

Gebruik van reMarkable in je organisatie

Door: Rijk Prosman
Datum: 29 augustus 2026

1. OVER REMARKABLE

reMarkable is een bedrijf dat de missie heeft om papier en digitale schrijfmiddelen bij elkaar samen te brengen in een zogenaamd “schrijftablet” (paper tablet). reMarkable is gevestigd in Noorwegen en is daarmee een puur Europese organisatie.

De afgelopen jaren is de populariteit van reMarkable schrijftablets sterk toegenomen. Steeds meer mensen ontdekken de voordelen van digitaal schrijven dat voelt als pen op papier, en waarderen de eenvoud, het design en de focus die het apparaat biedt. Deze trend beperkt zich niet tot individueel gebruik; binnen organisaties duiken de reMarkable tablets steeds vaker op als modern alternatief voor notitieblokken tijdens vergaderingen, brainstormsessies en persoonlijke aantekeningen. De groeiende vraag laat zien dat zowel individuen als bedrijven de overstap maken naar deze innovatieve technologie.

In de afgelopen jaren heeft reMarkable een ontwikkeling doorgemaakt van start-up naar volwassen organisatie. Op het gebied van data security zie je dat er meer aandacht is gekomen om ook de groeiende vraag vanuit de zakelijke markt te kunnen beantwoorden. Doordat organisaties steeds hogere eisen stellen aan informatiebeveiliging, was dit ook noodzakelijk. reMarkable probeert het vertrouwen van organisaties te krijgen door via het [Trust Center](https://trust.remarkable.com) op hun website maximaal transparant te zijn hoe zaken op het gebied van legal, compliance en security zijn geregeld. Enkele zaken die we hieruit kunnen noemen zijn:

- De organisatie heeft een ISO 27001 certificering
- Hosting gebeurt in de Google Cloud (België en Nederland)
- Duidelijk overzicht van alle sub-verwerkers

Zie: <https://trust.remarkable.com>

2. RISICO'S VOOR ORGANISATIES

Voor veel organisaties brengen deze ontwikkelingen echter ook nieuwe uitdagingen met zich mee. Zeker in de beginfase was het voor organisaties niet mogelijk om reMarkable-accounts en apparaten centraal te beheren. Als gevolg hiervan ontbrak het aan controle op de beveiliging van zowel accounts als de daadwerkelijke apparaten.

- **Informatie kwetsbaar voor ongeautoriseerde toegang door ontbreken van beveiliging cloud-accounts**

Het gebruik van multi-factor-authenticatie binnen de reMarkable cloud wordt vaak overgelaten aan individuele gebruikers, waardoor in de praktijk lang niet iedereen deze extra beveiliging heeft geactiveerd. En doordat veel gebruikers hun zakelijke Microsoft 365-omgeving koppelen aan de reMarkable cloud, krijgt het reMarkable-account zowel lees- als schrijftoegang tot bedrijfsdata binnen Microsoft. Dit resulteert dat ondanks het strenge beleid van multi-factor-authenticatie binnen Microsoft omgevingen, dezelfde data via de reMarkable cloud zonder

multi-factor-authenticatie toegankelijk is. Deze omzeiling vergrootte het risico dat gevoelige informatie kwetsbaar is voor ongeautoriseerde toegang.

- **Verlies en 'lekken' van data door ontbreken van adequate apparaatbeveiliging**
De beveiliging van reMarkable apparaten wordt vaak overgelaten aan de eindgebruikers zelf. Dit resulteerde erin dat gebruikers geen of makkelijk te raden pincodes gebruikten voor de beveiliging van hun apparaat. Daarnaast is, afhankelijk van het model van de schrijftablet, versleuteling niet mogelijk of standaard niet actief. In het geval dat een schrijftablet verloren of gestolen raakt, levert dit het risico op dat hierdoor gevoelige informatie toegankelijk wordt voor ongeautoriseerde personen.
- **Verlies van bedrijfsdata bij vertrek van medewerker**
Een ander belangrijk aandachtspunt is wanneer medewerkers uit dienst gaan. Doordat accounts vaak op individuele basis zijn aangemaakt en gebruikers deze accounts zelf beheren, hebben organisaties weinig grip op de data die medewerkers via de reMarkable cloud nog in hun bezit hebben of hier nog toegang toe hebben. Dit gebrek aan controle kan leiden tot ongewenst lekken van bedrijfsinformatie en vormt daarmee een potentieel beveiligingsrisico.

3. REMARKABLE FOR BUSINESS

3.1 Inleiding

Sinds enige tijd heeft reMarkable een oplossing voor bovenstaande risico's. Namelijk **reMarkable for Business**. Met reMarkable for Business is het mogelijk om accounts binnen organisaties te beheren, gebruikers via Single Sign-On te laten inloggen apparaten te beheren door beveiligingsmaatregelen af te dwingen en vanaf afstand te kunnen wissen.

Doordat reMarkable nu deze optie biedt, is het aan organisaties hoe ze hier mee omgaan. Blijven we wegstijgen? Of omarmen we deze ontwikkeling en zorgen we ervoor dat we reMarkable schrijftablets op een goede wijze een plaats geven in onze organisatie waarin beleid en alle securitymaatregelen worden gerespecteerd?

3.2 De impact van instappen op reMarkable Connect for Business

3.2.1 Proefperiode en overstap naar business abonnement

reMarkable biedt de mogelijkheid om gebruik te maken van proefperiode van 60 dagen. In deze 60 dagen kan je starten om de organisatie te "on-boarden" in Connect for Business omgeving. Bestaande gebruikers met een consumentenabonnement kunnen overstappen naar het zakelijke abonnement en hoeven het consumentenabonnement dan niet meer te betalen. De kosten voor een business abonnement zijn \$7.99 per maand en bij een jaarplan \$6.99 per maand.

3.2.2 Beheerfuncties voor IT-beheerders

IT-beheerders krijgen extra beheerfuncties, zoals het op afstand wissen van apparaten, het afdwingen van pincodelengte en schermvergrendelingstijd, en het inzien van apparaatinstellingen van gebruikers.

Het is aanbevolen dat de IT-beheerder, die verantwoordelijk is voor het beheer van de apparaten, het bedrijf aanmeldt bij Connect for Business. Voor de registratie van het bedrijf zijn de volgende gegevens nodig:

- Toegang tot de domeinnaamserver (DNS) van de organisatie, zodat een verificatiecode of token die reMarkable verstrekt, kan worden toegevoegd om het domein te verifiëren en te claimen.
- Mogelijkheid om reMarkable toe te voegen aan de Identity Provider van de organisatie voor het configureren van Single Sign-On.

3.2.3 Impact op gebruikers

Voor bestaande gebruikers geldt dat:

- Gebruikers met een **niet-zakelijk e-mailadres**, niet automatisch kunnen overstappen op reMarkable for Business. Daarom zullen organisaties deze gebruikers moeten informeren om voor werkdoeleinden over te stappen op een zakelijk account.
- Gebruikers een **zakelijk e-mailadres**, een melding zullen ontvangen over het zakelijke abonnement. Zij krijgen de keuze om over te stappen naar het zakelijke abonnement of hun e-mailadres te wijzigen om hun account als privé te behouden.

Als er een **nieuwe gebruiker** wordt aangemaakt met een **zakelijk e-mailadres**, zal deze automatisch worden doorgestuurd naar de Single Sign-On oplossing van de organisatie, waardoor deze vanaf dat moment automatisch in de beheerde omgeving terecht komt.

3.3 Beperkingen versleuteling voor specifieke (oudere) modellen

Hoewel de kans groot is dat de oudere reMarkable schrijftablets niet meer gebruikt worden binnen organisaties, is het wel goed om te controleren of alle schrijftablets in uw organisatie versleuteling ondersteunen. In de onderstaande tabel staat een overzicht van de verschillende reMarkable schrijftablets:

Model	Introductiejaar	Versleutelingsopties
reMarkable 1	2017	Geen schijf-encryptie; geen passcode-bescherming
reMarkable 2	2020	Tot firmware v3.18: alleen PIN-vergrendeling. Vanaf v3.18: optionele full-disk-encryptie (via Instellingen handmatig te activeren).
reMarkable Paper Pro	2024	Full-disk-encryptie standaard ingeschakeld, inclusief secure boot en device-login

4. ADVIES – KIJK NIET WEG!

De vraag is niet óf medewerkers de reMarkable gebruiken, maar hoe je er als organisatie mee omgaat. En daarom is het advies:

1. Onderzoek of de reMarkable cloud en het gebruik van Connect for Business voldoet aan het informatiebeveiligings- en privacybeleid van de organisatie.
2. Maak daarna een keuze:
 - o Omarm het gebruik: Neem de tablets op in beleid en beheer, regel SSO, MFA en device-management.
 - o Weer het gebruik: Blokkeer koppelingen met Microsoft 365 en maak het expliciet duidelijk in beleid.

Wat je ook kiest: Kijk niet weg! Juist door eerst te onderzoeken of de reMarkable Business in het beleid van jouw organisatie past en daarna bewust te beslissen, voorkom je dat de voordelen van de reMarkable worden overschaduwed door onnodige risico's.

Bronnen:

- <https://remarkable.com/business>
- <https://remarkable.com/business/connect-for-business>
- <https://trust.remarkable.com>
- <https://support.remarkable.com/s/article/Security-at-reMarkable>
- <https://support.remarkable.com/s/article/Enable-disk-encryption-on-reMarkable-2>