TLP:GREEN

OR-7 CONFIGURATIEHANDLEIDING

Monitoring & Detectie – SOC Operational Readiness – **Malware Protection**

Best Practice versie 1.2

Complexiteit document
Eenvoudig

Samenwerken maakt

DIGITAAL VEILIGER

VSSR

Inhoudsopgave

Voorwoord

De Rijksoverheid verwerkt grote hoeveelheden gevoelige informatie en is daarmee een interessant en gewild doelwit. Cybercriminelen en statelijke actoren zoeken naar kwetsbaarheden om zich zo toegang te verschaffen tot de supplychain, netwerken, systemen en (gevoelige) informatie.

De wereld van cyberdreigingen verandert snel en vraagt om gezamenlijke inspanning om weerbaar te zijn. Dit vraagt om samen te werken aan breder toegepaste én verbeterde SOC-dienstverlening. Het programma Versterken SOC Stelsel Rijk (VSSR) is opgezet om hieraan bij te dragen.

Een belangrijk onderdeel van SOC-diensten zijn de monitoring- en detectiediensten. Deze zijn erop gericht om een veelheid aan loggegevens en andere (meta-)datastromen afkomstig van de IT-infrastructuur, randapparatuur, bedrijfsapplicaties en andere dataverwerkingen in een organisatie te analyseren, aggregeren en correleren. Monitoring en detectiesystemen kunnen op basis hiervan verdachte gedragingen detecteren en alarm slaan.

Om een SOC effectief en doelmatig in te zetten is het noodzakelijk dat er een aantal onderwerpen binnen een organisatie zijn ingericht. VSSR levert diverse producten die rijksorganisaties ondersteunen bij het inrichten van een SOC en de daarvoor benodigde randvoorwaarden.

Achtergrond

VSSR levert verschillende kennisproducten. Dit document maakt onderdeel uit van een set van miniproducten die rijksorganisaties helpt om een aantal SOC operationele randvoorwaarden in te richten.

Doelgroep

Versterken SOC Stelsel Rijk (VSSR) biedt met dit document handvatten voor Windows IT-beheerders die verantwoordelijk zijn voor het beheer van Windows-systemen.

1. Documentgegevens

1.1 Documenthistorie

Versie	Datum	Omschrijving
V1.0	20-03-2025	Initiële versie
V1.1	31-10-2025	Toevoeging "Bijlage I – Configuratiestatus checklist"
V1.2	07-07-2026	Referenties geactualiseerd

1.2 Referenties

Document	Link
Checklist basisbeveiliging (OR-5)	Zie "Checklist basisbeveiliging ..(OR-5)" onder SOC Operational Readiness (Configuratie & Logging)
Generiek implementatieplan voor OR-6 t/m OR-9	Zie "Generiek implementatieplan" onder Platform/Applicatie Hardening & Malware bescherming (OR-6 t/m OR-9). Onderdeel van SOC Operational Readiness (Configuratie & Logging)
Microsoft Defender Documentation	https://docs.microsoft.com/en-us/microsoft-365/security/
VSSR-kennisdocumenten	VSSR (ncsc.nl)

1.3 Definities

Term	Omschrijving
Endpoint Detection and Response (EDR)	Oplossing voor continue monitoring en respons op dreigingen op eindpunten.
Microsoft Defender for Endpoint	Geïntegreerde beveiligingsoplossing voor bescherming van apparaten binnen het Microsoft-ecosysteem.
Attack Surface Reduction (ASR)	Beperkt aanvalsvectoren door scripts en onbetrouwbare applicaties te blokkeren.
Controlled Folder Access	Beschermt belangrijke mappen tegen ongeautoriseerde wijzigingen en ransomware.
Real-time bescherming	Voortdurende controle van bestanden en activiteiten om direct dreigingen te detecteren.
Cloud-delivered bescherming	Gebruik van cloudnetwerken en AI voor snelle detectie en blokkering van dreigingen.
Threat & Vulnerability Management (TVM)	Inzicht in kwetsbaarheden en prioritering van beveiligingsacties.
Microsoft Secure Score	Tool die aanbevelingen geeft om de beveiligingspositie te verbeteren.
Tamper Protection	Voorkomt dat malware beveiligingsinstellingen uitschakelt of aanpast.
Network Protection	Blokkeert verbindingen met malafide websites en downloadlocaties voor Microsoft Edge.
Scan Configuraties	Instellingen voor dagelijkse quick scans en wekelijkse volledige scans.
Performance Impact Management	Optimalisatie van systeemperformance tijdens beveiligingsoperaties.
Office Application Protection	Beperkingen op Office-applicaties om veelvoorkomende aanvalsvectoren te blokkeren.
Script Execution Control	Beperkt de uitvoering van potentieel schadelijke scripts.
Removable Storage Access	Controleert toegang tot verwijderbare opslag om malwareverspreiding te voorkomen.

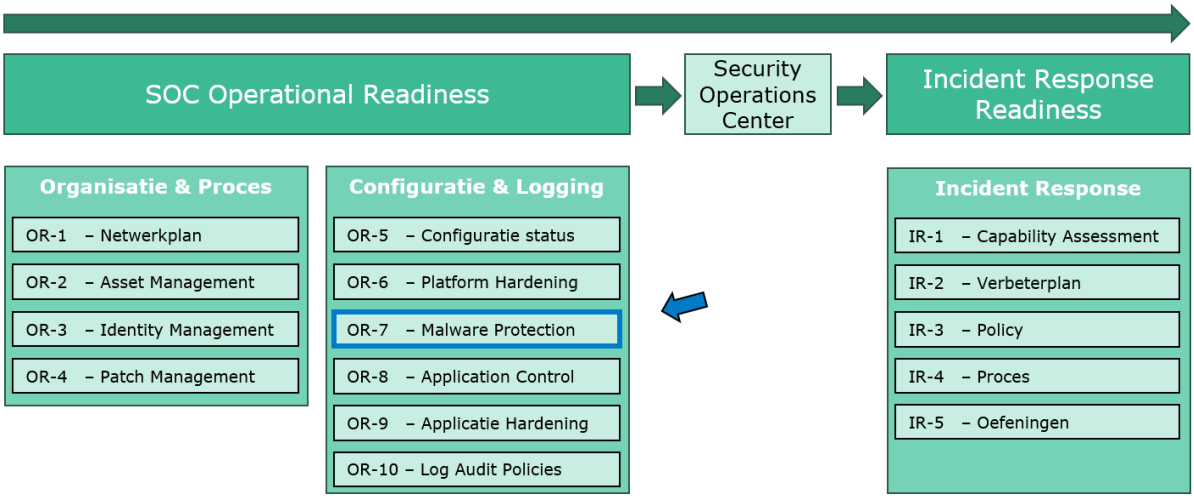
Ter verduidelijking van de overige terminologie en begrippen die in dit document worden gebruikt is er een verzameling van definities te vinden op Woordenboek - Cyberveilig Nederland.

2. Context miniproducten

Dit document maakt onderdeel uit van de SOC Readiness Assistance **miniproducten**. De SOC Readiness Assistance miniproducten ondersteunen uw organisatie bij de voorbereidingen die nodig zijn voor het optimaal benutten van een SOC(-dienst). Deze producten hebben een samenhangende opbouw maar kunnen ook los van elkaar worden gebruikt. De producten zijn in drie groepen te verdelen:

1) **Organisatie & Proces:** Helpt bij het inrichten van processen met als doel het SOC van de juiste informatie te voorzien om goed te kunnen monitoren.
2) **Configuratie & Logging:** Helpt bij het inrichten van basisbeveiliging met als doel om beter beschermd te zijn en de juiste logdata bij een SOC aan te kunnen leveren.
3) **Incident Response:** Met behulp van monitoring & Detectie zal een SOC security melding genereren. De Incident Response producten helpen bij het inrichten van de opvolging van deze meldingen binnen uw organisatie.

Onderstaande weergave toont dit document als onderdeel van **Configuratie & Logging** in het VSSR-Minipoducten raamwerk.



Figuur 1 - Dit document als onderdeel van het VSSR-Miniproducten raamwerk

De twee productgroepen behorende bij *SOC Operational Readiness* bestaan telkens uit een vergelijkbare set document die in figuur 1 per groep zijn weergegeven. Niet elk product bestaat uit exact de zelfde componenten maar veelal wordt de zelfde structuur gebruikt waarbij dit document de configuratiehandleiding is voor Malware Protection (OR-7), binnen **Configuratie & Logging**, behandelt.

3. Inleiding

Deze configuratiehandleiding biedt een praktische gids voor het instellen van malwarebescherming met Microsoft Defender for Endpoint. Ze is speciaal ontworpen voor IT-professionals in kleine en middelgrote organisaties die hun systemen beter willen beveiligen tegen moderne digitale dreigingen.

Belangrijk: Het correct instellen van de configuraties betekent niet automatisch dat deze direct zijn toegepast op de endpoints van gebruikers binnen de organisatie. Om te garanderen dat de instellingen daadwerkelijk actief zijn, is het noodzakelijk om het implementatieproces zorgvuldig te doorlopen. Het implementatieproces is afzonderlijk beschreven[1] en kan samen met dit document worden gebruikt.

De handleiding is onderverdeeld in de volgende hoofdsecties:

- Documentgegevens: Inzicht in de documenthistorie, referenties en definities.
- Introductie: Achtergrondinformatie, definities en een overzicht van de gebruikte EDR-oplossing.
- Initiële Setup & Configuratie: Stap voor stap handleiding voor de configuratie van Microsoft Defender for Endpoint, inclusief onboarding, security baseline configuratie, antivirus instellingen en geavanceerde beveiligingsfuncties.
- Logging van Malwarebescherming: Beschrijving van de logging en de specifieke locaties om de logging te kunnen inzien.

3.1 Doel

Deze handleiding focust op de configuratie van Microsoft Defender for Endpoint om een robuuste verdediging mogelijk te maken tegen malware, ransomware en andere cyberaanvallen. De nadruk ligt op een gestructureerde aanpak om:

- De betekenis en functie van een EDR-oplossing te begrijpen
- Randvoorwaarden te definiëren voor succesvolle implementatie.
- Beveiligingsraamwerken te gebruiken als basis voor de beveiliging.
- De impact van de implementaties te begrijpen.
- Aanbevelingen voor voortdurende beveiliging te bieden.
- Volgende stappen te bepalen.

3.2 Wat is een EDR-oplossing?

Endpoint Detection and Response (EDR) is een beveiligingstechnologie ontworpen om eindpunten zoals laptops, desktops en servers te beschermen tegen geavanceerde dreigingen. EDR biedt continue monitoring en geavanceerde analyses om verdachte activiteiten te detecteren en hierop te reageren. De technologie is een essentieel onderdeel van een moderne beveiligingsstrategie en helpt organisaties met:

- **Detectie:** Identificeren van verdachte of schadelijke activiteiten op eindpunten.
- **Respons:** Snel actie te ondernemen, zoals isoleren van besmette systemen.
- **Analyse:** Inzicht te krijgen in de oorzaak van incidenten voor betere preventie.

3.2.1 Waarom gebruiken we Defender for Endpoint?

Microsoft Defender for Endpoint bouwt voort op licenties en middelen die in veel organisaties reeds beschikbaar zijn, bijvoorbeeld via Microsoft 365 E3/E5. Door deze bestaande producten te

[1] Zie Generiek implementatieplan voor OR-6 t/m OR-9

benutten, kan uw organisatie zonder complexe of aanvullende integraties gebruikmaken van een geïntegreerde endpointbescherming. Deze oplossing biedt zowel basisfunctionaliteiten (beschikbaar in E3/P1) als geavanceerde EDR-capaciteiten (beschikbaar in E5/P2) en sluit naadloos aan op Microsoft Intune voor centraal beheer en configuratie. Hierdoor ontstaat een beheersbare en op uw bestaande infrastructuur aansluitende beveiligingsaanpak.

3.2.2 Welke componenten zitten er in Defender for Endpoint?

Microsoft Defender for Endpoint bevat een reeks geavanceerde functies en componenten die samen zorgen voor uitgebreide bescherming:

- Real-time bescherming: Continue controle van bestanden en activiteiten op eindpunten.
- Cloud-delivered bescherming: detectie van dreigingen met behulp van AI[2] en Microsoft's wereldwijde netwerk.
- Threat & Vulnerability Management (TVM): Inzicht in kwetsbaarheden en prioriteitstelling voor mitigatie.
- Attack Surface Reduction (ASR): Beperkt aanvalsvectoren door scripts en onbetrouwbare applicaties te blokkeren.
- Automatische incidentrespons: Biedt mogelijkheden voor geautomatiseerde mitigatie en herstel.
- Secure Score: Geeft aanbevelingen om de beveiligingspositie te verbeteren.

Deze componenten werken samen om proactieve bescherming, snelle detectie en effectieve respons te bieden tegen moderne dreigingen.

3.3 Randvoorwaarden

Om de configuraties in deze handleiding te kunnen implementeren, moet aan een aantal essentiële randvoorwaarden worden voldaan:

- U beschikt over een Microsoft 365 E3/E5 licentie of standalone Microsoft Defender for Endpoint licentie.
- U gebruikt een Windows 10/11 Enterprise omgeving.
- U gebruikt Microsoft Intune voor apparaatbeheer.
- U heeft voldoende beheerdersrechten voor configuratie.
- Er is netwerkconnectiviteit voor cloud-based bescherming.
- Alle Windows systemen zijn voorzien van de meest actuele updates.

Opmerking: Deze handleiding is specifiek gericht op systemen die zijn onboarded in Intune. Andere onboardingsopties bestaan, maar worden in dit document niet behandeld.

[2] Controleer of het gebruik van AI past binnen de wet- en regelgeving die van toepassing is

3.4 Raamwerken

Deze configuratiehandleiding is gebaseerd op erkende beveiligingsraamwerken en best practices om een effectieve en efficiënte implementatie van malwarebescherming te waarborgen. De richtlijnen en aanbevelingen in dit document maken gebruik van bewezen methodologieën om de beveiligingsstandaarden te optimaliseren en tegelijkertijd de operationele belasting te minimaliseren.

- Gebruik van Best Practices
- De implementatie van **Microsoft Defender for Endpoint** volgt de aanbevolen configuraties van verschillende beveiligingsstandaarden, waaronder:
- **Microsoft Security Baselines**: Deze baseline biedt een reeks aanbevolen instellingen voor Windows-beveiliging en endpointbescherming, waardoor organisaties eenvoudig een consistente beveiligingsaanpak kunnen hanteren.
- **Center for Internet Security (CIS) Benchmarks**: De configuraties in deze handleiding sluiten aan op CIS Benchmarks, een wereldwijd erkende standaard voor het veilig instellen van IT-systemen en software.
- **NIST Cybersecurity Framework**: Dit raamwerk biedt richtlijnen voor het identificeren, beschermen, detecteren, reageren en herstellen van cyberdreigingen. De aanbevelingen in dit document ondersteunen een defensieve strategie in lijn met NIST-richtlijnen.
- **Rijksoverheid BIO-normen**: Voor overheidsinstellingen worden de Baseline Informatiebeveiliging Overheid (BIO)-richtlijnen gevolgd, die eisen stellen aan IT-beveiliging en incidentrespons.

3.5 Hoe deze handleiding te gebruiken

Deze handleiding biedt een praktische aanpak voor het implementeren van malwarebescherming binnen uw organisatie op basis van Intune en Defender for Endpoint. Tijdens het uitvoeren van de stappen in dit document krijgt de organisatie toegang tot verschillende middelen. Hieronder volgt een overzicht van de behandelde onderdelen:

- **Onboarding naar Microsoft Defender for Endpoint via Intune:** Voor centraal beheer en real-time monitoring van apparaten.
- **Configuratie van real-time en cloudgebaseerde bescherming:** Voor proactieve detectie en blokkering van malwaredreigingen.
- **Implementatie van een uniforme antivirusbaseline:** Om consistente beveiligingsinstellingen over alle apparaten te waarborgen.
- **Activering van Attack Surface Reduction (ASR):** Om potentiële aanvalsvectoren te beperken en het risico op malware-infecties te verminderen.

De voorgestelde aanpassingen maken gebruik van bestaande middelen binnen uw organisatie. Hierdoor zijn deze stappen uitvoerbaar met beperkte inspanningen, terwijl u tegelijkertijd de weerbaarheid van uw IT-omgeving verbetert.

3.6 Aanbevelingen voor Voortdurende Beveiliging

Deze aanbevelingen zorgen voor een voortdurende versterking van uw beveiligingsstrategie door proactief beheer, het vergroten van beveiligingskennis, continue monitoring en het toevoegen van extra beveiligingslagen. De aanbevelingen voor voortdurende beveiliging:

- **Proactief Beheer:** Blijf proactief in uw cybersecuritystrategie door regelmatig beveiligingsupdates te implementeren.
- **Verhoog Beveiligingskennis:** Investeer in het vergroten van de beveiligingskennis binnen uw organisatie om bewustzijn en respons op dreigingen te verbeteren.
- **Monitor en Evalueer:** Gebruik de ingebouwde monitoring- en analysetools van Microsoft Defender for Endpoint om continu de effectiviteit van uw beveiligingsmaatregelen te evalueren en waar nodig aan te passen.
- **Breid Beveiligingsmaatregelen Uit:** Overweeg aanvullende beveiligingslagen, zoals netwerkbeveiliging en toegangsbeheer, om een holistische beveiligingsstrategie te waarborgen.

3.7 Volgende Stappen

Door de stappen in deze handleiding te volgen, legt uw organisatie een sterke basis voor effectieve malwarebescherming. Het is essentieel om deze maatregelen regelmatig te herzien en bij te werken in lijn met de evoluerende cyberdreigingen om de weerbaarheid van uw IT-infrastructuur te behouden en te versterken.

3.8 Leeswijzer

Dit document biedt een praktische handleiding voor de implementatie van Microsoft Defender for Endpoint en andere beveiligingsmaatregelen tegen malware.

Opbouw van het document:

- **Voorwoord & Inleiding:** Uitleg over de noodzaak van malwarebescherming en de rol van Microsoft Defender for Endpoint.
- **Initiële Setup & Configuratie:** Stap-voor-stap instructies voor de onboarding en basisconfiguratie.
- **Aanvullende Beveiligingsmaatregelen:** Instructies voor Attack Surface Reduction, logging en monitoring.
- **Logging & Monitoring:** Overzicht van hoe logs worden gegenereerd en geanalyseerd binnen Defender for Endpoint.

4. Initiële Setup & Configuratie Defender for Endpoint

In dit hoofdstuk wordt stap voor stap uitgelegd hoe **Microsoft Defender for Endpoint** correct wordt geïmplementeerd en geconfigureerd binnen de organisatie. De juiste setup is essentieel om endpoints effectief te beschermen tegen malware, ransomware en andere dreigingen. Hierdoor wordt de organisatie beter bestand tegen dreigingen en beschikt zij over de benodigde middelen die cruciaal zijn voor een effectief SOC.

De configuratie richt zich op:

- **Onboarding van apparaten** via Microsoft Intune om centraal beheer en monitoring mogelijk te maken.
- **Security Baseline Configuratie**, waarmee een gestandaardiseerde en veilige basis wordt gelegd voor endpointbeveiliging.
- **Instellingen voor antivirusbescherming**, zoals real-time scanning, cloud-delivered protection en geautomatiseerde bedreigingsdetectie.
- **Aanvullende beveiligingsmaatregelen**, zoals **Attack Surface Reduction (ASR)**, om risico's door schadelijke scripts en verdachte applicaties te minimaliseren.
- **Monitoring en beheer** via Microsoft Defender Portal, waarmee inzicht wordt verkregen in kwetsbaarheden en dreigingen binnen de IT-omgeving.

4.1 Microsoft Defender for Endpoint Onboarding

Om Microsoft Defender for Endpoint effectief te laten functioneren, moeten apparaten correct worden onboard. Dit proces zorgt ervoor dat endpoints worden opgenomen in de beveiligingsinfrastructuur en centraal beheerd kunnen worden. Tijdens de onboarding wordt de integratie met Microsoft Intune geconfigureerd, waardoor beleidsregels automatisch kunnen worden toegepast en monitoring direct beschikbaar is. Dit stelt organisaties in staat om real-time bedreigingsdetectie en geautomatiseerde responsmaatregelen in te schakelen.

Enable Intune and Microsoft Defender for Endpoint integration	
Configuratie-niveau	L1
Defender Portal	Settings > Endpoints > Advanced features
Aanbevolen configuratie	Microsoft Intune Connection Activeren
Toelichting	• Enable Microsoft Intune Connection: Deze instelling maakt het mogelijk om tussen Defender for Endpoint en Intune een verbinding te hebben.
Link naar documentatie	Enable Intune and Microsoft Defender for Endpoint integration

Navigatie: Intune (intune.microsoft.com) > Endpoint security > Endpoint detection and response > EDR Onboarding Status > Deploy preconfigured policy

Onboard Windows devices to Microsoft Defender for Endpoint	
Configuratie-niveau	L1
Intune	Endpoint security > Endpoint detection and response > EDR Onboarding Status > Deploy preconfigured policy > Windows
Aanbevolen configuratie	Microsoft Intune Connection Activeren
Toelichting	• Review and create policy to deploy defender for endpoint to all devices: Deze stap zorgt ervoor dat alle Windows apparaten binnen Intune automatisch zullen worden uitgerold met Defender for Endpoint.
Link naar documentatie	Onboard Windows devices

4.2 Security Baseline Configuratie

Een security baseline biedt een gestandaardiseerde set beveiligingsinstellingen die als uitgangspunt dient voor endpointbeveiliging. Door een baseline toe te passen, wordt een uniforme beveiligingsstandaard afgedwongen over alle apparaten binnen de organisatie. Dit minimaliseert risico's door consistente instellingen voor malwarebescherming, toegangsbeheer en systeemintegriteit te garanderen. De baseline helpt ook bij compliance met best practices zoals Microsoft Security Baselines en CIS Benchmarks.

Security Baseline Configuratie	
Configuratie-niveau	L1
Intune	Endpoint security > Security baselines > Microsoft Defender for Endpoint Baseline.
Aanbevolen configuratie	Microsoft Security Baseline definiëren
Toelichting	Een gestandaardiseerde baseline verzekert consistente beveiliging: • Voorgedefinieerde beveiligingsinstellingen • Compliance met best practices • Eenvoudig beheer en monitoring • Uniform beveiligingsniveau
Link naar documentatie	Microsoft Security Baselines Configuratie

4.3 Basis Antivirus Instellingen

Een goed geconfigureerde antivirusoplossing is essentieel voor het beschermen van endpoints tegen malware en andere dreigingen. In deze sectie worden de belangrijkste instellingen van Microsoft Defender Antivirus behandeld, die bijdragen aan een sterke verdedigingslijn tegen cyberaanvallen.

Navigatie: Intune (intune.microsoft.com) > Endpoint security > Manage > Antivirus

1. Maak een nieuwe policy aan of bewerk een bestaande policy.
2. Kies onder het tabblad "Settings" de sectie "Microsoft Defender Antivirus"
3. **Belangrijk:** Alle onderstaande instellingen (met uitzondering van Tamper Protection & Scan Configuraties) kunnen en moeten in één policy worden geconfigureerd. Plan de configuratie van deze instellingen als één geheel om een consistente beveiliging te waarborgen. Voor Tamper Protection moet een policy worden aangemaakt met als profiel "Windows Security Experience". Voor de Scan configuraties is een tweede policy nodig voor wekelijkse scans.

Real-time Monitoring	
Configuratie-niveau	L1
Intune	Endpoint security > Manage > Antivirus > Add/Edit Policy
Aanbevolen configuratie	Ingeschakeld
Toelichting	• Allow Real-time Monitoring Schakelt real-time monitoring van bestanden en processen in om malware te detecteren bij toegang of uitvoering.
Link naar documentatie	Real-Time Protection

Behaviour Monitoring	
Configuratie-niveau	L1
Intune	Endpoint security > Manage > Antivirus > Add/Edit Policy
Aanbevolen configuratie	Ingeschakeld
Toelichting	• Allow Behavior Monitoring Monitort het gedrag van processen en applicaties op verdachte activiteiten, die afwijken van de gebruikelijke patronen.
Link naar documentatie	Behaviour Monitoring

On Access Protection	
Configuratie-niveau	L2
Intune	Endpoint security > Manage > Antivirus > Add/Edit Policy
Aanbevolen configuratie	Ingeschakeld
Toelichting	• Allow On Access Protection Zorgt voor directe scanning van bestanden zodra ze worden geopend of uitgevoerd, waardoor malware in real-time wordt tegengehouden.
Link naar documentatie	On Access Protection

Cloud-delivered Protection	
Configuratie-niveau	L2
Intune	Endpoint security > Manage > Antivirus > Add/Edit Policy
Aanbevolen configuratie	Ingeschakeld
Toelichting	• Allow Cloud Protection

Cloud-delivered Protection	
	Cloud-delivered protection gebruikt Microsoft's wereldwijde sensornetwerk om nieuwe dreigingen snel te identificeren en te blokkeren.
Link naar documentatie	Cloud-Delivered Protection

Scan Configuraties	
Configuratie-niveau	L2
Intune	Endpoint security > Manage > Antivirus > Add/Edit Policy
Aanbevolen configuratie	Dagelijkse quick scan, Wekelijkse volledige scan (tweede policy voor wekelijkse scan)
Toelichting	Gestructureerde scanning is essentieel voor het detecteren van malware: • Quick scan: Dagelijks op rustige tijden (bv. lunchpauze) • Enable scheduled scan: Yes • Full scan: Wekelijks tijdens off-peak uren (Tweede policy) • Scan during suspicious activity: Direct en automatisch
Link naar documentatie	Quick Scan

Automatic Sample Submission	
Configuratie-niveau	L2
Intune	Endpoint security > Manage > Antivirus > Add/Edit Policy
Aanbevolen configuratie	Ingeschakeld op automatisch verzenden
Toelichting	• Submit Samples Consent Deze instellingen zorgen voor verbeterde bescherming door gebruik te maken van Microsoft's cloud-analyse capaciteiten.
Link naar documentatie	Automatic Sample Submission

Balanced mode for Performance Impact Management	
Configuratie-niveau	L4
Intune	Endpoint security > Manage > Antivirus > Add/Edit Policy
Aanbevolen configuratie	Gebalanceerde modus
Toelichting	Optimalisatie van systeem performance tijdens security operaties: • CPU-throttling tijdens actief gebruik • Scan scheduling tijdens inactieve periodes • Geleidelijke uitrol van updates • Resource-monitoring tijdens scans
Link naar documentatie	Scan performance settings

Controlled Folder Access Configuratie	
Configuratie-niveau	L3
Intune	Endpoint security > Manage > Antivirus > Add/Edit Policy
Aanbevolen configuratie	Ingeschakeld met standaard beschermde mappen
Toelichting	Beschermt tegen ransomware en ongeautoriseerde bestandswijzigingen: • Bescherming van systeem- en gebruikersmappen • Whitelist voor vertrouwde applicaties

Controlled Folder Access Configuratie	
	• Monitoring van toegangspogingen • Aanpasbare mapbescherming
Link naar documentatie	Enable Controlled Folder Access

Navigatie: Intune (intune.microsoft.com) > Endpoint security > Manage > Antivirus

1. Maak een nieuwe policy aan of bewerk een bestaande policy.
2. Kies onder het tabblad "Settings" de sectie "Windows Security Experience"

Tamper Protection	
Configuratie-niveau	L2
Intune	Endpoint security > Manage > Antivirus > Add/Edit Policy
Aanbevolen configuratie	Ingeschakeld
Toelichting	• Enable Tamper Protection: Voorkomt dat malware beveiligingsinstellingen kan uitschakelen of modificeren. Het is cruciaal voor het behoud van de integriteit van de beveiligingsmaatregelen.
Link naar documentatie	Tamper Protection

4.4 Aanvullende Beveiligingsfuncties (Attack Surface Reduction)

Attack Surface Reduction (ASR)-regels zijn beveiligingsmaatregelen binnen Microsoft Defender for Endpoint die ontworpen zijn om het aanvalsoppervlak van een organisatie te verkleinen. ASR voorkomt dat veelvoorkomende aanvalstechnieken worden misbruikt, zoals schadelijke macro's, onveilige scripts en ongewenste procesaanroepen. **Hoewel** de Attack Surface Reduction (ASR)-regels een sterke basis vormen voor beveiliging, is het belangrijk om te beseffen dat de impact van deze regels per organisatie kan verschillen. De standaardinstellingen in deze handleiding bieden een richtlijn voor het minimaliseren van risico's, maar niet alle regels zijn in elke omgeving direct toepasbaar zonder uitzonderingen.

Centrale locatie voor Attack Surface Reduction (ASR) regels:

1. **Navigatie:** Intune (intune.microsoft.com) > Endpoint security > Manage > Attack surface reduction
2. Maak een nieuwe policy aan of bewerk een bestaande policy.
3. **Belangrijk:** Alle ASR-regels kunnen binnen één policy worden geconfigureerd. Elke organisatie heeft unieke processen en applicaties die mogelijk worden beïnvloed door bepaalde ASR-regels. Het is daarom essentieel om vooraf een grondige analyse uit te voeren en **AUDIT-modus** te gebruiken om inzicht te krijgen in de impact.

Block Executable Content from Email and Webmail	
Configuratie-niveau	L4
Intune	Endpoint security > Manage > Attack surface reduction > Policy
Aanbevolen Configuratie	Ingeschakeld op block modus.
Toelichting	• Block executable content from email and webmail: Blokkeert uitvoerbare bestanden uit e-mails en webmail om te voorkomen dat gebruikers per ongeluk schadelijke bijlagen openen, een veelgebruikte aanvalsmethode.
Link naar documentatie	Attack Surface Reduction Rules

Block Execution of Potentially Obfuscated Scripts	
Configuratie-niveau	L4
Intune	Endpoint security > Manage > Attack surface reduction > Policy
Aanbevolen Configuratie	Ingeschakeld
Toelichting	• Block execution of potentially obfuscated scripts: Blokkeert scripts die zijn verhuld of versleuteld om detectie te ontwijken. Dit voorkomt dat aanvallers via scripts schadelijke acties kunnen uitvoeren.
Link naar documentatie	Attack Surface Reduction Rules

Block JavaScript or VBScript from Launching Downloaded Executable Content	
Configuratie-niveau	L5
Intune	Endpoint security > Manage > Attack surface reduction > Policy
Aanbevolen Configuratie	Ingeschakeld
Toelichting	• Block JavaScript or VBScript from launching downloaded executable content: Blokkeert scripts zoals JavaScript en VBScript die vaak worden gebruikt om malware bij gedownloade bestanden te starten.
Link naar documentatie	Attack Surface Reduction Rules

Use Advanced Ransomware Protection	
Configuratie-niveau	L5
Intune	Endpoint security > Manage > Attack surface reduction > Policy
Aanbevolen Configuratie	Ingeschakeld
Toelichting	• Use advanced ransomware protection Schakelt geavanceerde bescherming in tegen ransomware om te voorkomen dat bestanden worden versleuteld door aanvallers.
Link naar documentatie	Attack Surface Reduction Rules

Block All Office Applications from Creating Child Processes	
Configuratie-niveau	L5
Intune	Endpoint security > Manage > Attack surface reduction > Policy
Aanbevolen Configuratie	Ingeschakeld
Toelichting	• Block all Office applications from creating child processes Blokkeert het gedrag waarbij Office-toepassingen nieuwe processen starten, wat vaak wordt misbruikt door macrogebaseerde aanvallen.
Link naar documentatie	Attack Surface Reduction Rules

Block Office Applications from Injecting Code into other Processes	
Configuratie-niveau	L5
Intune	Endpoint security > Manage > Attack surface reduction > Policy
Aanbevolen Configuratie	Ingeschakeld
Toelichting	• Block Office applications from injecting code into other processes Voorkomt dat aanvallers via Office-toepassingen kwaadaardige code injecteren in andere processen om toegang te krijgen tot het systeem.
Link naar documentatie	Attack Surface Reduction Rules

Block Win32 API Calls from Office Macros	
Configuratie-niveau	L3
Intune	Endpoint security > Manage > Attack surface reduction > Policy
Aanbevolen Configuratie	Ingeschakeld
Toelichting	• Block Win32 API calls from Office macros: Blokkeert toegang tot systeem-API's vanuit Office-macro's, die vaak worden gebruikt voor het uitvoeren van schadelijke acties.
Link naar documentatie	Attack Surface Reduction Rules

Block Untrusted and Unsigned Processes Running from USB	
Configuratie-niveau	L3
Intune	Endpoint security > Manage > Attack surface reduction > Policy
Aanbevolen Configuratie	Ingeschakeld
Toelichting	• Block untrusted and unsigned processes running from USB: Blokkeert het uitvoeren van niet-vertrouwde processen vanaf USB-opslag, een veelgebruikte vector voor het verspreiden van malware.
Link naar documentatie	Attack Surface Reduction Rules

Block Process Creation from PSExec and WMI Commands	
Configuratie-niveau	L3
Intune	Endpoint security > Manage > Attack surface reduction > Policy
Aanbevolen Configuratie	Ingeschakeld
Toelichting	• Block process creation from PSExec and WMI commands: Blokkeert processen die ontstaan via PSExec- en WMI-opdrachten, tools die vaak worden misbruikt bij laterale beweging door aanvallers.
Link naar documentatie	Attack Surface Reduction Rules

Prevent Credential Theft from LSASS	
Configuratie-niveau	L3
Intune	Endpoint security > Manage > Attack surface reduction > Policy
Aanbevolen Configuratie	Ingeschakeld
Toelichting	• Prevent credential theft from LSASS: Blokkeert toegang tot de Local Security Authority Subsystem (LSASS) om te voorkomen dat wachtwoorden en inloggegevens worden gestolen.
Link naar documentatie	Attack Surface Reduction Rules

4.5 Monitoring en Beheer

Effectieve monitoring en beheer zijn cruciaal om de beveiligingsstatus van endpoints continu te bewaken en snel te reageren op dreigingen. In deze sectie wordt uitgelegd hoe Microsoft Defender for Endpoint geavanceerde inzichten biedt in kwetsbaarheden en beveiligingsincidenten.

Centrale locatie voor monitoring functionaliteiten:
Microsoft Defender Portal (security.microsoft.com)

Navigatie Threat & Vulnerability Management:
Microsoft Defender Portal (security.microsoft.com) > Endpoints > Vulnerability Management

Belangrijk: Deze monitoring tools zijn direct toegankelijk na implementatie van Microsoft Defender for Endpoint en vereisen geen additionele configuratie in Intune.

Threat & Vulnerability Management (TVM)	
Configuratie-niveau	L4
Defender Portal	Endpoints > Vulnerability Management
Aanbevolen configuratie	Actieve monitoring
Toelichting	TVM biedt essentieel inzicht in kwetsbaarheden: • Risicobeoordeling van apparaten • Prioritering van beveiligingsacties • Concrete aanbevelingen • Exposure score monitoring
Link naar documentatie	Threat & Vulnerability Management

Regular review of Microsoft Secure Score	
Configuratie-niveau	L4
Defender Portal	Home (Dashboard) > Microsoft Secure Score
Aanbevolen configuratie	Regelmatige review
Toelichting	Secure Score helpt bij het verbeteren van de beveiligingspositie: • Algemene Beveiliging score • Vergelijking met industrie benchmarks • Concrete verbetervoorstellen • Prioritering van acties
Link naar documentatie	Microsoft Secure Score

5. Logging van Malwarebescherming

Microsoft Defender for Endpoint is ontworpen met ingebouwde, uitgebreide logging, waardoor er geen extra configuratiestappen nodig zijn om de beschreven beveiligingsonderdelen te monitoren. Alle relevante gebeurtenissen, zoals malware-detecties, blokkades, wijzigingen in configuratie, en activiteiten van de verschillende beveiligingsfuncties (real-time bescherming, Attack Surface Reduction, Controlled Folder Access, etc.), worden automatisch gelogd. Deze logs zijn centraal toegankelijk via het Microsoft Defender portaal (security.microsoft.com).

5.1 Specifieke locaties voor logging:

- **Alerts (Incidents):** De meeste detecties en geblokkeerde acties verschijnen als *alerts* en zijn te vinden onder (*Incidents & alerts* > *Incidents*). Hier vind je een overzicht van alle gedetecteerde dreigingen, met details over wat er is gebeurd, wanneer en op welk apparaat.
- **Geavanceerd Opsporen:** Voor diepere analyse kun je gebruikmaken van (*Hunting* > *Advanced hunting*). Hier kun je op maat gemaakte query's uitvoeren op alle ruwe data van Defender for Endpoint, om te onderzoeken wat er in je omgeving heeft plaatsgevonden.
- **Apparaat tijdlijn:** Voor een overzicht van gebeurtenissen op een specifiek apparaat, ga je naar **Assets > Devices**. Selecteer het betreffende apparaat en ga naar het tabblad *Timeline*. Hier vind je een chronologische weergave van gebeurtenissen op dat apparaat.
- **Rapportages:** Defender for Endpoint biedt ook rapportages om de beveiligingsstatus inzichtelijk te maken. Deze vind je onder *Reports*. Rapporten zijn bijvoorbeeld beschikbaar over 'Security Posture', 'Apparaatbeveiliging', 'Dreigingen en Kwetsbaarheden' (*"Security Posture", "Device security", and "Threats and Vulnerabilities"*).

Deze logging maakt het mogelijk voor IT-beheerders om de effectiviteit van de ingestelde beveiligingsmaatregelen te beoordelen, verdachte activiteiten te analyseren en adequaat te reageren op dreigingen.

Bijlage I – Configuratiestatus checklist

Level	Configuration Control	Status
L1	Enable Intune and Microsoft Defender For Endpoint integration (H 4.1)	
	Onboard Windows devices to Defender for Endpoint (H 4.1)	
	Security Baseline Configuration (H 4.2)	
	Real-time monitoring (H 4.3)	
	Behavior monitoring (H 4.3)	
L2	On-access protection (H 4.3)	
	Cloud-delivered protection (H 4.3)	
	Tamper protection (H 4.3)	
	Scan Configuration (H 4.3)	
	Automatic sample submission (H 4.3)	
L3	Controlled Folder Access Configuration (H 4.3)	
	Block Win32 API calls from Office macros (H 4.4)	
	Block Untrusted and Unsigned Processes Running from USB (H 4.4)	
	Block Process Creation via PSExec and WMI Commands (H 4.4)	
	Prevent Credential Theft from LSASS (H 4.4)	
L4	Threat & Vulnerability Management (TVM) (H 4.5)	
	Regular review of Microsoft Secure Score (H 4.5)	
	Balanced mode for Performance Impact Management (H 4.3)	
	Block Executable Content from Email and Webmail (H 4.4)	
	Block Execution of Potentially Obfuscated Scripts (H 4.4)	
L5	Block JavaScript or VBScript when Launching Downloaded Executable Content (H 4.4)	
	Use Advanced Ransomware Protection (H 4.4)	
	Block all Office Applications from Creating Child Processes (H 4.4)	
	Block Office Applications from Injecting Code into other Processes (H 4.4)	

Uitgave

Versterken SOC Stelsel Rijk (VSSR)

Postbus 117, 2501 CC Den Haag

Turfmarkt 147, 2511 DP Den Haag

070 751 5555

Meer informatie

https://www.ncsc.nl/vssr

info@ncsc.nl

vssr.info@minjenv.nl (Rijksoverheid)

Maart 2025