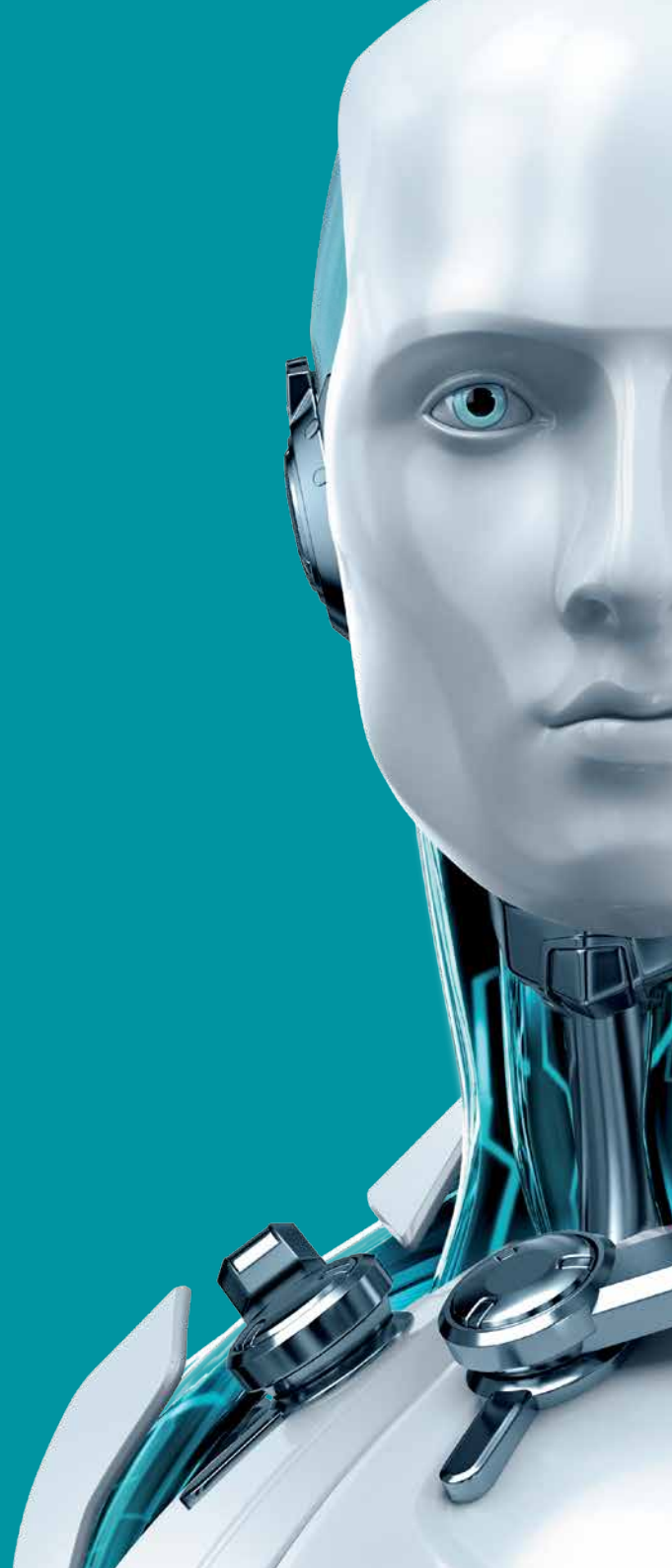
safetica

Protection contre les fuites de données

BUSINESS

ENJOY SAFER TECHNOLOGY™*

*Profitez de la vie numérique en toute sécurité.



Safetica

Solution de DLP (Data Loss Prevention) complète qui protège des menaces provenant d'une même source – le facteur humain. Safetica évite les fuites de données intentionnelles ou accidentelles, les actions malveillantes internes, les problèmes de productivité, les menaces liées au BYOD et bien plus encore.

La philosophie de Safetica repose sur trois piliers : exhaustivité, flexibilité et facilité d'utilisation.

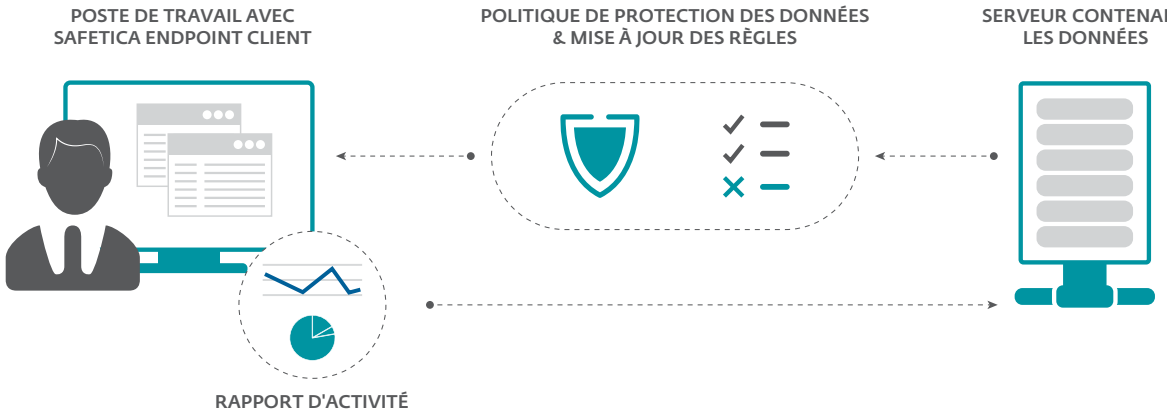
Safetica propose une solution DLP professionnelle complète qui fournit des rapports d'activité exhaustifs aux responsables et applique les stratégies de sécurité aux postes utilisateurs. Safetica est une solution complète, regroupant les outils de DLP nécessaires, ce qui vous évite de devoir faire appel à plusieurs fournisseurs.

Avantages

Solution DLP complète	Couvre tous les canaux de fuite de données. Safetica protège les terminaux et les réseaux contre les fuites de données.
Mise en œuvre rapide	Grâce à une approche flexible de blocage des canaux de fuite de données, Safetica présente un délai de mise en oeuvre le plus court sur le marché.
Résistance élevée aux violations	Safetica offre une protection permanente, y compris pour les utilisateurs disposant de droits d'administrateur.
Protection étendue contre la fuite des données	Safetica protège les données contre la capture d'écran, accès au presse-papiers, impression virtuelle, transformation de fichiers, archivage et chiffrement.
Compatibilité universelle	La protection des données assurée par Safetica ne se limite pas à des protocoles ou applications spécifiques.
Etablissement de zone de sécurité	Le responsable sélectionne simplement les emplacements auxquels les données confidentielles doivent être confinées.
Surveillance du temps d'activité	Un élément ouvert n'est pas forcément utilisé de manière active. Les rapports d'activité indiquent le temps d'activité effectif des utilisateurs sur les sites web visités ou dans les applications.
Évaluation et alertes automatiques	Safetica envoie un rapport de synthèse comportant les informations les plus importantes aux destinataires désignés. Les informations complètes sont disponibles si besoin.

Fonctionnement

Déployé sur les terminaux, là où les utilisateurs manipulent des données d'entreprise critiques, accèdent à Internet, consultent leurs e-mails, envoient des documents à l'imprimante et connectent des périphériques amovibles. Un agent Safetica est installé (**Safetica Endpoint Client**) sur les terminaux souhaités et maintient une connexion régulière avec ceux-ci via le serveur (**Safetica Management Service**). Ce serveur héberge une base de données sur l'activité des postes de travail et envoie les nouvelles stratégies et règles de protection des données à chacun d'entre eux.



Points clés

Protection complète contre les fuites de données	Facile à installer et à utiliser, Safetica couvre tous les canaux de fuite de données. Pour plus d'informations, consultez la section « Événements pris en charge sur les terminaux ».
Analyse comportementale	Avertit les responsables de l'entreprise en cas de modifications soudaines de l'activité des employés et montre l'évolution de la productivité de chaque service dans le temps. Ces changements pourraient être liés à des risques de sécurité.
Rapports d'activité	Identifie les violations de sécurité sur de nombreux fronts en recherchant les signes d'une menace au niveau des activités des utilisateurs, avant même le transfert des données.
Protection contre les fuites de données par e-mail	Empêche les données de partir vers un mauvais correspondant. Enregistre les adresses auxquelles des fichiers sensibles ont été envoyés et conserve ces informations pour de futurs rapports.
Contrôle des applications avec des règles temporelles	Permet aux applications professionnelles sélectionnées de s'exécuter et bloque les autres programmes, pour un environnement plus sûr. Il est possible de définir les créneaux horaires auxquels les applications sont disponibles.
Filtrage web	Applique votre politique de filtrage en toute simplicité reposant sur des catégories et mots clés présélectionnés.
Contrôle des impressions	Permet de définir les documents imprimables et de restreindre l'impression à certains utilisateurs, avec des quotas pour chaque utilisateur et service.
Contrôle des périphériques	Empêche les employés de connecter des périphériques non autorisés. Les filtrages peuvent être activés pour certains appareils ou bloqués de manière générale.
Gestion du chiffrement	Il est possible de chiffrer des disques ou des partitions et créer des lecteurs virtuels locaux ou réseau, pour un stockage de fichiers sécurisé. Outre les méthodes d'accès par mot de passe ou par clé, vous avez la possibilité de créer des travels disks (disques sécurisés accessibles depuis d'autres postes), ainsi que de forcer le chiffrement pour les données qui quittent la zone de sécurité.
Mode informatif et test	Aide les entreprises à mettre en place progressivement la protection des données, grâce à la possibilité de réaliser des tests selon tous types de scénarios sans interrompre les processus métiers.
Classification des données en temps réel	Protège immédiatement les nouvelles informations après la création ou la réception d'un fichier classé.
Console de gestion unique	Safetica Management Console vous permet de gérer la sécurité et les rapports via une interface unique intégrant toutes les stratégies de l'entreprise en matière de protection des données, de reporting et de blocage.
Inspection SSL/HTTPS	Vérifie et protège les lignes de communication sécurisées, notamment les sites web utilisant le protocole HTTPS, les applications de messagerie instantanée avec des connexions sécurisées et la transmission sécurisée d'e-mails.
Coût total de possession minimal	Les utilisateurs n'ont pas besoin d'acheter des appliances de sécurité supplémentaire. Les agents pour terminaux déployés avec Safetica offrent des fonctionnalités DLP destinées aux réseaux d'entreprise.
Flexibilité	Safetica couvre tous types d'applications, de protocoles de messagerie instantanée et de service webmail, grâce à son approche universelle unique.

ESET Technology Alliance

Les cybercriminels, les menaces, les réglementations tout comme les comportements des utilisateurs imposent aux entreprises de multiplier leurs lignes de défenses.

Les solutions « ESET Technology Alliance » apportent, au-delà des outils ESET, des réponses afin de mieux protéger les entreprises.

ESET sélectionne avec soin ses partenaires, par leur expertise dans des domaines précis et complémentaires en sécurité informatique.

Si les aspects technologiques sont importants, nous ne négligeons pas la stabilité et la santé financière de nos partenaires.

Grâce à cela, ESET peut fournir des solutions à la fois puissantes et flexibles qui répondront aux besoins grandissants en matière de sécurité de nos clients.

Événements pris en charge sur les terminaux

Reporting et blocage d'activités

- Toutes opérations sur fichiers
- Tendances à long terme, fluctuations d'activité à court terme
- Sites web (tous navigateurs, y compris trafic HTTPS) – temps d'activité et d'inactivité
- E-mails et webmails (tous fournisseurs)
- Mots-clés recherchés (principaux moteurs de recherche et Windows Search)
- Messagerie instantanée (tous protocoles et applications)
- Utilisation des applications, avec temps d'activité et d'inactivité
- Imprimantes virtuelles, locales et réseau
- Activité de l'écran (capture intelligente)
- Enregistrement de frappe

Protection contre les fuites de données

- Tous disques durs, USB, FireWire, cartes SD/MMC/CF, lecteurs SCSI
- Transfert de fichiers en réseau (sécurisé ou non)
- E-mails (protocoles SMTP, POP, IMAP, Microsoft Outlook / MAPI)
- SSL/HTTPS (tous navigateurs et applications avec gestion des certificats standard)
- Copier-coller, presse-papiers, glisser-déposer
- Imprimantes virtuelles, locales et réseau
- Bluetooth, ports IR/COM/parallèles
- Lecteurs et graveurs CD/DVD/BluRay
- Contrôle de l'accès des applications aux fichiers

Cas d'utilisation

Sécurisation des informations importantes de l'entreprise	Une fois les zones de sécurité établies pour toutes les données protégées, Safetica surveille toutes les interactions avec ces fichiers et, en cas d'opération non autorisée, la bloque ou exécute d'autres actions prédéfinies. L'entreprise peut par exemple choisir d'informer le responsable sécurité de chaque événement, de chiffrer les données ou de proposer un autre emplacement sûr pour les données. Les données des ordinateurs portables et des clés USB sont protégées, même en dehors de l'entreprise.
Gestion des périphériques amovibles	Les responsables peuvent définir les appareils que chaque utilisateur peut connecter aux ordinateurs de l'entreprise, ce qui élimine un canal de fuite de données et réduit considérablement le nombre d'interventions de maintenance.
Conformité réglementaire	L'installation de Safetica Endpoint Client sur les ordinateurs de votre entreprise et l'activation de la gestion des stratégies dans Safetica Management Console vous permettent de vous conformer aux réglementations régissant la protection des données personnelles.
Chiffrement des données	Safetica permet de chiffrer des disques complets, de protéger un système de stockage de fichiers chiffrés, de gérer les clés connectées et d'empêcher le stockage de données à des emplacements non sécurisés.
Contrôle de la productivité	Même sans passer par l'interface Safetica Management Console, les responsables peuvent recevoir régulièrement des rapports de synthèse sur les utilisateurs ou groupes.

Architecture

POSTES DE TRAVAIL AVEC SAFETICA ENDPOINT CLIENT

SAFETICA MANAGEMENT SERVICE ET BASE DE DONNÉES SQL

SAFETICA MANAGEMENT CONSOLE AVEC PARAMETRAGES ET RAPPORTS

SAFETICA MANAGEMENT SERVICE SERVEURS DANS UN AUTRE EMPLACEMENT

1. Les actions sont enregistrées et les règles de stratégie sont appliquées via un agent (pouvant être masqué à l'utilisateur).
2. Les données sont automatiquement synchronisées des ordinateurs vers le serveur lors d'une connexion.
3. Toutes les données peuvent être visualisées depuis la console d'administration. Toutes les configurations se font à partir de cette même console.
4. Safetica permet la prise en charge de plusieurs filiales depuis une console de gestion unique.

Configuration système requise

Client Safetica

- Processeur dual-core 2,4 GHz
- 2 Go de mémoire RAM
- 10 Go d'espace disque disponible
- Installation sur poste client
- MS Windows 7 et versions ultérieures, 32 bits et 64 bits

Serveur Safetica

- Processeur dual-core 2 GHz (quad-core recommandé)
- 4 Go de mémoire RAM
- 20 Go d'espace disque disponible
- Installation sur serveur d'applications ou serveur dédié (virtualisation possible)
- Active Directory pris en charge
- MS Windows Server 2008 R2 et versions ultérieures, 32 bits et 64 bits
- Requiert une connexion à un serveur lors du partage avec MS SQL , un processeur quad-core, 8 Go de RAM et 100 Go d'espace disque disponible minimum sont recommandés

MS SQL (base de données pour serveur)

- Configuration requise pour la version de MS SQL utilisée
- Serveur partagé ou dédié, 100 Go d'espace disque disponible minimum recommandés
- MS SQL 2008 R2 et versions ultérieures, éventuellement MS SQL 2012 Express et versions ultérieures (version gratuite)
- MS SQL Express est une option lors de l'installation

ENJOY SAFER TECHNOLOGY™

30 ANNÉES D'INNOVATION POUR PROTÉGER VOTRE VIE NUMÉRIQUE

Consultez notre offre complète des solutions et services sur :

WWW.ESET.COM/FR/BUSINESS

Besoin de renseignements ? Contactez-nous :

Vous êtes une entreprise
01.55.89.08.85
clientsfinaux@eset-nod32.fr

Vous êtes un revendeur
01.55.89.08.85
technoalliance@eset-nod32.fr