Guard | by INFARIS

WHITEPAPER
FÜR MANAGED SERVICE PROVIDER

SICHERHEIT · PERFORMANCE · SEO · UPTIME

Messen ist erst der Anfang. Infaris hilft auch bei der Behebung.

Guard führt Ergebnisse aus Scans und Monitoring zusammen. Infaris bietet Leistungen, um die gefundenen Probleme zu untersuchen und zu beheben, abgestimmt auf Ihre Umgebung und Ihr Team.

EBENEN IM BLICK	MESSSTANDORTE	KÜRZESTES INTERVALL	AUSGABE
4	NL DE US UK	30s	2026.1

ZUSAMMENFASSUNG

Die Lücke steckt nicht in Ihrer Firewall. Sie steckt zwischen Ihren Tools.

Ein ernsthafter Angriff verlangt kein Spezialwissen mehr. Wer einem KI-Modell die richtige Frage stellt, bekommt eine Schritt-für-Schritt-Anleitung und funktionierenden Code zurück. Wie viele Akteure Schaden anrichten können, lässt sich nicht mehr überblicken.

Für einen Managed Service Provider ändert das die Rechnung, denn Sie werden an mehr gemessen als nur an Sicherheit. Ein gehackter Shop, ein Server, der hängt, eine Seite, die acht Sekunden braucht, eine Suchposition, die verschwindet: Für den Kunden ist das dieselbe Geschichte. Sein Betrieb steht still, und Sie hätten es kommen sehen müssen.

Guard verbindet Ergebnisse zu Uptime, Sicherheit, Performance und SEO auf einer Zeitleiste. Dieses Whitepaper zeigt, wie Sie binnen neunzig Tagen vom Messen zum Handeln kommen. Auf Grundlage der Befunde bietet Infaris Leistungen für Analyse und Behebung. Wir führen vereinbarte Arbeiten aus und prüfen danach das Ergebnis mit Guard.

DER KERN IN FÜNF ZEILEN

- Die Hürde für einen Angriff ist weg. KI liefert das Wissen, das ein Angreifer früher selbst mitbringen musste.
- Ihr Kunde unterscheidet nicht zwischen Hack, Störung und Langsamkeit. Alle drei kosten Sie Vertrauen.
- Einzelne Tools liefern vier Bilder und keinen Zusammenhang. Ein Vorfall beginnt selten genau dort, wo Sie zufällig hinsehen.
- Eine Meldung ist erst der Anfang. Legen Sie fest, wer untersucht, behebt und das Ergebnis prüft, damit ein Vorfall nicht im Dashboard endet.
- Der Nachweis gehört dazu. NIS2, ISO 27001 und Ihr eigener Quartalsbericht verlangen belegbare Kontrolle, kein Bauchgefühl.

INHALT

01 Die Hürde ist weg 03
02 Angesehen werden Sie, nicht der Angreifer 04
03 Vier Tools, kein Zusammenhang 05
04 Das ganze Haus: vier Ebenen 06
05 Vom Messen zum Eingreifen 10
06 Nachweise für Kunden und Auditoren 11
07 In neunzig Tagen proaktiv 12
08 Checkliste für Ihre eigene Umgebung 13

KAPITEL 01

Einen ernsthaften Cyberangriff kann heute jeder ausführen.

Es genügt, ein beliebiges KI-Modell zu fragen, was zu tun ist, und man bekommt alles Schritt für Schritt: die passenden Anweisungen und fertigen Code. Wissen ist keine Hürde mehr.

Bis vor Kurzem war Wissen der knappe Faktor eines Angriffs. Jemand musste wissen, was eine Injection ist, woran sich ein veraltetes Plugin verrät, wie ein Payload aussieht, der an einem Filter vorbeikommt. Das kostete Jahre. Es filterte von selbst: Die meisten Versuche kamen von automatisierten Bots, die nur an bekannte Türen klopften.

Dieser Filter ist weg. Der Angreifer muss nicht mehr verstehen, was er tut, er muss nur fragen. Die Folge ist doppelt: Es gibt mehr Versuche, und der durchschnittliche Versuch ist besser als früher. Buchstäblich jeder mit einem Internetanschluss ist plötzlich gefährlich.

> **Wissen war die Bremse für die Zahl der Angriffe. Diese Bremse wurde gelöst, und niemand hat sie wieder eingebaut.**
>
> DIE VERSCHIEBUNG, DIE 2025 UND 2026 PRÄGT

Gleichzeitig wächst die Fläche, an die geklopft werden kann. Ein typischer Kunde betreibt heute ein CMS mit fünfzehn Plugins, eine Anbindung an ein Buchhaltungssystem, einen Mailweg über drei Parteien, Zertifikate, die still auslaufen, und DNS bei einem Registrar, für den irgendwann jemand ein Konto angelegt hat. Jeder dieser Bausteine kann die Schwachstelle sein, und keiner meldet sich von selbst.

01

Wissen ist gratis geworden

Was früher Spezialgebiet war, ist heute ein Prompt. Das Können des Angreifers sagt nichts mehr über die Qualität des Angriffs aus.

02

Die Fläche wächst

Plugins, Schnittstellen, Subdomains, Zertifikate, DNS und Mail. Jeder Baustein ist ein Zugang, und vergessene Subdomains sind der beliebteste.

03

Das Zeitfenster schrumpft

Zwischen einer veröffentlichten Schwachstelle und dem ersten Missbrauch liegen oft Stunden. Eine Patchrunde pro Quartal ist dann keine Richtlinie mehr, sondern eine Wette.

WARUM ES SIE FRÜHER TRIFFT ALS IHRE KUNDEN

Ein Managed Service Provider ist per Definition ein attraktiveres Ziel als der Kunde selbst. Bei Ihnen liegt ein Satz Zugänge zu Dutzenden Umgebungen. Das bedeutet zweierlei: Ihre eigene Hygiene wiegt schwerer als die Ihrer Kunden, und Sie müssen belegen können, dass sie stimmt. Um diesen Nachweis geht es in Kapitel 06.

KAPITEL 02

Wenn etwas schiefgeht, schaut der Kunde auf Sie. Nicht auf den Angreifer.

Ihren Kunden ist es gleich, ob es ein Hack war, ein langsamer Server, eine verlorene Suchposition oder ein System, das hängt. Sie wollen eines: dass Shop, Portal und Systeme immer laufen, schnell sind und auffindbar bleiben.

Das ist keine unbillige Erwartung, genau dafür zahlen sie. Unangenehm ist nur, dass der Kunde die vier Ursachen unten nicht unterscheiden kann, während Sie sie in vier verschiedenen Tools nachschlagen müssen.

WAS DER KUNDE MELDET	WAS TATSÄCHLICH DAHINTERSTECKT	WAS ES KOSTET
"Die Seite geht nicht"	Abgelaufenes Zertifikat, geänderter DNS-Eintrag, umgefallener Container	Umsatz pro Minute, plus ein Abend Wiederherstellung
"Es ist so langsam"	Eine schwere Abfrage, ein unkomprimiertes Bild, ein Skript von Dritten	Conversion und Ranking, langsam und unsichtbar
"Wir stehen nicht mehr bei Google"	Eine Robots-Regel, die bei einem Release mitgefahren ist, ein verschwundenes Canonical, weggefallene Backlinks	Monate, um zurückzukommen
"Unsere Mails kommen nicht an"	SPF, DKIM oder DMARC nicht in Ordnung, Domain missbraucht	Zustellbarkeit und Reputation
"Wir wurden gehackt"	Ein Plugin, das drei Monate hinterherhing	Wiederherstellung, Meldepflicht, Vertrauen

> Ein wütender Anruf ist keine Alarmierung. Er ist eine Rechnung, die Sie nicht mehr verhindern können.

In dem Moment, in dem der Betrieb Ihres Kunden stillsteht und Sie es erst durch diesen Anruf erfahren, sind Sie zu spät. Nicht ein bisschen zu spät: Sie beginnen dann drei Dinge gleichzeitig. Herausfinden, was los ist, es beheben, und erklären, warum Sie es nicht früher wussten. Das Dritte kostet am meisten, denn das verlieren Sie immer.

Genau hier knirscht auch das Geschäftsmodell. Ein SLA mit vier Stunden Reaktionszeit ist nichts wert, wenn der Startschuss ein anrufender Kunde ist. Die Uhr lief da schon eine Stunde. Wer proaktiv arbeitet, verkauft keine schnellere Reaktion, sondern einen kleineren Vorfall, und nur diesen Unterschied merkt der Kunde wirklich.

KAPITEL 03

Das Problem ist nicht, dass Sie nichts messen. Es ist, dass niemand das Ganze sieht.

Fast jeder Anbieter hat einen Uptime-Pinger, irgendwo einen Sicherheitsscan, einen Performancebericht aus einem Browser-Tool und eine SEO-Übersicht von der Agentur des Kunden. Jedes Tool hat recht über sein eigenes Stück. Genau darin liegt das Problem, denn eine Störung hält sich nicht an diese Einteilung.

Nehmen Sie ein auslaufendes Zertifikat. Das Uptime-Tool prüft, ob der Server antwortet, und er antwortet einwandfrei, also bleibt das Dashboard grün. Browser verweigern derweil die Verbindung, die Conversion bricht ein, und Suchmaschinen protokollieren Fehler. Wochen später steht etwas im SEO-Bericht. Zu keinem Zeitpunkt stand etwas auf Rot, das auch jemand gelesen hätte.

SYMPTOM 01

Blinde Flecken zwischen den Tools

Jedes Tool bewacht seine eigene Ebene. Was zwischen zwei Ebenen fällt, bewacht niemand. Genau dort beginnen Vorfälle.

SYMPTOM 02

Alarm ohne Eigentümer

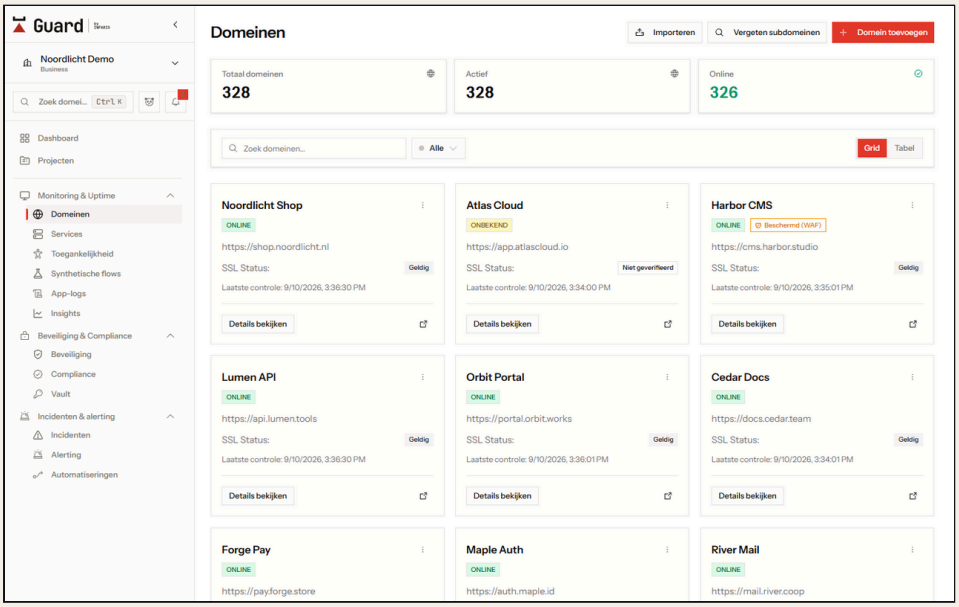
Meldungen laufen an vier Stellen ein, zwei davon liest nur ein Postfach, das niemand betreut. Ohne Route ist eine Meldung dasselbe wie keine Meldung.

SYMPTOM 03

Keine Geschichte im Nachhinein

Fragt der Kunde, wie das letzte Quartal lief, kleben Sie vier Exporte zusammen. Das ist Arbeit, und es überzeugt niemanden.

Es gibt einen vierten Effekt, und der ist der teuerste. Wenn niemand das Ganze sieht, wird jede Meldung ein Einzelereignis statt ein Muster. Beim dritten Mal, dass derselbe Kunde langsam ist, behandeln Sie es wie beim ersten Mal.



DOMAINS ALLE KUNDEN, ALLE DOMAINS, EIN STATUS

KAPITEL 04

Wir prüfen nicht nur, ob die Tür abgeschlossen ist, sondern das ganze Haus.

Sicherheit, Performance, SEO und Uptime, vom Klick bis zur Schnittstelle. Sobald etwas zu haken beginnt, weiß Ihr Team es zuerst und sieht sofort, wo es sitzt.

Das Modell unten hat vier Ebenen. Sie sind nicht einzeln zu haben, denn genau das ist der Fehler aus Kapitel 03. Sie teilen eine Zeitleiste, eine Kundenstruktur und eine Alarmroute. Die nächsten vier Seiten gehen sie einzeln durch.

EBENE 01

Uptime und Stack

Läuft es, und worauf läuft es? Prüfungen aus vier Ländern, SSL und DNS, die Maschinen darunter und was darauf installiert ist.

EBENE 02

Vom Klick zur Schnittstelle

Funktioniert es auch wirklich, für echte Besucher? Synthetische Flows, Core Web Vitals aus echtem Verkehr, Barrierefreiheit und Auffindbarkeit.

EBENE 03

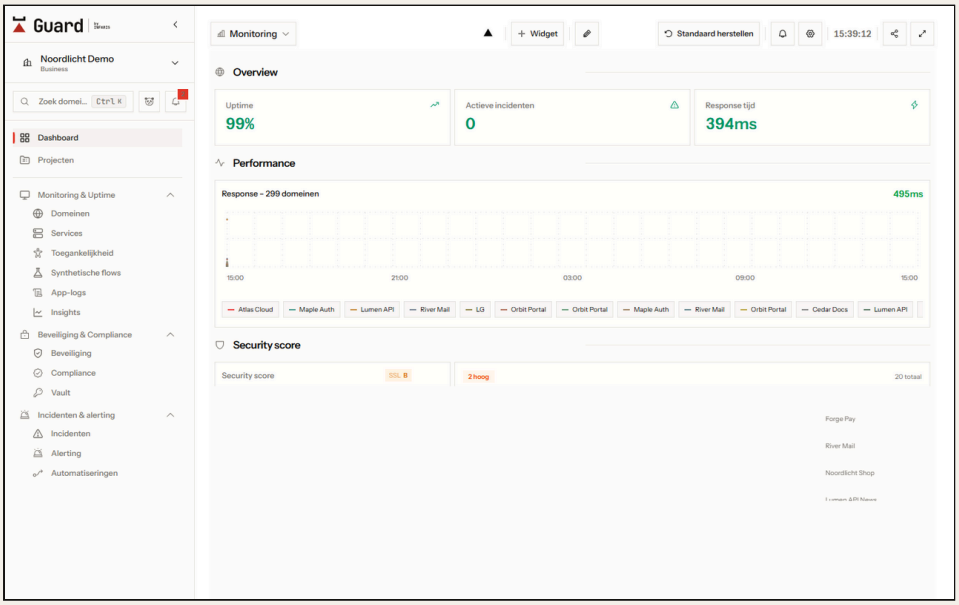
Die Tür und das Schloss

Ist es sicher, und können Sie das belegen? Security-Score, CVEs gegen Ihren eigenen Stack, Mailsicherheit, Geheimnisse und Compliance.

EBENE 04

Früher als der Kunde

Wer weiß es zuerst, und was passiert dann? Vorfälle, Alerting, Automatisierung, Statusseite und Berichte.



DASHBOARD

VIER EBENEN, EIN BILD

EBENE 01

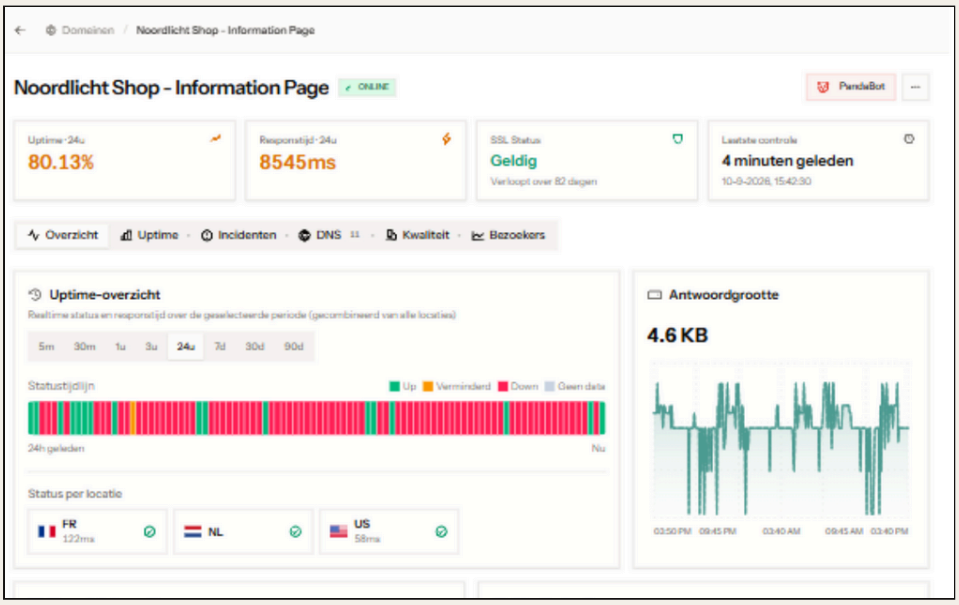
Läuft es, und worauf läuft es?

Die Basisebene beantwortet die Frage, die Ihr Kunde beim Anruf stellt, aber bevor er anruft. Prüfungen laufen alle 30 oder 60 Sekunden aus den Niederlanden, Deutschland, den Vereinigten Staaten und dem Vereinigten Königreich, damit eine Störung bei einem Provider nicht wie eine Störung beim Kunden aussieht.

- **Uptime und Antwortzeit.** Mehrere Standorte, mehrere Protokolle, mit einer Antwortzeit, die Sie über die Zeit verfolgen können statt nur einem grünen oder roten Punkt.
- **SSL und DNS.** Die vollständige Zertifikatskette, das Ablaufdatum rechtzeitig, und eine Meldung, sobald sich ein DNS-Eintrag ändert. Letzteres ist häufiger ein Angriff als ein Zufall.
- **Services und Topologie.** Welche Maschinen es gibt, was darauf läuft, wie sie voneinander abhängen und welche Pakete hinterherhinken. Patchmanagement als Liste, nicht als Vorsatz.
- **Der Agent auf der Maschine selbst.** Ein schlanker Agent meldet Speicherplatz, Arbeitsspeicher, Prozesse und Updates von innen. Von außen sieht man nämlich nicht, dass die Platte in zwei Tagen voll ist.
- **Projekte pro Kunde.** Alles nach Kunde oder Umgebung gruppiert, damit die Rufbereitschaft nicht raten muss, welche Domain zu wem gehört.

WO ES MEISTENS SCHIEFGEHT

Vergessene Subdomains. Eine alte Staging-Umgebung, eine Kampagnenseite von 2021, eine Testdomain, die nie aufgeräumt wurde. Sie stehen offen, laufen mit veralteter Software und tauchen in keiner Liste auf. Beginnen Sie Ihre Inventur dort, nicht bei der Produktivseite, die Sie ohnehin bewachen.



DOMAINDETAIL UPTIME, ANTWORTZEIT UND STATUS JE STANDORT

EBENE 02

Funktioniert es auch wirklich, für echte Besucher?

Ein Server, der antwortet, ist noch kein funktionierender Shop. Diese Ebene testet, was der Besucher tatsächlich tut, und misst, was er tatsächlich erlebt, einschließlich des Teils, der auf seinem eigenen Gerät passiert.

NACHGESPIELT

Synthetische Flows laufen in einem echten Chromium und klicken den Weg ab, der Geld bringt: anmelden, suchen, in den Warenkorb, bezahlen. Fällt Schritt vier aus, wissen Sie es um drei Uhr nachts und nicht um neun.

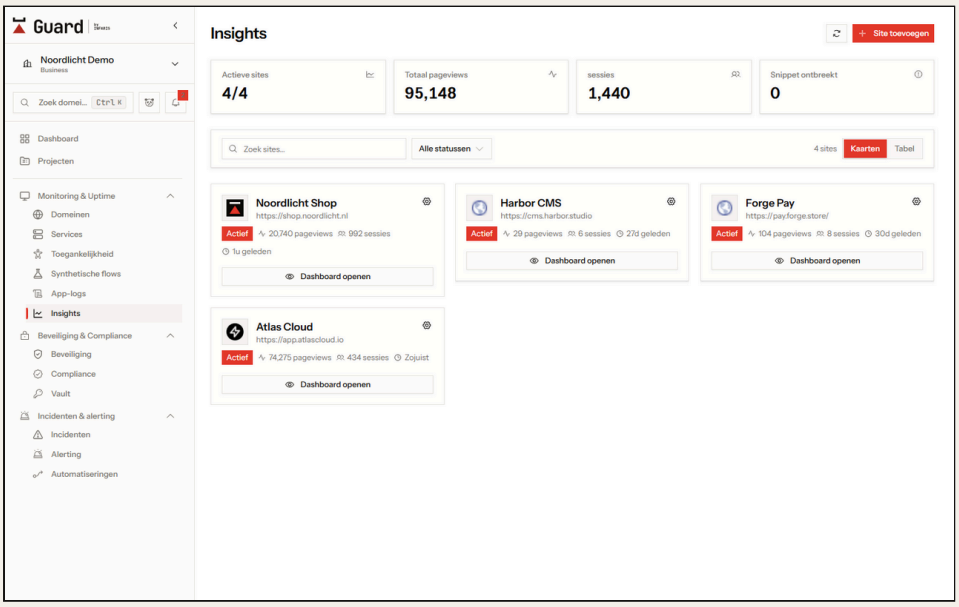
Change Detection vergleicht Seiten mit dem Stand von gestern. Ein Preis, der springt, ein Formular, das verschwindet, oder ein Skript, das dazukommt, fällt sofort auf.

TATSÄCHLICH GEMESSEN

Insights sammelt Core Web Vitals echter Besucher: wie schnell die Seite auf ihrem Gerät und ihrer Verbindung geladen hat. Das ist der Wert, nach dem Suchmaschinen steuern, nicht das Ergebnis einer Testmaschine am Glasfaseranschluss.

App-Logs fangen die Fehler ab, die der Besucher nicht meldet, aber erlebt, und verknüpfen sie mit dem Zeitpunkt, an dem sie begannen.

- **Barrierefreiheit.** WCAG-Prüfungen je Seite, mit einer Bewertung, die misst, wie zugänglich die Seite ist, und nicht wie komplex. Relevant, seit die europäische Richtlinie auch kommerzielle Seiten erfasst.
- **SEO und Backlinks.** Auffindbarkeit in derselben Schleife wie der Rest: Indexierbarkeit, Struktur und die Links, die auf den Kunden zeigen. Eine verlorene Suchposition ist eine Störung, nur eine langsame.
- **Die Browser-Erweiterung.** Prüft den gerade geöffneten Tab auf Cookies, Header, Mixed Content, Barrierefreiheit, SEO, Datenschutz und Performance. Praktisch im Erstgespräch, ohne dass vorher etwas eingerichtet werden muss.



INSIGHTS ECHTE BESUCHER, ECHTE LADEZEITEN

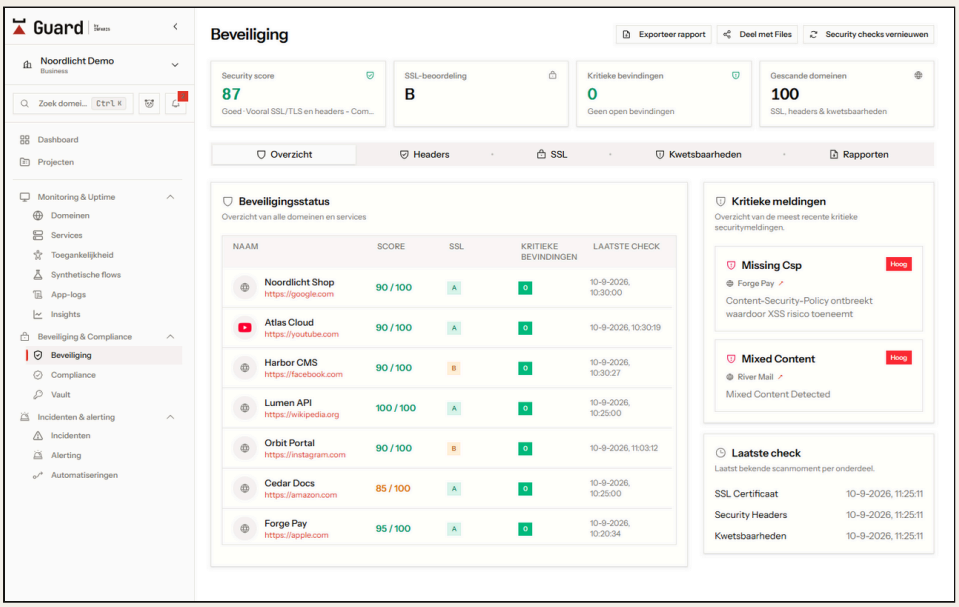
EBENE 03

Ist es sicher, und können Sie das belegen?

Sicherheit ist in diesem Aufbau kein eigenes Produkt, sondern eine Ebene über denselben Domains, Maschinen und Schnittstellen, die Sie ohnehin bewachen. Das ist der Unterschied zwischen einem Scan, der quartalsweise ein PDF liefert, und einem Wert, der sich mit dem bewegt, was Sie heute ausgerollt haben.

- **Security-Score je Domain.** Header, Cookies, Verschlüsselung, Mixed Content und offene Pfade, zusammengefasst in einer Zahl mit den Befunden darunter. Brauchbar gegenüber dem Kunden, detailliert genug für Ihre Technik.
- **CVEs gegen Ihren eigenen Stack.** Schwachstellen werden gegen das abgeglichen, was tatsächlich läuft, CMS und Plugins eingeschlossen, damit Sie nicht tausend Hinweise bekommen, von denen drei zutreffen.
- **Mailsicherheit.** SPF, DKIM und DMARC, samt der stillen Fälle, in denen der Eintrag zwar existiert, aber nichts durchsetzt.
- **Vault.** Passwörter, Schlüssel und Tokens bei dem Produkt, zu dem sie gehören, statt in einer Tabelle oder einem Chatverlauf von 2023.
- **Patchmanagement.** Eine Liste mit dem, was hinterherhinkt, wie lange schon und wie schlimm das ist. Das ist die Liste, nach der ein Audit fragt.

> Ein Sicherheitsbericht vom letzten Quartal beschreibt eine Umgebung, die Sie seither zwölfmal ausgerollt haben.



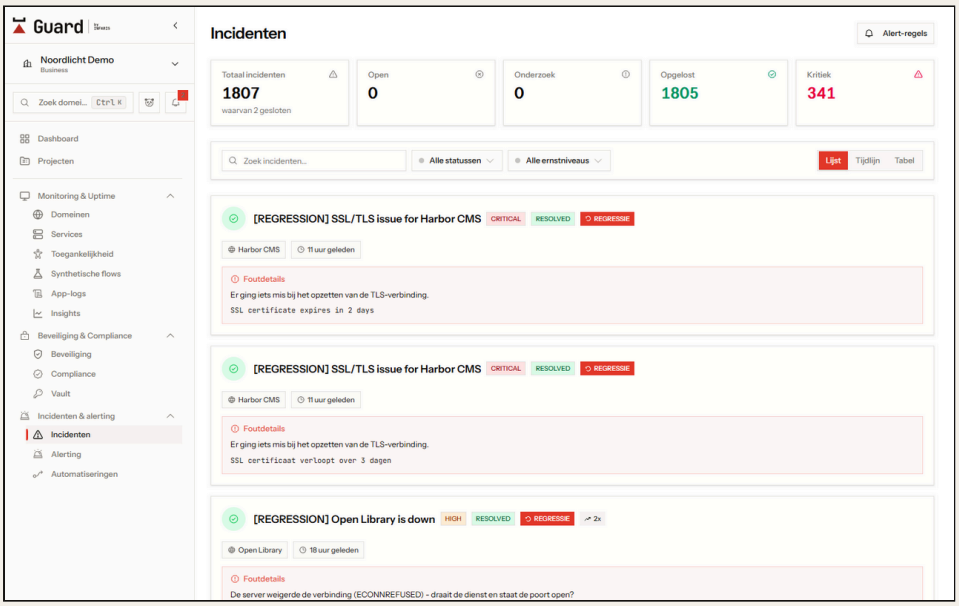
SICHERHEIT WERT, BEFUNDE UND VERLAUF JE DOMAIN

EBENE 04

Wer weiß es zuerst, und was passiert dann?

Messen hat nur Sinn, wenn jemand darauf reagiert. Diese Ebene macht aus einer Messung einen Eingriff und aus einem Eingriff eine Geschichte, die Sie nacherzählen können.

- **Vorfälle auf einer Zeitleiste.** Signale aus allen Ebenen laufen in einem Vorfall zusammen, samt den Ereignissen drumherum. Ein Deploy, eine DNS-Änderung und ein Fehleranstieg stehen dann untereinander statt in drei Systemen.
- **Alerting dort, wo Ihr Team schon ist.** Slack, Teams, Discord, Telegram, E-Mail, Push oder ein eigener Webhook, mit Regeln je Kunde, je Schweregrad und je Zeitfenster.
- **Automatisierung.** Feste Reaktionen auf wiederkehrende Signale: ein Neustart, ein Ticket, eine Nachricht an den Kunden. Was Sie dreimal von Hand gemacht haben, gehört in eine Regel.
- **Öffentliche Statusseite.** Passiert doch etwas, zeigt eine klare Statusseite, dass Sie die Fäden in der Hand halten. Das spart Anrufe und es spart Erklärungen.
- **Berichte und SLA.** Je Kunde, je Zeitraum, automatisch. Kein Zusammenkleben von Exporten mehr in der Woche vor dem Quartalsgespräch.
- **MCP, CLI und API.** Alles, was das Dashboard zeigt, ist auch aus Ihren eigenen Skripten, Ihrem eigenen Portal oder einem KI-Assistenten Ihres Teams abrufbar.



VORFÄLLE JEDES SIGNAL, MIT SEINEM KONTEXT

KAPITEL 05

Fünf Stufen. Die meisten Anbieter stehen auf zwei.

Monitoring einzuführen ist nicht ein Schritt, sondern fünf, und der Gewinn liegt nicht im ersten. Nutzen Sie das Modell unten, um zu bestimmen, wo Sie stehen, je Kunde und nicht insgesamt. Die Spannweite im eigenen Portfolio ist meist größer als gedacht.

STUFE	WORAN SIE SIE ERKENNEN	WAS DER KUNDE MERKT
00 BLIND	Keine strukturelle Prüfung. Probleme kommen über den Kundendienst herein.	Er weiß es immer als Erster.
01 PINGEND	Uptime wird bewacht, der Rest nicht. Meldungen landen in einem Postfach.	Harte Störungen fallen auf, der Rest nicht.
02 GESAMMELT	Alle vier Ebenen werden gemessen, aber in einzelnen Tools und ohne gemeinsame Zeitleiste.	Sie wissen mehr, reagieren aber weiter im Nachhinein.
03 VERBUNDEN	Eine Zeitleiste, eine Alarmroute, klare Eigentümer und vereinbarte Reaktionszeiten je Schweregrad.	Störungen werden kürzer und seltener.
04 VORAUSSCHAUEND	Trends und Schwellen führen zu Eingriffen, bevor etwas kaputt geht. Wiederkehrende Reaktionen sind automatisiert.	Er merkt vor allem, dass er selten anrufen muss.

Die drei Vereinbarungen, die den Unterschied machen

Der Sprung von Stufe 02 auf 03 ist keine Anschaffung, sondern eine Vereinbarung. Drei Stück, und sie passen auf eine Seite.

VEREINBARUNG 01

Jede Meldung hat einen Eigentümer

Legen Sie je Schweregrad fest, wer untersucht, behebt und prüft. Das kann Ihr Team oder Infaris im vereinbarten Umfang und innerhalb der vereinbarten Reaktionszeit übernehmen.

VEREINBARUNG 02

Schwellen je Kunde, nicht je Tool

Was für einen Shop kritisch ist, ist für eine Broschürenseite Rauschen. Setzen Sie Schwellen je Kunde, sonst lernt Ihr Team, Meldungen wegzuklicken.

VEREINBARUNG 03

Was dreimal vorkam, wird eine Regel

Jeder Handgriff, den Ihr Team zum dritten Mal manuell macht, ist ein Kandidat für Automatisierung. Führen Sie diese Liste ausdrücklich.

KAPITEL 06

Kontrolle, die Sie nicht belegen können, zählt nicht.

Irgendwann fragt jemand nach Nachweisen. Ein Kunde, der seine eigene NIS2-Pflicht an seine Lieferanten weitergibt. Ein Auditor, der eine ISO-27001-Zertifizierung vorbereitet. Ein Versicherer. Oder schlicht ein Interessent, der wissen will, wie Sie arbeiten.

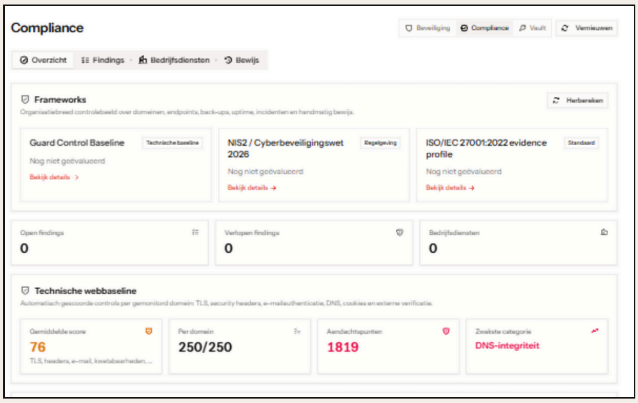
In dem Moment reicht ein Werkzeug, das nur Alarm schlägt, nicht. Sie brauchen Historie, und diese Historie muss von einer Stelle kommen, an der sie niemand nachträglich zurechtrücken kann.

WAS GEFRAGT WIRD

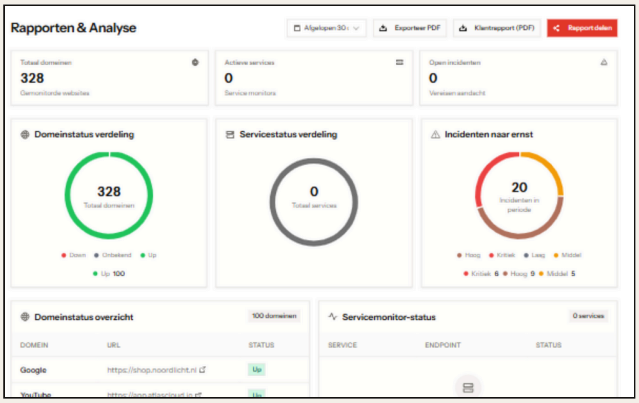
- Welche Systeme Sie betreuen, und seit wann.
- Welche Schwachstellen bekannt waren, und wann sie geschlossen wurden.
- Wie viele Vorfälle es gab, wie lange sie dauerten und was die Ursache war.
- Ob die vereinbarte Verfügbarkeit tatsächlich erreicht wurde.

WAS ES BRINGT, WENN SIE ES HABEN

- Eine Compliance-Übersicht, die NIS2, ISO 27001 und eine eigene Baseline neben Ihre echten Messwerte stellt.
- Berichte je Kunde und je Zeitraum, automatisch, im eigenen Erscheinungsbild.
- Eine SLA-Übersicht, die zeigt, ob das Ziel erreicht wurde, ohne vorheriges Rechnen.
- Eine öffentliche Statusseite, die während einer Störung das Gespräch führt, das Sie sonst fünfzehnmal führen.



COMPLIANCE NORM NEBEN MESSUNG



BERICHTE JE KUNDE, JE ZEITRAUM

PRAKTISCH

Beginnen Sie mit dem Quartalsbericht, nicht mit der Zertifizierung. Sobald Ihre Kunden jedes Quartal eine Übersicht bekommen, die stimmt, haben Sie die Historie bereits stehen, nach der ein Auditor später fragt. Andersherum klappt es selten.

KAPITEL 07

Nicht alles auf einmal. Aber in dieser Reihenfolge.

Der häufigste Fehler ist, alles gleichzeitig für alle Kunden einzuschalten. Dann kommt in Woche eins ein Strom von Meldungen. Ihr Team lernt, viele davon zu Recht zu ignorieren, klickt aber bald auch Meldungen weg, die Aufmerksamkeit verdienen. Bauen Sie es in drei Blöcken zu dreißig Tagen auf.

TAG 1 BIS 30 · INVENTUR UND SICHT

- Erfassen Sie alle Domains und Subdomains, auch die vergessenen. Gruppieren Sie sie je Kunde.
- Schalten Sie Uptime, SSL und DNS für alles ein. Noch keine Alarmierung nach außen, nur messen.
- Lassen Sie einmal einen vollständigen Sicherheitsscan über das Portfolio laufen und nutzen Sie das Ergebnis als Nullmessung.
- Wählen Sie die drei Kunden mit dem größten Risiko. Die gehen zuerst in die nächste Phase.

TAG 31 BIS 60 · VERTIEFEN UND ROUTEN

- Bauen Sie synthetische Flows für den Weg, der bei jedem Kunden Geld bringt. Beginnen Sie mit Bezahlen und Anmelden.
- Schalten Sie Insights auf den wichtigsten Seiten ein, damit Sie echte Besucherdaten aufbauen statt Testwerte.
- Richten Sie die Alarmroute ein: je Schweregrad ein Kanal, ein Eigentümer und eine Reaktionszeit. Halten Sie das schriftlich fest.
- Stimmen Sie die Schwellen je Kunde ab. Rechnen Sie mit zwei Runden Nachjustieren, das ist normal.

TAG 61 BIS 90 · BELEGEN UND AUTOMATISIEREN

- Stellen Sie den ersten Quartalsbericht bereit und besprechen Sie ihn mit drei Kunden. Ihre Fragen zeigen, was noch fehlt.
- Veröffentlichen Sie eine Statusseite für die Kunden mit den meisten Endnutzern.
- Automatisieren Sie die drei Handgriffe, die Ihr Team in diesem Zeitraum am häufigsten von Hand gemacht hat.
- Legen Sie die Nullmessung von Tag 1 neben den Stand von Tag 90. Das ist direkt Ihre Verkaufsgeschichte.

EINE FALLE, DIE SIE VERMEIDEN SOLLTEN

Schalten Sie die Alarmierung erst ein, wenn die Schwellen stimmen. Ein Team, das in Woche eins lernt, dass Meldungen meist nichts bedeuten, klickt sie ein Jahr später immer noch weg.

NACH TAG 30

Eine vollständige Inventur und eine Nullmessung. Allein dieses Gespräch ist bei den meisten Kunden ein Verkaufsgespräch.

NACH TAG 60

Meldungen, die stimmen, bei der richtigen Person, in vereinbarter Zeit. Das ist der Sprung auf Stufe 03.

NACH TAG 90

Ein Bericht, den Sie zu versenden wagen, und ein belegbarer Unterschied zur Nullmessung von Tag 1.

KAPITEL 08

Sechzehn Fragen zu Ihrer eigenen Umgebung.

Gehen Sie sie für einen Kunden durch, nicht für Ihr ganzes Portfolio. Bleiben mehr als vier Kästchen leer, steht dieser Kunde auf Stufe 02 oder darunter aus Kapitel 05.

- [ ] Ich habe eine aktuelle Liste jeder Domain und Subdomain dieses Kunden, alte Kampagnen- und Testumgebungen eingeschlossen.
- [ ] Ich weiß es, wenn ein Zertifikat in dreißig Tagen abläuft, nicht erst wenn es abgelaufen ist.
- [ ] Ich bekomme eine Meldung, wenn sich ein DNS-Eintrag ändert, auch wenn ich die Änderung selbst vorgenommen habe.
- [ ] Ich messe von mehr als einem Standort, damit ein Netzproblem nicht wie eine Störung aussieht.
- [ ] Ich weiß, welche Software auf den Maschinen läuft und was davon hinterherhinkt.
- [ ] Der Weg, der bei diesem Kunden Geld bringt, wird automatisch durchlaufen, nicht nur die Startseite abgerufen.
- [ ] Ich messe Ladezeiten echter Besucher, nicht nur einer Testmaschine.
- [ ] Ich sehe es, wenn die Seite aus dem Index fällt oder wichtige Backlinks wegbrechen.
- [ ] SPF, DKIM und DMARC stehen richtig und setzen auch wirklich etwas durch.
- [ ] Schwachstellen werden gegen das abgeglichen, was bei diesem Kunden läuft.
- [ ] Zugangsdaten liegen in einem Tresor, nicht in einer Tabelle oder einem Chatverlauf.
- [ ] Jede Meldung hat einen Eigentümer und eine vereinbarte Reaktionszeit, auch außerhalb der Geschäftszeiten.
- [ ] Meldungen kommen dort an, wo mein Team ohnehin arbeitet, nicht in einem ungelesenen Postfach.
- [ ] Bei einer Störung sieht der Kunde selbst, was los ist, ohne anzurufen.
- [ ] Ich kann in fünf Minuten zeigen, ob die vereinbarte Verfügbarkeit im letzten Quartal erreicht wurde.
- [ ] Ich kann belegen, wann eine bekannte Lücke geschlossen wurde, mit Datum und Nachweis.

0 BIS 2 LEER

Dieser Kunde steht auf Stufe 03 oder höher. Zielen Sie auf den Schritt zum vorausschauenden Arbeiten: Trends, Schwellen und Automatisierung.

3 BIS 6 LEER

Sie messen viel, aber das Bild zerfällt. Der Gewinn liegt in einer Zeitleiste und einer Alarmroute mit Eigentümern, nicht in noch einem Tool.

7 ODER MEHR LEER

Beginnen Sie bei der Inventur aus Kapitel 07. Mit hoher Wahrscheinlichkeit stehen Domains offen, die in keiner Liste vorkommen.

ZUM SCHLUSS

Zu warten, bis das Telefon klingelt, ist ein Spiel mit dem Feuer.

Guard ist gebaut, um dieses Modell auszuführen und nicht nur zu beschreiben. Sicherheit, Performance, SEO und Uptime laufen über dieselben Domains, dieselbe Kundenstruktur und dieselbe Zeitleiste. Die Ergebnisse von Guard bilden die Grundlage für unsere Leistungen: Infaris untersucht gefundene Probleme, führt vereinbarte Behebungen und Verbesserungen aus und prüft das Ergebnis mit Guard. Unsere Arbeit stimmen wir auf Ihre Umgebung und Ihr Team ab.

EBENE 01 UND 02

Messen

Uptime, SSL, DNS, Services und Agent. Synthetische Flows, Core Web Vitals, App-Logs, WCAG, Change Detection, SEO und Backlinks.

EBENE 03

Absichern

Security-Score, CVE-Abgleich gegen Ihren Stack, SPF, DKIM und DMARC, Vault, Patchmanagement und Compliance gegen NIS2, ISO 27001 oder eine eigene Baseline.

EBENE 04

Reagieren

Vorfälle auf einer Zeitleiste, Alerting nach Slack, Teams, Discord, Telegram, E-Mail, Push oder Webhook, Automatisierung, Statusseite, Berichte, SLA sowie MCP, CLI und API.

GEMEINSAM ANFANGEN

- Probieren Sie die Browser-Erweiterung auf einer Kundenseite. Sie braucht keine Einrichtung und liefert binnen einer Minute ein Bild.
- Nehmen Sie einen Kunden vollständig auf, vergessene Subdomains eingeschlossen. Die erste Inventur bringt fast immer eine Überraschung.
- Fragen Sie eine Demo mit Ihren eigenen Domains an. Wir besprechen, welche Vorfälle und Verbesserungen wir übernehmen können, mit klaren Absprachen zu Zugang, Umfang und Zuständigkeiten.

Guard by INFARIS

guard.infaris.com

DEMO ANFRAGEN: INFARIS.COM/DE/DEMO
FRAGEN: INFARIS.COM/DE/CONTACT

GUARD BY INFARIS · WHITEPAPER, AUSGABE 2026.1 · HERAUSGEGEBEN VON INFARIS, NIEDERLANDE
MONITOR EVERYTHING. MISS NOTHING. · BILDSCHIRMFOTOS STAMMEN AUS EINER DEMO-UMGEBUNG MIT ERFUNDENEN KUNDENNAMEN.