

Als zelfs oma kan hacken, kunt u het zich **niet meer veroorloven** om reactief te werken.

01 DE DREMPEL IS WEG

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. Letterlijk iedereen met een internetverbinding is opeens gevaarlijk. De aanval hoeft niet meer van een specialist te komen.

02 U WORDT AANGEKEKEN

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.

Het moment dat hun bedrijf stilvalt en u dat pas via een woedend telefoontje hoort, bent u te laat. Dan verliest u niet alleen uren, maar het vertrouwen van die klant.

03 GUARD DRAAIT DE ROLLEN OM

Wachten tot de telefoon gaat, is spelen met vuur.

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 waar het zit. U grijpt in voordat de klant er iets van merkt.

En als er toch iets gebeurt, laat een heldere statuspagina zien dat u de touwtjes in handen heeft.

HET HELE HUIS

UPTIME EN STACK

VAN KLIK TOT KOPPELING

DE DEUR ÉN HET SLOT

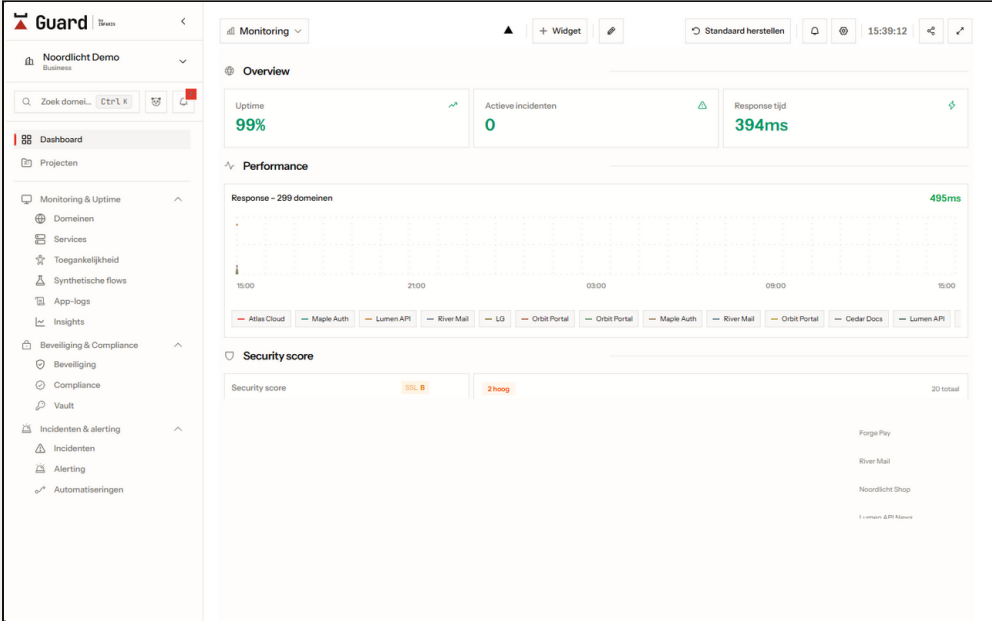
EERDER DAN DE KLANT

Probes elke 30 of 60 seconden vanuit NL, DE, US en UK. **SSL en DNS** (keten, verloop, recordwijziging). **Services** met topologie, inventaris en patchbeheer. De **Go-agent** op de machine zelf. **Projecten** per klant.

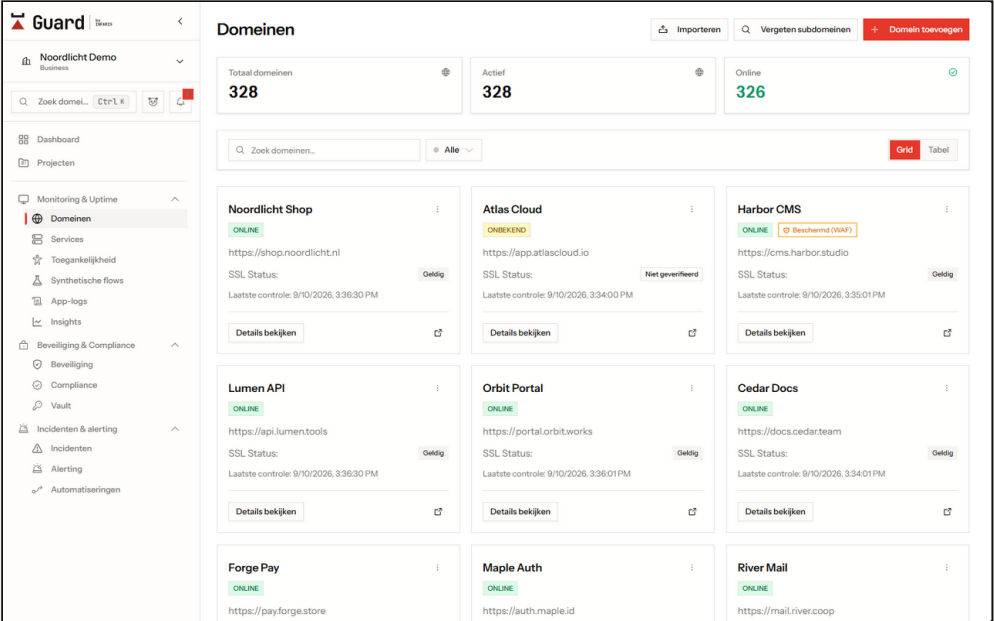
Synthetische flows in echte Chromium. **Insights** voor Core Web Vitals van echte bezoekers. App-logs, WCAG, change detection, SEO-scan en backlinks in dezelfde loop. De extensie scant de tab die openstaat.

Security-score per domein, CVEs tegen uw stack, SPF/DKIM/DMARC. **Vault** bij het product. **Compliance** als bewijs: NIS2, ISO 27001, baseline. Patchbeheer toont wat achterstallig is.

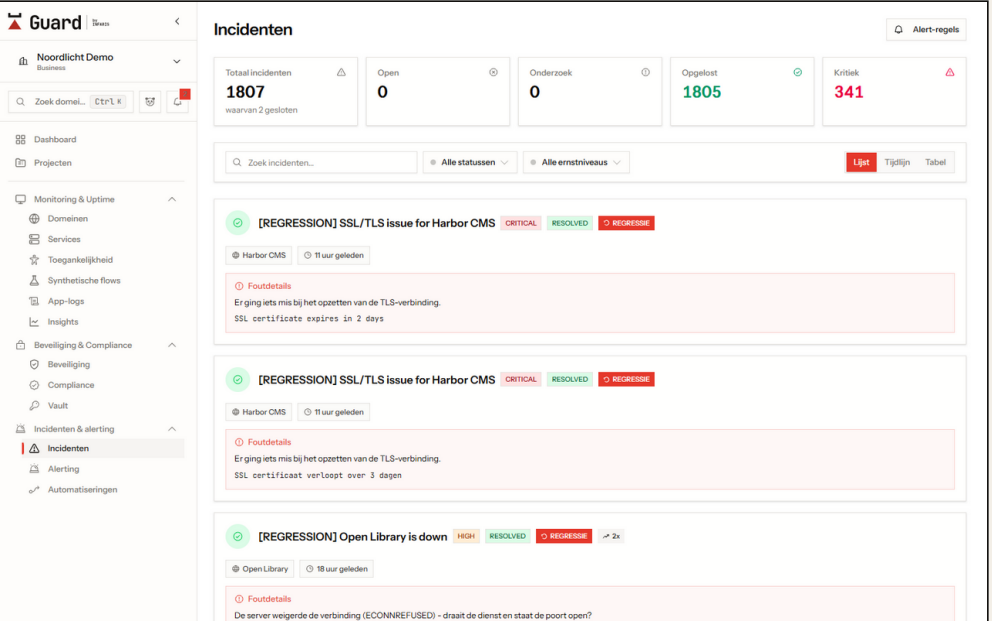
Incidenten op één tijdlijn. Alerting naar Slack, Teams, e-mail, Telegram, push of webhook. Automatisering of PandaBot. Publieke **statuspagina**, Status Hub, rapporten, SLA, MCP/CLI/API.



DASHBOARD U ZIET HET EERST



DOMEINEN HET HELE LANDSCHAP



INCIDENTEN VOOR HET TELEFOONTJE