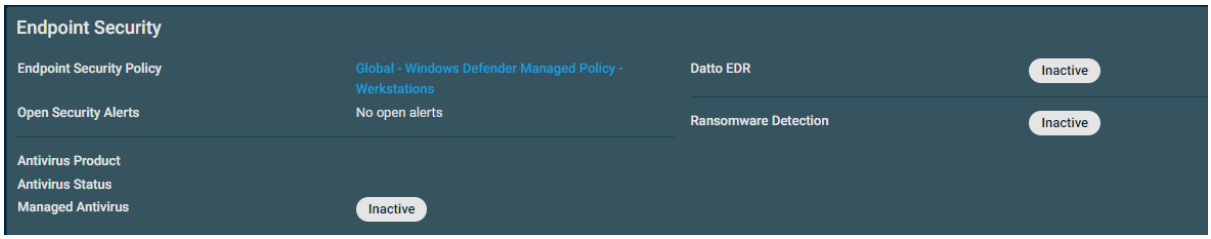
Ransomware detections

Datto kan automatisch endpoint in quarantaine zetten waar verdachte omstandigheden op aanwezig zijn. Deze endpoints hebben dan geen toegang meer tot het netwerk. Hierdoor verkleint de kans dat indien de verdachte omstandigheden echt zijn en er ransomware op het device staat, deze zich verspreid over het netwerk.



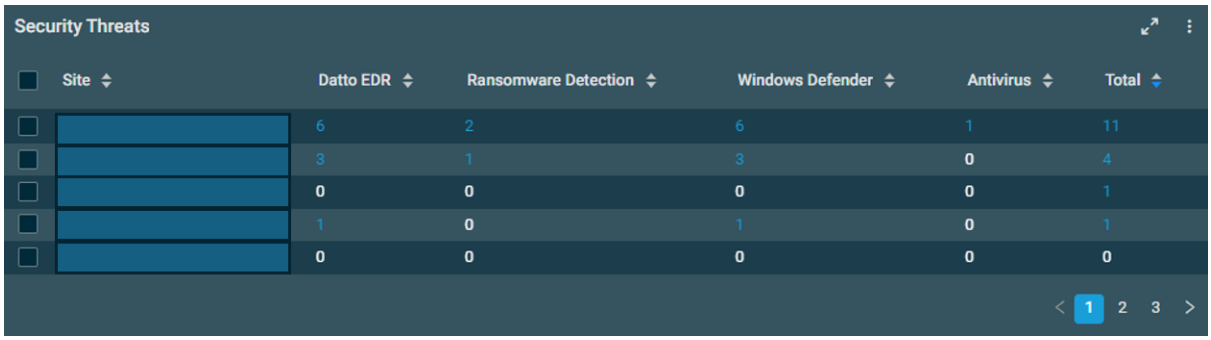
Figuur 18 Ransomware alert

Op de endpoints moeten dan wel de onderdelen actief zijn die in figuur 19 op inactive staan.



Figuur 19 Overzicht endpoint security

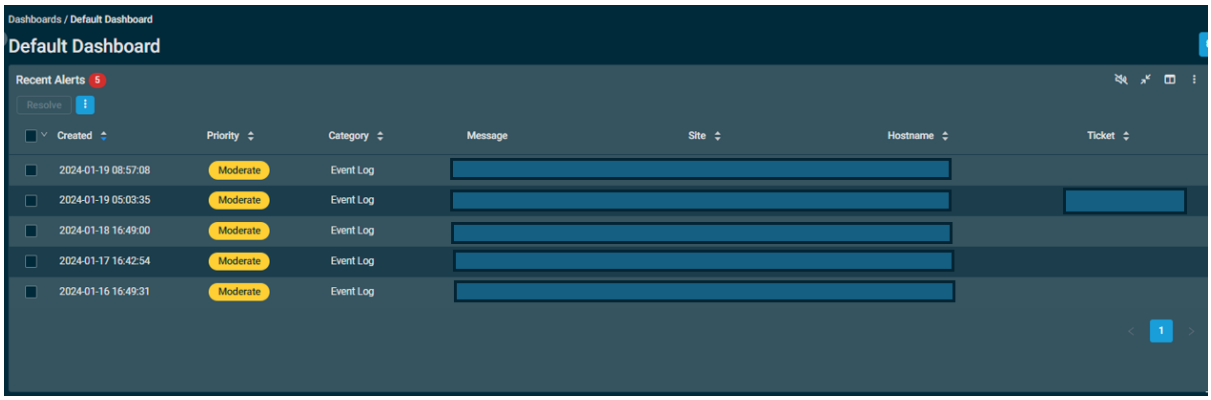
Per bedrijf is het mogelijk om een overzicht te krijgen van de security threats. Hierin is ook te zien waar deze threats onder vallen.



Figuur 20 Lijst van threats

Monitoring and Alerts

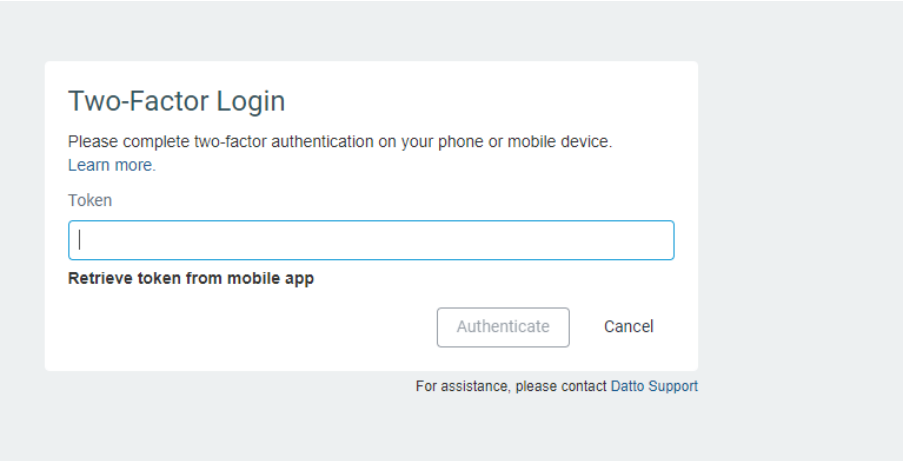
Binnen Datto kunnen er alerts worden gegenereerd. Deze zullen zichtbaar zijn in het dashboard. Elk alert kan een andere priority hebben en zal ook om een andere reden in de alert lijst staan. De alert kan gaan over hoog verbruik zijn van een pc tot een virus.



Figuur 21 Alerts van endpoints

Multi-Factor Authentication (MFA)

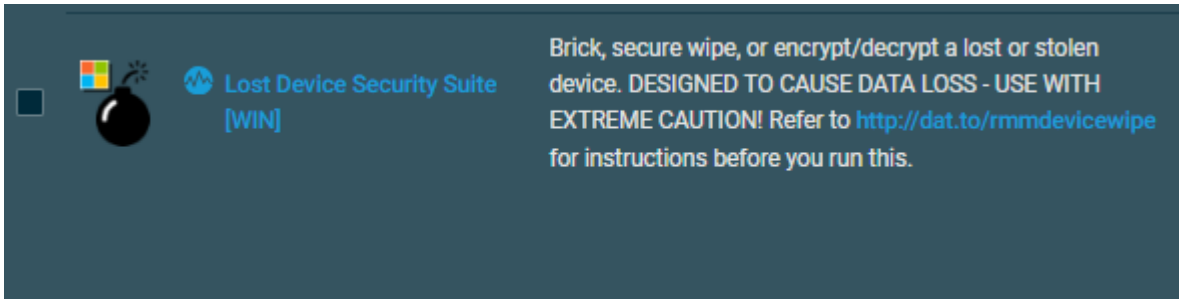
De eindgebruikers van de portal van Datto zullen niet zonder goede beveiliging in de portal mogen komen. Het is daarom van belang dat Multi-Factor Authentication wordt gebruikt. Hierdoor is er een extra beveiliging stap aanwezig om in de portal van Datto te komen.



Figuur 22 Multi-Factor Authentication (MFA)

Lost Device security

Endpoints die zijn gestolen of die kwijt zijn geraakt door een medewerker moeten gewist kunnen worden. Het is mogelijk om via Datto een component toe te voegen die dit mogelijk maakt. Voor Bradon is dit handig. Het kan namelijk zijn dat een van haar klanten een endpoint kwijt raakt en hierdoor kan Bradon voorkomen dat de data die op de endpoint staat misbruikt kan worden. Best practices for lost Device Security, z.d.)



Figuur 23 Mogelijkheden Lost Device

5.5 Testplan

Voor het gestructureerd kunnen testen wordt een testplan opgesteld waarin de aanpak wordt beschreven. Hierin zal worden beschreven wat de opdracht is, wie er mee te maken hebben en verantwoordelijk zijn, welke informatie er beschikbaar is welke testsoorten er gebruikt zullen worden en welke testen er uitgevoerd zullen worden en hoe de resultaten worden vastgelegd.

5.5.1 Methodiek

Voor het te opstellen van het testplan is gebruik gemaakt van de smarTEST van Valori (SmarTEST, z.d.). Niet alle onderdelen van de smarTEST zijn gebruikt, de onderdelen die in het testplan zijn beschreven zijn de bruikbare onderdelen voor de teststrategie. In het testplan worden de volgende onderdelen uitgewerkt: de opdracht en een korte beschrijving van de omgeving, welke testbasis er beschikbaar is en met welke testsoorten er getest zal worden. Verder wordt er gekeken naar de organisatie waarvoor de test uitgevoerd zal worden en in welke omgeving. Na het opstellen van het testplan is er duidelijk welke teststrategie en testen er uitgevoerd gaan worden. De resultaten van de uitgevoerde testen zijn te vinden in het testrapport.

5.5.2 Testopdracht

Onderstaand een korte beschrijving van het project en de betrokkenen.

5.5.2.1 Inleiding en korte projectbeschrijving

Bedrijven stappen steeds meer af van desktops en thin clients en gaan over op laptops om thuiswerken (beter) mogelijk te maken. Steeds meer bedrijven staan het concept “bring your own device” toe. Hierdoor wordt online thuiswerken aantrekkelijker voor zowel werkgevers als werknemers. Doordat er meer gebruik gemaakt wordt van laptops en er meer thuis wordt gewerkt is het belangrijk dat de endpoint protection goed in orde is. Het beheren en beheersen van de endpoint protection is ook zeer belangrijk. Vanuit de overheid worden er steeds meer eisen gesteld waaraan bedrijven moeten voldoen zoals de NIS2.

De opdracht houdt het onderzoeken en adviseren van de verschillende mogelijkheden van endpoint protection in en hieruit een endpoint protection oplossing adviseren. Tevens dient de endpoint oplossing te voldoen aan de gestelde eisen van de NIS2 die momenteel bekend zijn. Om het vraagstuk vanuit Bradon vast te stellen is een probleemanalyse uitgevoerd. Onderstaand wordt de methodiek besproken die gebruikt is bij het vaststellen van het vraagstuk. Het doel van de projectopdracht en probleemanalyse is door middel van de verschillende perspectieven de hoofd - en deelvragen te bepalen.

5.5.2.2 Opdrachtgever en opdrachtnemer

De opdrachtgever in dit project is Bradon, de opdracht nemer is de student.

5.5.2.3 Stakeholders en acceptanten

De stakeholder binnen dit project is Bradon en haar medewerkers. Binnen Bradon zijn de stakeholders de senior engineers, backoffice, service delivery manager en de Chief Executive Officer. Zij hebben de wens uitgebracht om onderzoek te doen naar welke endpoint protection het beste bij Bradon past.

5.5.2.4 Testopdracht

De test houdt het controleren van de opgestelde requirements in. Deze requirements zijn beschreven in de behoefte analyse. De system requirements zullen worden getest en uitgewerkt in bijlage D. Dit wordt gedaan omdat de system requirements aansluiten op de user requirements

5.5.3 Test basis

De testen zullen worden uitgevoerd met behulp van requirements die eerder zijn opgesteld in dit project.

5.5.3.1 Wat is er beschikbaar?

Document naam	Versie	Auteur	Korte toelichting
Plan van aanpak	1.0	Sem Vreeman	Hierin wordt het project kort beschreven.
Scriptie	1.0 Eindversie	Sem Vreeman	Hierin staat alle informatie over het project die gebruikt kan worden voor het testen

Tabel 15 Beschikbare documenten

5.5.3.2 Review aanpak

Alle gemaakte onderdelen van het project worden gecontroleerd door de maker zelf, ook wordt er feedback gevraagd van de stagebegeleider vanuit Bradon en stagebegeleider vanuit school. Hierdoor wordt er op verschillende manieren gekeken naar het opgeleverde werk.

5.5.4 Test strategie

De afspraken die gemaakt zijn tijdens dit project zijn als volgt:

De opgestelde requirements zullen getest worden in Datto. De resultaten van deze testen zullen worden verwerkt in het testrapport en in de bijhorende bijlage. In deze bijlage staan de testresultaten. Deze gegevens samen zijn het proof of concept en geven een overzicht over of de gestelde eisen daadwerkelijk gehaald zijn.

5.5.4.1 Keuze van de testsoorten

UT (Unittest)

De UT test of het proof of concept voldoet aan de gestelde eisen. Dit wordt gedaan door de projectuitvoerder. Er zal worden gekeken of Datto werkt zoals gewenst.

ST (Systeemtest)

Doormiddel van deze test wordt er getest of het gemaakte systeem daadwerkelijk functioneert zoals gesteld in de requirements. Hierdoor worden de systeem eigenschappen getest die zijn opgesteld in de system requirements.

SIT (Systeemintegratietest)

Doormiddel van deze test zal er getest worden of het beheren van endpoints, het uitdraaien van lijsten en andere gewenste onderdelen binnen Datto mogelijk is.

FAT (Functionele acceptatietest)

De FAT zorgt ervoor dat de functionaliteiten die gewenst zijn vanuit Bradon getest worden, zodat er vast gesteld kan worden of de deze mogelijk zijn.

5.5.5 Test organisatie

De testen zijn uitgevoerd op de testomgeving die binnen Bradon draait.

5.5.5.1 Rollen & taken

De volgende medewerkers zijn betrokken bij het opstellen, uitvoeren en ondersteunen bij van deze test.

Naam	Rol	Beschrijving
Ronald Letema	Opdrachtgever	Opdrachtgever van het project
Ernst Bakker	Stagebegeleider	Adviseert waar nodig en geeft feedback
Sem Vreeman	Stagiair/Opdracht uitvoerder	Verantwoordelijk voor de uitvoering van het project

Tabel 16 Rollen & Taken

5.5.5.2 Communicatie

Onderstaand zijn de afspraken te zien die van toepassing zijn op dit project.

Doel communicatie	Vorm	Frequentie	Contactpersonen
Voortgang bewaking met opdrachtgever	Mondeling overleg	Wekelijks	Ernst Bakker
Voortgang bewaking met school	Online vergadering	Maandelijks	Steven van der Linden

Tabel 17 Communicatie

5.5.6 Testproducten

Het testen van de system requirements zal verschillende resultaten opleveren. Deze zullen in de onderstaande paragrafen worden uitgewerkt.

5.5.6.1 Project documentatie

Tijdens het project zijn de volgende testproducten van belang.

- Testplan
- Proof of concept doormiddel van testrapport

5.5.6.2 Testware

De uitgevoerde testen zullen met hun resultaten worden vermeld in het testrapport, deze dient opgeleverd te worden als bewijsstuk voor de uitgevoerde testen is tevens het proof of concept. Deze is na het project nog van belang.

5.5.7 Testinfrastructuur

De testen zullen in een bepaalde infrastructuur worden uitgevoerd. Deze is onderstaand beschreven.

5.5.7.1 Testomgeving

De testomgeving zal binnen Datto gebeuren. Datto wordt momenteel gebruikt door Bradon als een beheer portaal van endpoints voor bepaalde klanten, de licentie van Datto RMM is hier niet op actief. Gewenste testen kunnen wel worden uitgevoerd.

5.5.7.2 Testtools

Doel	Tooling
Testen endpoint applicatie	Datto

Tabel 18 Beschikbare testtools

5.5.8 Beheer

De testresultaten van de uitgevoerde testen dienen opgeslagen en uitgewerkt te worden. Onderstaand wordt uitgelegd hoe dit gedaan zal worden.

5.5.8.1 Opslaglocaties, versie & configuratiebeheer

De testomgeving zal zich bevinden binnen de Datto omgeving van Bradon. Het testplan zal beschikbaar zijn in de OneDrive van de projectuitvoerende student.

5.5.8.2 Bevindingenbeheer

Bevindingen tijdens het testen zullen genoteerd worden in het testrapport. Hierdoor is er een duidelijk overzicht van de uitgevoerde testen en hiervan de resultaten. Er zal worden gekeken welke requirements gefaald is en hierbij wordt uitleg gegeven en een mogelijke oplossing of alternatief.

5.5.8.3 Overdracht testware

De Datto omgeving zal niet worden leeggemaakt, omdat de Datto omgeving van Bradon is. Hier zal alleen het testmateriaal uit gehaald worden. Het testplan en testrapport zullen opgeleverd worden aan Bradon.

5.5.9 Planning en resourcing

In tabel 19 zijn de system en user requirements te zien die getest zullen worden, waar deze testen aan moeten voldoen om te slagen, welke datum de testen zijn uitgevoerd en de geschatte tijd per test. System requirement 10 (Het systeem zal aan het nieuwe beleid voldoen) is niet meegenomen in de test. Deze requirement houdt in dat het moet voldoen aan de gestelde eisen van de NIS2 (meldplicht en zorgplicht), dit is niet testbaar. Er zijn een aantal user requirements getest die niet onder een system requirements vielen of een andere functie beschreven. Deze zijn in tabel 20 te zien en in het testrapport.

Nr.	Belang	Beschrijving	Moet voldoen aan	Datum test	Geschatte tijd
U01	4	Senior engineer zal endpoints kunnen toevoegen	Endpoints moeten toegevoegd kunnen worden	19-1-2024	5 Minuten
U02	4	Senior engineer zal werkstations kunnen overnemen	De senior engineer zal endpoints kunnen overnemen	19-1-2024	5 Minuten
U03	4	Senior engineer zal endpoints kunnen verwijderen	De endpoints moeten verwijdert kunnen worden	19-1-2024	5 Minuten
U04	4	Senior engineer zal endpoints kunnen vergrendelen op afstand	De endpoints moeten op afstand vergrendeld kunnen worden	19-1-2024	10 Minuten
U05	3	Senior engineer zal endpoints en/of files in quarantaine kunnen zetten	Endpoints dienen in quarantaine gezet te kunnen worden	19-1-2024	20 Minuten
S01	4	Het systeem zal benaderbaar zijn via de webbrowser	De oplossing moet toegankelijk zijn via de webbrowser	15-1-2024	5 Minuten
S02	3	Het systeem zal een uptime van 99.9% hebben	Een gemiddelde uptime van 99.9%	15-1-2024	5 Minuten

S03	4	Het systeem zal gebruik maken van Multi Factor Authentication	Multi factor authentication is van toepassing bij het inloggen	15-1-2024	5 Minuten
S04	3	Het systeem zal toepasbaar zijn op de volgende operating systemen: Windows, MacOS en Linux.	De oplossing dient toegepast te zijn op een endpoint	15-1-2024	30 Minuten
S05	3	Het systeem zal toepasbaar zijn op de volgende mobiele operating systemen: IOS en Android	Endpoints met IOS en Android dienen toegevoegd te zijn	16-1-2024	10 Minuten
S06	3	Het systeem zal mails kunnen genereren	Meldingen dienen via mail verstuurd te worden	15-1-2024	10 Minuten
S07	2	Het system zal een sandbox hebben voor het testen van zero days	Een sandbox omgeving dient beschikbaar te zijn	16-1-2024	10 Minuten
S08	4	Het systeem zal werkstations kunnen beheren	Endpoints kunnen toegevoegd, verwijdert, bekeken, overgenomen, etc. worden	15-1-2024	20 Minuten
S09	3	Het systeem zal multi tenant ingericht zijn	Verschillende klanten zijn zichtbaar in de oplossing	15-1-2024	10 Minuten
S11	4	Het systeem zal scans kunnen uitvoeren	De endpoints kunnen gescand worden	15-1-2024	15 Minuten
S12	4	Het systeem zal overzichten kunnen genereren	De oplossing zal overzichten kunnen genereren	15-1-2024	15 Minuten
S13	2	Het systeem zal back-ups kunnen maken	De oplossing kan back-ups maken	16-1-2024	10 Minuten

Tabel 19 Planning testen

5.6 Testrapport

In dit hoofdstuk zullen de resultaten worden beschreven van de uitgevoerde testen, welke omgeving er gebruikt gaat worden en vervolgens wat de resultaten van de uitgevoerde testen zijn met hier een koppeling aan het proof of concept.

5.6.1 Methodiek

Voor het testen is een versimpelde versie van de SmarTEST gebruikt. Deze methodiek gaat ervan uit dat de uitgevoerde testen zullen voldoen aan de opgestelde requirements en dit ook de acceptatiecriteria zijn. Aan elke requirement zit een belang gekoppeld, dit belang is gebaseerd op het soort requirement dat het is. Deze belangen zijn:

- Must have requirement: 4 punten
- Should have requirement: 3 punten
- Could have requirement: 2 punten
- Wont have requirement: 1 punt

Om een advies te kunnen geven over Datto, gaan de requirements getest worden. De omgeving wordt in het kopje testomgeving beschreven. In bijlage D zullen deze requirements worden weergegeven door middel van een proof of concept.

5.6.2 Testomgeving

Voor het testen van Datto zal er in de portal van deze optie de gestelde requirements worden uitgevoerd. Dit is een portaal dat al gebruikt wordt door Bradon maar niet voor de endpoint protection doeleinden. Hierin kunnen onderdelen die gewenst zijn bij de endpoint protection worden gebruikt en weergegeven om zo goed te testen wat de mogelijkheden zijn.

5.6.3 Testresultaten requirements

In tabel 20 zijn de requirements te zien en de resultaten van de testen. De testen zijn uitgevoerd in de omgeving die bovenstaand is beschreven.

Nr.	Belang	Beschrijving	Hoe getest	Resultaat
U01	4	Senior engineer zal endpoints kunnen toevoegen	Endpoints zijn toegevoegd	Geslaagd
U02	4	Senior engineer zal werkstations kunnen overnemen	Endpoint via agentbrowser benaderd	Geslaagd
U03	4	Senior engineer zal endpoints kunnen verwijderen	Endpoint verwijdert	Geslaagd
U04	4	Senior engineer zal endpoints kunnen vergrendelen op afstand	De Datto databank bekeken	Gefaald
U05	3	Senior engineer zal endpoints en/of files in quarantaine kunnen zetten	De Datto databank bekeken	Gefaald
S01	4	Het systeem zal benaderbaar zijn via de webbrowser	Inloggen via verschillende browsers	Geslaagd
S02	3	Het systeem zal een uptime van 99.9% hebben	Datto hun informatie over de uptime bekeken	Geslaagd
S03	4	Het systeem zal gebruik maken van Multi Factor Authentication	Inloggen met behulp van Multi Factor Authentication	Geslaagd

S04	3	Het systeem zal toepasbaar zijn op de volgende operating systemen: Windows, MacOS en Linux.	Agent geïnstalleerd op endpoint	Geslaagd
S05	3	Het systeem zal toepasbaar zijn op de volgende mobiele operating systemen: IOS en Android	Tablet en telefoon toevoegen aan Datto	Gefaald
S06	3	Het systeem zal mails kunnen genereren	Instellen dat een melding een mail kan genereren	Geslaagd
S07	2	Het system zal een sandbox hebben voor het testen van zero days	Het testen van een sandbox	Gefaald
S08	4	Het systeem zal werkstations kunnen beheren	Werkstations toevoegen verwijderen, overnemen en scannen	Geslaagd
S09	3	Het systeem zal multi tenant ingericht zijn	Verschillende klanten zijn zichtbaar in de oplossing	Geslaagd
S11	4	Het systeem zal scans kunnen uitvoeren	Er is een test scan gedraaid op een endpoint	Geslaagd
S12	4	Het systeem zal overzichten kunnen genereren	Een overzicht is gegenereerd	Geslaagd
S13	2	Het systeem zal back-ups kunnen maken	Databank van Datto bekeken	Gefaald

Tabel 20 System requirements resultaten

5.6.4 Bevindingen

Er zijn een aantal testen gefaald om verschillende redenen, deze zullen worden beschreven. Er zal ook gekeken worden naar alternatieven of mogelijkheden indien deze er zijn.

Nr.	Beschrijving	Resultaat	Alternatief/Mogelijkheden
U04	Senior engineer zal endpoints kunnen vergrendelen op afstand	Gefaald: omdat er geen mogelijkheid is om een endpoint op afstand te vergrendelen	Er is een component aanwezig die het mogelijk maakt om endpoint te wissen, data te vergrendelen en de endpoint niet bruikbaar te maken
U05	Senior engineer zal endpoints en/of files in quarantaine kunnen zetten	Gefaald: senior engineer kan niet handmatig een endpoint in quarantaine zetten	Datto EDR kan zelf endpoints in quarantaine zetten als er verdachte omstandigheden zijn
S05	Het systeem zal toepasbaar zijn op de volgende mobiele operating systemen: IOS en Android	Gefaald: Het is niet mogelijk op endpoints met IOS of Android toe te voegen aan Datto	Er is hiervoor binnen Datto geen alternatief of andere mogelijkheid. Als dit gewenst is bij een klant zal dit in een andere tool geregeld moeten worden

S07	Het system zal een sandbox hebben voor het testen van zero days	Gefaald: Er is geen mogelijkheid om zero days te testen. Hiervoor is geen sandbox aanwezig binnen Datto	Er is geen alternatief of mogelijkheid binnen Datto. Hiervoor zal naar een andere optie gekeken moeten worden
S13	Het systeem zal back-ups kunnen maken	Gefaald: Er kunnen geen back-ups gemaakt worden	Binnen Datto is het mogelijk om met de juiste licentie structuur back-ups te maken. Er zal dus een licentie aangeschaft moeten worden als deze functie gewenst is

Tabel 21 Bevindingen

5.6.5 Randvoorwaarden

In het begin van het project zijn er randvoorwaarden opgesteld. Deze zijn te zien in de onderstaande tabel. Deze randvoorwaarden zijn niet getest zoals de requirements zijn getest. Echter zal er beschreven worden per randvoorwaarde of Datto hieraan voldoet.

Code	Randvoorwaarden
R1	De oplossing dient als dienst aangeboden te kunnen worden
R2	De oplossing dient cloudbased te zijn
R3	Bradon heeft voorkeur om de oplossing af te nemen bij een van haar leveranciers
R4	De oplossing dient maandelijks te kunnen worden betaald

Tabel 22 Randvoorwaarden

R1: De oplossing dient als dienst aangeboden te kunnen worden

Als Bradon Datto EDR zal gaan gebruiken is dit ook als dienst aan te bieden. Bradon kan met oude en nieuwe klanten bespreken of zij interesse hebben in deze dienst. Voor Bradon is het een belangrijke mogelijkheid, omdat het ervoor zorgt dat zij al voorbereidende stappen nemen voor de NIS2. Datto EDR voldoet aan de randvoorwaarde.

R2: De oplossing dient cloudbased te zijn

Datto EDR is cloud based. Bradon maakt gebruik van een cloud first strategie. Hierdoor past Datto EDR in hun beleid. Datto EDR voldoet aan de randvoorwaarde.

R3: Bradon heeft voorkeur om de oplossing af te nemen bij een van haar leveranciers

Bradon neemt momenteel Datto af bij hun leverancier “Kaseya”. Dit is de maker van Datto en Autotask. Hierdoor zal het afnemen van Datto EDR bij Kaseya gebeuren en voldoet Datto EDR aan deze randvoorwaarde.

R4: De oplossing dient maandelijks te kunnen worden betaald

Datto EDR is maandelijks te betalen. Datto EDR voldoet aan deze randvoorwaarde.

5.6.6 Conclusie

Aan alle randvoorwaarden wordt voldaan. Datto EDR voldoet aan veel van de gestelde requirements. Er zijn requirements waar het niet aan voldoet. Voor een groot deel van deze requirements zijn er alternatieven waardoor de gestelde requirement niet volledig werkend is maar wel grotendeels. In het volgende hoofdstuk zal advies gegeven worden over Datto EDR.

6. Eindadvies

In dit hoofdstuk zal er antwoord gegeven worden op deelvraag acht en de hoofdvraag: Hoe kan endpoint protection aansluiten op de NIS2 en hoe kan Bradon endpoint protection inrichten voor de endpoints bij haar klanten, zodat endpoint beheer als dienst kan worden aangeboden aan klanten en hoe kan Bradon de endpoint protection laten aansluiten op de NIS2?

6.1 Methodiek

Om tot een duidelijk advies te komen zal er gekeken worden naar de gekozen oplossing. Hier worden de benodigdheden voor besproken, de voordelen en de nadelen. De requirements waar het advies op gebaseerd is, zijn in het testrapport getest en de resultaten zijn in bijlage D te zien.

6.2 Advies

Mijn advies voor Bradon is Datto EDR. Datto EDR voldoet aan vrijwel alle gewenste requirements die door Bradon zijn opgesteld en Datto EDR effectief en efficiënt endpoints kan beheren. Echter is dit niet de enige reden waarom Datto EDR geadviseerd wordt. Datto EDR sluit aan op de kennis die momenteel aanwezig is bij Bradon. De NIS2 heeft momenteel drie bekende eisen waaraan Datto EDR kan voldoen, dit zijn meldplicht, zorgplicht en toezicht. Meldplicht en zorgplicht zijn de eisen waar Datto EDR daadwerkelijk aan kan voldoen. De eis toezicht moet gehandhaafd worden vanuit de overheid.

Bradon zal door middel van Datto EDR een duidelijk overzicht krijgen van de mogelijke risico's bij bedrijven en zal hierdoor zelf snel een risicobeoordeling kunnen uitvoeren. Ook dient Bradon meldingen te maken van incidenten die de verlening van essentiële diensten zal verstoren. Door een overzichtelijk dashboard met de benodigde informatie kan Bradon zien als er incidenten zijn en deze melden indien dit nodig is.

Niet alle requirements zijn behaald. Als een klant mobiele apparaten in beheer wil hebben, zal er gekeken moeten worden naar een andere tool die dit mogelijk maakt. Het maken van back-ups is mogelijk in Datto, echter dient hiervoor een extra licentie aangeschaft te worden die niet onder Datto EDR valt. Ik adviseer daarom als klanten de back-up mogelijkheid voor de endpoints willen hebben dit met hen te bespreken en indien nodig de extra licentie aan te schaffen.

Voor het vergrendelen op afstand is het mogelijk om met een component deze actie en meer optie uit te voeren (Wissen van de laptop en vergrendelen van de bestanden). Mijn advies is om hier onderzoek naar te doen en indien gewenst dit component in gebruik te nemen. Datto heeft geen eigen sandbox, deze functie heeft in de requirement analyse dan ook de "Could have" weging gekregen. Mijn advies is: onderzoek in de toekomst de mogelijke oplossingen voor een sandbox omgeving.

6.2.1 Voordelen

- Door Datto EDR te gebruiken wordt het voor Bradon makkelijk op endpoints te beheren
- Bradon maakt gebruik van Autotask, als er gekozen wordt voor Datto EDR dan is dit te integreren met elkaar. Waardoor endpoints overzichtelijker en eenvoudiger te beheren zijn.
- Er is al kennis aanwezig binnen Bradon over Datto, hierdoor is er minder tijd nodig om de endpoint protection oplossing te kunnen begrijpen.

6.2.2 Nadelen

- Door Datto EDR te kiezen, neem je een dienst af van een developer waarvan je al een dienst afneemt. Hierdoor ontstaat er een single point of failure en vendor lock-in.
- Datto heeft geen mogelijkheid om smartphones en tablets toe te voegen, om dit te realiseren zal er een extra tool aangeschaft moeten worden als dit gewenst is bij een klant.

6.2.3 Conclusie hoofdvraag

Zoals in de voorgaande hoofdstukken is te zien, kan Bradon gebruik maken van verschillende widgets om zo het dashboard in Datto RMM overzichtelijk te maken. De agents zijn simpel te installeren bij de klanten en komen na installatie in Datto RMM te staan. Hierdoor zal Bradon de endpoints simpel kunnen beheren en bewaken en dit op een zo efficiënt en effectief mogelijke manier kunnen doen door de integratie met Autotask. Zoals voorgaand aangegeven in dit hoofdstuk sluit endpoint protection aan op de eisen die momenteel bekend zijn vanuit de NIS2.

7. Inhoudelijke reflectie

Door mijn afstudeerstage heb ik geleerd dat het goed kunnen onderzoeken van belang is. Tijdens mijn afstudeerstage heb ik uitgebreid onderzoek gedaan om in kaart te brengen welke endpoint oplossing voor Bradon de beste is.

Tijdens de gehele stage was het prettig om te kunnen sparren met HBO geschoolde medewerkers die ook ervaring hadden met het maken van een scriptie. Bij hen heb ik vragen kunnen stellen indien dat nodig was. Door de verkregen feedback heb ik mijn scriptie kunnen verbeteren en aanvullen. Ook heb ik gesproken met deze medewerkers om een duidelijk beeld te krijgen over de gewenste situatie. De requirements die hieruit zijn ontstaan in combinatie met het uitgevoerde onderzoek, hebben geleid tot de keuze en het proof of concept.

Hieruit zijn requirements gekomen waarmee de ontwerpen zijn opgesteld en getest.

Het onderzoeken van de verschillende mogelijkheden van endpoint security vond ik het leukst. Hierdoor kon ik zien hoeveel verschillende oplossingen er op de markt zijn en wat deze allemaal kunnen. Veel van de oplossingen hebben functies die ik nog nooit heb gezien en ook niet aan heb gedacht dat dit nuttig was.

Tijdens de stage heb is er besloten samen met de stagebegeleider vanuit Saxion om het beleid wat gemaakt ging worden te laten vallen. Dit was in zijn ogen een project op zich en dit zal niet haalbaar zijn geweest in de afstudeer periode. Daarom is het beleid aangepast naar voorbereidende stappen nemen voor de NIS2. Hier is het de bedoeling dat de gekozen oplossing voldoet aan meldplicht en zorgplicht. De NIS2 had aan het begin van de stage vertaald moeten zijn door de overheid. Echter is dit vertaalde NIS2 nog steeds niet beschikbaar. Het was dus niet mogelijk om de endpoint oplossing te kiezen met behulp van alle gestelde eisen vanuit de NIS2.

Conclusie: tijdens het schrijven van deze scriptie ben ik mij nog meer bewust geworden van de hoeveelheid mogelijkheden die een endpoint security oplossing kan bieden en dat deze in de tijd waar wij in leven van groot belang zijn.

8. Bibliografie

6. Motivation elements : ArchiMate® 3.1 specification. (z.d.). https://pubs.opengroup.org/architecture/archimate31-doc/chap06.html

ArchiMate - Motivation Concepts - ArchiMate Quick Guide. (z.d.). https://archimatetool.gitbook.io/quick_guide/archimate-language-extension/archimate-motivation-concepts

Barrington, R. (2020, 1 augustus). What is Mendelow's Matrix and why is it useful for marketers? Oxford College of Marketing Blog. https://blog.oxfordcollegeofmarketing.com/2018/04/23/what-is-mendelows-matrix-and-how-is-it-useful/

Benders, L. (2023, 10 november). Het 7S-model van McKinsey toepassen in je scriptie | Voorbeelden. Scribbr. https://www.scribbr.nl/modellen/7s-model-mckinsey/

Best practices for lost Device Security. (z.d.). https://rmm.datto.com/help/en/Content/2SETUP/BestPractices/Best_Practices_Lost_Device_Security.htm

Choose your cloud firewall wisely | Fortinet. (2021, 1 september). Fortinet Blog. https://www.fortinet.com/blog/industry-trends/choose-your-cloud-firewall-wisely

Complete Guide to Endpoint Security: Solutions and best practices. (2023, 26 oktober). BlueVoyant. https://www.bluevoyant.com/knowledge-center/complete-guide-to-endpoint-security-solutions-and-best-practices#endpoint-security-best-practices

Data Classification (Data Management): A complete overview | Spirion. (2023, 9 juli). Spirion. https://www.spirion.com/data-classification/#phase-1

Dingemanse, K. (2021a, november 12). Soorten interviews: voor- en nadelen. Scribbr. https://www.scribbr.nl/onderzoeksmethoden/soorten-interviews/

Endpoint Security: 8 Best Practices | NinjaOne. (2023, 4 december). NinjaOne. https://www.ninjaone.com/blog/endpoint-security-8-best-practices/

Eset. (2023, 4 juli). De zin en onzin van Managed Detection & Response (MDR)| ESET. © 2024, Eset s.r.o. All right reserved. https://digitalsecurityguide.eset.com/nl/de-zin-en-onzin-van-managed-detection-response-mdr

Felton B.V. (2021, 29 april). Wat zijn de voordelen van Endpoint Security? - Felton. Felton. https://felton.nl/artikelen/endpoint-security-voordelen/

GeeksforGeeks. (2022, 2 december). Functional vs non functional requirements. https://www.geeksforgeeks.org/functional-vs-non-functional-requirements/

Genau, L. (2023, 23 januari). Semigestructureerde of half-gestructureerde interviews in je scriptie. Scribbr. https://www.scribbr.nl/onderzoeksmethoden/semigestructureerd-interview/

Heinbach, C. (2022, 7 maart). How RMM Tools Help MSPs Combat Ransomware. Datto. https://www.datto.com/blog/why-rmm-is-crucial-for-msps-to-fight-ransomware

Infrastructure and security. (z.d.). https://rmm.datto.com/help/en/Content/1INTRODUCTION/Infrastructure/INFRASTRUCTUREANDSECURITY.htm

Murray, L. (2023, 4 april). What is Data Loss Prevention (DLP) | Data leakage Mitigation | Imperva. Learning Center. https://www.imperva.com/learn/data-security/data-loss-prevention-dlp

Nationaal Cyber Security Centrum. (2023, 7 november). Wat gaat de NIS2 richtlijn betekenen voor uw organisatie? Over het NCSC | Nationaal Cyber Security Centrum. https://www.ncsc.nl/over-ncsc/wettelijke-taak/wat-gaat-de-nis2-richtlijn-betekenen-voor-uw-organisatie

Nationaal Cyber Security Centrum. (2023a, november 6). Samenvatting van de NIS2-richtlijn. Over het NCSC | Nationaal Cyber Security Centrum. https://www.ncsc.nl/over-ncsc/wettelijke-taak/wat-gaat-de-nis2-richtlijn-betekenen-voor-uw-organisatie/samenvatting-richtlijn

Networking4all B.V. (z.d.). Wat is Security Information and Event Management (SIEM)? Networking4all Cybersecurity Specialist. https://www.networking4all.com/nl/nieuws/blog/post/wat-is-security-information-and-event-management-siem

Ninja, T. (2023, 5 juni). Wat is RMM Software? Evaluatiecriteria voor 2023 - NinjaOne. NinjaOne. https://www.ninjaone.com/nl/blog/wat-is-rmm-software/

Richter, S. (2022, 7 augustus). Wat is MSP (Managed IT Service Provider)? Datto. https://www.datto.com/nl/blog/wat-is-msp

Security best practices. (z.d.). https://rmm.datto.com/help/en/Content/1INTRODUCTION/Infrastructure/SecurityBestPractices.htm

Sophos. (z.d.). Endpoint Management explained: Best practices for security. SOPHOS. https://www.sophos.com/en-us/cybersecurity-explained/endpoint-management

Stakeholders. (z.d.). SURF.nl. https://www.surf.nl/stakeholders

UML Use Case Diagram Tutorial. (z.d.). Lucidchart. https://www.lucidchart.com/pages/uml-use-case-diagram

Van der Kuil, J. (2017, 4 februari). Zakelijke eisen, gebruikerseisen, en systeemeisen voor productiesystemen. Quality Business Support Blog. https://qualitybs.wordpress.com/2014/10/13/zakelijke-eisen-gebruikerseisen-en-systeemeisen-voor-productiesystemen/

Vullings, J. (2023, 4 april). Leer prioriteiten stellen door de MOSCOW-methode. OMCBase. https://www.omcbase.nl/moscow/

Wat is cloud computing? (z.d.). Salesforce. https://www.salesforce.com/nl/learning-centre/tech/cloudcomputing/

Wat is tweefactorauthenticatie? (z.d.). Digital Trust Center (Min. van EZK). https://www.digitaltrustcenter.nl/tweefactorauthenticatie

Wat is unified modeling Language? (z.d.). Lucidchart. https://www.lucidchart.com/pages/nl/wat-is-unified-modeling-language

Wat is XDR? – uitgebreide detectie en respons. (2023, 13 februari). Cisco. https://www.cisco.com/c/nl_nl/products/security/what-is-xdr.html

What is a secure email gateway (SEG)? (z.d.). Cloudflare2. https://www.cloudflare.com/learning/email-security/secure-email-gateway-seg/

What is a URL filtering? | Fortinet. (z.d.). Fortinet. https://www.fortinet.com/resources/cyberglossary/what-is-url-filtering

What is an insider threat? Definition, Types, & Examples | OpenText. (z.d.). OpenText. https://www.opentext.com/what-is/insider-threat

What is browser isolation? (z.d.). cloudflare. https://www.cloudflare.com/learning/access-management/what-is-browser-isolation/

What is endpoint encryption? Definition, architecture, and best practices - Spiceworks. (2022, 5 augustus). Spiceworks. https://www.spiceworks.com/it-security/network-security/articles/what-is-endpoint-encryption/

What is Endpoint Security? how it works & its importance | Trellix. (z.d.). Trellix. https://www.trellix.com/security-awareness/endpoint/what-is-endpoint-security/

What is IoT security? Definition and challenges of IoT security. (z.d.). Fortinet. https://www.fortinet.com/resources/cyberglossary/iot-security

What is network access control? | VMware Glossary. (2023, 16 mei). VMware. https://www.vmware.com/topics/glossary/content/network-access-control.html

What is sandboxing? Sandbox security and environment | Fortinet. (z.d.). Fortinet. https://www.fortinet.com/resources/cyberglossary/what-is-sandboxing

Widget Library. (z.d.). https://rmm.datto.com/help/en/Content/3NEWUI/Dashboards/WidgetLibrary.htm

Wij geloven in de kracht van samenwerken! - Bradon B.V. (2021, 15 januari). Bradon B.V. https://bradon.nl/

Bijlagen

9. Bijlage A: Stakeholderanalyse

In deze bijlage is de stakeholders analyse te vinden. Hierin zijn de stakeholders die te maken met de afstudeeropdracht gedefinieerd.

- Chief Executive Officer
- Senior engineer
- Backoffice
- Service delivery manager
- Overheid
- Klanten Bradon

9.1 Categoriseren stakeholders

Om te kunnen bepalen wat voor invloed verschillende stakeholders hebben binnen dit project zijn deze opgedeeld in de volgende drie groepen: interne stakeholders, externe stakeholders en de interface stakeholders.

De interne stakeholders maken deel uit van Bradon. De externe stakeholders zijn partijen die betrokken zijn bij mijn afstudeerproject, maar maken geen deel uit van Bradon en de interfacestakeholders hebben invloed op de organisatie, maar hebben geen direct belang. (Stakeholders, z.d.).

Categorie	Stakeholders
Interne stakeholders	• Chief Executive Officer • Senior engineer • Backoffice • Service delivery manager
Externe stakeholders	• Klanten Bradon
Interface stakeholders	• Overheid

Tabel 23 Stakeholder categorisatie

Na het categoriseren van de stakeholders is er bepaald welke invloed zij hebben.

Categorie	Stakeholders
Direct invloed	• Chief Executive Officer • Senior engineer • Backoffice • Service delivery manager
Indirect invloed	• Klanten Bradon • Overheid

Tabel 24 Invloed stakeholders

In de tabel 25 is toelichting te vinden over de stakeholders.

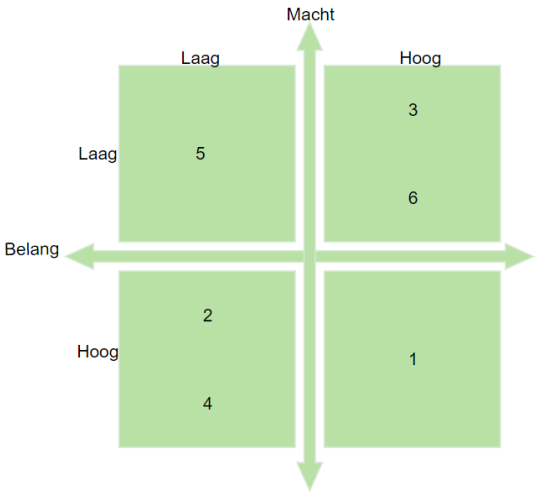
Nr.	Stakeholder	Toelichting
1	Chief Executive Officer	De Chief Executive Officer heeft als opdrachtgever veel invloed en belang bij de uitkomst van mijn afstudeeropdracht
2	Senior engineer	De Senior engineers binnen Bradon zullen gebruik gaan maken van de software en het beleid
3	Backoffice	De backoffice medewerker bij Bradon zal met het beleid en de software bekend moeten zijn, omdat zij deze zal kunnen verkopen aan klanten
4	Service delivery manager	De service delivery manager zal bekend met de oplossing moeten zijn, omdat hij contact heeft met klanten. Hij zal adviezen en informatie mee moeten kunnen nemen naar klanten
5	Overheid	De overheid verwerkt de NIS2 in de wetgeving en bedrijven zullen hieraan moeten gaan voldoen
6	Klanten Bradon	De klanten van Bradon zullen een groot belang hebben naar een goede endpoint protection. Echter hebben zij hier niet veel invloed op

Tabel 25 Stakeholder toelichting

9.2 Prioritering stakeholders

Om een duidelijk beeld te krijgen van de prioriteit van de stakeholders zijn deze geprioriteerd op basis van de Mendelow's matrix (Barrington, R. 2020, 1 augustus). Met behulp van deze matrix is te zien wat voor invloed de stakeholders hebben binnen het project. Er zijn vier categorieën waar de stakeholders in verdeeld kunnen worden:

- **Key players (Hoog, Hoog):** Deze groep dient volledig betrokken te worden en vergen de grootste inspanning om tevreden te houden
- **Keep satisfied (Hoog, Laag):** Deze groep dient tevreden gehouden te worden
- **Keep informed (Laag, Hoog):** Deze groep dient geïnformeerd te worden
- **Low priority (Laag, Laag):** Deze groep hoeft niet geïnformeerd te worden, maar wel in de gaten gehouden worden indien er veranderingen zijn



Figuur 24 Mendelow's matrix

10. Bijlage B: Behoefteanalyse

Er wordt gekeken naar de perspectieven van de stakeholders om zo tot een lijst van aspecten te komen.

10.1 Perspectieven medewerkers Bradon

Chief executive office:

Er is gesproken met de Directeur van Bradon. Vanuit het gesprek met de directie is gebleken dat er vanuit Bradon behoefte is voor een endpoint protection beleid. De Europese unie heeft na COVID-19 en de toenemende cyberdreigingen de Network and Information Security (NIS2) directie opgesteld. Dit is een richtlijn die zich op een verbetering van de digitale en economische weerbaarheid van de Europese lidstaten focust. Momenteel is de Nederlands overheid bezig met het omzetten van de NIS2-richtlijn naar de nationale wetgeving. Bradon wil zich voorbereiden op de komst van de NIS2-richtlijn. Door het invoeren van een beleid voor endpoint protection en de keuze maken voor een softwaremogelijkheid die het beheren en beheersen van de endpoints efficiënt kan uitvoeren, kan Bradon een grote stap nemen om te voldoen aan de NIS2-richtlijn.

Bradon levert een groot aantal IT-diensten aan haar klanten. Deze klanten maken gebruik van endpoints die beheerd en beheerst kunnen worden. Momenteel is er bij Bradon geen beleid aanwezig voor het beheren en beheersen van de endpoint protection. Bradon maakt gebruik van verschillende soorten software, echter is er geen uniforme software die gebruikt wordt voor al Bradon haar klanten. De software die momenteel aanwezig zijn worden ook niet volledig gebruikt waar deze gebruikt voor kunnen worden met betrekking tot endpoint protection.

Senior engineer:

Er is gesproken met een senior engineer. Hij geeft aan dat er momenteel geen beleid en software aanwezig is bij Bradon voor endpoint protection. Er zal onderzocht moeten worden welk product het beste bij Bradon past en de klanten goed beschermd. Verder geeft de senior engineer aan dat de software makkelijk in gebruik moet zijn en dat er informatie beschikbaar moet zijn als een klant aangeeft dat er iets geks speelt of dat Bradon de klant op de hoogte kan stellen indien Bradon iets ziet.

Backoffice:

Er is gesproken met de backoffice. Zij geeft aan dat er momenteel geen beleid is voor de endpoint security binnen Bradon en ook geen mogelijkheid om hier een dienst van te maken**.** Dit zorgt ervoor dat bij het bepalen van het beleid een vrije keuze welke regels er dienen te komen en van toepassing zijn op Bradon. Bij sommige klanten wordt momenteel deels de endpoints gemanaged, echter is de wens om dit als dienst aan te kunnen bieden aan alle klanten. Ook biedt het inrichten van endpoints bij klanten leermogelijkheden aan binnen Bradon voor de medewerkers. Bradon heeft verschillende leveranciers, er zal gekeken moeten worden wat deze leveranciers leveren aan endpoint management om deze eventueel af te kunnen nemen bij een huidige leverancier.

Service delivery manager:

Er is gesproken met de service delivery manager: Hij geeft aan dat Bradon diensten levert aan haar klanten en in sommige gevallen ICT'ers op locatie levert en verantwoordelijk is voor de beveiliging van de omgeving. Er is veel belang voor endpoint security, omdat Bradon de verantwoording hiervoor draagt. Bradon is verantwoordelijk voor het operationeel houden van de ICT bij haar klanten en endpoint protection kan hierbij helpen. Een gebruiker neemt een groot risico mee en dit kan niet opgelost worden. Het feit dat er vanuit de Europese Unie aan de NIS2 voldaan moet worden heeft een grote impact voor een kleine organisatie zoals Bradon. Echter geeft dit wel duidelijkheid aan klanten dat Bradon te vertrouwen is als zij aan de NIS2 zal voldoen.

Bij de keuzes van de mogelijke oplossing gaat het om het gemak van de beheerders, er moet niet te veel tijd verloren gaan en er moet zo snel mogelijk geholpen kunnen worden. Het hebben van een praatplaat is ook van belang. Hierdoor kan er met klanten gesproken worden over hun security en kunnen hier rapportages van worden weergegeven.

10.2 Perspectief overheid

Om het overheidsperspectief de bepalen is er gekeken naar het Nationaal Cyber Security Centrum (NCSC). Zoals eerder aangegeven is deze richtlijn gericht op het verbeteren van de digitale en economie weerbaarheid van Europa (Nationaal Cyber Security Centrum, 2023). Het Nationaal Cyber Security Centrum is bezig met het vertalen van de NIS2 naar de Nederlandse wetgeving. Bedrijven binnen verschillende sectoren zullen hieraan moeten gaan voldoen einde 2024. In het eerste kwartaal van 2024 zal er een consulatie periode gestart worden waarin de conceptwetteksten gereed zijn.

10.3 Methodiek Requirements

In gesprekken met de interne stakeholders zijn de behoeften van Bradon inzichtelijk gemaakt. Uit deze gesprekken zijn de requirements ontstaan.

10.4 Categoriseren

Om de opgestelde requirements onderling verifieerbaar te maken zijn deze opgedeeld in de volgende drie categorieën: "Business", "User" en "System". Een business requirement beschrijft waarom de organisatie bezig is met het project en welke voordelen de organisatie verwacht met de aanschaf of ontwikkeling van het product. De user requirement beschrijft wat de gebruiker moet kunnen met de oplossing. De laatste categorie system requirements zijn de bouwstenen van een engineer en beschrijft wat de oplossing zal gaan doen. (Van der Kuil, J. 2017, 4 februari).

10.5 Functionaliteit

Requirements kunnen verdeeld worden in functionele en Niet-functionele requirements. Functionele requirements zijn eisen die de eindgebruiker eist van de oplossing. Deze requirements moeten terug te zien zijn in de eindoplossing. Niet-functionele requirements zijn eisen waaraan het system moet voldoen. (GeeksforGeeks, 2022, 2 december).

10.6 Prioritering

Om een duidelijk beeld te krijgen van welke requirements absolute eisen zijn en welke minder belangrijk zijn, zal de MoSCoW methode worden toegepast. Deze methode wordt gebruikt om binnen een project de requirements te verdelen in vier categorieën: must have, should have, could have en would/won't have. Must have zijn eisen die noodzakelijk zijn om ervoor te zorgen dat het eindresultaat functioneert zoals gewenst is. Should have zijn requirements die zeer gewenst zijn, maar niet direct noodzakelijk zijn voor een goede functionaliteit. Could have requirements zijn wenselijk, echter niet noodzakelijk. Would/Won't have zijn requirements die gewenst zijn in een later project. (Vullings, J. 2023, 4 april).

10.7 Verbanden

Om een verband te kunnen leggen tussen de requirements zal er gebruik gemaakt worden van de termen "genereert" en "realiseert". Genereert laat zien welke requirements voorkomen uit het requirement. Realiseert geeft aan welke requirements worden gelegaliseerd uit de requirements.

11. Bijlage C: 7-S Model

11.1 Methodiek

Om de interne analyse uit te voeren voor Bradon is gebruik gemaakt van het 7-S model van McKinsey (Benders, 2023).

11.2 Resultaten

11.2.1 Structuur

Bradon levert verschillende diensten aan haar klanten. Deze diensten worden onderhouden door de 2e lijn medewerkers (senior engineers) binnen Bradon zelf en de 1e lijn medewerkers die Bradon inhuurt. De inkoop wordt gedaan door de backoffice medewerker en het contact met de klanten door de CEO en de service delivery manager. Alle medewerkers binnen Bradon worden gelijk behandeld om zo geen verdeling binnen het bedrijf te krijgen. Bradon wil de endpoint security als nieuwe dienst kunnen aanbieden aan haar klanten.

11.2.2 Strategie

Bradon levert als IT-specialist verschillende diensten aan haar klanten. Zo ontwerpen, onderhouden en ondersteunen zij de ICT-omgeving van verschillende bedrijven in diverse omvang. Bradon hun ambitie is om IT-zaken, beter, slimmer en sneller te laten verlopen. (Bradon B.V, 2021, 15 januari).

Bradon maakt gebruik van een cloud first strategie. Bradon wil haar klanten het liefst zo snel mogelijk in de cloud krijgen. Ook maakt Bradon gebruik van maandelijkse afschriften. Hiermee wordt bedoeld dat Bradon maandelijks facturen naar haar klanten stuurt en ook zelf maandelijks hun eigen kosten betaald. Hierdoor blijft er een duidelijke lijn in hoeveel inkomsten binnen komen en hoeveel kosten eruit gaan.

11.2.3 Systemen

Bradon maakt gebruik van verschillende systemen die zij levert aan haar klanten. Bradon levert verschillende soorten hardware en software aan haar klanten. Zo levert Bradon servers, netwerk hardware, telefonie en werplekken met de randapparatuur.

Bradon levert ook verschillende producten aan klanten zoals: Back-up, handtekening, telefonie, security, printing software. Ook levert Bradon software die helpt bij het automatiseren van de werkplekken.

11.2.4 Staf

Binnen Bradon werken vijf vaste medewerkers en één ingehuurde accountant. Ook heeft Bradon verschillende medewerkers gedetacheerd door heel Nederland. De medewerkers binnen Bradon zijn: Chief Executive Officer, service delivery manager, backoffice, ingehuurde accountant en twee senior engineers. Het grootste deel van de medewerkers binnen Bradon zijn HBO geschoold. De medewerkers zijn flexibel in werkuren en werken regelmatig in de avonduren om bij klanten onderhoud uit te voeren op de servers.

11.2.5 Stijl

Binnen Bradon werken medewerkers op een zelfstandige wijze er is weinig sturing op de medewerkers nodig vanuit management, coachend managen wordt gehanteerd. Tweede lijn medewerkers werken dagelijks aan incidenten en projecten die zijn toegewezen of hebben opgepakt. De andere medewerkers houden zich vooral bezig met de inkoop en het klantcontact.

11.2.6 Skills

Bradon is een IT-specialist die zich richt op het ontwerpen, onderhouden en ondersteunen van de ICT-omgeving bij verschillende bedrijven. Bradon heeft verschillende partners. Dit houdt in dat de medewerkers van Bradon gecertificeerd zijn en veel kennis hebben over de geleverde diensten.

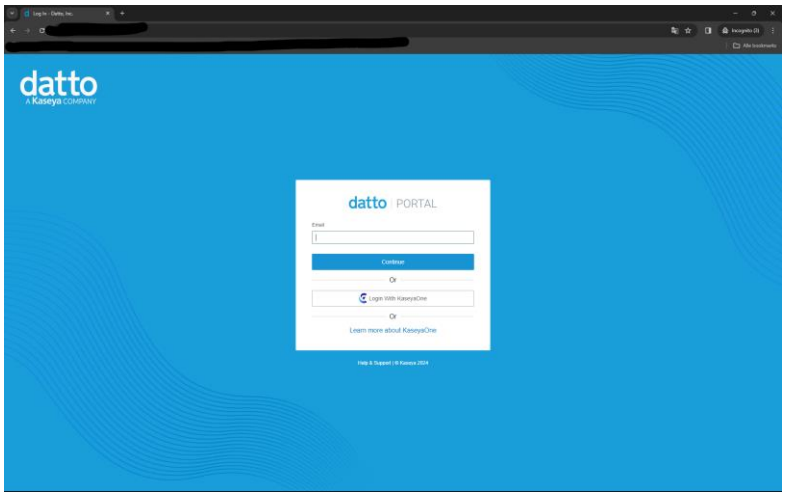
11.2.7 Significante waarden

Bradon geeft in haar missie en visie aan dat Bradon gezien wil worden als “De ICT-Infrastructuur & Cloud provider van Nederland”. Binnen Bradon geloven zij in de kracht van samenwerken om zo hun klanten het beste te kunnen ondersteunen (Bradon B.V, 2021, 15 januari).

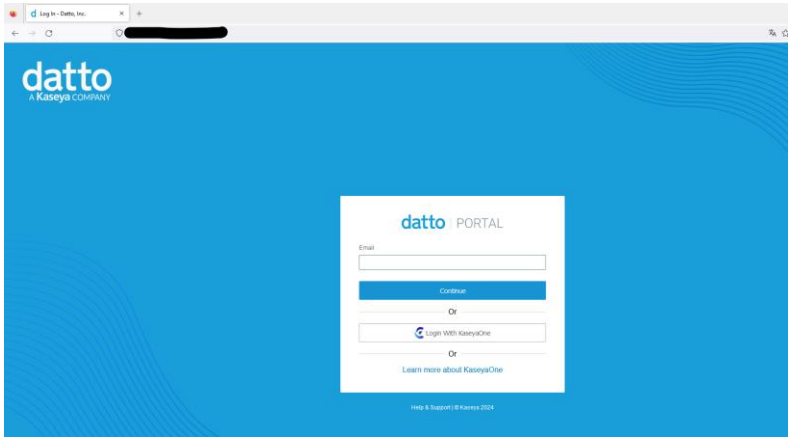
12. Bijlage D: Proof of concept

S01: Het systeem zal benaderbaar zijn via de webbrowser

Datto is benaderbaar via verschillende browser zoals in figuur 25 & 26 te zien. Het maakt niet uit welke browser er gebruikt wordt, Datto zal goed functioneren in elke browser. Er is gekozen voor google Chrome en Firefox als webbrowsers, omdat dit de meest gebruikte webbrowsers zijn.



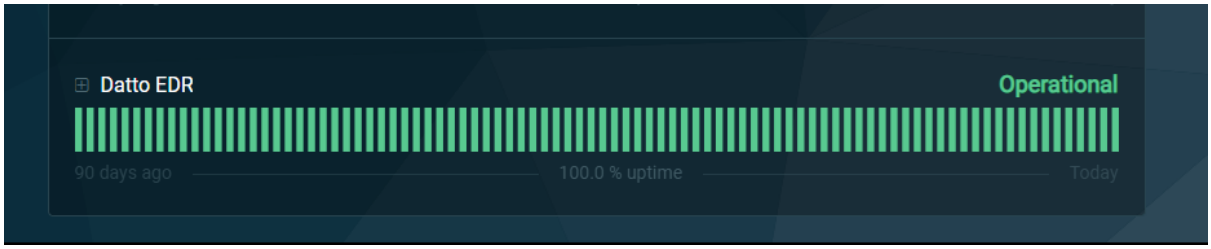
Figuur 25 Inloggen via Chrome



Figuur 26 Inloggen via Firefox

S02: Het systeem zal een uptime van 99.9% hebben

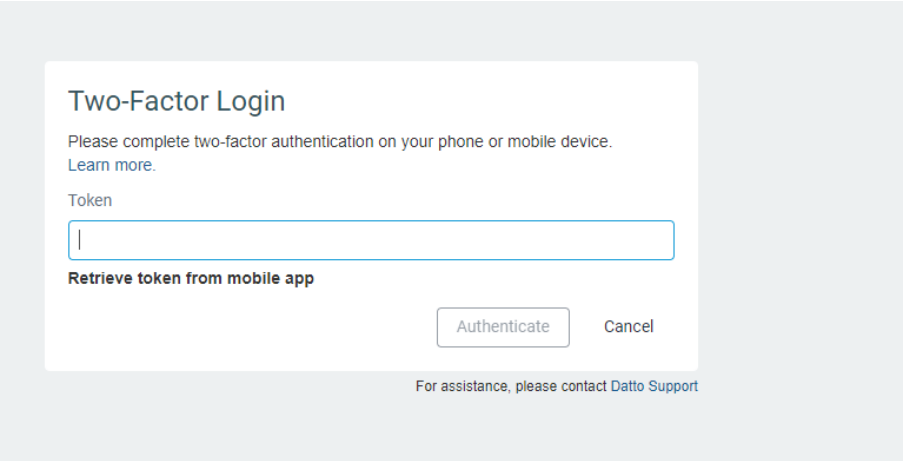
Datto heeft een uptime website voor hun verschillende onderdelen. In figuur 26 is te zien dat Datto EDR, het onderdeel waar deze scriptie over gaat een uptime heeft van 100% in de laatste 90 dagen.



Figuur 27 Uptime Datto RMM

S03: Het systeem zal gebruik maken van Multi Factor Authentication

In system requirement 1 is te zien dat Datto te benaderen is via een webbrowser, na het invoeren van de inloggegevens moet een Two-Factor code worden ingevoerd. Dit zorgt voor extra beveiliging om in de portal te komen.



Figuur 28 Multi Factor Authenticatie Datto

S04: Het systeem zal toepasbaar zijn op de volgende operating systemen: Windows, MacOS en Linux.

Windows, macOS en Linux zijn toe te voegen als device, ook is het mogelijk om een ander network device toe te voegen en een printer.

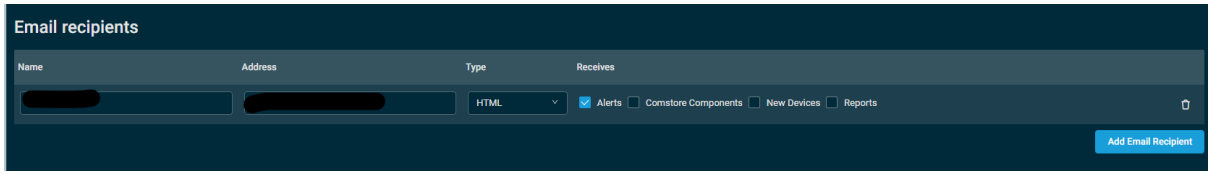
Figuur 29 Add device verschillende OS

S05: Het systeem zal toepasbaar zijn op de volgende mobiele operating systemen: IOS en Android

Binnen Datto EDR is het niet mogelijk om smartphones of tablets toe te voegen.

S06: Het systeem zal mails kunnen genereren

Datto EDR kan zoals in figuur 30 te zien is mails genereren. Er zijn verschillende mogelijke keuzes die gemaakt kunnen worden over het soort melding waarover een mail gestuurd zal worden.



Figuur 30 Alert via mail instellingen

S07: Het system zal een sandbox hebben voor het testen van zero days

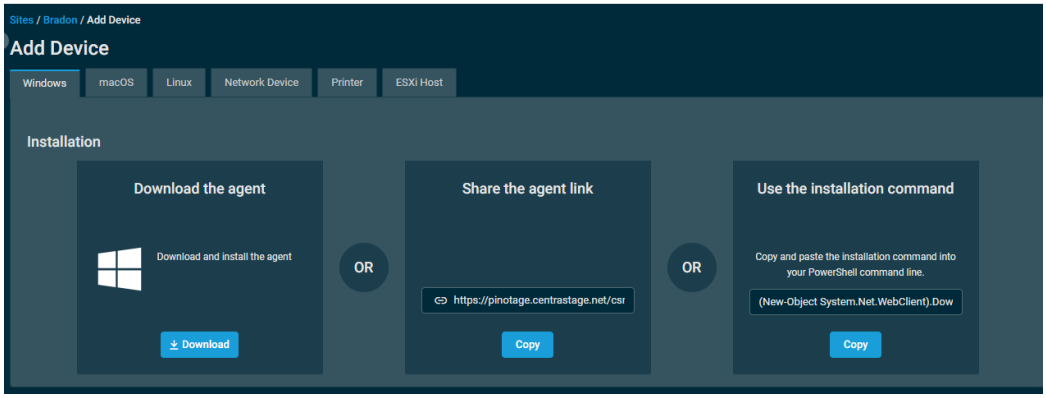
Datto heeft geen mogelijkheid om dingen te testen in een sandbox. Het is dus niet mogelijk om zero days of andere mogelijke risico's te testen in een veilige omgeving.

S08: Het systeem zal werkstations kunnen beheren

Onder het beheren van de endpoints vallen verschillende user requirements. Deze zijn hieronder te zien.

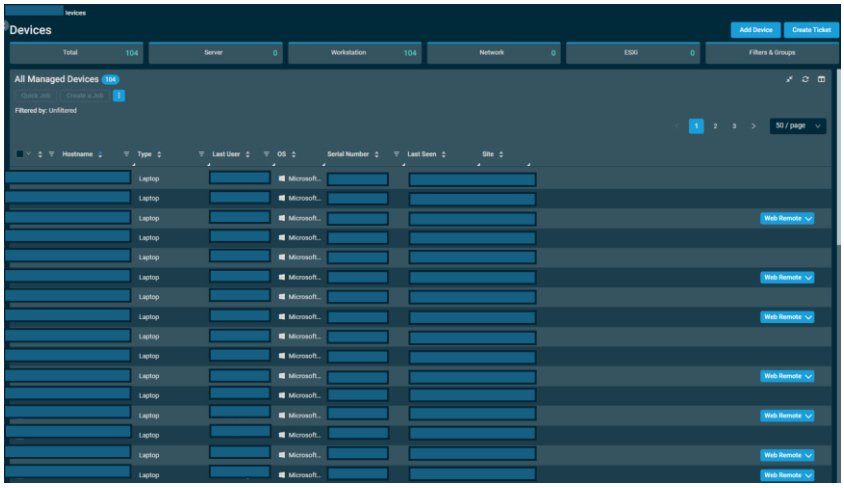
U01: Senior engineer zal endpoints kunnen toevoegen

Een senior engineer kan op verschillende manieren een endpoint toevoegen. Dit kan worden gerealiseerd met behulp van de agent te installeren op de endpoint. De verschillende manieren van het installeren van de agent zijn in het technische ontwerp uitgewerkt. Hieronder is te zien dat de agent gedownload kan worden voor verschillende operating systems of er een download link gestuurd kan worden.



Figuur 31 Toevoegen endpoint

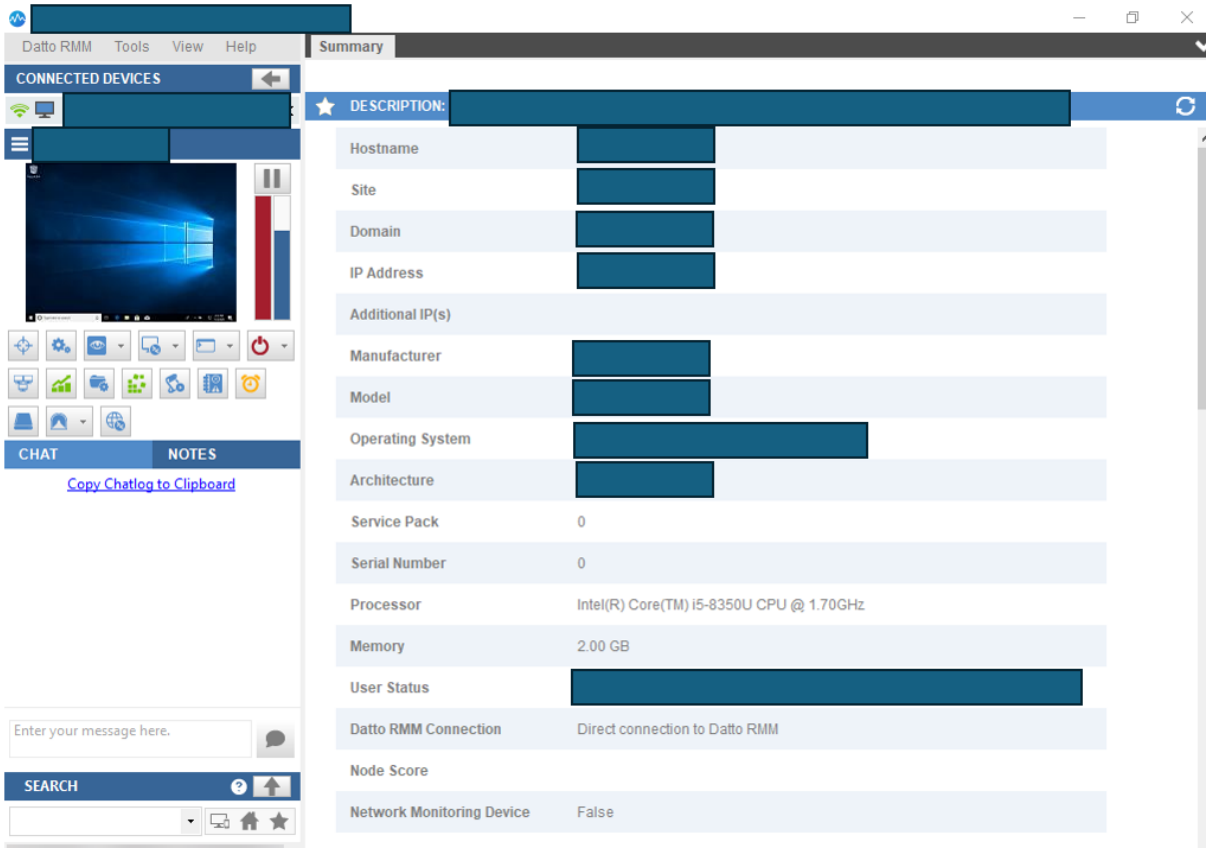
Nadat de agent geïnstalleerd is op de endpoint komen ze in een lijst met unmanaged devices te zien. Hieruit moet de endpoint in de juiste lijst gezet worden van het bedrijf waar deze bij hoort. In figuur 32 is een overzicht te zien van toegevoegde endpoints en informatie over deze endpoints.



Figuur 32 Overzicht verschillende endpoints

U02: Senior engineer zal werkstations kunnen overnemen

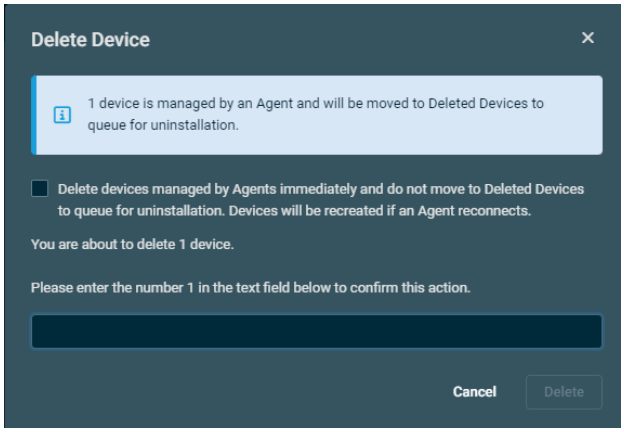
Doormiddel van de agent die geïnstalleerd wordt op de endpoints kunnen senior verschillende activiteiten op deze endpoints doen, zoals het overnemen van de endpoint. In figuur 33 is de agent te zien die een senior engineer ziet als hij een endpoint wil overnemen.



Figuur 33 Agent endpoint overnemen

U03: Senior engineer zal endpoints kunnen verwijderen

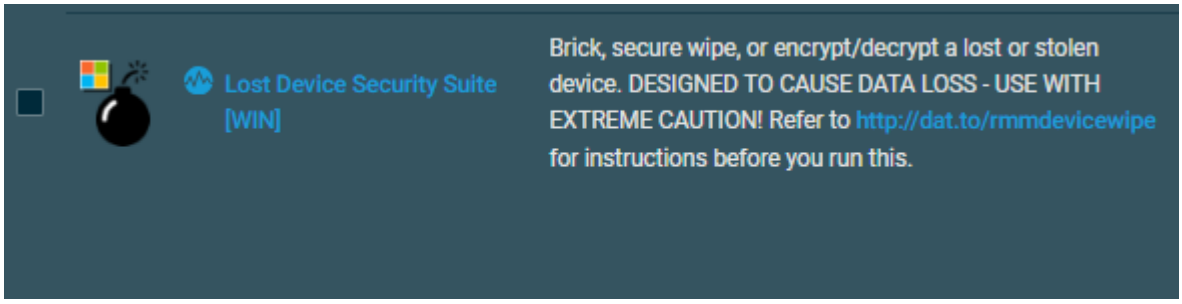
Het is ook van belang om endpoints te kunnen verwijderen. In figuur 32 is de lijst met endpoints te zien. Hier kan een endpoint geselecteerd worden en vervolgens verwijdert.



Figuur 34 Verwijderen endpoint

U04: Senior engineer zal endpoints kunnen vergrendelen op afstand

Binnen Datto is het niet mogelijk op endpoints te vergrendelen op afstand. Het is echter wel mogelijk om een component toe te voegen. Met behulp van deze component die te zien is in figuur 35 kunnen er verschillende dingen gedaan worden op de endpoint om ervoor te zorgen dat de informatie die op de endpoint niet toegankelijk zal zijn.



Figuur 35 Mogelijkheden verloren endpoint

U05: Senior engineer zal endpoints en/of files in quarantaine kunnen zetten

Een senior engineer hoeft zelf geen endpoints in quarantaine te zetten, Datto kan dit automatisch doen. Datto doet dit doormiddel van behavioral analysis van files. Dit brengt verschillende voordelen met zich mee: Monitor for ransomware at scale, Receive immediate notification when ransomware is detected, Prevent the spread of ransomware through network isolation en Remediate issues remotely (Heinbach, 2022).

S09: Het systeem zal multi tenant ingericht zijn

Voor de senior engineers is het belangrijk dat alle bedrijven waarvan endpoints gehost worden, zichtbaar zijn in één portaal. In figuur 36 is te zien dat dit mogelijk is. Per bedrijf (Site) zijn ook het aantal devices te zien de beheerd worden.

Figuur 36 Overzicht verschillende klanten

S11: Het systeem zal scans kunnen uitvoeren

Senior engineers kunnen per endpoint handmatig een scan uitvoeren. Dit kunnen snelle scans zijn of volledige systeem scans.

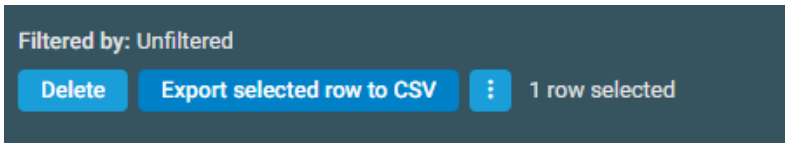
Figuur 37 Scan on demand functie

De resultaten van deze scan, indien er een beveiliging probleem is gevonden zal deze worden weergegeven in alerts. In de event log van de endpoint is de handeling die is uitgevoerd te zien.

Figuur 38 Resultaten van on demand scan

S12: Het systeem zal overzichten kunnen genereren

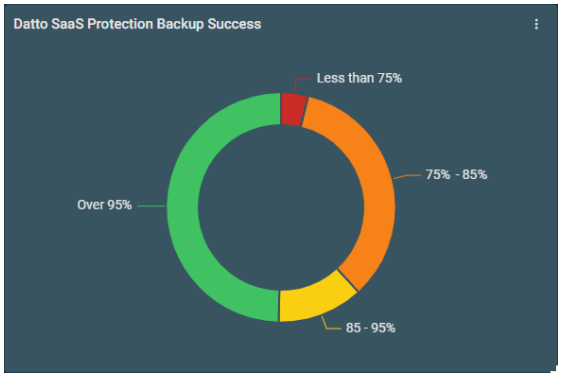
Binnen Datto kan er op verschillende plekken een export worden gemaakt. Denk hierbij aan de beheerde endpoints, licenties **(U09)** en de alerts.



Figuur 39 Exporteer functie Datto

S13: Het systeem zal back-ups kunnen maken

Voor het kunnen uitvoeren van back-ups is een nieuwe licentie structuur nodig, dit is een apart component van Datto RMM. Hierdoor is het testen van de back-ups niet mogelijk in de testomgeving die aanwezig is. Echter is op de website van Datto overzichtelijk uitgelegd hoe back-ups uitgevoerd kunnen worden, dit is in de onderstaande afbeeldingen te zien (Widget Library, z.d.).



Figuur 40 Back-up resultaten