



Plus de la moitié des pertes de données se produisent en interne – souvent de manière involontaire. La transmission de données non autorisées peut causer des dommages considérables. Les lois sur la protection des données et les réglementations sectorielles exigent que les entreprises soient en mesure d'assurer la sécurité des données clients.

Avec Data Loss Prevention, vous empêchez la fuite non autorisée d'informations sensibles et fournissez les preuves requises.

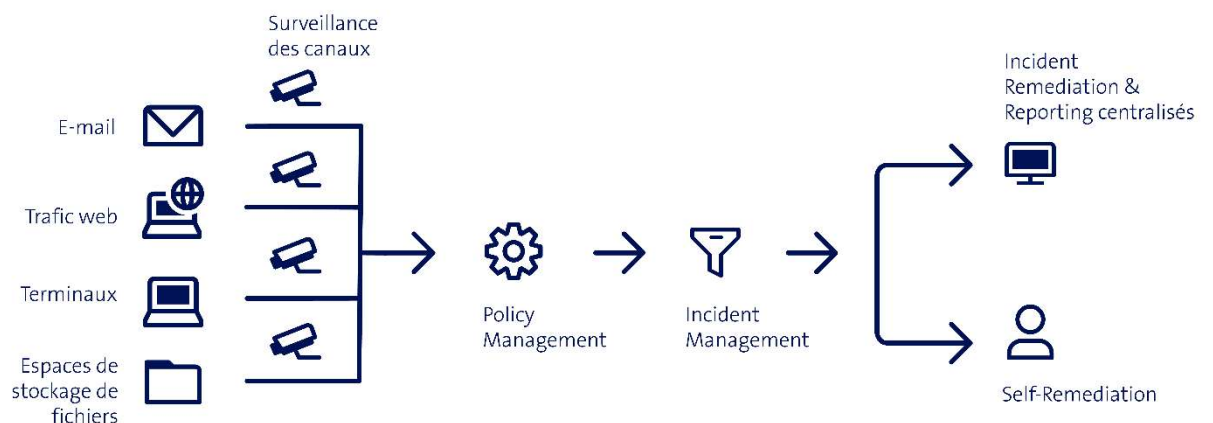
Qu'est-ce que Data Loss Prevention?

Le service *Data Loss Prevention* surveille les interactions de vos collaborateurs et de vos fournisseurs par e-mail ainsi que sur le web, les espaces de stockage et les terminaux. Ces canaux sont contrôlés pour détecter les données sensibles et leur contenu est comparé à un ensemble de règles standardisées. En cas de violation, une alerte de sécurité est créée et déclenchée. Un outil de remédiation est mis à disposition pour traiter les incidents. De plus, les preuves requises sont générées périodiquement.

Vos avantages avec Data Loss Prevention

- Détection précoce des interactions non autorisées
- Prévention de la transmission non autorisée de données sensibles (p. ex. propriété intellectuelle)
- Génération des preuves de conformité requises
- Concept de protection individuel et, si nécessaire, mise en place en plusieurs phases
- Respect du devoir de diligence dans le traitement des données clients sensibles
- Formation de vos collaborateurs au traitement des informations sensibles
- Managed Service – bénéficiez de nos nombreuses années d'expertise

La solution en un coup d'œil








Les informations contenues dans le présent document ne constituent pas une offre contractuelle. Elles peuvent être modifiées à tout moment.

Swisscom (Suisse) SA Enterprise Customers, Case postale,
CH-3050 Berne, tél. 0800 800 900, www.swisscom.ch/entreprise

swisscom

Faits et chiffres

	Canaux à combiner librement:
Prestations de base	<ul style="list-style-type: none">- Mail (Data in Motion)- Web (Data in Motion)- Client Endpoints (Data in Use)- Sharepoint & Filer (Data at Rest)
	Gestion centralisée des incidents
	Outil central de remédiation et de reporting
	15 Politiques au choix dans le catalogue standard:
	<ul style="list-style-type: none">- Described Content Match (DCM)- Exact Data Match (EDM)- Configuration individuelle selon le niveau de gravité
	Notifications et rappels par e-mail
	Mode blocage ou quarantaine (selon le canal)
Prestations en option	Gestion décentralisée des incidents:
	<ul style="list-style-type: none">- Self-Remediation par l'utilisateur final/business pour l'e-mail
	Politiques supplémentaires du catalogue standard
	Politiques individuelles
	Whitelists spécifiques au client
	Le service Audit Guard consigne les activités des utilisateurs et du système sur les objets à protéger définis, tels que des applications, des bases de données ou des serveurs, et déclenche une alerte en cas de violation. Vous bénéficiez d'une transparence totale et disposez d'une preuve du bon respect des règles de conformité.
Services supplémentaires	Avec Sensitive Data Services (SDS) , vous avez une vue d'ensemble précise de toutes vos données sensibles stockées (p. ex. données personnelles et clients, informations sur les patients, contrats et brevets).
	Compliance Consulting : via le «contrôle de protection des données», nous définissons ensemble les données indispensables à protéger pour votre entreprise dans le cadre du RGPD.
	Pour en savoir plus sur Data Loss Prevention: www.swisscom.ch/dlp