Guard | by INFARIS

WHITEPAPER
VOOR MANAGED SERVICE PROVIDERS

BEVEILIGING · PERFORMANCE · SEO · UPTIME

Meten is pas het begin. Infaris helpt ook problemen oplossen.

Guard brengt de uitkomsten van scans en monitoring samen. Infaris biedt diensten om de gevonden problemen te onderzoeken en op te lossen, afgestemd op uw omgeving en team.

LAGEN IN BEELD	MEETLOCATIES	KORTSTE INTERVAL	EDITIE
4	NL DE US UK	30s	2026.1

SAMENVATTING

Het gat zit niet in uw firewall. Het zit tussen uw tools.

Een serieuze aanval vraagt geen specialistische kennis meer. Wie een AI-model de juiste vraag stelt, krijgt een stappenplan en werkende code terug. Daarmee is de rem eraf: het aantal partijen dat schade kan aanrichten is niet meer te overzien.

Voor een managed service provider verandert dat de rekensom, want u wordt afgerekend op iets breders dan veiligheid alleen. Een gehackte webshop, een server die vastloopt, een pagina die er acht seconden over doet, een zoekpositie die verdwijnt: voor de klant is het hetzelfde verhaal. Hun bedrijf staat stil, en u had het moeten zien aankomen.

Guard brengt uitkomsten over uptime, security, performance en SEO op één tijdlijn. Deze whitepaper laat zien hoe u daarmee in negentig dagen van meten naar handelen gaat. Op basis van de bevindingen biedt Infaris diensten voor onderzoek en herstel. Wij voeren het afgesproken werk uit en controleren daarna het resultaat met Guard.

DE KERN IN VIJF REGELS

- De drempel voor een aanval is weg. AI levert de kennis die een aanvaller vroeger zelf moest hebben.
- Uw klant maakt geen onderscheid tussen een hack, een storing en traagheid. Alle drie kosten u vertrouwen.
- Losse tools geven vier beelden en nul samenhang. Een incident begint zelden precies daar waar u toevallig kijkt.
- Een melding is pas het begin. Spreek af wie onderzoekt, herstelt en controleert, zodat een incident niet bij een dashboard stopt.
- Bewijs hoort erbij. NIS2, ISO 27001 en uw eigen kwartaalrapportage vragen om aantoonbare controle, niet om een onderbuikgevoel.

INHOUD

01 De drempel is weg 03
02 U wordt aangekeken, niet de hacker 04
03 Vier tools, nul samenhang 05
04 Het hele huis: vier lagen 06
05 Van meten naar ingrijpen 10
06 Bewijs leveren aan klant en auditor 11
07 In negentig dagen proactief 12
08 Checklist voor uw eigen omgeving 13

HOOFDSTUK 01

Zelfs oma kan vandaag een serieuze cyberaanval uitvoeren.

Ze hoeft maar aan een willekeurig AI-model te vragen wat ze moet doen, en ze krijgt stap voor stap alles: de juiste instructies en de kant-en-klare code. Kennis is geen drempel meer.

Tot voor kort was kennis de schaarse factor in een aanval. Iemand moest weten wat een injectie is, waar een verouderde plugin zich verraadt, hoe een payload eruitziet die langs een filter komt. Die kennis kostte jaren. Dat filterde vanzelf: de meeste pogingen kwamen van geautomatiseerde bots die alleen op bekende deuren klopten.

Die filter is weg. De aanvaller hoeft niet meer te begrijpen wat hij doet, hij hoeft alleen de vraag te stellen. Het gevolg is dubbel: er worden meer pogingen gedaan, en de gemiddelde poging is beter dan hij vroeger was. Letterlijk iedereen met een internetverbinding is opeens gevaarlijk.

> **Kennis was de rem op het aantal aanvallen. Die rem is eruit gehaald, en niemand heeft hem teruggezet.**
>
> DE VERSCHUIVING DIE 2025 EN 2026 KENMERKT

Ondertussen groeit het oppervlak waar ze op kunnen kloppen. Een doorsnee klant heeft tegenwoordig een CMS met vijftien plugins, een koppeling naar een boekhoudpakket, een mailstroom die door drie partijen loopt, certificaten die stilletjes verlopen en DNS bij een registrar waar ooit iemand een account voor aanmaakte. Elk van die onderdelen kan het zwakke punt zijn, en geen enkel onderdeel meldt zichzelf aan.

01

Kennis is gratis geworden

Wat vroeger een specialisme was, is nu een prompt. De vaardigheid van de aanvaller zegt niets meer over de kwaliteit van de aanval.

02

Het oppervlak groeit

Plugins, koppelingen, subdomeinen, certificaten, DNS en mail. Elk onderdeel is een ingang, en vergeten subdomeinen zijn de populairste.

03

De tijd krimpt

Tussen een gepubliceerde kwetsbaarheid en het eerste misbruik zitten vaak uren. Een patchronde per kwartaal is dan geen beleid meer, maar een gok.

WAAROM DIT U EERDER RAAKT DAN UW KLANTEN

Een managed service provider is per definitie een aantrekkelijker doelwit dan de klant zelf. Bij u ligt één set toegangen naar tientallen omgevingen. Dat betekent twee dingen: uw eigen hygiëne telt zwaarder dan die van uw klanten, en u moet kunnen aantonen dat u hem op orde heeft. Hoofdstuk 06 gaat over dat bewijs.

HOOFDSTUK 02

Als het misgaat, kijkt de klant naar u. Niet naar de hacker.

Uw klanten interesseert het niets of het een hack is, een trage server, een verdwenen zoekpositie of een systeem dat vastloopt. Ze willen één ding: dat hun webshop, portaal en systemen altijd draaien, snel zijn en vindbaar blijven.

Dat is geen onredelijke verwachting, het is precies waarvoor ze betalen. Het vervelende is alleen dat de klant het verschil niet ziet tussen de vier oorzaken hieronder, terwijl u ze in vier verschillende tools moet opzoeken.

WAT DE KLANT MELDT	WAT ER WERKELIJK SPEELT	WAT HET KOST
"De site doet het niet"	Verlopen certificaat, gewijzigd DNS-record, container die is omgevallen	Omzet per minuut, plus een avond herstel
"Het is zo traag"	Een zware query, een ongecomprimeerde afbeelding, een script van derden	Conversie en zoekpositie, traag en onzichtbaar
"We staan niet meer in Google"	Een robots-regel die bij een release meeliftte, een canonical die verdween, backlinks die wegvielen	Maanden om terug te komen
"Onze mail komt niet aan"	SPF, DKIM of DMARC niet op orde, domein misbruikt	Deliverability en reputatie
"We zijn gehackt"	Een plugin die drie maanden achterliep	Herstel, meldplicht, vertrouwen

> Een woedend telefoontje is geen alarmering. Het is een factuur die u al niet meer kunt voorkomen.

Het moment dat het bedrijf van uw klant stilvalt en u dat pas via dat telefoontje hoort, bent u te laat. Niet een beetje te laat: u begint op dat moment aan drie dingen tegelijk. Uitzoeken wat er aan de hand is, het oplossen, en uitleggen waarom u het niet eerder wist. De derde kost het meest, want die verliest u altijd.

Dat is ook waar het verdienmodel kraakt. Een SLA met een reactietijd van vier uur is niets waard als het startschot een klant is die belt. De klok liep toen al een uur. Wie proactief werkt, verkoopt geen snellere reactie maar een kleiner incident, en dat is het enige verschil dat de klant echt merkt.

HOOFDSTUK 03

Het probleem is niet dat u niets meet. Het is dat niemand het geheel ziet.

Vrijwel elke provider heeft een uptime-pinger, ergens een securityscan, een performancerapport uit een browsertool en een SEO-overzicht dat het bureau van de klant aanlevert. Elke tool heeft gelijk over zijn eigen stukje. Precies daar zit het probleem, want een storing houdt zich niet aan die indeling.

Neem een certificaat dat verloopt. De uptime-tool controleert of de server antwoordt en die antwoordt keurig, dus het dashboard blijft groen. Browsers weigeren ondertussen de verbinding, de conversie valt stil, en zoekmachines gaan fouten registreren. Pas weken later staat er iets in de SEO-rapportage. Op geen enkel moment stond er iets op rood dat iemand ook las.

SYMPTOOM 01

Blinde vlekken tussen de tools

Elke tool bewaakt zijn eigen laag. Wat tussen twee lagen valt, bewaakt niemand. Dat is precies waar incidenten beginnen.

SYMPTOOM 02

Alarm zonder eigenaar

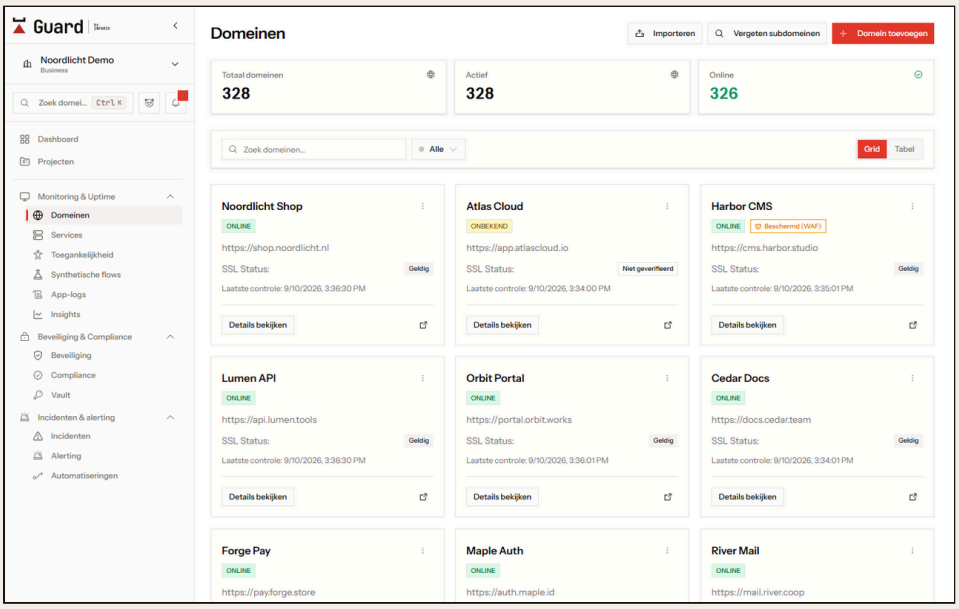
Meldingen komen op vier plekken binnen, waarvan er twee alleen door een mailbox worden gelezen die niemand beheert. Zonder duidelijke route is een melding hetzelfde als geen melding.

SYMPTOOM 03

Geen verhaal achteraf

Vraagt de klant hoe het vorig kwartaal ging, dan plakt u vier exports aan elkaar. Dat is werk, en het overtuigt niemand.

Er is nog een vierde effect, en dat is het duurste. Als niemand het geheel ziet, wordt iedere melding een losse gebeurtenis in plaats van een patroon. De derde keer dat dezelfde klant traag is, behandelt u als de eerste keer.



DOMEINEN ALLE KLANTEN, ALLE DOMEINEN, ÉÉN STATUS

HOOFDSTUK 04

Wij checken niet alleen of de deur op slot zit, maar het hele huis.

Beveiliging, performance, SEO en uptime, van klik tot koppeling. Begint er iets te haperen, dan weet uw team dat als eerste en ziet u meteen waar het zit.

Het model hieronder heeft vier lagen. Ze zijn niet los te koop, want dat is precies de fout die hoofdstuk 03 beschrijft. Ze delen één tijdlijn, één klantindeling en één alarmroute. De volgende vier pagina's lopen ze stuk voor stuk langs.

LAAG 01

Uptime en stack

Draait het, en waar draait het op? Probes vanuit vier landen, SSL en DNS, de machines eronder en wat daarop is geïnstalleerd.

LAAG 02

Van klik tot koppeling

Werkt het ook echt, voor een echte bezoeker? Synthetische flows, Core Web Vitals van werkelijk verkeer, toegankelijkheid en vindbaarheid.

LAAG 03

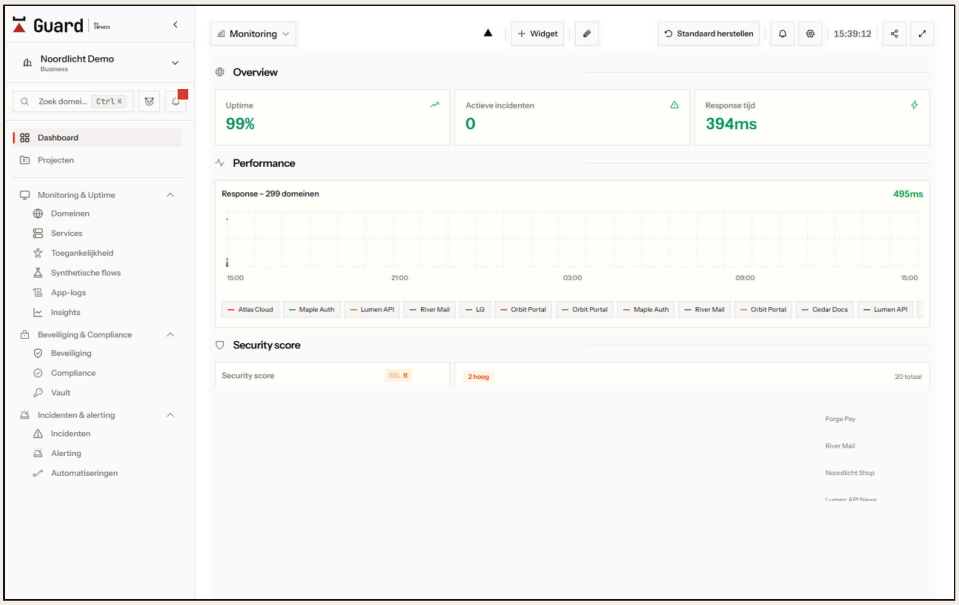
De deur én het slot

Is het veilig, en kunt u dat aantonen? Securityscore, CVE's tegen uw eigen stack, mailbeveiliging, geheimen en compliance.

LAAG 04

Eerder dan de klant

Wie weet het als eerste, en wat gebeurt er dan? Incidenten, alerting, automatisering, statuspagina en rapportage.



DASHBOARD VIER LAGEN, ÉÉN BEELD

LAAG 01

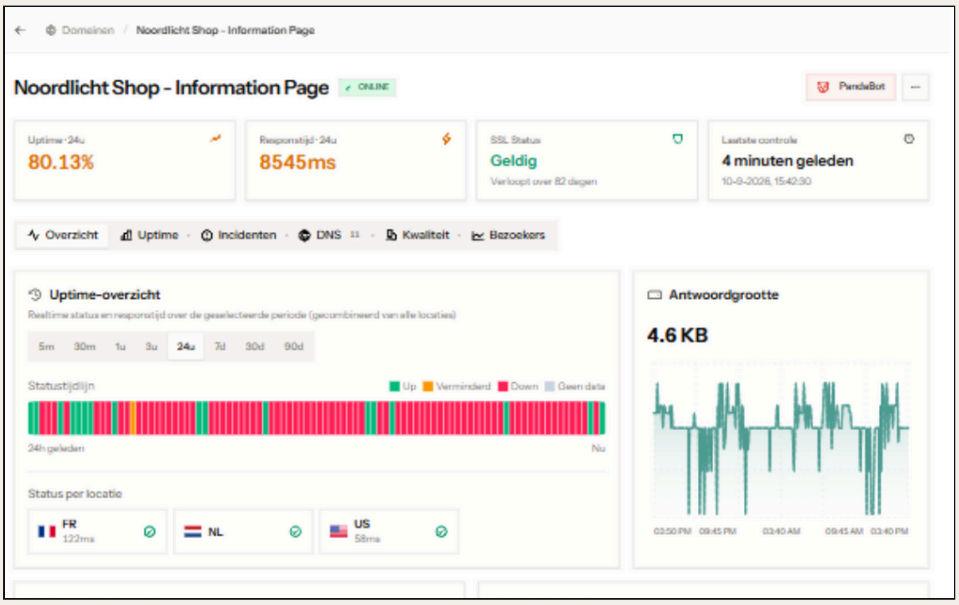
Draait het, en waar draait het op?

De basislaag beantwoordt de vraag die uw klant stelt als hij belt, maar dan voordat hij belt. Controles lopen elke 30 of 60 seconden vanuit Nederland, Duitsland, de Verenigde Staten en het Verenigd Koninkrijk, zodat een storing bij één provider zich niet voordoet als een storing bij de klant.

- **Uptime en respons.** Meerdere locaties, meerdere protocollen, met een responstijd die u over de tijd kunt volgen in plaats van alleen een groen of rood bolletje.
- **SSL en DNS.** De volledige certificaatketen, de verloopdatum ruim op tijd, en een melding zodra een DNS-record verandert. Dat laatste is vaker een aanval dan een toeval.
- **Services en topologie.** Welke machines er zijn, wat erop draait, hoe ze van elkaar afhangen, en welke pakketten achterlopen. Patchbeheer als lijst, niet als voornemen.
- **De agent op de machine zelf.** Een lichte agent rapporteert schijfruimte, geheugen, processen en updates van binnenuit. Buiten kijken laat namelijk niet zien dat de schijf over twee dagen vol is.
- **Projecten per klant.** Alles gegroepeerd per klant of per omgeving, zodat een dienstdoende collega niet hoeft te raden welk domein bij wie hoort.

WAAR HET MEESTAL MISGAAT

Vergeten subdomeinen. Een oude staging-omgeving, een campagnesite uit 2021, een testdomein dat nooit is opgeruimd. Ze staan open, ze draaien verouderde software, en ze staan in geen enkele lijst. Begin uw inventarisatie daar, niet bij de productiesite die u toch al bewaakt.



DOMEINDETAIL UPTIME, RESPONS EN STATUS PER LOCATIE

LAAG 02

Werkt het ook echt, voor een echte bezoeker?

Een server die antwoordt is nog geen werkende webshop. Deze laag test wat de bezoeker daadwerkelijk doet en meet wat hij daadwerkelijk ervaart, inclusief het stuk dat op zijn eigen apparaat gebeurt.

NAGESPEELD

Synthetische flows draaien in een echte Chromium en klikken het pad af dat geld oplevert: inloggen, zoeken, in de winkelwagen, afrekenen. Valt stap vier weg, dan weet u dat om drie uur 's nachts en niet om negen uur 's ochtends.

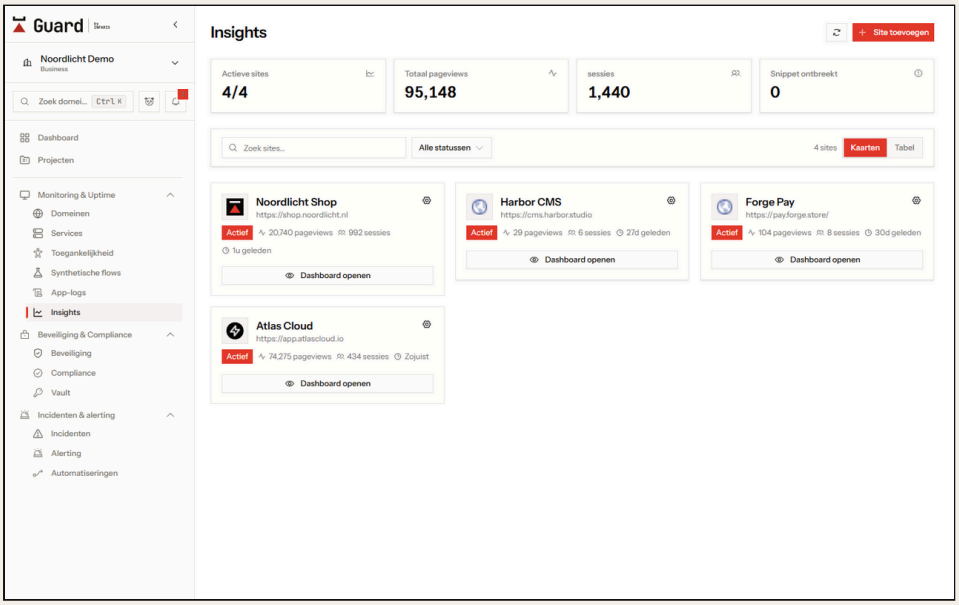
Change detection vergelijkt pagina's met hoe ze gisteren waren. Een prijs die verspringt, een formulier dat verdwijnt of een script dat erbij komt valt dan meteen op.

WERKELIJK GEMETEN

Insights verzamelt Core Web Vitals van echte bezoekers: hoe snel laadde de pagina op hun apparaat, op hun verbinding. Dat is het cijfer waar zoekmachines op sturen, niet de score van een testmachine met glasvezel.

App-logs vangen de fouten die de bezoeker niet meldt maar wel tegenkomt, en koppelen ze aan het moment waarop ze begonnen.

- **Toegankelijkheid.** WCAG-controles per pagina, met een score die meet hoe toegankelijk de pagina is en niet hoe complex hij is. Relevant nu de Europese toegankelijkheidsrichtlijn ook commerciële sites raakt.
- **SEO en backlinks.** Vindbaarheid in dezelfde loop als de rest: indexeerbaarheid, structuur, en de links die naar de klant wijzen. Een verdwenen zoekpositie is een storing, alleen een langzame.
- **De browserextensie.** Scant de tab die op dat moment openstaat op cookies, headers, mixed content, toegankelijkheid, SEO, privacy en performance. Handig tijdens een intake of een salesgesprek, zonder dat er iets hoeft te worden ingericht.



INSIGHTS ECHTE BEZOEKERS, ECHTE LAADTIJDEN

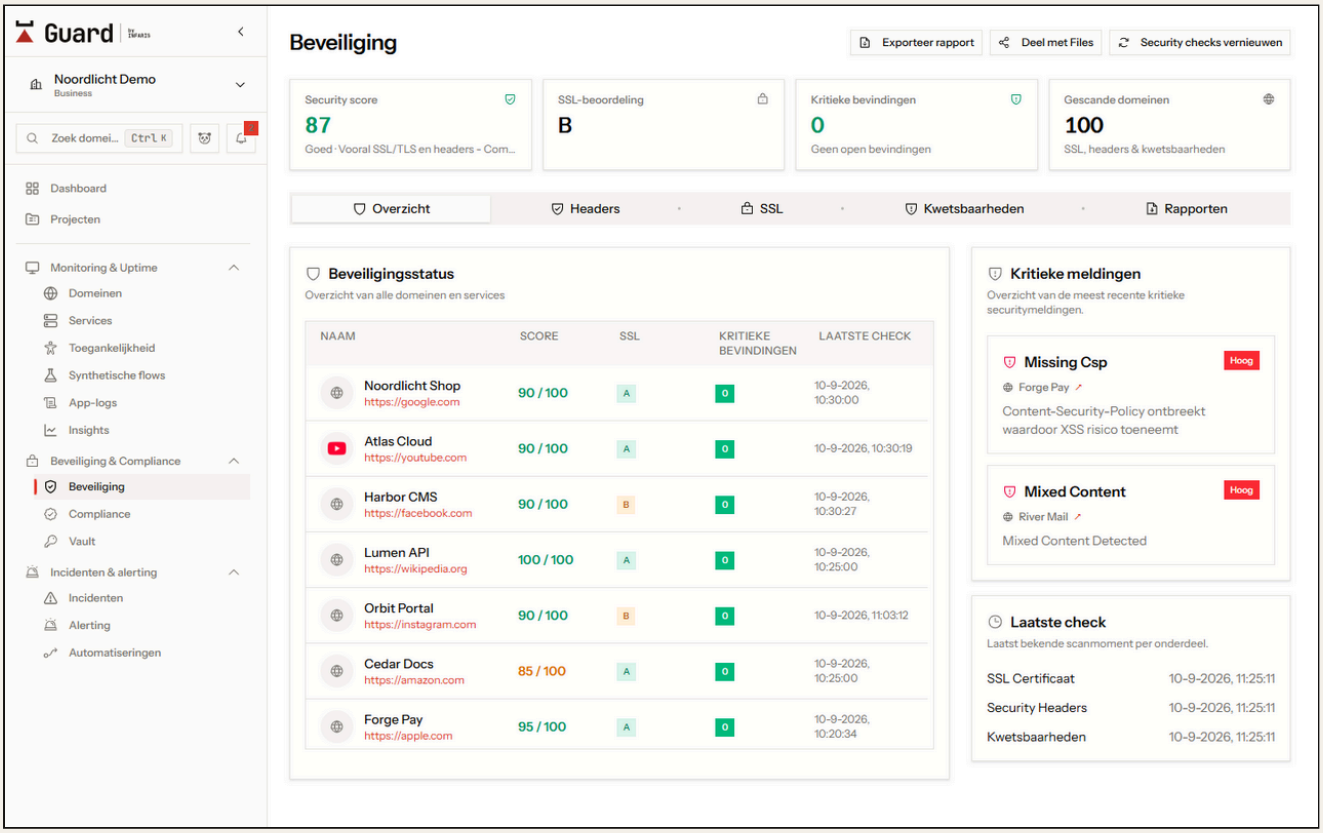
LAAG 03

Is het veilig, en kunt u dat aantonen?

Beveiliging is in deze opzet geen apart product maar een laag over dezelfde domeinen, machines en koppelingen die u al bewaakt. Dat is het verschil tussen een scan die per kwartaal een pdf oplevert en een score die meebeweegt met wat u vandaag hebt uitgerold.

- **Securityscore per domein.** Headers, cookies, versleuteling, gemengde inhoud en blootgestelde paden, samengevat in één cijfer met de bevindingen eronder. Bruikbaar richting de klant, gedetailleerd genoeg voor uw engineer.
- **CVE's tegen uw eigen stack.** Kwetsbaarheden worden gematcht tegen wat er werkelijk draait, inclusief CMS en plugins, zodat u niet duizend adviezen krijgt waarvan er drie op u slaan.
- **Mailbeveiliging.** SPF, DKIM en DMARC, inclusief de stille gevallen waarin het record er wel staat maar niets afdwingt.
- **Vault.** Wachtwoorden, sleutels en tokens bij het product waar ze bij horen, in plaats van in een spreadsheet of een chatgesprek uit 2023.
- **Patchbeheer.** Eén lijst met wat achterloopt, hoe lang al en hoe erg dat is. Dat is de lijst waar een audit naar vraagt.

> Een securityrapport van vorig kwartaal beschrijft een omgeving die u sindsdien twaalf keer hebt uitgerold.



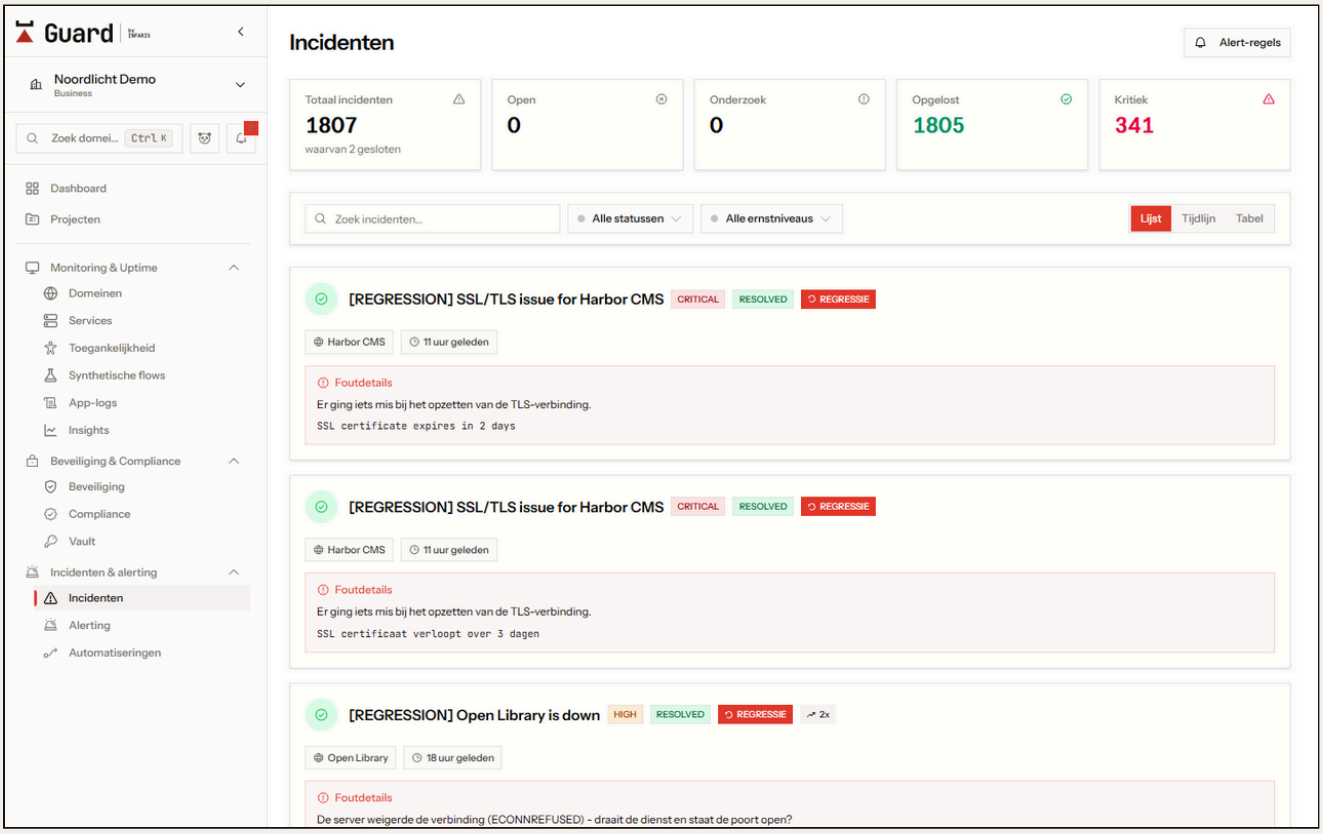
BEVEILIGING SCORE, BEVINDINGEN EN VERLOOP PER DOMEIN

LAAG 04

Wie weet het als eerste, en wat gebeurt er dan?

Meten heeft alleen zin als er iemand op reageert. Deze laag maakt van een meting een ingreep, en van een ingreep een verhaal dat u kunt navertellen.

- **Incidenten op één tijdlijn.** Signalen uit alle lagen komen samen in één incident, met de gebeurtenissen eromheen. Een deploy, een DNS-wijziging en een piek in fouten staan dan onder elkaar en niet in drie systemen.
- **Alerting waar uw team al is.** Slack, Teams, Discord, Telegram, e-mail, push of een eigen webhook, met regels per klant, per ernst en per tijdvenster.
- **Automatisering.** Vaste reacties op terugkerende signalen: een herstart, een ticket, een bericht naar de klant. Wat u drie keer met de hand hebt gedaan, hoort een regel te zijn.
- **Publieke statuspagina.** Gebeurt er toch iets, dan laat een heldere statuspagina zien dat u de touwtjes in handen heeft. Dat scheelt telefoontjes, en het scheelt uitleg.
- **Rapportage en SLA.** Per klant, per periode, automatisch. Geen exports meer aan elkaar plakken de week voor het kwartaalgesprek.
- **MCP, CLI en API.** Alles wat het dashboard laat zien is ook opvraagbaar vanuit uw eigen scripts, uw eigen portaal of een AI-assistent die uw team gebruikt.



INCIDENTEN ELK SIGNAAL, MET DE CONTEXT EROMHEEN

HOOFDSTUK 05

Vijf niveaus. De meeste providers zitten op twee.

Monitoring invoeren is niet één stap maar vijf, en de winst zit niet in de eerste. Gebruik het model hieronder om te bepalen waar u nu staat, per klant en niet als geheel. De verschillen binnen uw eigen portfolio zijn vaak groter dan u denkt.

NIVEAU	HOE U HET HERKENT	WAT DE KLANT MERKT
00 BLIND	Geen structurele controle. Problemen komen binnen via de klantenservice.	Hij is altijd de eerste die het weet.
01 PINGEND	Uptime wordt bewaakt, de rest niet. Meldingen komen in een mailbox binnen.	Harde storingen worden opgemerkt, de rest niet.
02 VERZAMELD	Alle vier de lagen worden gemeten, maar in losse tools en zonder gedeelde tijdlijn.	U weet meer, maar reageert nog altijd nadat het al misging.
03 VERBONDEN	Eén tijdlijn, één alarmroute, duidelijke eigenaren en afgesproken reactietijden per ernst.	Storingen worden korter en zeldzamer.
04 VOORSPELLEND	Trends en drempels leiden tot ingrepen voordat iets stukgaat. Terugkerende reacties zijn geautomatiseerd.	Hij merkt vooral dat hij u zelden hoeft te bellen.

De drie afspraken die het verschil maken

De sprong van niveau 02 naar 03 is geen aanschaf maar een afspraak. Drie stuks, en ze passen op een A4.

AFSPRAAK 01

Elke melding heeft een eigenaar

Leg per ernstniveau vast wie onderzoekt, herstelt en controleert. Dat kan uw team zijn, of Infaris binnen de afgesproken inzet en reactietijd.

AFSPRAAK 02

Drempels per klant, niet per tool

Wat voor een webshop kritiek is, is voor een brochuresite ruis. Stel drempels in per klant, anders leert uw team meldingen wegklikken.

AFSPRAAK 03

Wat drie keer gebeurde, wordt een regel

Elke handeling die uw team voor de derde keer handmatig doet, is een kandidaat voor automatisering. Houd dat lijstje expliciet bij.

HOOFDSTUK 06

Controle die u niet kunt aantonen, telt niet mee.

Er komt een moment waarop iemand vraagt om bewijs. Een klant die zijn eigen NIS2-verplichting doorvertaalt naar zijn leveranciers. Een auditor die een ISO 27001-certificering voorbereidt. Een verzekeraar. Of gewoon een prospect die weten wil hoe u het aanpakt.

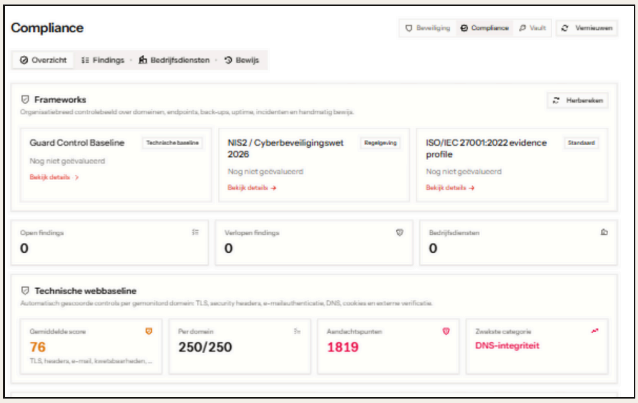
Op dat moment is een tool die alleen alarm slaat niet genoeg. U hebt historie nodig, en die historie moet ergens vandaan komen waar niemand hem achteraf kan bijstellen.

WAT ER GEVRAAGD WORDT

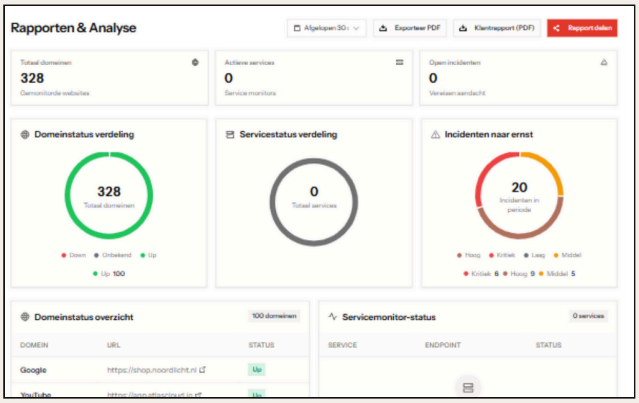
- Welke systemen vallen onder uw beheer, en sinds wanneer.
- Welke kwetsbaarheden bekend waren, en wanneer ze zijn gedicht.
- Hoeveel incidenten er waren, hoe lang ze duurden en wat de oorzaak was.
- Of de afgesproken beschikbaarheid werkelijk is gehaald.

WAT HET OPLEVERT ALS U HET HEEFT

- Een compliance-overzicht dat NIS2, ISO 27001 en een eigen baseline naast uw werkelijke meetgegevens legt.
- Rapporten per klant en per periode, automatisch, in uw eigen huisstijl.
- Een SLA-overzicht dat laat zien of de norm is gehaald, zonder rekenwerk vooraf.
- Een publieke statuspagina die tijdens een storing het gesprek voert dat u anders vijftien keer moet voeren.



COMPLIANCE NORM NAAST METING



RAPPORTAGE PER KLANT, PER PERIODE

PRAKTISCH

Begin met het kwartaalrapport, niet met de certificering. Zodra uw klanten elk kwartaal een overzicht krijgen dat klopt, hebt u de historie al staan die een auditor later vraagt. Andersom werkt het zelden.

HOOFDSTUK 07

Niet alles tegelijk. Wel in deze volgorde.

De meest gemaakte fout is alles tegelijk aanzetten voor alle klanten. Dan krijgt u in week één een stroom meldingen. Uw team leert er een groot deel terecht te negeren, maar klikt daarna ook meldingen weg die wel aandacht verdienen. Bouw het op in drie blokken van dertig dagen.

DAG 1 TOT 30 · INVENTARISEREN EN ZIEN

- Breng alle domeinen en subdomeinen in kaart, inclusief de vergeten. Groepeer ze per klant.
- Zet uptime, SSL en DNS aan voor alles. Nog geen alarmering naar buiten, alleen meten.
- Draai één keer een volledige securityscan over het hele portfolio en gebruik de uitkomst als nulmeting.
- Kies drie klanten waar het risico het grootst is. Die gaan als eerste naar de volgende fase.

DAG 31 TOT 60 · VERDIEPEN EN ROUTEREN

- Bouw synthetische flows voor het pad dat bij elke klant geld oplevert. Begin met afrekenen en inloggen.
- Zet Insights aan op de belangrijkste sites, zodat u echte bezoekersdata opbouwt in plaats van testscores.
- Richt de alarmroute in: per ernst een kanaal, een eigenaar en een reactietijd. Leg dat schriftelijk vast.
- Stem drempels af per klant. Reken op twee rondes bijstellen, dat is normaal.

DAG 61 TOT 90 · AANTONEN EN AUTOMATISEREN

- Zet het eerste kwartaalrapport klaar en bespreek het met drie klanten. Hun vragen bepalen wat er nog mist.
- Publiceer een statuspagina voor de klanten met de meeste eindgebruikers.
- Automatiseer de drie handelingen die uw team in deze periode het vaakst met de hand deed.
- Leg de nulmeting van dag 1 naast de stand van dag 90. Dat is meteen uw verkoopverhaal.

EÉN VALKUIL OM TE VERMIJDEN

Zet alarmering pas aan als de drempels kloppen. Een team dat in de eerste week leert dat meldingen meestal niets betekenen, klikt ze een jaar later nog steeds weg. Vertrouwen in het alarm is het product, niet het alarm zelf.

NA DAG 30

Een complete inventaris en een nulmeting. Alleen dat gesprek is bij de meeste klanten al een verkoopgesprek.

NA DAG 60

Meldingen die kloppen, bij de juiste persoon, binnen een afgesproken tijd. Dit is de sprong naar niveau 03.

NA DAG 90

Een rapportage die u durft te versturen, en een aantoonbaar verschil met de nulmeting van dag 1.

HOOFDSTUK 08

Zestien vragen over uw eigen omgeving.

Loop ze langs voor één klant, niet voor uw hele portfolio. Blijven er meer dan vier vakjes leeg, dan zit die klant op niveau 02 of lager uit hoofdstuk 05.

- [ ] Ik heb een actuele lijst van élk domein en subdomein van deze klant, inclusief oude campagne- en testomgevingen.
- [ ] Ik weet het als een certificaat over dertig dagen verloopt, niet als het verlopen is.
- [ ] Ik krijg een melding als een DNS-record wijzigt, ook als ik die wijziging zelf heb doorgevoerd.
- [ ] Ik meet vanaf meer dan één locatie, zodat een netwerkprobleem geen storing lijkt.
- [ ] Ik weet welke software op de machines draait en wat daarvan achterloopt.
- [ ] Het pad dat bij deze klant geld oplevert wordt automatisch doorlopen, niet alleen de homepage opgevraagd.
- [ ] Ik meet laadtijden van echte bezoekers, niet alleen van een testmachine.
- [ ] Ik zie het als de site uit de index verdwijnt of als belangrijke backlinks wegvallen.
- [ ] SPF, DKIM en DMARC staan goed en dwingen ook werkelijk iets af.
- [ ] Kwetsbaarheden worden gematcht tegen wat er bij déze klant draait.
- [ ] Toegangsgegevens staan in een kluis, niet in een spreadsheet of een chatgesprek.
- [ ] Elke melding heeft een eigenaar en een afgesproken reactietijd, ook buiten kantooruren.
- [ ] Meldingen komen binnen waar mijn team al werkt, niet in een ongelezen mailbox.
- [ ] Bij een storing kan de klant zelf zien wat er speelt, zonder te bellen.
- [ ] Ik kan binnen vijf minuten laten zien of de afgesproken beschikbaarheid vorig kwartaal is gehaald.
- [ ] Ik kan aantonen wanneer een bekend lek is gedicht, met datum en bewijs.

0 TOT 2 LEEG

Deze klant zit op niveau 03 of hoger. Richt u op de stap naar voorspellend werken: trends, drempels en automatisering.

3 TOT 6 LEEG

U meet veel, maar het beeld valt uit elkaar. De winst zit in één tijdlijn en een alarmroute met eigenaren, niet in nog een tool.

7 OF MEER LEEG

Begin bij de inventarisatie uit hoofdstuk 07. Vrijwel zeker staan er domeinen open die in geen enkele lijst voorkomen.

TOT SLOT

Wachten tot de telefoon gaat, is spelen met vuur.

Guard is gebouwd om dit model uit te voeren in plaats van het alleen te beschrijven. Beveiliging, performance, SEO en uptime lopen over dezelfde domeinen, dezelfde klantindeling en dezelfde tijdlijn. De uitkomsten van Guard vormen de basis voor onze diensten: Infaris onderzoekt gevonden problemen, voert afgesproken herstel en verbeteringen uit en controleert het resultaat met Guard. De inzet stemmen we af op uw omgeving en team.

LAAG 01 EN 02

Meten

Uptime, SSL, DNS, services en agent. Synthetische flows, Core Web Vitals, app-logs, WCAG, change detection, SEO en backlinks.

LAAG 03

Beveiligen

Securityscore, CVE-matching tegen uw stack, SPF, DKIM en DMARC, Vault, patchbeheer en compliance tegen NIS2, ISO 27001 of een eigen baseline.

LAAG 04

Reageren

Incidenten op één tijdlijn, alerting naar Slack, Teams, Discord, Telegram, e-mail, push of webhook, automatisering, statuspagina, rapportage, SLA en MCP, CLI en API.

SAMEN AAN DE SLAG

- Probeer de browserextensie op een site van een klant. Die vraagt geen inrichting en geeft binnen een minuut een beeld.
- Zet één klant volledig in, inclusief alle vergeten subdomeinen. De eerste inventarisatie levert vrijwel altijd een verrassing op.
- Vraag een demo aan met uw eigen domeinen. We bespreken welke incidenten en verbeteringen wij voor u kunnen oppakken, met heldere afspraken over toegang, inzet en verantwoordelijkheden.

Guard by INFARIS

guard.infaris.com

DEMO AANVRAGEN: INFARIS.COM/DEMO
VRAGEN: INFARIS.COM/CONTACT

GUARD BY INFARIS · WHITEPAPER, EDITIE 2026.1 · UITGAVE VAN INFARIS, NEDERLAND
MONITOR EVERYTHING. MISS NOTHING. · SCHERMAFBEELDINGEN KOMEN UIT EEN DEMO-OMGEVING MET FICTIEVE KLANTNAMEN.