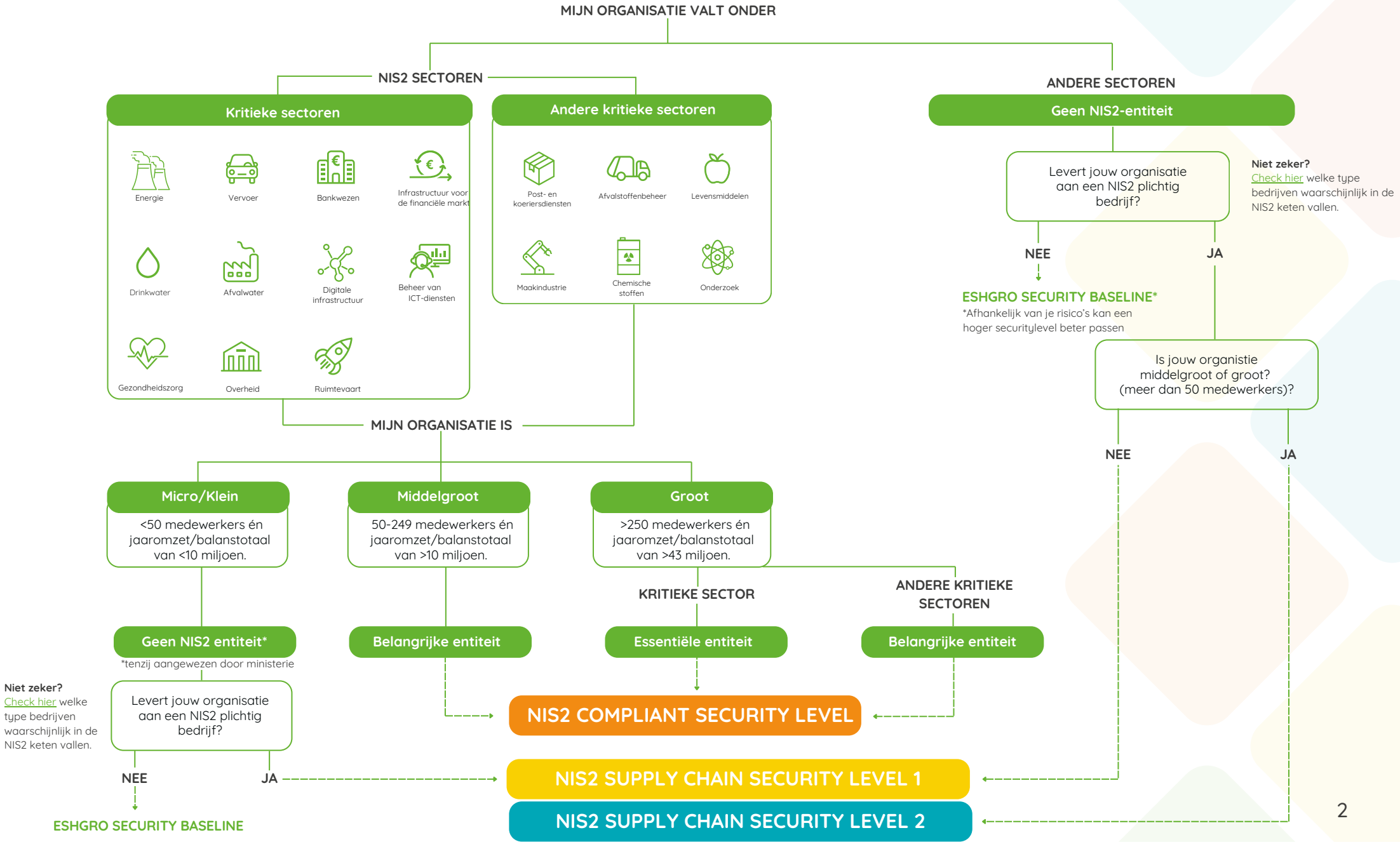
eshgro

Eshgro Security Levels

Jouw organisatie veiliger met onze security-oplossingen

Welke security oplossing past bij jouw organisatie?

NIS2 stelt strengere eisen aan IT-beveiliging en ketenverantwoordelijkheid. **Eshgro biedt 4 security levels, van basisbeveiliging tot volledige NIS2-compliance. Gebruik de onderstaande beslisboom om te zien welk niveau bij jouw organisatie past.** Meer weten over NIS2? Bekijk onze NIS2 whitepaper.



Overzicht van de Eshgro security levels

Eshgro biedt vier security levels, afhankelijk van de risico's en compliance-eisen van jouw organisatie.

Minimale beveiliging, verplicht voor alle klanten

Eshgro Security Baseline

Onze Security Baseline biedt een solide basisbeveiliging die noodzakelijk is voor een veilige IT-omgeving. Dit pakket bevat de essentiële beveiligingsmaatregelen die de eerste verdedigingslinie vormen tegen cyberaanvallen en datalekken. Het helpt bedrijven bij het beschermen van gebruikers, endpoints en cloud-omgevingen tegen phishing, malware en andere bedreigingen.

Waarom deze update?

Zoals eerder gecommuniceerd, is deze baseline noodzakelijk vanwege de toenemende cyberdreigingen en de wettelijke verplichtingen onder NIS2. Daarnaast hebben MSP's onder NIS2 een zorgplicht en kunnen we aansprakelijk worden gesteld bij gebrekkige beveiliging. Dit pakket waarborgt de minimale securitystandaarden.

Voor ketenverantwoordelijkheid

NIS2 Supply Chain Security Level 1

Dit level is speciaal ontworpen voor (kleinere) organisaties die **actief zijn in een keten met NIS2-plichtige bedrijven** en daarom extra beveiligingsmaatregelen moeten treffen. Level 1 biedt een verhoogde beveiliging voor identiteiten, communicatie en bedrijfsgegevens, en helpt organisaties om compliant te blijven met de nieuwste regelgeving.

Waarom belangrijk?

Ketenverantwoordelijkheid speelt een grote rol en bedrijven worden verplicht hun beveiliging op orde te hebben om risico's binnen de toeleveringsketen te beperken. Dit level helpt bedrijven om hun digitale weerbaarheid te vergroten en aan de wettelijke eisen te voldoen.

Voor verhoogde ketenrisico's

NIS2 Supply Chain Security Level 2

Voor organisaties die een verhoogd risico lopen binnen de keten, biedt dit pakket nog uitgebreidere beveiligings-maatregelen en diepgaande risicoanalyses. Dit level is ideaal voor bedrijven die te maken hebben met gevoelige data en uitgebreide compliance-eisen.

Waarom extra bescherming?

Wetgeving richt zich steeds meer op ketenrisico's. Dit level geeft bedrijven niet alleen geavanceerde tools en inzichten om kwetsbaarheden te identificeren en te minimaliseren, Bovendien kan een NIS2 Compliant keurmerk verkregen worden, wat extra zekerheid biedt binnen de keten.

Voor volledige NIS2-compliance

NIS2 Compliant Security Level

Voor organisaties die direct onder de NIS2-regelgeving vallen en een maximale beveiligingsaanpak nodig hebben, biedt dit level de meest uitgebreide bescherming en compliance-ondersteuning.

Waarom dit niveau?

Organisaties die onder de NIS2-verordening vallen, kunnen met dit pakket niet alleen de maximale beveiligingsstandaarden behalen en risico's minimaliseren, maar ook besparen op hun cybersecurityverzekering. Daarnaast biedt dit level de mogelijkheid om een NIS2 Compliant certificaat te verkrijgen, wat extra zekerheid biedt binnen de keten. Dit level zorgt ervoor dat jouw organisatie volledig compliant is en optimaal beveiligd blijft.

Ontdek hier (SamenDigitaalVeilig) of jouw bedrijf tot één van de veelvoud aan typen bedrijven behoort die indirect met NIS2 te maken krijgen als leverancier

Meer weten over de volledige invulling van de Security Levels ?

Bekijk de levels op onze website

Wat zit er in de Eshgro security levels?

Onderstaand vind je een overzicht van de securitypakketten en hun bijbehorende diensten. Elk niveau bouwt voort op het vorige en biedt steeds uitgebreidere beveiligingsmaatregelen om aan de eisen van NIS2 en de toenemende cyberdreigingen te voldoen.

De Microsoft Licentie is de minimaal benodigde licentie voor het security level, de Microsoft licenties zijn niet inbegrepen in de prijs

Minimale beveiliging, verplicht voor alle klanten

Eshgro Security Baseline

- **Microsoft Business Premium**
  Inclusief MFA, dataclassificatie en beveiligingsbeheer binnen Microsoft 365.
- **Eshgro Managed Detection & Response (MDR) Bundel 1**
  24/7 monitoring, dreigingsdetectie en basisincidentrespons.
- **Security Standard+**
  Basisbescherming tegen malware, phishing en datalekken, met focus op identiteiten en endpoints.
- **Immutable Back-up**
  Geïsoleerde back-upoplossing ter bescherming tegen ransomware en dataverlies.

Voor ketenverantwoordelijkheid

NIS2 Supply Chain Security Level 1

- **Alles uit de Security Baseline, plus:**
- **Microsoft Business Premium**
  Inclusief MFA, dataclassificatie en beveiligingsbeheer binnen Microsoft 365.
- **Eshgro Managed Detection & Response (MDR) Bundel 2**
  Geavanceerde dreigingsanalyse en cloud security bescherming.
- **Managed Awareness Training**
  Doorlopende security-trainingen en phishing-tests voor medewerkers.
- **E-mailbeveiliging (DMARC, DKIM, DANE)**
  Voorkomt spoofing, phishing en misbruik van e-maildomeinen.
- **Bedrijfsspecifieke risico-analyse**
  Identificeert en beoordeelt specifieke kwetsbaarheden binnen de IT-omgeving.
- **Maandelijkse rapportages + jaarlijks security-overleg**
  Inzicht in beveiligingsstatus en risico's.

Voor verhoogde ketenrisico's

NIS2 Supply Chain Security Level 2

- **Alles uit Level 1, plus:**
- **Microsoft E3 licentie**
  Uitgebreidere beveiligings- en compliance-functionaliteiten.
- **Security Advanced**
  Inclusief dreigingsanalyse, Shadow IT-detectie en geautomatiseerd risicobeheer.
- **Extended rapportages en risicobeoordeling**
  Kwartaalrapportages met diepgaande analyses en verbeteradviezen.
- **Optioneel: NIS 2.0 keurmerk**
  Aantoonbare compliance-oplossing voor bedrijven onder de NIS2-verordening.

Voor volledige NIS2-compliance

NIS2 Compliant Security Level

- **Alles uit Level 2, plus:**
- **Microsoft E3 + E5 Security**
  Volledige bescherming voor identiteiten, data en netwerken.
- **Security Advanced+**
  Dynamisch toegangsbeheer, Risk-Based Conditional Access en Insider Risk Management.
- **Incident Response Plan & Business Impact Analyse**
  Beheer en mitigatie van cyberdreigingen en crises.Voorkomt spoofing, phishing en misbruik van e-maildomeinen.
- **Disaster Recovery Plan & Simulatie**
  Herstelscenario's en realistische tests voor cyberincidenten.
- **Pentesting**
  Simulatie van cyberaanvallen om kwetsbaarheden bloot te leggen en proactieve verbeteringen door te voeren.

Uitgebreide beschrijving van de security-diensten

Om organisaties te helpen voldoen aan de steeds strenger wordende beveiligingseisen, zoals NIS 2.0, hebben wij de vereisten vertaald naar concrete en kant-en-klare diensten. Dit betekent dat bedrijven zich geen zorgen hoeven te maken over de complexe wetgeving en technische implementaties: wij bieden direct toepasbare oplossingen die voldoen aan de hoogste beveiligingsstandaarden. Hieronder vind je een overzicht van de beveiligingsdiensten die deel uitmaken van onze pakketten en hoe deze jouw organisatie beschermen.

Op de volgende pagina's vind je een gedetailleerd overzicht van alle securitydiensten die deel uitmaken van onze pakketten en hoe deze bijdragen aan een sterke en weerbare IT-omgeving.

➡ Bekijk de inhoudsopgave op de volgende pagina om direct naar de beschrijving van een specifieke dienst te navigeren!

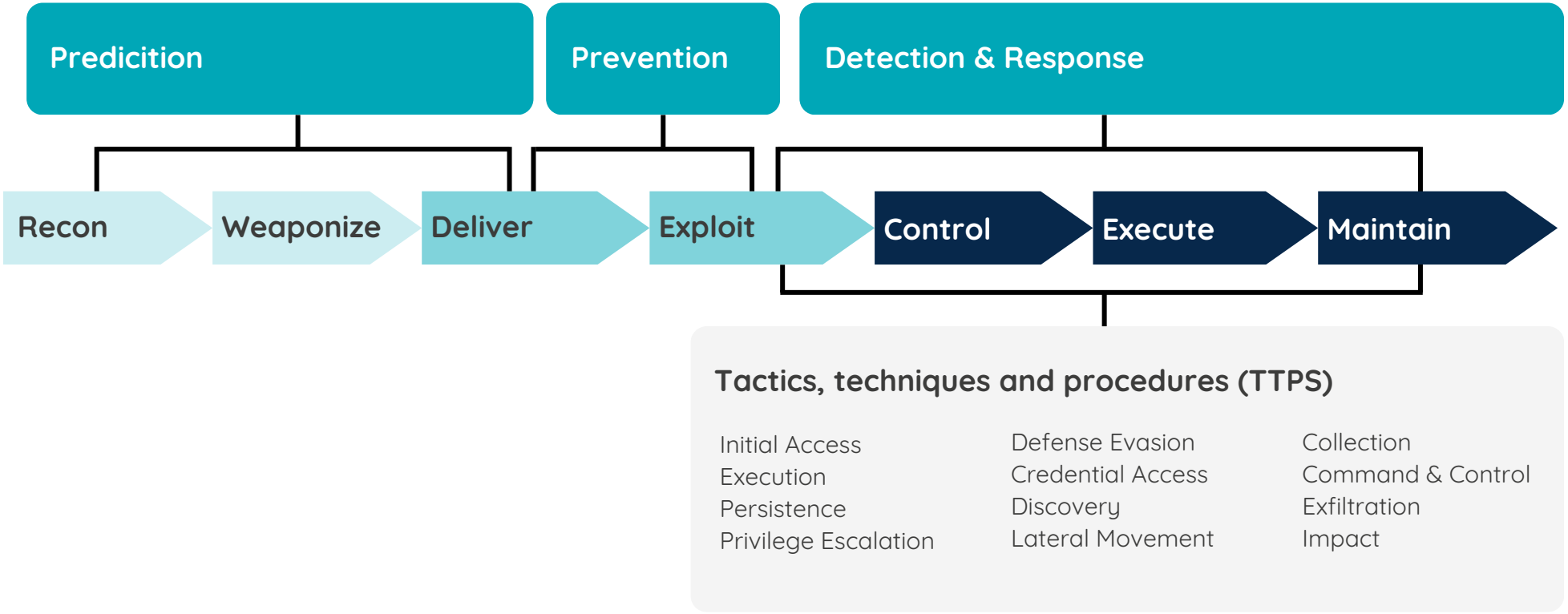
Inhoudsopgave dienstomschrijving

Eshgro Managed Detection & Response (MDR) Bundel 1 & 2

Eshgro Managed Detection & Response (MDR) is een volledig beheerde security-oplossing die proactief cyberdreigingen detecteert, analyseert en neutraliseert.
De dienst is beschikbaar in twee bundels, afhankelijk van de beveiligingsbehoefte van jouw organisatie:

Functionaliteit	MDR bundel 1 (basisbeveiliging)	MDR bundel 2 (uitgebreide beveiliging)
24/7 Monitoring en threat detection	✓ Servers, devices, netwerkactiviteiten, identiteiten (Microsoft Entra ID)	✓ Servers, devices, netwerk, cloud, identiteiten, User & Entity Behavior Monitoring
Incident response & containment	✓ Realtime detectie en actie bij incidenten	✓ Uitgebreidere response, inclusief forensische analyse
Exposure management (kwetsbaarheden identificeren)	✗	✓ Detectie van zwakke plekken in servers, applicaties en identiteiten
Collaboration protection (Microsoft 365 beveiliging)	✗	✓ Outlook, Teams, SharePoint, OneDrive beveiliging
Mobile protection (beveiliging voor mobiele apparaten)	✗	✓ Detectie van dreigingen op mobiele devices (iOS & Android)
Vulnerability management (beperken van zwakke plekken in systemen)	✗	✓ Automatische detectie van ontbrekende patches en kwetsbaarheden op servers, endpoints en cloudomgevingen
Cloud Security Posture Management	✗	✓ Security monitoring voor cloud-omgevingen en applicaties

Om aanvallen effectief te bestrijden, maakt Eshgro MDR gebruik van het MITRE ATT&CK-framework. Dit model brengt in kaart hoe hackers te werk gaan, van het eerste verkennen van een doelwit tot het buitmaken van gegevens of het verstoren van systemen. Door deze inzichten te combineren met een proactieve beveiligingsstrategie, helpt Eshgro MDR organisaties om aanvallen sneller te detecteren en direct te neutraliseren.



Eshgro MDR bestrijdt dreigingen in drie fases:

- Prediction (Voorspellen) – Voorkomen dat aanvallers zwakke plekken kunnen misbruiken.
- Prevention (Voorkomen) – Beperken van aanvalsmogelijkheden door beveiligingsmaatregelen.
- Detection & Response (Detectie & Reactie) – Real-time detectie en actie bij dreigingen.

Security Standard+, Advanced & Advanced+

Onze securitypakketten zijn ontwikkeld op basis van de Microsoft Security Baseline, een set van essentiële beveiligingsmaatregelen die organisaties beschermen tegen veelvoorkomende cyberdreigingen. Afhankelijk van de complexiteit en risico's binnen jouw organisatie bieden wij drie securityniveaus: Security Standard +, Securtiy Advanced en Security Advanced+.

- **Security Standard+** is gebaseerd op Microsoft Business Premium en biedt een solide basisbeveiliging voor identiteiten, endpoints en e-mail.
- **Security Advanced** vereist Microsoft E3 en breidt de beveiliging uit met geavanceerde detectie- en beschermingsmechanismen, zoals exploit-preventie en Shadow IT-detectie.
- **Security Advanced+** vereist Microsoft E3 + E5 Security en biedt maximale bescherming met geautomatiseerd risicobeheer, insider risk management en geavanceerde compliance-functionaliteiten.

Security Standard+	Security Advanced	Security Advanced+
Message Encryption	Alles uit Standard +	Alles uit Standard + & Advanced
Azure Information Protection Plan 1	Endpoint Analytics	App Governance
BitLocker	Password policy	Defender for Cloud Apps
Conditional Access	Wachtwoord Hash Synchronisatie	DLP Teams
Defender Anti-Malware	Autopilot	Endpoint DLP
Defender Firewall	Anti-Phishing	Risk-based Conditional Access / Identity Protection
DLP Emails & Files	Anti-Spam	Azure Information Protection Plan 2*
MFA	Anti-malware	Advanced Message Encryption
Self-service password reset	Safe Attachments en Safe Links	Automatic Sensitivity Labels*
Windows Hello for Business	Defender Exploit Guard	Access Reviews
Windows Information Protection	Advanced Security Reports	Entitlement Management
Manual Sensitivity Labels	Advanced Threat Analytics	Privileged Access Management
Break the Glass Accounts	Defender for Cloud Apps Discovery	Sensitivity Label Classifiers*
Secure Browser	Sensitivity labels for Containers	Privileged Identity Management*
	Microsoft Defender Vulnerability Management*	Microsoft Purview Insider Risk Management*
		Adaptive Protection*
		Communication Compliance*
		Information Barriers*
		Microsoft 365 E5 eDiscovery and Audit
		10-year Audit Log Retention*

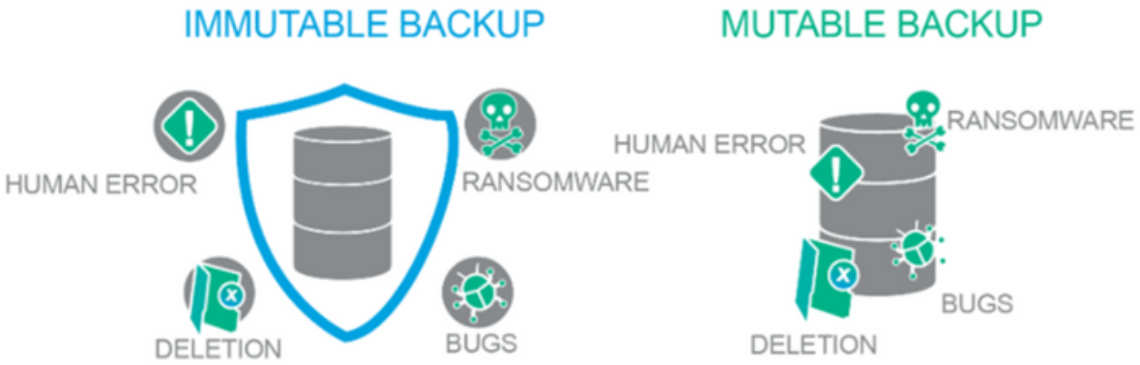
***Beschikbaar als add-on**

Eshgro Immutable Back-up

Immutable Back-up zorgt ervoor dat je gegevens niet kunnen worden aangepast, overschreven of verwijderd door kwaadwillenden. Door een air-gapped opslag en encryptie blijven je back-ups volledig onaantastbaar, waardoor ransomware en dataverlies effectief worden tegengegaan.

Waarom Immutable?

Een traditionele back-up kan nog steeds worden gewijzigd of verwijderd door cybercriminelen. Immutable back-ups daarentegen kunnen niet worden aangepast, overschreven of verwijderd, waardoor ze een essentiële verdedigingslaag vormen tegen ransomware en dataverlies.



Managed Awareness Training

Mensen vormen nog altijd de zwakste schakel in cybersecurity. Onze (Managed) Awareness Training helpt medewerkers om bewust en veilig om te gaan met digitale dreigingen.

Wat is Managed Awareness Training?

Het programma is ontworpen om medewerkers continu op de hoogte te houden van de nieuwste bedreigingen en hen regelmatig te testen. De kracht van ons programma ligt in de combinatie van herhaling, praktijkgerichte trainingen en continue monitoring.

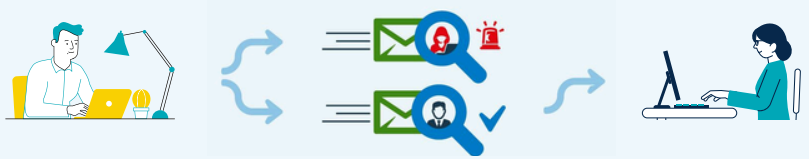
Belangrijke onderdelen van het programma:

- **Fysieke trainingen op locatie:** Jaarlijks komen onze security consultants bij jouw bedrijf langs om de nieuwste ontwikkelingen en risico's te bespreken in een interactieve training.
- **Online trainingen en simulaties:** Door het jaar heen hebben medewerkers toegang tot flexibele online trainingen en phishing-simulaties om hun vaardigheden up-to-date te houden.
- **Phishing-campagnes en Mystery Visits:** Maandelijks voeren we phishing-campagnes uit en kunnen we op aanvraag mystery visits organiseren om het bewustzijn van fysieke beveiliging te testen.

E-mailbeveiliging (DMARC, DKIM, DANE)

E-mail blijft een van de grootste aanvalsvectoren voor cybercriminelen. Onze e-mailbeveiliging beschermt je organisatie tegen spoofing, phishing en misbruik van je domeinnaam. Door middel van DMARC, DKIM en DANE wordt e-mailverkeer geauthenticeerd en beveiligd, waardoor je communicatie betrouwbaar blijft.

SPF

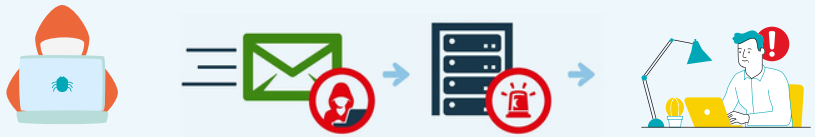


SPF voorkomt dat iemand in naam van jouw organisatie een e-mail kan sturen. SPF controleert de afzender van een e-mail op echtheid.

DKIM

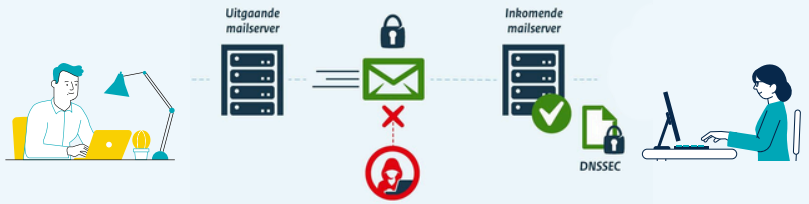
DKIM voorkomt vervalising van e-mail. Als iemand knoeit met de inhoud van een e-mail, detecteert DKIM dat.

DMARC



DMARC vertelt jouw e-mailserver wat hij moet doen als hij een verdachte e-mail ontvangt.
Ook zorgt DMARC ervoor dat jouw organisatie informatie krijgt over vervalste e-mails die in jouw naam verstuurd is.

STARTTLS & DANE



STARTTLS zorgt voor een beveiligde verbinding tussen verzendende en ontvangende mailserver. DANE dwingt STARTTLS af en geeft zekerheid over de identiteit van de ontvangende mailserver. DNSSEC waarborgt in deze keten de echtheid van DANE.

Bedrijfsspecifieke risico-analyse

Elke organisatie heeft unieke dreigingen en kwetsbaarheden. Een consultant van Audit Connect voert een bedrijfsspecifieke risico-analyse uit om de IT-risico's in kaart te brengen. Hierbij wordt diepgaand en gericht gekeken naar de specifieke situatie van jouw organisatie en de keten waarin je opereert. Op basis van deze analyse bepalen we samen welk securityniveau noodzakelijk is.
Deze aanpak is cruciaal om te voldoen aan de eisen van onder andere de NIS2-richtlijn en zorgt ervoor dat beveiligingsmaatregelen niet alleen aansluiten bij jouw bedrijfsrisico's, maar ook bij de ketenverantwoordelijkheid.

Bovendien wordt deze risico-analyse jaarlijks herhaald, zodat veranderende dreigingen, nieuwe wet- en regelgeving en aanpassingen in de IT-infrastructuur tijdig worden meegenomen. Dit stelt jouw organisatie in staat om de beveiligingsstrategie continu te optimaliseren en up-to-date te blijven met de nieuwste beveiligingsstandaarden. Dankzij deze periodieke evaluatie blijft jouw securityniveau altijd in lijn met de eisen van de keten en jouw zakelijke partners.

Uitgevoerd door **onafhankelijke security consultants** van AuditConnect

AUDIT CONNECT

Maandelijkse rapportages + jaarlijks security-overleg

Met onze maandelijkse securityrapportages krijg je inzicht in de status van je beveiliging, de gedetecteerde dreigingen en aanbevelingen voor verbetering. Daarnaast organiseren we jaarlijks een security-overleg waarin we strategische beveiligingsplannen bespreken en optimaliseren.

Business Impact Analyse

Een Business Impact Analyse (BIA) helpt je om de gevolgen van mogelijke cyberincidenten of IT-verstoringen in kaart te brengen. Dit stelt je in staat om kritieke bedrijfsprocessen te identificeren en strategische herstelmaatregelen te plannen om downtime en financiële schade te minimaliseren.

Disaster recovery plan & Disaster Simulation

Het Disaster Recovery Plan zorgt ervoor dat je IT-omgeving snel hersteld kan worden na een cyberaanval, stroomuitval of ander incident. Dit plan omvat noodprocedures, back-upstrategieën en herstelscenario's om de continuïteit van je bedrijf te waarborgen. Door middel van een Disaster Simulation testen we de effectiviteit van je herstelstrategieën en identificeren we verbeterpunten in je beveiligings- en noodplannen. Dit stelt je in staat om de respons op echte incidenten te optimaliseren en de impact ervan te minimaliseren.

Pentest

Een penetratietest (pentest) simuleert realistische cyberaanvallen om kwetsbaarheden in je IT-systemen bloot te leggen. Door ethische hackers in te zetten om je netwerk, applicaties en systemen te testen, ontdek je potentiële zwakke plekken voordat kwaadwillenden dit doen. Met een pentest zorg je ervoor dat je beveiliging up-to-date en weerbaar blijft tegen aanvallen.

Uitgevoerd door **onafhankelijke security consultants** van AuditConnect

NIS2 keurmerk (Quality Mark)

Als jouw organisatie levert aan een NIS2-plichtig bedrijf, wordt van jou verwacht dat je digitale beveiliging aantoonbaar op orde is. Daarom is er het NIS2 Quality Mark – een haalbare en erkende cybersecuritynorm. Dit keurmerk helpt om risico's in de keten te verkleinen, terwijl zakelijke relaties en contracten juist worden versterkt.

Voor Toeleveranciers

Jouw klant eist naleving van NIS2 wetgeving

NIS2 keurmerk

Makkelijkste manier om samen te werken

Voor NIS2 plichtige bedrijven

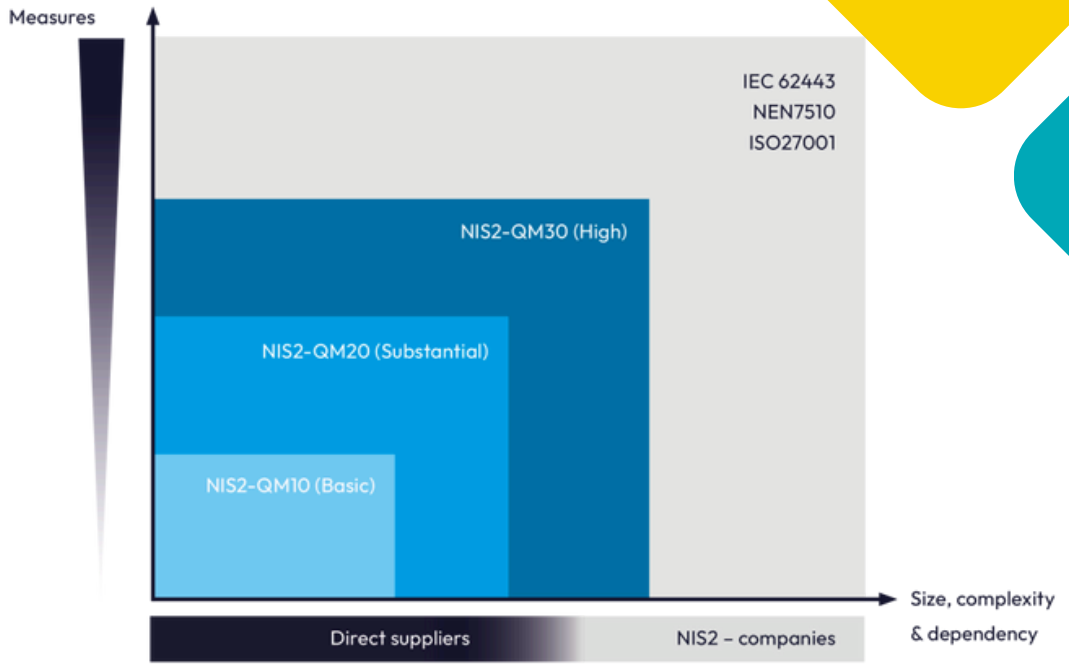
Maak de NIS2 wet haalbaar voor je toeleveranciers (en weet met wie je zaken doet)

NIS2 QUALITY MARK

De drie niveaus van het NIS2 Quality Mark:

- QM10 BASIC – Voor bedrijven met beperkt risico die leveren aan NIS2-plichtige bedrijven.
- QM20 SUBSTANTIAL – Voor bedrijven met verhoogd risico, bijvoorbeeld door toegang tot gevoelige data.
- QM30 HIGH – Voor kritische bedrijven in de keten, waarbij een cyberincident grote impact kan hebben.

Door te kiezen voor een van de Eshgro securitypakketten – Supply Chain Security Level 1, Level 2 of NIS2 Compliant – voldoe je al aan de technische en organisatorische eisen van het keurmerk.
Onze externe partner AuditConnect kan vervolgens jouw bedrijf begeleiden bij het officiële aanvraagproces en certificering van het NIS2 Quality Mark. Zo ben je volledig voorbereid en aantoonbaar compliant binnen de keten.



Bron: https://nis2qualitymark.eu/

Uitgevoerd door **onafhankelijke security consultants** van AuditConnect

AUDIT CONNECT

Samenvattend

Onze securitypakketten bieden niet alleen bescherming tegen cyberdreigingen, maar helpen jouw organisatie ook om te voldoen aan wet- en regelgeving zoals NIS2. Door te kiezen voor Eshgro profiteer je van:

- **Volledige naleving van beveiligingsnormen** – Onze diensten zijn ontworpen op basis van de nieuwste wet- en regelgeving, zodat je voldoet aan de eisen voor ketenverantwoordelijkheid en compliance.
- **Proactieve bescherming tegen cyberdreigingen** – Door middel van 24/7 monitoring, geavanceerde detectie en respons minimaliseren we de risico's van ransomware, phishing en datalekken.
- **Schaalbare en toekomstbestendige security-oplossingen** – Kies een securityniveau dat aansluit bij jouw organisatie, met de mogelijkheid om op te schalen indien de dreigingen of compliance-eisen veranderen.
- **Efficiënte implementatie zonder verstoring** – Onze securitydiensten zijn kant-en-klaar en direct toepasbaar, zonder ingrijpende wijzigingen in jouw IT-infrastructuur.
- **Ondersteuning en inzicht in securitystatus** – Met periodieke risicoanalyses, rapportages en overlegmomenten blijf je altijd op de hoogte van je beveiligingsstatus en verbeterkansen.

Neem contact op met ons voor meer informatie en specifieke vragen:

securitybaseline@eshgro.nl

Klaar voor NIS2?

Samen met Eshgro zet je de stappen om te voldoen aan de minimale NIS2-eisen. Wij zorgen ervoor dat je security up-to-date blijft, zodat jij je zorgeloos kunt focussen op je business.