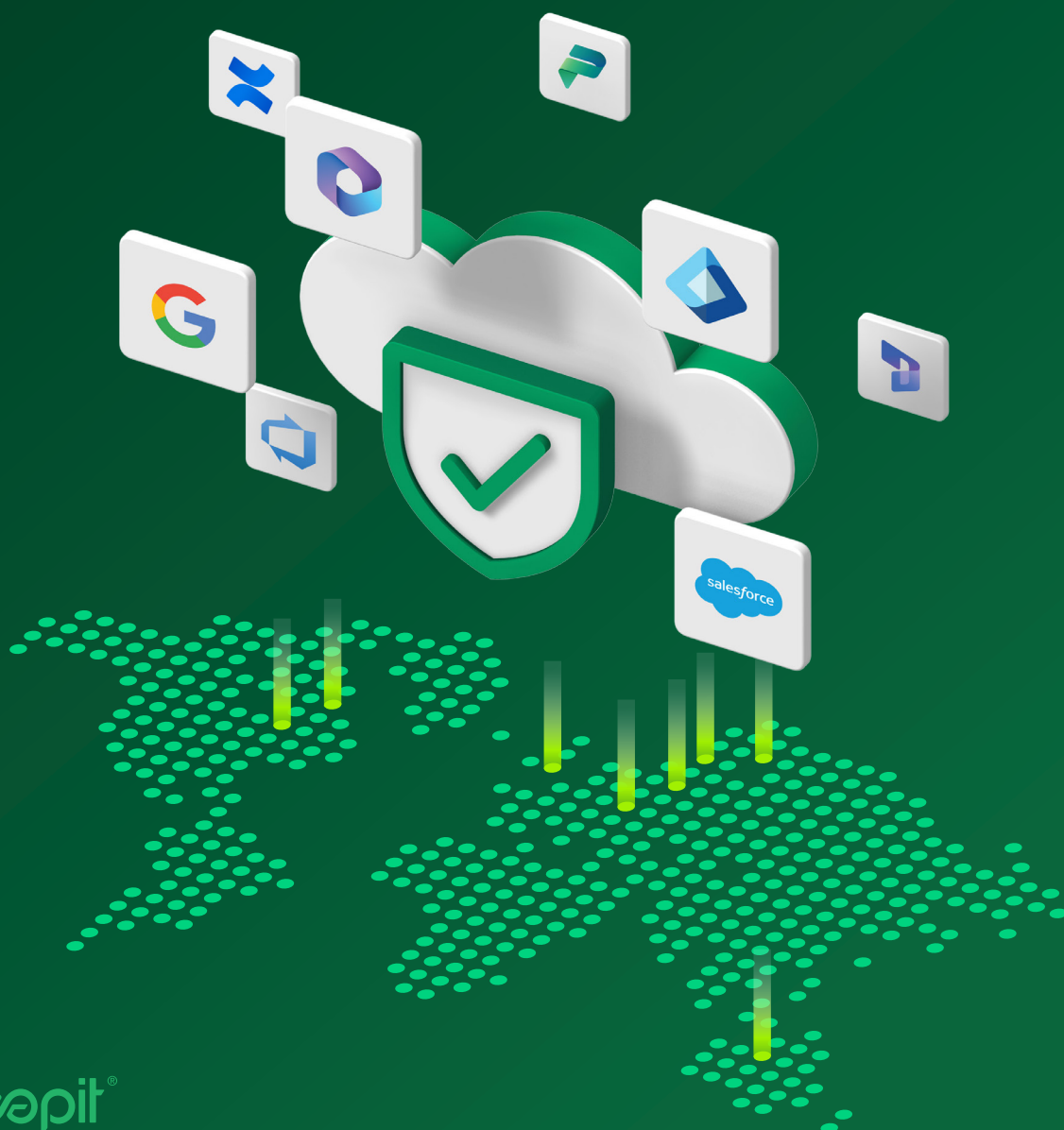


Leg de lat hoger voor gegevensbescherming van SaaS-applicaties



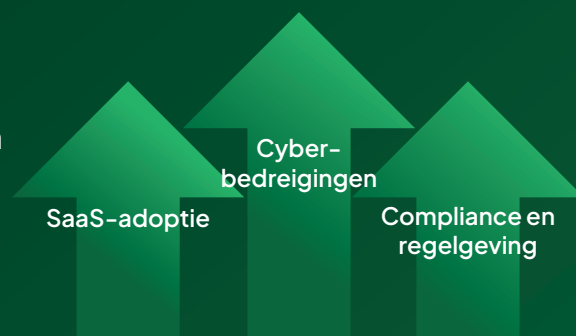
keepit®

Born in the Cloud
Built in Europe

De uitdaging van SaaS-dataprotectie

We leven in cruciale jaren voor cybersecurity. Het gebruik van SaaS-applicaties neemt toe, de hoeveelheid data groeit razendsnel, bedrijven worden steeds meer geconfronteerd met cyberdreigingen en de regelgeving voor datacompliance verandert voortdurend. Tegen die achtergrond vormen kwetsbaarheden in wereldwijde, gedeelde cloud-omgevingen een steeds groter risico.

Hoe kunt u uw SaaS-data in de cloud blijvend beschermen in de toekomst? In deze gids laten wij u zien hoe Keepit de lat hoger legt voor veilige back-up van SaaS-applicaties.



Groeiende SaaS-adoptie in combinatie met toenemende cyberdreiging en veranderende regelgeving betekent dat de lat hoger gelegd moet worden als het gaat om SaaS-dataprotectie.

Inhoud

Uw data, uw verantwoordelijkheid	3
Echte back-up vereist een aparte logische infrastructuur	4
Het Keepit-onderscheid	5
Back-up en recovery voor Microsoft 365	8
Back-up en recovery voor Microsoft Entra ID	10
Samenvatting	11
Over Keepit	12



Uw data, uw verantwoordelijkheid

Steeds meer organisaties zijn afhankelijk van SaaS-technologie (Software-as-a-Service). Daarom is het hoog tijd om de strategieën voor het beheren, beschermen en herstellen van de snel groeiende hoeveelheid SaaS-data onder de loop te nemen. Kritieke services zijn immers gemigreerd van de vertrouwde, on-premises IT-omgeving naar cloud-providers, ver weg van traditionele back-up oplossingen die niet meer voldoen. Bovendien introduceert deze verschuiving een model waarin de SaaS-provider en u als SaaS-klant verantwoordelijkheden delen met betrekking tot gegevensbeveiliging (zie figuur 1).

Vertrouwen op de SaaS-provider?

Veel bedrijven ontdekken dat vertrouwen op hun SaaS-provider voor de veiligheid van hun gegevens een risicovolle aangelegenheid is: in 2023 had 65% van de datalekken betrekking op gegevens die waren opgeslagen in een publieke cloud of hybride omgeving*.

Keepit

Om bedrijven te helpen verlies van SaaS-gegevens te voorkomen, heeft Keepit een specifieke, leveranciersafhankelijke SaaS-oplossing ontwikkeld voor back-up van gegevens. Deze is veerkrachtig, veilig, gebruiksvriendelijk en wordt geleverd volgens een voorspelbare, transparante prijsstructuur.

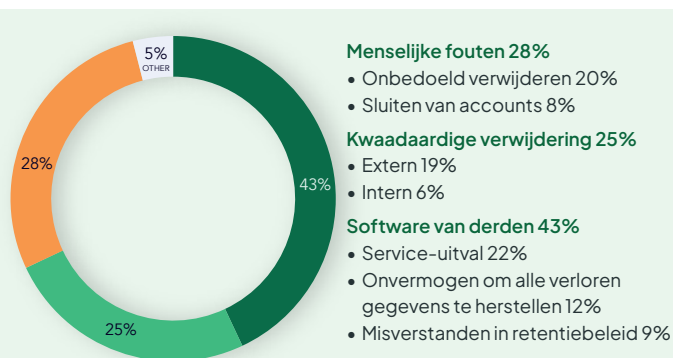
Verantwoordelijkheden van de SaaS-provider

Applicaties	Hardwarestoringen
Besturingssysteem	Softwarestoringen
Virtualisatie	Natuurrampen
Hardware	Stroomstoringen
Netwerk	Fysieke inbraken

Uw data – uw verantwoordelijkheid

Gebruikers	Menselijke fouten
Gegevens	Programmafouten
Beheer	Kwaadwillende insiders
	Ransomware-aanvallen
	Virussen/malware

Figuur 1. Gedeelde verantwoordelijkheden voor SaaS-providers en SaaS-gebruikers



Bron: Enterprise Strategy Group, "ESG Showcase: De belangrijkste trends en uitdagingen voor SaaS-gegevensbescherming in 2022"

Figuur 2. Redenen voor dataverlies

* Cost of Data Breach Report 2024 [IBM]

Echte back-up vereist een aparte logische infrastructuur

SaaS-workloads vereisen een dedicated back-up oplossing

	On-premises back-up	Generieke cloud back-up	Dedicated back-up
Herstel	Hersteltijd varieert afhankelijk van de oplossing	Prestatieverlies – cold storage	Herstelt uw gegevens volledig binnen enkele minuten
Eenvoud	Dagelijkse ondersteuning van het IT-team	Complex te beheren – certificering	Eenvoudig te beheren – geen training nodig
Beveiliging	Gevoelig voor fysieke schade	Opslag in dezelfde cloud met productiedata	Onveranderbare blockchain-opslag
Kosten	Aanzienlijke investering en moeilijk te schalen	Hoogwaardig te schalen met netwerk- en verborgen kosten	Geen CapEx en eenvoudig te schalen – geen opslaglimieten, geen extra kosten
Bedrijfscontinuïteit	Geen 2e kopie of 2e datacenter	Geen 2e kopie of 2e datacenter	Standaard 2e kopie en 2e datacenter (4 kopieën)

Figuur 3. Het verschil tussen on-premises back-up, generieke cloud back-up en speciaal gebouwde back-up voor SaaS

Het 3-2-1-principe van back-up (zie **figuur 4**) vereist dat u één kopie van uw gegevens off-site bewaart. De off-site kopie zorgt ervoor dat uw back-up gegevens elke calamiteit overleven. De meeste back-up oplossingen voor cloud-omgevingen slaan uw back-up echter op in dezelfde cloud-infrastructuur die uw primaire gegevens host. Dit brengt onnodige risico's met zich mee.

Zelfs als u kiest voor een datacenter-locatie die geografisch gescheiden is van uw primaire gegevens, worden al uw gegevens (inclusief uw enige back-ups!) beheerd onder dezelfde administratieve infrastructuur (zie **figuur 3**). Bovendien kan een cloud offline worden gehaald om de primaire bedrijfsbelangen van de provider te beschermen.



Figuur 4. 3-2-1-principe van back-up

Omdat back-up in het cloud-tijdperk veel complexer is geworden, heeft Keepit een eigen, dedicated cloud gebouwd. Deze draait in verschillende regio's, op dedicated hardware en beheerd door Keepit. Zodra een klant een Keepit-regio kiest voor back-up, verlaten de gegevens die regio nooit meer. Door de eigen cloud, kan Keepit risico's minimaliseren met meer controle over de kosten, waardoor Keepit eenvoudige, transparante prijzen kan bieden.

Het Keepit-onderscheid

Met een eigen, intelligent gebouwde cloud biedt Keepit een eenvoudige, innovatieve en veelzijdige back-up oplossing voor SaaS-data.

Keepit maakt snel herstel van bedrijfskritische gegevens mogelijk en garandeert tegelijkertijd de naleving van regelgeving met betrekking tot gegevensbescherming (AVG) en cybersecurity (NIS2). Dat maakt Keepit de intelligente keuze voor een toekomstbestendige dataprotectie-strategie.

Keepit Simple

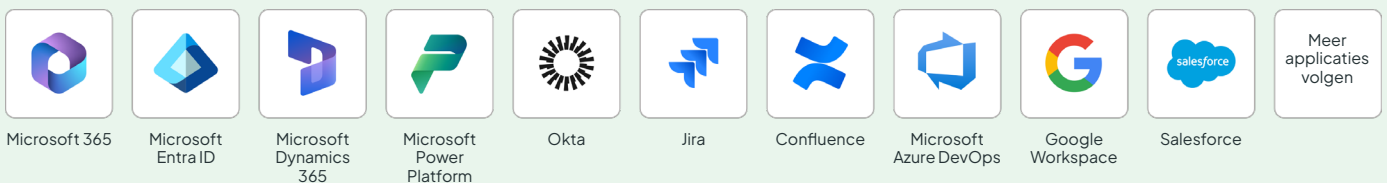
De Keepit-filosofie is altijd geweest 'keep it simple', omdat een beveiligingsoplossing alleen werkt als deze correct is geïmplementeerd en geïntegreerd in de dagelijkse bedrijfsvoering van een organisatie. En dat kan alleen als de oplossing intuïtief en efficiënt is!

Om het voor de gebruiker eenvoudig te houden, wordt er op de achtergrond continu gewerkt aan verbetering van het beheer van bedrijfscontinuïteit en disaster recovery.

Superieure bescherming

Doorlopende prestatiebeoordelingen en interne audits zorgen ervoor dat Keepit blijft voldoen aan de eisen van de ISO/IEC 27001-norm. De systematische, geverifieerde aanpak van informatiebeveiliging resulteert in superieure bescherming van klantgegevens, met brede ondersteuning van SaaS-applicaties ([zie hieronder](#)) en naleving van huidige en toekomstige wet- en regelgeving.

Brede en groeiende ondersteuning van SaaS-applicaties



Keepit: de intelligente keuze

INTELLIGENT GEBOUWD – Schaalbaar, immutable, compliant

Cloud-native dataprotectie

- Schaalbaar en adaptief, in tegenstelling tot on-premises oplossingen die achteraf voor de cloud zijn aangepast
- Geen infrastructuur- en onderhoudskosten verbonden aan on-premises of hybride alternatieven

Veilig en versleuteld

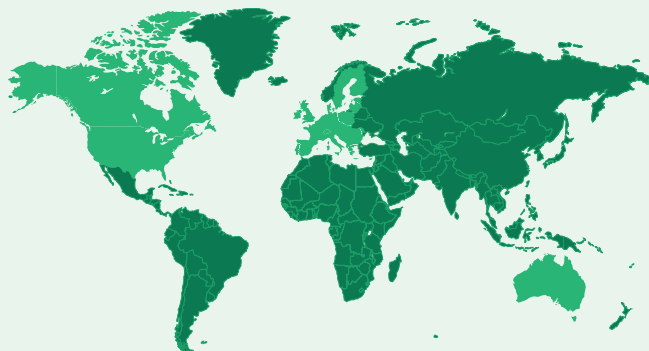
- Geavanceerde AES-versleuteling zowel 'in flight' als 'at rest' toegepast op onze opslagsystemen
- Rechtstreekse uitwisseling met workload-providers via grote internetknooppunten

Volledig immutable back-ups

- Zo ontworpen dat het onmogelijk is om bestanden te wijzigen of te verwijderen, wat echte onveranderlijkheid (immutability) garandeert

Datasoevereiniteit en compliance

- Data blijft in de door u gekozen regio
- Eigen datacenters in zeven landen op drie continenten, beheerd door Keepit
- Beveiliging van SaaS-applicatiegegevens met naleving van privacyregelgeving
- ISO/IEC 27001-gecertificeerd en ISAE 3402-II compliance-rapport (Deloitte)



Figuur 5. Keepit heeft eigen datacenters in zeven landen op drie continenten, beheerd door Keepit. Uw data blijft bewaard in de door u gekozen regio.

INTELLIGENT HERSTEL – Flexibel, intuïtief, nauwkeurig

Directe toegang tot alle versies van uw gegevens

- Directe toegang tot alles, altijd en overal, vanaf elk apparaat
- Hot storage: altijd actieve opslag
- Ongeacht hoe oud ze zijn, direct een voorbeeld bekijken, delen of herstellen van dataobjecten
- Intuïtieve zoekfunctie met voorbeeldweergave vóór herstel

Transparantie en verantwoording

- Aanpasbare alerts en rapporten voor compliance en voorbereiding voor disaster recovery

Flexibele herstelopties

- Snel en nauwkeurig herstel, in bulk of granulair
- Integratie met SIEM voor verder onderzoek en actie.

Praktische inzichten

- Geconsolideerd overzicht van de status en prestaties van back-up en hersteltaken
- Pro-actieve waarschuwingen voor afwijkingen en bedreigingen voor de gegevensintegriteit
- Integratie met beveiligingstools

INTELLIGENTE KEUZE – Veilig, uniform, kosteneffectief

Leverancieronafhankelijke cloud

- Keepit is eigenaar van de infrastructuur, onafhankelijk van openbare cloudproviders en hyperscalers
- Back-ups blijven gescheiden van productiedata en voldoen aan de hoogste beveiligingsnormen
- Keepit maakt geen gebruik van sub-processors

Uniform platform voor alle applicaties

- Eén centraal punt voor alle SaaS-applicaties
- Gestroomlijnde processen voor optimale productiviteit

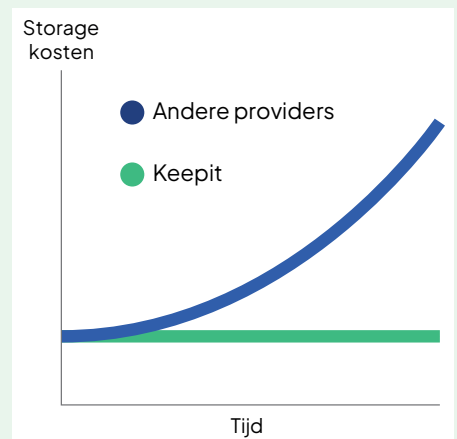
Tijdbesparend en gebruiksvriendelijk

- Zonder de infrastructuur te hoeven onderhouden kunnen uw medewerkers zich concentreren op hun kernactiviteiten
- Eenvoudige installatie en intuïtieve interface versnellen de implementatie
- Flexibele, role-based access

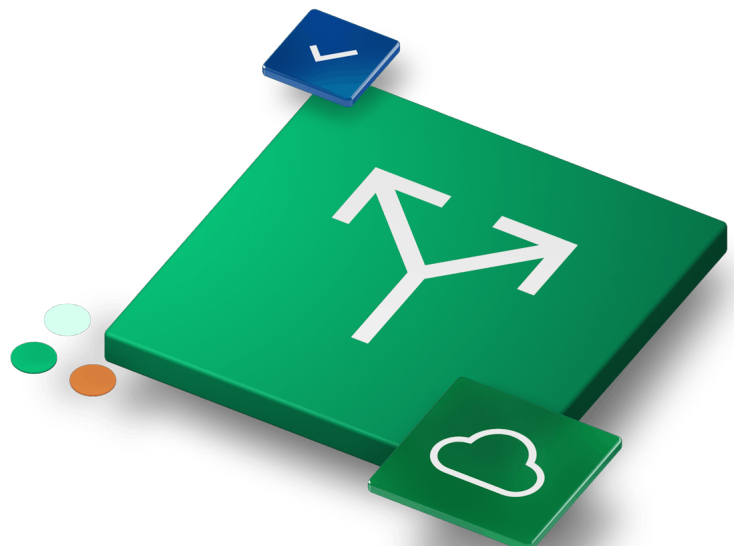
Voorspelbare, stabiele kosten.

Geen kleine lettertjes

- Prijzen gebaseerd op licenties met onbeperkte data-opslag
- Onbeperkte, aanpasbare retentie (tot 99 jaar)
- Geen kosten voor ingress, egress of overdracht van data
- Dezelfde kosten voor extra gebruikersaccounts
- Off-boarded gebruikers zijn gratis



Figuur 6. Kosten versus datagroei in de tijd, het Keepit-onderscheid in kostenstructuur



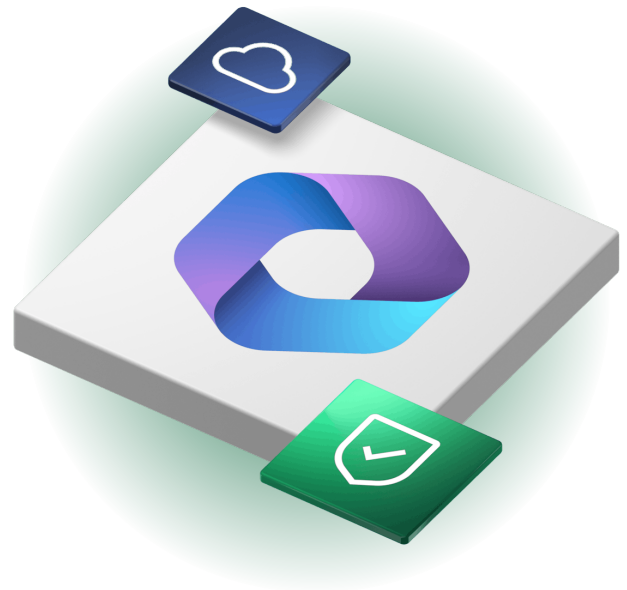
Back-up en recovery voor Microsoft 365

Zonder een off-site back-up van uw Microsoft 365 (M365)-gegevens loopt u risico op het niet kunnen herstellen van uw gegevens na een ransomware aanval en zelfs op gegevensverlies. Zelfs Microsoft raadt aan gebruik te maken van een back-up oplossing van derden. Daarom hebben duizenden bedrijven gekozen voor Keepit om hun M365-gegevens veilig te houden.

Keepit: uw doelgerichte third party back-up platform voor Microsoft 365

Met de meest uitgebreide M365-dekking op de markt houdt Keepit uw bedrijf draaiende met directe toegang tot al uw gegevens – altijd.

Doordat vier kopieën worden opgeslagen op twee afzonderlijke, leveranciersonafhankelijke locaties, hebt u altijd toegang tot uw gegevens. Ongeëvenaard gebruiksgemak, onbeperkte opslag en archivering met snelle herstelfuncties die downtime minimaliseren, maken van Keepit de eenvoudigste en meest kosteneffectieve manier om uw M365-gegevens te beschermen.



Uw gegevens verdienen de beste dekking

Keepit biedt de meest uitgebreide en gedetailleerde beschermings- en archiveringsondersteuning voor alle belangrijke applicaties in Microsoft 365. Keepit biedt de beste dekking op de markt.

Uw gegevens terug in seconden

Keepit is speciaal ontworpen voor beheerders en maakt handmatige herstelprocessen verleden tijd. Met ultrasnelle, slimme zoek- en herstelfuncties kunt u meerdere terabytes per dag herstellen en uw M365-gegevens terugzetten op de oorspronkelijke locatie, inclusief de oorspronkelijke bestandsstructuur en metadata.





Exchange Online

- Outlook Mail
- Contacten
- Taken
- Agenda
- Archiveren
- Publieke Folders
- Subfolders
- Gebruikerstoegang



+



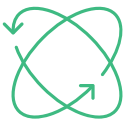
OneDrive

- Alle documenten
- Formuliersjablonen
- Stijlbibliotheek
- Versies
- Intelligente geïntegreerde Azure AD groep-selectie
- Geautomatiseerde OneDrive-selectie (gebaseerd op Exchange-selectie)
- Intelligente selectie van SharePoint sites en teams



SharePoint

- Alle site-collecties
- Lijsten
- Documentbibliotheken
- Site contenttypen
- Site kolommen
- Permissies
- Maatwerk aanpassingen
- Pagina's
- Subsites



Bedrijfs-continuïteit

Behoud toegang tot essentiële gegevens en zet uw bedrijfsvoering voort met schone kopieën van uw gegevens



Directe recovery

Vind snel wat u nodig hebt en herstel individuele records of complete datasets in een paar klikken



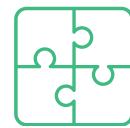
Toonaangevende beveiliging

Voorkom dat kwaadwillenden uw back-ups manipuleren en minimaliseer het risico op datalekken met betrouwbare beveiliging



Kosten-effectiviteit

Maak u geen zorgen over extra kosten of verborgen verrassingen dankzij een eenvoudige en transparante kostenstructuur die u geld bespaart

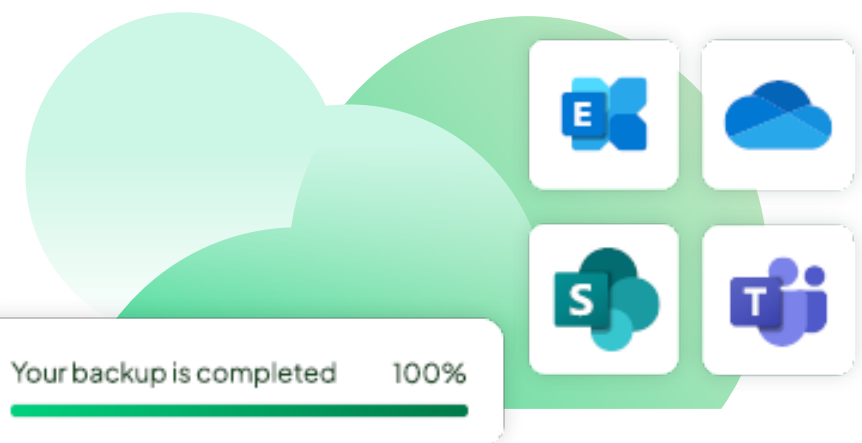


Uitstekende eenvoud

Minimaliseer de implementatie en het beheer met een eenvoudig platform dat is ontworpen voor hogere efficiëntie.



Scan de QR code of klik [hier](#) om een korte demo van Keepit te bekijken.



Back-up en recovery voor Microsoft Entra ID

Microsoft Entra ID beheert identiteiten en biedt authenticatie en autorisatie voor de kritieke SaaS-applicaties van uw organisatie. Het verlies van Entra ID objecten en beleidsregels – door cyberaanvallen, onbedoelde verwijdering of storingen – betekent verstoring van uw business en extra stress voor u en uw team.



Toonaangevende dekking van Entra ID

Bekroond om zijn gebruiksgemak, zorgt Keepit's uitgebreide dekking van Microsoft Entra ID ervoor dat uw gegevens veilig worden gback-upt in een leveranciersonafhankelijke cloud en snel en

nauwkeurig kunnen worden hersteld wanneer zich incidenten voordoen. Keepit minimaliseert de impact van gegevensverlies en maakt het opnieuw moeten opbouwen van de Microsoft Entra ID-omgeving verleden tijd.



Ongeëvenaarde dekking

Met de breedste dekking van objecten en beleidsregels, waaronder Intune, BitLocker en LAPS, kunt u erop vertrouwen dat u altijd uw gegevens kunt herstellen.



Snel herstel

U kunt onbedoelde wijzigingen in objecten en beleidsregels snel herstellen. Identificeer de wijzigingen en bepaal welke u moet herstellen in geval van een storing.



Gegarandeerde gegevensintegriteit

U kunt erop vertrouwen dat uw gegevens niet kunnen worden gewijzigd of verwijderd. Microsoft Entra ID-objecten en -beleid worden opgeslagen in een leveranciersonafhankelijke cloud en blijven altijd toegankelijk.

Het risico

Microsoft Entra ID registreerde meer dan 7.000 geblokkeerde wachtwoorden aanvallen per seconde in 2024.

Bron: Microsoft Digital Defense Report 2024

De impact

\$ 500.000 waren de herstelkosten voor Carlsbad nadat een contractant 1.200 gebruikersaccounts had verwijderd.

Bron: Ministerie van Justitie van de Verenigde Staten

Bewezen voordeel

Hersteltijd van minder dan 3 uur voor een Keepit-klant na een gerichte aanval.

Bron: "Keepit maakt snel herstel na cyberaanval mogelijk"

Wat Keepit back-up en recovery voor Microsoft Entra ID dekt

GEbruikersGroepen | BEHEERDERSEENHEDEN | ROLLEN EN ROLTOEWIJZINGEN | APP-REGISTRATIES
SERVICEPRINCIPALS / ENTERPRISE-APPS | BELEID VOOR VOORWAARDELIJKE TOEGANG
INTUNE-APPARAATCONFIGURATIEPROFIELEN | INTUNE-COMPLIANCEBELEID | BITLOCKER-HERSTELSLEUTELS | AUDITLOGBOEKEN
AANMELDINGSLOGBOEKEN | WINDOWS LAPS-BELEID EN WACHTWOORDGESCHIEDENIS

Keepit: dé SaaS Data Protection provider!

Het Keepit-onderscheid

- Deense software vendor met onafhankelijke eigen cloud
- Geen onderaannemers / subprocessoren
- Uw data gegarandeerd in de EU
- Uw data standaard in meerdere datacenters veilig, immutable opgeslagen
- Onbeperkte retentie, onafhankelijk van hoeveelheid data
- Uw data wel beschikbaar bij niet-beschikbaar zijn van een SaaS-applicatie
- Voorspelbaar en transparant; geen verborgen bijkomende kosten
- Eenvoudig in gebruik: instellen en vergeten – herstel met een klik
- Voldoet aan wetgevingen voor privacy en compliance
- Nieuwe SaaS-applicaties worden regelmatig toegevoegd



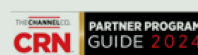
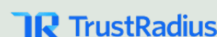
“Keepit werkt gewoon op de achtergrond terwijl wij onze dagelijkse taken uitvoeren, wat tijd en middelen bespaart. Het gebruiksgemak van dit product is een enorme kracht.”

Ton Van der Hagen,
Manager ICT Hardware & Infrastructure bij Smulders



“Door Emmi’s internationale bedrijfsactiviteiten was het ook belangrijk dat technologiepartners een wereldwijd beschikbaar en schaalbaar aanbod konden bieden. Keepit blijkt de ideale partner te zijn voor het aangaan van de uitdagingen van een wereldwijd actieve zuivelonderneming.”

Marc Baumann,
Lead Data Platform Services, Emmi



Keepit future-proof

Zet de volgende stap in de bescherming van uw SaaS-gegevens



Scan de QR code
of klik [hier](#) om een
korte demo van
Keepit te bekijken.



Keepit biedt geavanceerde SaaS-gegevens-
bescherming, speciaal ontwikkeld voor de
cloud. Dit gebeurt door gegevens te back-
uppen in een leveranciersafhankelijke cloud
die essentiële bedrijfsapplicaties beschermt, de
cyberveiligheid vergroot en gegevensbescherming
toekomstbestendig maakt.

Met het hoofdkantoor in Kopenhagen en kantoren
en datacenters wereldwijd, vertrouwen meer dan
tienduizend bedrijven op Keepit vanwege het
gebruiksgemak en de moeiteloze back-up en herstel
van cloudgegevens.

Meer weten: sales@keepit.com

HQ - Copenhagen

Denmark
Keepit A/S
Per Henrik Lings Allé 4, 7.
2100 København, Denmark
CVR: 30806883
+45 8987 7792
sales@keepit.com

Dallas, Texas

United States
Keepit USA Inc.
3232 McKinney Avenue Suite 820
Dallas TX 75204, USA
TIN: 85-358 6335
+1 469-461-4892
sales@keepit.com

London

United Kingdom
Keepit Technologies UK, LTD.
Warnford Court
29, Throgmorton Street
London EC2N 2AT, UK
Company reg. no.: 13785045
sales@keepit.com

Munich

Germany
Keepit Germany GmbH
Maximiliansplatz 22
D-80333 München
Amtsgericht München
HRB 270094
Geschäftsführer Morten Felsvang
sales@keepit.com