Digitaal veilig onderwijs als basisvoorwaarde

Cybersecurity as a Service (CaaS)

2 maart 2026

cloudwise

Kan je een krantenkop voorstellen met jouw school in de hoofdrol?

2 maart 2026

DE CLOUDWIJZER

Digitaal veilig onderwijs is niet langer een optie maar een basisvoorwaarde

DOOR TEUN BRUINSMA

Misbruik leerlinggegevens zorgt voor stress op school

WOERDEN Onvoldoende afspraken op gedeeld beheer, wachtwoordbeleid en het openstellen van de omgeving voor derden kunnen leiden tot onbevoegde toegang tot en misbruik van persoons-gegevens.

Dit kan de privacy van leerlingen en medewerkers ernstig in gevaar kan brengen. De kans op datalekken wordt groter, waardoor gevoelige informatie in verkeerde handen kan vallen.

> *Als we er op deze manier mee om blijven gaan dan lopen we een groot risico op onze scholen.*
> *– Directrice de Saffier*

Digitale omgeving school gegijzeld door aanvallen van hackers op het netwerk

Hackers gebruiken ransomware om systemen en gegevens te gijzelen, waardoor onderwijsactiviteiten en overig administratieve processen worden verstoord. Deze aanvallen kunnen ernstige financiële en operationele gevolgen hebben voor onderwijsinstellingen.

90% van de datalekken begint met menselijke fout

Menselijke fouten, zoals het onbedoeld delen van gevoelige informatie of het vallen voor phishing-aanvallen, zijn de oorzaak van het merendeel van de beveiligingsincidenten.

Het bevorderen van een cultuur van bewustzijn en zorgvuldigheid is cruciaal om deze risico's te beperken.

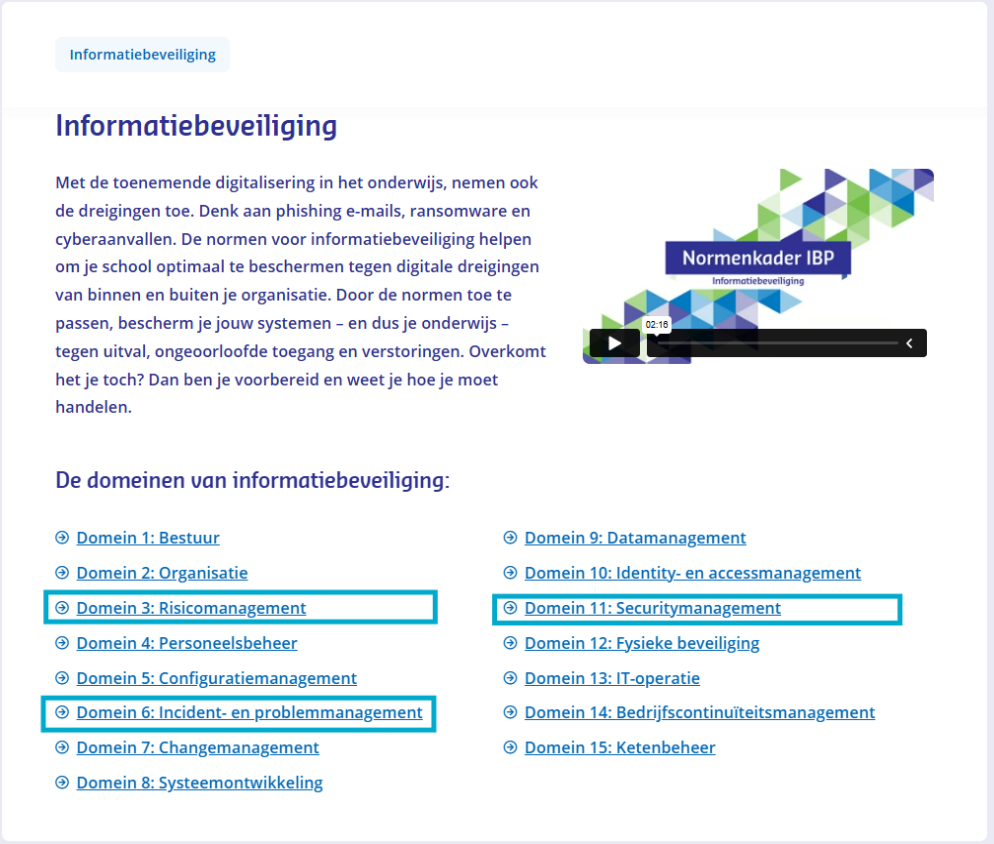
Slimme leerlingen vinden een uitweg uit leeromgeving

Leerlingen zijn slimmer en technischer dan we ons soms realiseren. Ze vinden manieren om beveiligingssystemen te omzeilen of te manipuleren, wat kan leiden tot ongeautoriseerde toegang tot systemen of het wijzigen van gegevens. Dit onderstreept het belang van zowel technische beveiliging als bewustwording en training.

cloudwise

Wat zien wij gebeuren in de markt?

De bewustwording en urgentie neemt toe

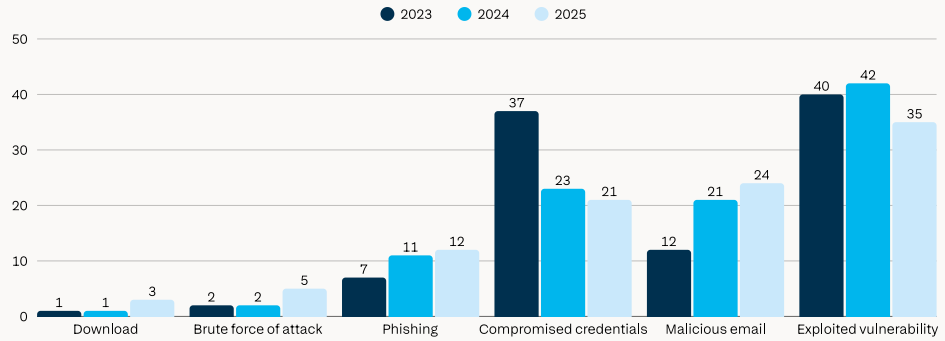


cloudwise

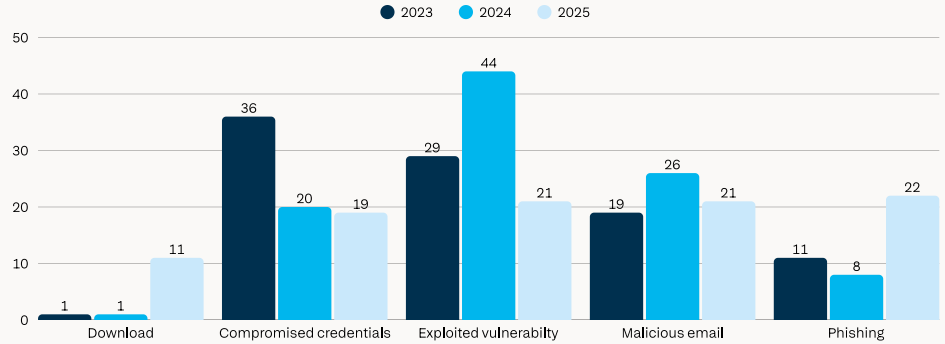
Wat zien wij gebeuren in de markt?

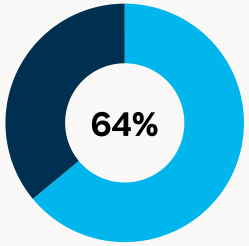
De digitale zorgen worden groter

Grafiek 1: Technische grondoorzaak van ransomware-aanvallen in het hoger onderwijs

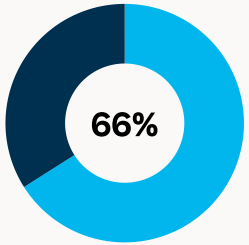


Grafiek 2: Technische grondoorzaak van ransomware-aanvallen in het funderend onderwijs

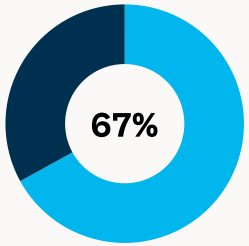




Beveiligingsincidenten
Gebrek aan bescherming of beschermingsoplossingen van slechte kwaliteit die de aanval niet konden stoppen



Kennis en vaardigheden
Gebrek aan menselijke expertise (vaardigheden of capaciteit) om de aanval op tijd te detecteren en te stoppen



Onbekend terrein
Een bekende of onbekende zwakte in hun verdediging hadden

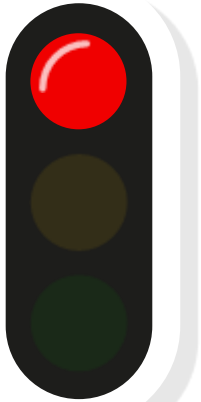
Bron: State of Ransomware (Sophos)

cloudwise

De vraag is dus niet óf..

cloudwise

De vraag is dus niet óf..
..maar wannéér



cloudwise

Hoe helpt Cloudwise het onderwijs vooruit?

Cybersecurity as a Service (CaaS)

2 maart 2026

cloudwise

Cloudwise helpt onderwijs vooruit

Digitaal veilig als basisvoorwaarde

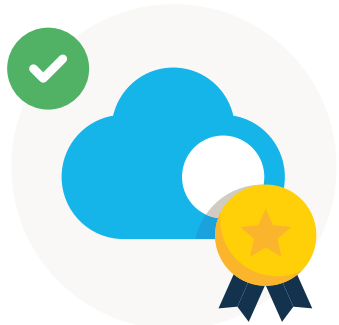
- Een veilige (ICT-)omgeving **begint met een visie**, passend beleid en het neerzetten van een juiste organisatie.
- Hoe goed je de techniek ook voor elkaar hebt, uiteindelijk geeft **de mens** de doorslag. Awareness en bewust handelen is een must.
- Met onze veilige ICT-oplossingen kunnen scholen direct veilig aan de slag. In onze secure by design **standaardconfiguraties** hebben we al een heleboel solide securityservices ingebouwd.
- Er zijn situaties waarin het raadzaam kan zijn om **extra securitymaatregelen** te treffen. CAAS is een van grotere hierin.

cloudwise

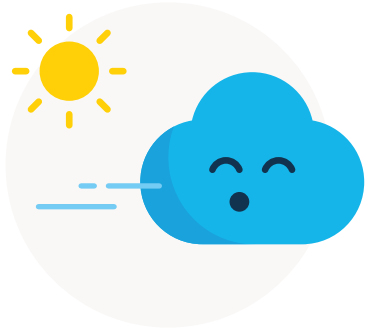
Cloudwise helpt onderwijs vooruit

Wij zorgen voor grip & rust op digitale zorgen

Operationele & gemoedsrust
Een 24/7 beheerde dienst waar IT-specialisten continue bedreigingen zoeken, meekijken en voor afhandeling zorgen.



Aantoonbaar veilig & compliant
Bij audits/inspecties kun je aantonen dat je voldoet aan gestelde digitale veiligheidsnormen en visie hierop. En los van aantoonbaarheid ben je ook echt veilig



Speciaal educatief aanbod
Bij ons betaal je niet voor alle users maar:

- ✓ Enkel per windows device
- ✓ Is ChromeOS kosteloos inbegrepen
- ✓ Google Workspace monitoring
- ✓ Firewall security monitoring
- ✓ De Sophos Endpoint agent

Volledig beheerd en proactief 24/7
monitoring en directe respons door Sophos-experts.

Op het onderwijs gericht
Afgestemd op het normenkader en de praktijk van scholen.

Breder beveiligingsbereik
Naast endpoints beveiligen we ook servers, cloud en netwerk.

Geen extra belasting voor IT-teams
Nederlandstalige ondersteuning en regie vanuit Cloudwise.

Compliance-ready
Ondersteuning bij cyberverzekeringen en audits.

cloudwise

Bescherming via CAAS?

Waarom heb je MDR en Managed Risk nodig?

2 maart 2026

cloudwise

Een digitale school gaat nooit dicht

Cybersecurity-as-a-Service

In simpele woorden uitgelegd

Concept	Waar kan je het mee vergelijken?	Wat het doet?
Traditionele virusscanner (A3)	Kan je bijvoorbeeld vergelijken met een simpele rookmelder.	Piept alleen bij bekende, duidelijke rook (een bekende virus-handtekening).
EDR (A5/Sophos agent)	Staat symbool voor een slimme conciërge	Ziet niet alleen rook, maar ruikt ook een brandlucht, ziet verdachte vonken, en kan direct een deur sluiten om het vuur in te dammen.
MDR	Zorgt voor aansluiting op de “112-meldkamer”	De slimme conciërge (EDR) is aanwezig, maar de melding gaat direct naar de professionals naar de meldkamer (het MDR-team) die 24/7 meekijken en direct de juiste actie coördineren.
Managed Risk	Is de auditer van de school die de inspectie doet om te controleren of alles goed staat en welke verbeteringen er zijn.	Het controleert, herkent en adviseert zwakke plekken en zorgt voor een security score.

cloudwise

En hoe beveiligen we tegen verdacht gedrag?

De slimme conciërge kan gebruik maken van twee diensten:

MDR

Managed Detection & Response (SOC/SIEM)

Een 24/7 pro-actieve bescherming van Google Workspace, Microsoft & Google werkplekken, Servers, Dark web en Cloud (M365) om dreigingen direct te **detecteren** en **en isoleren**. Dit minimaliseert potentiële schade en zorgt ervoor dat onderwijsprocessen ongestoord en veilig kunnen doorgaan.

Managed Risk

Gezondheids- en risicobeheersing (Vulnerability scanning)

Proactieve identificatie, analyse en mitigatie van cyberrisico's en kwetsbaarheden, specifiek afgestemd op de ICT omgeving binnen het onderwijs. Dit omvat structurele risicoanalyses (plus risicobeoordeling en benchmark), beleidsadvies en ondersteuning bij compliancy (AVG).

2 maart 2026

cloudwise

Cybersecurity as a Service

Wij houden jullie deuren dicht door inzet van:

cloudwise

Cybersecurity-as-a-Service

Virusscanner (A3) versus MDR

Van bekend gedrag naar verdacht gedrag
Waar een virusscanner scant op bekende risico's kijkt MDR verder en heeft vooral oog voor verdachte processen.

Van zelfstandig naar beheersbaar
Met MDR hoeven IT-verantwoordelijken op scholen niet zelf continu alert te zijn op meldingen van firewalls en virusscanners.

Van signaleren naar isoleren, analyseren en reageren
Een laptop die ongewenste dingen doet direct van het schoolnetwerk wordt geïsoleerd, zodat de infectie zich niet kan verspreiden.

cloudwise

Cybersecurity-as-a-Service

Welke ernstige dreigingen met directe impact op het onderwijs zien we!

Gestolen accounts (leerling of medewerker)

Wat is het? Iemand logt in op een schoolaccount met een gestolen wachtwoord, vaak vanaf een vreemde locatie of buiten schooltijden.

Mogelijke gevolgen:

- Inzien of stelen van leerling- en personeelsgegevens
- Versturen van phishing vanuit een vertrouwd schoolaccount
- Misbruik van Teams, e-mail of cloudbestanden

Phishing & e-mailfraude

Wat is het? Nepmails die lijken te komen van collega's, leveranciers of directie, met als doel klikken of betalen.

Mogelijke gevolgen:

- Financiële schade (nep-facturen)
- Verdere verspreiding van malware binnen de school
- Vertrouwensverlies bij ouders en partners

Onzichtbare aanvallen op werkplekken

Wat is het? Aanvallen die geen "virusbestand" achterlaten, maar misbruik maken van standaard software op laptops.

Mogelijke gevolgen:

- Aanval blijft lange tijd onopgemerkt
- Aanvallers kunnen meekijken of data verzamelen
- Voorbereiding op zwaardere aanvallen (zoals ransomware)

cloudwise

Cybersecurity-as-a-Service

Welke ernstige dreigingen met directe impact op het onderwijs zien we!

Ransomware (systemen op slot)

Wat is het? Kwaadaardige software die bestanden en systemen versleutelt en losgeld eist.

Mogelijke gevolgen!

- Geen toegang tot lesmateriaal of leerlingadministratie
- Lessen vallen uit, examens in gevaar
- Herstel kost veel tijd en geld.

Misbruik van e-mail en cloud (Microsoft 365 / Google Workspace)

Wat is het? Aanvallers gebruiken schoolaccounts om bij e-mail, documenten en gedeelde mappen te komen.

Mogelijke gevolgen!

Datalekken (AVG-meldplicht)Onbedoelde verspreiding van vertrouwelijke informatie

Reputatieschade voor de school of scholengroep

Aanvallen buiten schooltijden

Wat is het? Digitale aanvallen vinden vaak plaats ’s avonds, ’s nachts of in het weekend.

Mogelijke gevolgen

Problemen worden pas ontdekt als de school weer open is

Schade is dan vaak al groot

Extra druk op ICT bij start van de schooldag

Deze dreigingen zijn dagelijkse realiteit in het onderwijs en vragen om continue bewaking — niet alleen tijdens schooluren.

2 maart 2026

cloudwise

Cloudwise helpt onderwijs vooruit

Sophos MDR en Microsoft? Het verschil!

Cybersecurity-as-a-Service (Caas) in vergelijking tot Microsoft Defender A3 & A5

Beschrijving van de norm	Sophos MDR Essentials + MDR Agent	MS Defender A3	MS Defender A5
Patch-management	Automatische Detectie & advies via MDR	Via Intune (handmatige configuratie vereist)	Automatisch via Intune (handmatige configuratie vereist)
Threat & Vulnerability Management	Continue beoordeling via MDR en agent	Basisdetectie, geen risicobeoordeling	Via TVM-dashboard (handmatige activatie vereist)
Bescherming infrastructuur	Automatische Real-time bescherming, exploit prevention, device control	Basisbescherming	Geavanceerde bescherming (handmatige configuratie vereist)
Incidentdetectie en -respons	24/7 SOC & monitoring inbegrepen	✖ Alleen basisdetectie, geen SOC	✖ SOC & response niet inbegrepen
Logging en monitoring	Via Sophos Central en MS API (standaard)	Beperkt, geen centrale logging	Basis logging, geen SIEM zonder extra licentie
Externe ondersteuning	Cloudwise + Sophos-team inbegrepen	✖ Niet beschikbaar	Alleen via aanvullende supportcontract
Malware-bescherming	Geavanceerde detectie	Basisbescherming	Geavanceerde detectie
Endpoint-beveiliging	Volledig via agent	Basisfunctionaliteit	Inclusief EDR (handmatige configuratie & controle vereist) geen student use benefit op EDR
Toegangs-beveiliging	Volledig en automatisch via de MS Management activity API.	Via Entra ID (handmatige configuratie vereist geen identity)	Identity protection, Conitional Access (handmatige configuratie vereist)
Beveiliging mobiele apparaten	Via Sophos Mobile (optioneel af te nemen)	Via Intune (handmatige configuratie vereist)	Via Intune + Defender Mobile (handmatige configuratie vereist)
Beveiliging van netwerken	Network Detection & response (optioneel)	Niet standaard	Defender for Network (optioneel)

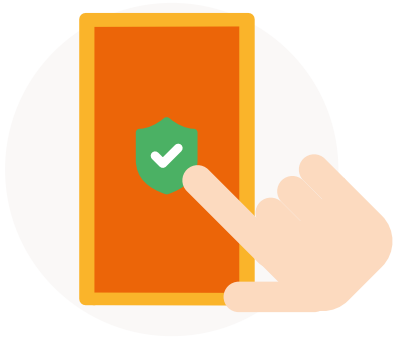
MDR werkt ook op A5!!

2 maart 2026

cloudwise

Cybersecurity-as-a-Service

En dus zorgt de slimme conciërge voor...



...alle fysieke en digitale eindpunten op school beschermt
Beschermt alle potentiële digitale deuren voor een digitale inbreker (hacker). Het gaat hier simpelweg om elk apparaat of account dat verbinding maakt met het schoolnetwerk.

...verdacht gedrag opmerkt
Kijkt niet alleen naar bekende gezichten, maar vooral naar verdacht gedrag. Bij risicovol afwijkend gedrag slaat de conciërge alarm in het systeem en de beveiliging houdt de verdachte tegen voordat deze binnen is.

...direct ingrijpt wanneer dat nodig is
Indien er toch een deur open is gezet via een phishing link of BYOD device dan wordt er niet afgewacht, maar gehandeld. Isoleren is hierbij de basis. Het verdachte proces wordt gestopt en er wordt terugkoppeling gegeven over de situatie.

cloudwise

Een gestructureerde aanpak en duidelijke verantwoordelijkheden

Cybersecurity is meer dan alleen checkboxes aanvinken

2 maart 2026

cloudwise

Cybersecurity-as-a-Service

Cybersecurity is geen eenmalige actie

We voeren **continu geautomatiseerde scans en assessments** uit op systemen, applicaties en netwerken. Hierdoor ontstaat een actueel en compleet beeld van de risico's binnen de IT-omgeving. Met de koppeling aan het NCSC en CVE database weten we altijd direct welke kritieke updates moeten worden uitgevoerd.

Niet elk risico is even urgent. Daarom **koppelen** we **technische kwetsbaarheden aan de schoolcontext**. Zo weet je precies welke risico's directe actie vereisen, welke prio ze hebben en welke beheers / mitigerende maatregelen het meeste effect hebben.

We **begeleiden en adviseren bij het nemen van concrete stappen** om risico's te verlagen. Denk aan patchmanagement, configuratieverbeteringen of beleidsaanpassingen. Alles wordt vastgelegd en opgevolgd, zodat je aantoonbaar in control bent.

cloudwise

Cybersecurity-as-a-Service

Inzien van advies en weloverwogen beslissingen

..op basis van de analyses, resultaten en adviezen.

Waar het SOC team en/of uw IT team mee kan kijken in het security dashboard krijgt directie en bestuur **transparante en begrijpelijke rapportages over de beveiligingsstatus**, inclusief strategische aanbevelingen en overzichtelijke dashboards die direct bruikbaar zijn voor het bestuur.

Hiermee kun je:

1. Security Risico score continue beoordelen
2. Risico's analyseren en herkennen
3. Continue mitigerende maatregelen toepassen
4. Incidenten en trents zichtbaar krijgen incl. adviezen
5. Strategische en tactische optimalisaties doorvoeren
6. Vragen rondom normenkader en security bij inspecties / audits inzichtelijk maken

cloudwise

Van behoefte naar succes

Hoe ziet de samenwerking eruit?

Projectleider

- Planning, scope afstemming, fasering en verantwoordelijkheden.
- Coördinatie en begeleiding van het project.
- Toezicht op inrichting, configuratie & compliance.
- Afstemming en toezicht op uitrol agent & profielen.
- Rapportage en overdracht inclusief documentatie en klantinstructies

Security Service Level Manager

- Bewaken & naleving van de SLA & DAP op responstijden, rapportages en (escalatie)procedures.
- Escalatiecoördinator en aanspreekpunt bij Prio 1 beveiligingsincidenten.
- Communicatie: Maandelijkse rapportage & 2 of 4x per jaar afstemming over status, trends en optimalisatie.

Cloudwise Managed Services

- Proactieve monitoring van meldingen en incidenten door Sophos gegenereerd.
- Informatie en uitleg over de aard van een incident, genomen acties en eventuele vervolgstappen.
- Activeert & coördineert escalaties richting de SSLM en Sophos bij Prio 1 incidenten.
- Vertaalt technische data naar begrijpelijke rapportages en aanbevelingen.
- Opvolging & bewaking van de SLA.

Sophos

- 24/7 Analyseren, tegenhouden en isolatie van aanvallen & dreigingen d.m.v. AI en specialisten.
- Risicobeoordeling & monitoring van Google, M365 & endpoints met continu inzichten in actuele dreigingen en kwetsbaarheden.
- Integraties en koppelingen op endpoint-, netwerk- en cloudbeveiliging voor een holistisch (360°) overzicht.

Stichting & scholen

- Beschikbaarheid van een aanspreekpunt binnen de school voor opvolging van meldingen en adviezen
- Toestemming en medewerking bij het uitvoeren van wijzigingen en incidentrespons
- Bereidheid om rapportages en risico-analyses te bespreken en actie te ondernemen
- Duidelijke rolverdeling met het ICT-team van de school of externe beheerpartij
- Toegang tot relevante systemen en informatie voor effectieve monitoring en threat hunting
- Commitment om samen te werken aan continue verbetering van de digitale veiligheid

cloudwise

Van behoefte naar succes

Implementatietraject

Fase 1 - Inventarisatie & Risicoanalyse

- Om te beginnen voeren we een eerste risicoanalyse-Quickscan uit op basis van IP-adressen, domeinnamen en belangrijkste e-mailadressen.

Fase 2 - Intake en advies

- We doen een intake met de directeur & ICT-coördinator en/of bestuurder over de huidige omgeving, de risico's en de verwachtingen.
- We inventariseren de huidige omgeving in termen van aantal & type endpoints, policies, configuraties etc.
- We stellen een adviesrapport op en bespreken dat.
- We verwerken de feedback vanuit het gesprek in het plan van aanpak.
- We zorgen voor een heldere uitleg over de functionele werking van de oplossing.

Fase 3 - Projectvoorbereiding

- We stellen het projectplan op (het definitieve plan van aanpak, inclusief de planning).
- We stemmen het project af met de stakeholders (ICT, directie, bestuur).
- We richten communicatie in en stellen escalatieprocedures op.
- We bereiden het plan/advies voor de technische omgeving voor (profielen Intune, endpoint updates, accounts, rollen & rechten etc.).
- We rollllen Sophos endpoint agent uit (of Sensor bij Defender A5) via de Intune-omgeving.

Fase 4 - Implementatie

- Activatie MDR Essentials via Sophos Central.
- Integratie koppelingen met endpoints, servers en cloud.
- Configuratie van policies, alerts en rapportages.
- Inrichting van managed detection en response dashboard.
- Inrichting van Managed Risk-dashboard en workflows.

Fase 5 - Testen & productie

- Overdracht aan directie, ICT-coördinator en bestuur.
- Overdracht aan Cloudwise-beheerorganisatie.
- Training en uitleg voor betrokken medewerkers.
- Oplevering documentatie & checklist.
- Volledig beheer: meer ondersteuning is mogelijk, maar Managed Risk (incident response) blijft een aparte dienst, tenzij expliciet opgenomen in de overeenkomst.

Traject van 90 dagen

2 maart 2026

cloudwise

2 maart 2026

cloudwise