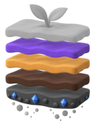
IT en security

Bijlage bij Het verhaal →



LAAG
Toegang, gegevens, beheer en data

Het IT-factsheet

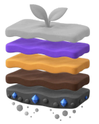
Architectuur, toegang en gegevens op één blad. Om door te sturen naar wie het precies wil weten.

Opzet	Eigen installatie per klant, met één opdracht neergezet. Alles draait in containers, elke versie vastgepind.
Inloggen	Eén inlogsysteem op een open standaard (OIDC), te koppelen aan je Microsoft- of Google-account. Twee stappen: app-code plus herstelcodes.
AI en apps	Zien alleen wat nodig is, nooit meer dan de persoon namens wie ze werken. Model naar keuze: als dienst, Europees of lokaal. Toegang via REST en MCP.
Data	Eigen gegevens in PostgreSQL. Gegevens uit je systemen met geschiedenis en versheid in ClickHouse.
Koppelingen	Eerst alleen lezen. Uitgaand verkeer alleen naar adressen die je toestaat.
Updates	Ondertekende releases, met security-scans bij elke release. Een mislukte update draait zichzelf terug.
Open source	Groundware is open source: de broncode kun je zelf inzien en met je eigen securitytools testen. Kijk op groundware.io.
Beheer	Een kleine beheerdienst voert alleen wijzigingen uit die een mens heeft goedgekeurd.
Waar het draait	Volledig beheerd door Denkbaar in Europese datacenters, of op je eigen server.
Rechten	Standaard geen toegang. Rollen en rechten per persoon en per soort gegevens.
Logboek	Elke wijziging wordt vastgelegd: wie, namens wie, via welke app of assistent.
Geheimen	Wachtwoorden van koppelingen versleuteld in een aparte kluis. Nooit in de browser of een export.
Eigen apps	Draaien buiten de kern en praten alleen via de officiële ingang, met eigen sleutel en logging.
Back-up en herstel	Back-ups buiten de server. Herstelsleutel alleen bij jou. Herstel op een lege server is geoefend.
Weggaan	Export in open formaten. Je data blijft leesbaar zonder Groundware.

KORT **Veilig van de grond tot het scherm**

Meer detail op aanvraag: technische documentatie, een ingevulde beveiligingsvragenlijst of een sessie met je IT-partner.

Privacy en security



LAAG
Toegang, gegevens, beheer en data

Veilig, en aantoonbaar

De vragen die je CISO en privacy officer stellen. Met het antwoord.

Weten we wat er draait?

Alles wat op Groundware landt, staat op één lijst: wie het maakte, welke data het gebruikt, wie erbij kan.

✓ Overzicht in plaats van schaduw-AI

Kunnen we het aantonen?

Rechten per persoon en per soort gegevens, en elke wijziging wordt vastgelegd. Een AI ziet nooit meer dan de persoon namens wie hij werkt.

✓ Hulp bij AVG-verantwoording

Blijven gevoelige gegevens binnen?

Jij kiest per soort gegevens welke AI ze mag zien, of geen enkele. Het logboek laat zien wat er naar buiten ging.

✓ Jij houdt de regie

Zitten we vast?

Open standaarden voor koppelingen en inloggen. Vandaag Claude, morgen een ander model: je data en regels blijven staan.

✓ Geen lock-in

En bij een lek?

Je weet welke tools er zijn en waarop ze draaien. Updates gaan centraal, een mislukte update draait zichzelf terug.

✓ Weten wat je moet bijwerken

Andere vraag?

Stel hem. Juist de lastige vragen maken de basis sterker.

DOCUMENTEN Het verhaal · Voor je IT-afdeling · IT-factsheet JE BENT HIER · Aanbod en prijzen · Overheid en zorg

Plan een kosteloos uur · hallo@denkbaar.nl