

DATA & MORE DLP · ECHTZEIT-SCHUTZ VOR DATENVERLUST FÜR MICROSOFT 365

# Data & More | DLP

**Senden Sie nicht die falsche Nachricht.**

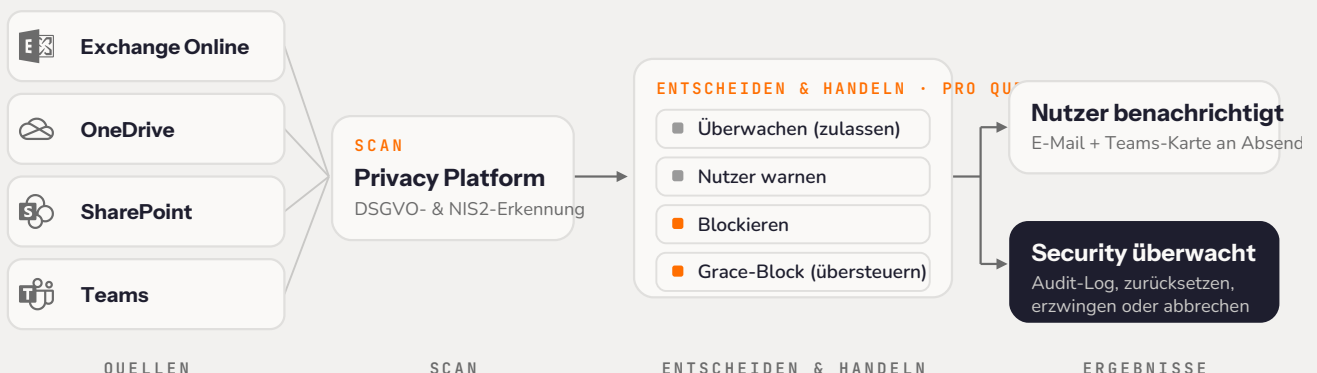
Data & More DLP überwacht die Inhalte, die Ihre Mitarbeitenden über Microsoft 365 teilen, und greift in dem Moment ein, in dem etwas Sensibles an die falsche Stelle gelangen soll. Es arbeitet **in Echtzeit, direkt in den Tools, die Ihre Teams bereits nutzen**, sodass personenbezogene und vertrauliche Daten erfasst werden, während sie sich bewegen, nicht Wochen später in einem Audit.

DECKT AB	ERKENNT	REAGIERT	FUSSABDRUCK
Exchange· OneDrive· SharePoint· Teams	<b>DSGVO- &amp; NIS2-</b> <b>Daten in Gefahr</b>	<b>Überwachen·</b> <b>Warnen·</b> <b>Blockieren· Grace-</b> <b>Block</b>	<b>Nativ in M365, kein</b> <b>Agent</b>

## SO FUNKTIONIERT ES

### Eine Engine für alle Microsoft 365-Kanäle

Jede E-Mail, Datei und Nachricht wird mit derselben Data & More-Profileng-Engine geprüft, die unsere Risikobewertung antreibt, und dann nach der von Ihnen festgelegten Richtlinie behandelt, pro Quelle und pro Dokumenttyp.



01

## Deckt jeden M365-Kanal ab

Ein Dienst überwacht **Exchange-Online-E-Mails, OneDrive- und SharePoint-Dateien sowie Teams-Nachrichten**. Er läuft nativ in Ihrem Microsoft-365-Tenant, ohne Installation auf den Geräten.

02

## Reagiert, wie Sie wollen

Legen Sie die Reaktion pro Quelle und pro Dokumenttyp fest: **überwachen** Sie still, **warnen** Sie den Nutzer, **blockieren** Sie sofort, oder **Grace-Block**, das die Durchsetzung für einen festgelegten Zeitraum aufschiebt, damit ein Mensch eingreifen kann, bevor sie wirksam wird.

03

## Menschen informiert, Security in Kontrolle

Die Person, die riskante Inhalte teilt, wird sofort per **E-Mail und Teams** benachrichtigt. Security erhält einen vollständigen **Audit-Trail** darüber, wie sich sensible Daten verbreiten, und kann jede ausstehende Aktion zurücksetzen, erzwingen oder abbrechen.

### WARUM ES ZÄHLT

## Firewalls stoppen kein Leck. Weniger Daten in Bewegung schon.

Zugriffskontrollen und Firewalls hindern eine Kollegin nicht daran, die falsche Datei weiterzuleiten, oder Copilot daran, sie zu lesen. **Data & More DLP sorgt dafür, dass sensible Inhalte gar nicht erst an die falsche Stelle gelangen**, und verringert Ihr Risiko, Ihren Schadensumfang und den Aufwand hinter jeder DSGVO- und NIS2-Pflicht, mit einem klaren, prüffähigen Nachweis.

Was nicht da ist, kann nicht geleakt werden!

## Erleben Sie Data & More DLP in Ihrem eigenen Tenant.

Aktivieren Sie es über Exchange, OneDrive, SharePoint und Teams und sehen Sie, wie echtes Risiko in Echtzeit erfasst wird. Beginnen Sie mit Überwachung und verschärfen Sie zur Blockierung, wenn Sie bereit sind.

[Demo buchen](#)