



Über die Hälfte aller Vorfälle von Datenverlust geschehen betriebsintern – oft unbeabsichtigt. Der Abfluss von kritischen Daten kann dabei erheblichen Schaden anrichten. Schützen Sie Ihr Unternehmen und erhöhen Sie die Affinität Ihrer Mitarbeitenden in Bezug auf den Umgang mit kritischen Daten.

Mit «Microsoft Data Loss Prevention as a Service» verhindern Sie den unerlaubten Abfluss sensibler Informationen aus Ihren Microsoft 365- & Cloud-Applikationen.

Mit Microsoft DLP as a Service überwachen Sie die Interaktionen der Nutzer in ihrem Microsoft Tenant über die Microsoft 365-Applikationen und Cloud Apps.

Diese Kanäle werden inhaltlich auf kritische Daten überprüft und können so vor unerlaubten Abflüssen geschützt werden. Wird ein Verstoß aufgedeckt, wird eine Sicherheitsmeldung (Incident) aufbereitet und ausgelöst. Für die Bearbeitung der Incidents steht Ihnen ein Remedierungsprozess zur Verfügung.

Microsoft DLP as a Service

Ihr Nutzen mit Microsoft DLP as a Service

Transparenz

Erhalten Sie umfassende Transparenz der Daten, welche Ihr Unternehmen verlassen.



Umfassender Datenschutz

Verhindern Sie unberechtigte Weitergabe kritischer Daten aus Ihrem Unternehmen.



Compliance

Erfüllung der geforderten Nachweise für die Compliance und der Sorgfaltspflicht im Umgang mit sensiblen Kundendaten.



Datenklassifizierung

Wir unterstützen Sie bei der Applizierung Ihrer Datenklassifizierungsstrategie für die Datensicherheit in Ihrem Unternehmen.



Erhöhung der Security Awareness

Training Ihrer Mitarbeitenden im Umgang mit kritischen Daten.



Managed Service

Profitieren Sie von unserer langjährigen Expertise sowie von unseren branchenoptimierten und markterprobten DLP Policies.



So funktioniert Microsoft DLP as a Service

Überwachung folgender Locations



swisscom



Facts & Figures

Die Informationen in diesem Dokument stellen kein verbindliches Angebot dar. Änderungen sind jederzeit vorbehalten.

Swisscom (Schweiz) AG Enterprise Customers, Postfach, CH-3050 Bern, Tel. 0800 800 900, www.swisscom.ch/enterprise

Sie haben die Möglichkeit, den benötigten Schutz optimal auf Ihre Bedürfnisse zuzuschneiden. Folgende Service-Ausprägungen stehen Ihnen dafür zur Verfügung:

Basisleistungen

DLP Channels (Locations)	Basic	Standard	Advanced
OneDrive	✓	✓	✓
SharePoint Online	✓	✓	✓
Mail (Exchange Online)	✓	✓	✓
Microsoft Teams	✗	✓	✓
Endpoint	✗	✓	✓
Cloud Apps	✗	✓	✓

Services	Basic	Standard	Advanced
Applizierung von Datenklassifizierung (Labelling)	Manuell	Automatisch	Automatisch
DLP Governance & Foundation	✓	✓	✓
Vordefinierte Sensitive Info Types	✓	✓	✓
Individuelle Sensitive Info Types	✗	✓	✓
Trainable Classifiers/Fingerprint	✗	✓	✓
EDM Policies	✗	✗	✓

Lizenzierung

Microsoft DLP as managed Service baut auf Ihren Microsoft-Lizenzen auf und benötigt keine zusätzliche Lizenzierung.

Folgende Microsoft-Lizenzen sind als Vorbedingung nötig für den Bezug des Service «Microsoft DLP as a Service»:

Microsoft-Lizenzen	Basic	Standard	Advanced
Microsoft 365 – E3	✓	✗	✗
Microsoft 365 – E3 (oder Modul «Information Protection & Governance»)	✓	✓	✓

Optionale Leistungen

- Blockieren von Datenabflüssen (z. B. E-Mail)
- Einbezug der Endanwender in die Incident-Remedierung
- Zusätzliche DLP Policies aus dem Standardkatalog (vordefiniert)
- Bei Bedarf haben Sie jederzeit die Möglichkeit, zusätzlich individuelle DLP Policies zu applizieren.
- Konfiguration und Management von Ausnahmen (Allow List)

Zusatzservices

- Der **Service Audit Guard** protokolliert User- und Systemaktivitäten auf definierten Schutzobjekten wie Applikationen, Datenbanken oder Servern und alarmiert bei Regelverstößen. Dabei haben Sie volle Transparenz und erbringen die geforderten Nachweise für die Einhaltung der Compliance.
- **Microsoft 365 Management**: Überlassen Sie uns das Management von Microsoft 365 und fokussieren Sie sich auf Ihr Kerngeschäft. Das Management des Kunden-Tenants und die Lizenzen sind hier verfügbar.
- **Microsoft XDR as a Service**: Lifecycle Management der XDR-Agenten, Health Management der Service-Komponenten, Konfiguration der Security Policies, Kommunikation von neuen Funktionen und Änderungen und ein jährliches Security Policy Assessment sind in der Verantwortung von Swisscom.

Mehr Informationen und den Kontakt zu unseren Experten finden Sie auf [swisscom.ch/dlp](https://www.swisscom.ch/dlp)