

safetica ONE

Prévention des pertes de données **et** protection contre les menaces internes **sans intervention**

- ✓ **Sans impact** sur les utilisateurs et l'infrastructure
- ✓ **Implacable** contre les menaces internes et les pertes de données
- ✓ Prise en charge **active** de la conformité réglementaire

Sécurisation de vos données et amélioration de l'efficacité opérationnelle

Safetica ONE est la seule solution mature de protection des données conçue pour répondre aux besoins et à l'évolutivité des PME et des grandes entreprises. Maîtrisez vos précieuses données au meilleur rapport qualité-prix. Dépassez le simple cadre de la prévention des pertes de données grâce à une analyse globale des comportements, permettant de détecter les menaces internes encore plus tôt et de réagir avant qu'elles ne se transforment en incidents. Tirez parti de connaissances sur l'espace de travail, les ressources digitales et les activités de l'entreprise pour optimiser les coûts.



Les personnes et les données sont le moteur des entreprises modernes. Lorsque des données sensibles sont perdues ou volées, la réputation de l'entreprise, sa compétitivité et sa rentabilité en souffrent.

Le coût moyen d'une fuite de données est de **3,27 millions d'euros**.*

60 % des petites entreprises font faillite **dans les six mois** suivant une fuite de données majeure**

* Rapport de 2020 sur le coût des fuites de données, Ponemon Institute ; ** National Cyber Security Alliance, octobre 2012

Chaque entreprise peut protéger ses données

La sécurité interne n'a jamais été aussi facile. Nous vous aidons à protéger vos données, guider vos collaborateurs et assurer la conformité de vos activités. Safetica ONE empêche les fuites de données et facilite le respect des réglementations en matière de protection des données, en protégeant votre entreprise contre les erreurs humaines et les comportements malveillants.

Protection experte des données

Nous couvrons tous les domaines des risques liés aux données internes, et protégeons les données précieuses contre les erreurs humaines et les intentions malveillantes.

Réduction du délai de rentabilité

La sécurité ne doit jamais se faire au détriment de la productivité. Safetica ONE n'entraîne aucun tracas supplémentaire pour les collaborateurs ou le département informatique. Son rapport qualité-prix est imbattable.

Intégration transparente

Seule une solution de sécurité parfaitement intégrée peut fonctionner efficacement. En collaboration avec nos partenaires technologiques, nous protégeons les données sur tous les appareils, les principaux systèmes d'exploitation et dans le Cloud.

Scénarios clés de protection des données

Découverte des flux de données et détection des risques

Safetica audite et consigne toute tentative de fuite de données, intentionnelle ou non, quel que soit l'endroit où les informations sensibles sont stockées, ou qui y a accédé. L'analyse des risques vous aide à détecter et déterminer comment vos données pourraient être divulguées ou volées.

Conformité réglementaire

Safetica ONE vous aide à détecter et empêcher les infractions de la réglementation, et enquêter sur les incidents pour vous conformer aux réglementations et aux normes de protection des données telles que RGPD, HIPAA, SOX, PCI-DSS, GLBA, ISO/IEC 27001 et CCPA.

Protection des données et sensibilisation des collaborateurs

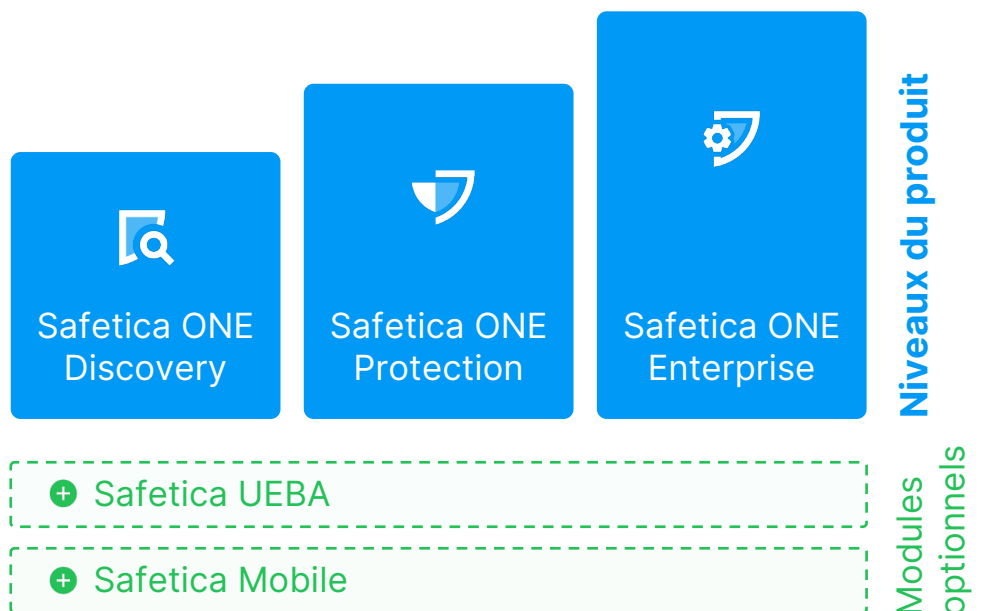
N'importe qui peut faire une erreur qui pourrait mettre votre entreprise en danger. Avec Safetica ONE, vous pouvez analyser les risques internes, détecter les menaces et les atténuer rapidement. Les notifications sur la façon de traiter les données sensibles peuvent contribuer à sensibiliser les collaborateurs à la sécurité des données.

Analyse de l'espace de travail et des comportements

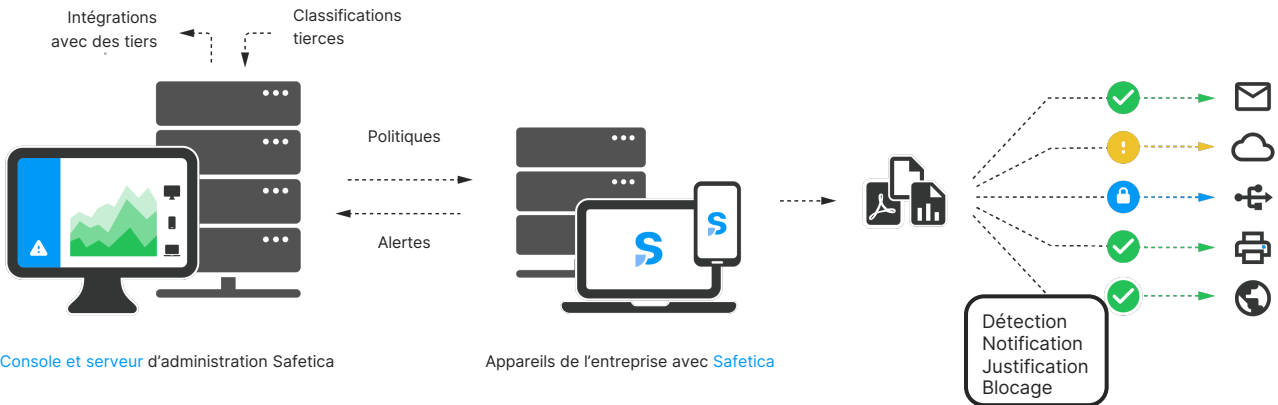
L'analyse des espaces de travail et du comportement des utilisateurs fournit un niveau de détail supplémentaire pour détecter les risques internes. En comprenant comment vos collaborateurs travaillent, impriment et utilisent les licences matérielles et logicielles coûteuses, vous pouvez également optimiser vos coûts et améliorer l'efficacité opérationnelle.

Safetica ONE protège

- vos données personnelles
- les documents stratégiques de l'entreprise
- les bases de données clients
- les données relatives aux paiements, telles que les numéros de cartes bancaires
- la propriété intellectuelle : schémas industriels, secrets d'affaires et savoir-faire
- les contrats



Architecture de référence



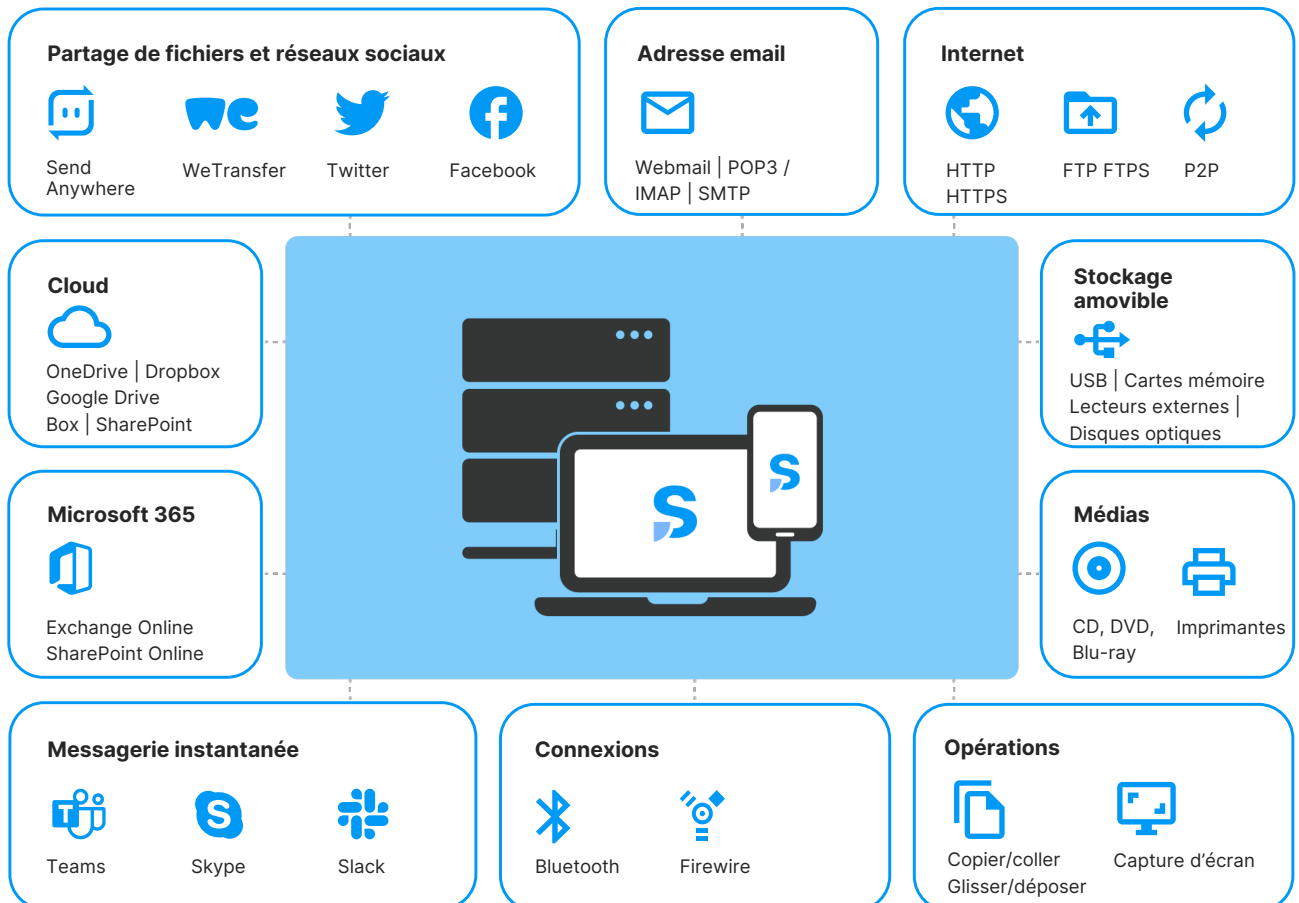
Le serveur utilise une base de données contenant les enregistrements des activités et de la sécurité des terminaux. La console d'administration de Safetica permet aux administrateurs de gérer les politiques de sécurité et de consulter les informations collectées.

Toutes les actions sont consignées et les politiques de sécurité sont appliquées sur les ordinateurs et autres appareils mobiles distants ou même hors ligne (smartphones gérés par MDM uniquement) avec un client Safetica.

Les données sensibles sont protégées sur tous les canaux.

Canaux de données couverts

Safetica protège les données sur une multitude de canaux et de plateformes, quel que soit l'endroit où elles résident ou circulent.



Avantages clés de Discovery

Safetica ONE Discovery audite et classe tous les flux de données dans votre entreprise. Il identifie les informations sensibles et les risques pour la sécurité en inspectant les contenus grâce à la reconnaissance optique de caractères (ROC). Bénéficiez d'un aperçu rapide sur ce qui se passe dans votre espace de travail en temps réel. Comprenez toutes les activités, les processus et les risques internes associés aux données pour améliorer la sécurité de vos données.



Bénéficiez d'une visibilité sur les incidents liés à la sécurité des données et aux infractions de la **conformité réglementaire** afin de pouvoir réagir et atténuer leurs impacts



Auditez et classez vos flux de données sensibles dans n'importe quel canal ou activité afin de déterminer où vos données risquent d'être perdues ou volées



Obtenez des **notifications instantanées** ainsi que des **rapports** utilisables et faciles à comprendre présentant une évaluation du niveau de risque et un aperçu des incidents



Découvrez et supprimez les logiciels, services dans le Cloud ou matériels/périphériques indésirables ou inutiles



Une solution **facile à déployer**, s'intégrant en un clic avec **Microsoft 365**, respectueuse des processus établis, et fournissant de premiers rapports en quelques jours

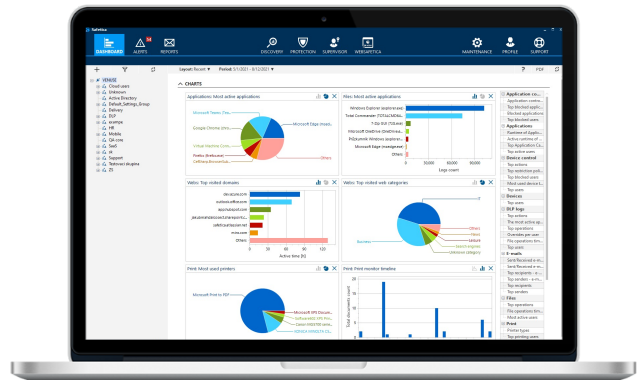


Analysez objectivement **les activités des utilisateurs** dans votre environnement et déterminez si **les équipements et le réseau de l'entreprise sont utilisés correctement**

Principaux éléments

Identifiez comment les données de l'entreprise sont utilisées et où elles sont stockées et envoyées, quel que soit le lieu où elles résident ou circulent

- ✓ Prise en charge de Windows et macOS
- ✓ Intégration avec Microsoft 365 en un clic
- ✓ Inspection et classification du contenu des fichiers
- ✓ Mise à jour facile vers la plateforme complète de sécurité des données
- ✓ Fonctionne sur du matériel ou virtualisé sur site, hébergé, hébergé dans une VM dans le Cloud



La console d'administration de Safetica ONE Discovery fournit un aperçu approfondi de toutes les opérations consignées sur les fichiers, avec différentes vues pour faciliter l'interprétation.

Avantages clés de Protection

Safetica ONE Protection identifie les risques, sensibilise vos collaborateurs, et empêche les erreurs et les actes malveillants des collaborateurs pour protéger vos données. La combinaison de l'analyse des données, de leur classification et de la prévention des pertes de données (DLP) avec la protection contre les menaces internes crée un environnement sécurisé, et garantit l'efficacité des activités de l'entreprise.



Contrôle total sur les flux de données sensibles et les risques internes grâce à l'analyse des comportements et l'inspection des contenus



Obtenez régulièrement des rapports de sécurité et des notifications en temps réel sur les incidents



Utilisez Safetica Zones pour une sécurité des données simplifiée et de haut niveau



Créez une copie masquée des données qui fuient afin de conserver des preuves pour une enquête ultérieure

Définissez des politiques claires pour tous les utilisateurs et les canaux de données

Définissez des politiques de sécurité pour des groupes ou des individus spécifiques. Sélectionnez le flux de travail souhaité avec des actions configurables : audit silencieux, blocage strict et notifications.

Détectez les menaces et analysez les risques internes

Réagissez aux menaces avant même qu'un incident majeur ne se produise grâce à la détection précoce des comportements anormaux et des risques liés aux flux de données dans votre entreprise. Safetica ONE utilise une classification avancée des contenus et la reconnaissance optique de caractères pour détecter les données sensibles dans les fichiers images et les documents PDF scannés.

Maîtrisez les données sensibles confiées aux collaborateurs

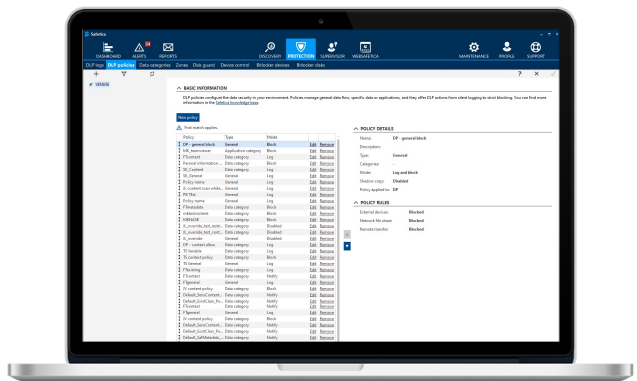
Présentez des notifications pédagogiques aux collaborateurs en cas de risque d'infraction de la politique de sécurité, afin de les informer ou de les laisser décider. Appliquez des processus spécifiques pour protéger les données les plus précieuses.

Contrôlez tous les appareils, connectés ou non

Limitez l'utilisation des périphériques portables ou des supports non autorisés. Contrôlez les appareils mobiles appartenant à l'entreprise, et conservez une trace des données qui sortent de Microsoft 365. Safetica reste totalement actif, quelle que soit la connexion au réseau. Tous les enregistrements collectés sont synchronisés lorsque la connexion est rétablie.

Principaux éléments

En se basant sur l'inspection des contenus, l'analyse des risques internes et des politiques claires mises en place pour tous les canaux de données, Safetica ONE Protection est en mesure de reconnaître lorsqu'un collaborateur commet une erreur ou prend des risques avec vos données sensibles. Selon le mode de fonctionnement de Safetica ONE, il peut soit bloquer l'activité à risque, soit avertir l'administrateur, soit rappeler aux collaborateurs les directives de sécurité de l'entreprise.



La console d'administration de Safetica permet une configuration détaillée mais facile des politiques de DLP, des catégories de données ou des rapports.

Avantages clés d'Enterprise

Safetica ONE Enterprise étend la prévention des pertes de données et la protection contre les menaces internes grâce au contrôle supplémentaire des flux de travail, l'automatisation et l'intégration transparente avec des solutions de sécurité réseau tierces, des SIEM et des outils d'analyse de données. Constituez votre infrastructure de sécurité informatique en toute simplicité.



Intégration automatisée de tiers et de fonctionnalités pour des cas d'utilisation avancés.



Politiques de contrôle des flux de travail sur les terminaux de l'entreprise



Prise en charge d'Active Directory dans les environnements multidomains



Personnalisation à la marque de l'entreprise des notifications de sécurité envoyées aux utilisateurs sur les terminaux

Intégrations transparentes

L'automatisation des politiques de sécurité et l'intégration avec votre infrastructure informatique vous aident à protéger vos ressources, même dans des environnements complexes.

L'intégration native avec Microsoft 365 ou les Appliances réseau Fortinet permet un contrôle étendu des appareils inconnus, et crée une robuste solution de sécurité réseau de bout en bout.

Tous les incidents et journaux audités peuvent être automatiquement envoyés à des solutions de SIEM, par exemple Splunk, IBM QRadar, LogRhythm ou ArcSight, pour une enquête plus approfondie. L'API REST fournit les données collectées à des outils tels que Power BI ou Tableau pour une analyse avancée.

Contrôle avancé des flux de travail

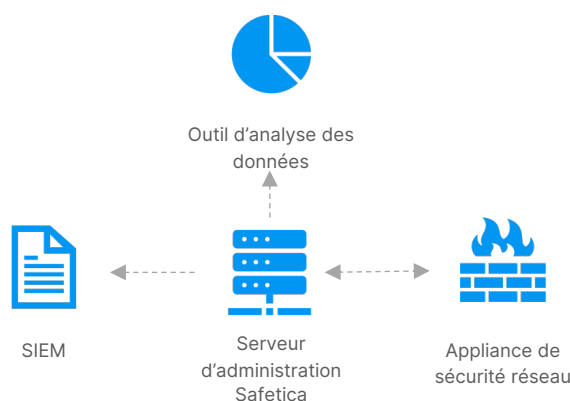
L'ensemble des fonctions de contrôle vous permet de définir comment les utilisateurs sont autorisés à travailler, quelles que soient les données concernées.

Grâce au contrôle des flux de travail, vous pouvez appliquer un processus sécurisé spécifique et bloquer toutes les autres façons d'effectuer une action.

Le contrôle des flux de travail comprend des politiques de DLP applicatives afin de gérer le comportement de différents types d'applications, telles que des CRM ou la messagerie instantanée, et des règles de politique de DLP avec des configurations personnalisées appliquées à différents réseaux, chemins locaux ou accès exclusif pour les utilisateurs privilégiés.

Principaux éléments

- ✓ Prise en charge de Windows et macOS
- ✓ Intégration en un clic à Microsoft 365
- ✓ Intégration des Appliances réseau Fortinet
- ✓ Intégration avec Power BI ou Tableau via API
- ✓ Notifications immédiates dans votre boîte de messagerie
- ✓ Inspection du contenu des fichiers à l'aide de modèles prédéfinis
- ✓ Classification des contenus basée sur différentes approches



Avantages clés du UEBA

Obtenir des connaissances est la première et la plus importante étape pour comprendre les flux de travail de votre entreprise, les habitudes de travail et la productivité des collaborateurs. Enrichissez n'importe quel produit Safetica ONE avec le module User and Entity Behavior Analytics (UEBA) pour consulter les activités des utilisateurs en détail et découvrir les comportements anormaux. Assurez le bon déroulement des activités, même lorsque vous travaillez à distance.



Identifiez les activités des utilisateurs grâce à l'audit des activités de travail, ainsi qu'à la catégorisation et au tagging automatisés des applications utilisées et des sites web consultés



Obtenez des informations plus approfondies sur la communication par email grâce la consignation de tous les emails, tout en respectant la confidentialité des collaborateurs



Suivez les changements de comportement des utilisateurs grâce à une visibilité sur les tendances et les changements de comportement des utilisateurs dans votre réseau au fil du temps



Audit de l'utilisation des ressources pour obtenir un aperçu précis de la répartition et de l'utilisation efficace des licences logicielles et du matériel achetés



Obtenez des rapports complets et des alertes en temps réel sur les activités de chaque utilisateur, même en télétravail, par exemple via RDP, etc.



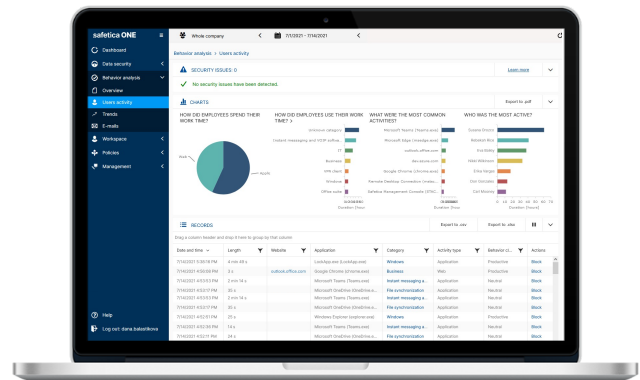
Auditez les recherches d'emploi pour identifier les portails consultés par des utilisateurs spécifiques, qui pourraient présenter un risque futur pour la sécurité des données

Identification des causes profondes des anomalies

Identifiez les éléments problématiques de votre environnement et approfondissez leur analyse pour répondre aux préoccupations de sécurité ou d'efficacité métier. Analysez objectivement les activités professionnelles de chaque employé à l'aide d'informations détaillées. Découvrez si quelqu'un consulte des sites web dangereux ou utilise des applications indésirables.

Transparence du travail, même à distance

Permettez aux cadres supérieurs et aux responsables de service de déterminer comment leurs collaborateurs travaillent. Restez maître de la situation, même lorsque vos collaborateurs travaillent à domicile ou en déplacement. Prévenez les risques pour la sécurité et gérez l'efficacité des collaborateurs en identifiant l'inactivité, les recherches d'emploi et les comportements suspects.



WebSafetica fournit une visibilité facile à comprendre sur toutes les menaces possibles. Obtenez des statistiques importantes via le tableau de bord, configurez des vues et des rapports personnalisés sur les enregistrements.

Avantages clés du Mobile

Safetica ONE Mobile est un outil léger de gestion des appareils mobiles (MDM) qui améliore la sécurité des données sur les smartphones et les tablettes, afin d'en faire des éléments de confiance de votre environnement informatique. Obtenez une vue d'ensemble sur l'état des appareils mobiles afin d'identifier les risques pour la sécurité et être en mesure de réagir rapidement. Tout cela à partir d'une seule interface.



Protection des données sur les appareils mobiles

Isolez les applications et les données professionnelles dans un espace de travail protégé, identifiez les applications nuisibles sur certains appareils, et bloquez ou effacez à distance les appareils égarés ou volés.



Vue d'ensemble de l'état des utilisateurs et des appareils

Contrôlez la sécurité et la connectivité des appareils, suivez et retrouvez les appareils perdus grâce à la localisation à distance.



Administration centralisée à distance

Utilisez l'administration avancée des applications pour contrôler leur paramètres et leur comportement, définir des politiques de sécurité pour des groupes d'appareils, et les configurer et les gérer automatiquement à partir d'un seul endroit.

Protection et administration de tous les appareils mobiles

Vérifiez tous les appareils de l'entreprise et découvrez les risques pour la sécurité en un seul coup d'œil. Configurez les politiques des appareils et même les comptes Wifi à distance. Utilisez Android EMM et iOS Managed Apps pour créer un espace de travail distinct sur les appareils de l'entreprise, et les utiliser pour le travail à distance et à des fins personnelles.

Audit des fichiers entrants sur Android

Obtenez une vue d'ensemble de l'endroit où vos données sont stockées, même sur les appareils mobiles appartenant à l'entreprise (disponible pour Android 6-10). En utilisant Safetica ONE Mobile avec WebSafetica, vous pouvez repérer les incidents de sécurité d'un seul coup d'œil, qu'ils se produisent sur votre téléphone, votre ordinateur ou dans le Cloud Microsoft 365.

Protection antivol

La perte des appareils mobiles appartenant à l'entreprise et le roulement du personnel sont des problèmes courants qui peuvent mettre en danger vos données sensibles. Safetica ONE Mobile localise les appareils mobiles de l'entreprise et les efface à distance s'ils sont inaccessibles. Cela vous permet de sécuriser votre infrastructure et maîtriser la propriété de vos données critiques.

Principaux éléments

- ✓ MDM et sécurité : espace de travail sécurisé, politiques relatives aux appareils, administration des applications avec configuration à distance, état de la sécurité
- ✓ Protection antivol : localisation, robustesse du mot de passe, verrouillage à distance, effacement des données à distance

Configuration requise

- **Android :**
Android 6+ et Google Play Services
- **iOS :**
iOS 10+

Liste détaillée des fonctionnalités I

Compatible avec Windows, macOS, Microsoft 365, Android, iOS	Safetica ONE Discovery	Safetica ONE Protection	Safetica ONE Enterprise
Audit de sécurité	✓	✓	✓
Audit de sécurité des flux de données Audit de sécurité des flux de données sur l'ensemble des canaux, y compris les dispositifs externes, le téléchargement web, la messagerie par email, la messagerie instantanée, l'impression et le stockage dans le Cloud.	✓	✓	✓
Audit des fichiers et des emails Office 365 Audit des opérations sur les fichiers et des communications par email sortant dans Office 365.	✓	✓	✓
Visibilité sur la conformité réglementaire Découvrez les infractions des réglementations les plus courantes, telles que PCI-DSS, GDPR ou HIPAA, dans toutes les variantes régionales.	✓	✓	✓
Audit de sécurité de l'espace de travail Auditez l'utilisation des appareils, des applications, des réseaux et de l'impression. Découvrez les ressources inutilisées ou mal utilisées pour faciliter la maintenance de l'espace de travail, assurer la fidélisation et réduire les coûts.	✓	✓	✓
Inspection des contenus Classez les fichiers et les emails sensibles via l'inspection avancée des contenus, à l'aide de modèles prédéfinis ou de règles et de dictionnaires personnalisés.	✓	✓	✓
Détection des activités suspectes Réagissez rapidement grâce à la détection en temps réel des activités suspectes et aux alertes immédiates par email.	✓	✓	✓
Protection des données sur les terminaux	✗	✓	✓
Protection de la messagerie et du réseau Protection des données pour la messagerie, le téléchargement web, la messagerie instantanée et les partages réseau.	✗	✓	✓
Protection des appareils et de l'impression Gérez les flux de données vers les appareils externes et empêchez l'impression des données sensibles sur les imprimantes locales, réseau ou virtuelles.	✗	✓	✓
Protection du télétravail Évitez les fuites de données sur les terminaux distants ou les connexions RDP. Prise en charge un large éventail de solutions d'accès à distance.	✗	✓	✓
Classification avancée des données Utilisez des technologies avancées pour détecter et tagger les données sensibles en fonction de leur origine, du contexte du flux de travail ou du type de fichier. Profitez de la détection des métadonnées pour utiliser des classifications tierces. Permettez aux utilisateurs de classer eux-mêmes les fichiers.	✗	✓	✓
Différentes politiques de remédiation Réagissez avec souplesse aux incidents détectés pour sensibiliser et responsabiliser vos collaborateurs. Les incidents peuvent être consignés, bloqués, ou justifiés/bloqués avec dérogation.	✗	✓	✓
Copie masquée des incidents Conservez des preuves des incidents en créant des copies masquées des données qui fuient. Les copies masquées sont entièrement chiffrées et peuvent être conservées sur des ordinateurs locaux avec une politique de conservation.	✗	✓	✓

Liste détaillée des fonctionnalités II

Compatible avec Windows, macOS, Microsoft 365, Android, iOS	Safetica ONE Discovery	Safetica ONE Protection	Safetica ONE Enterprise
Protection des données sur les terminaux	×	✓	✓
Contrôle de l'espace de travail Définissez votre espace de travail sécurisé, et réduisez le périmètre en contrôlant les applications et les sites web. Évitez les comportements indésirables dans votre entreprise et réduisez le coût de l'administration de la sécurité.	×	✓	✓
Zones Safetica Administration facile du périmètre de sécurité des données grâce aux zones uniques de Safetica, qui réduisent considérablement le nombre de politiques de protection des données.	×	✓	✓
Gestion du chiffrement BitLocker Administration centralisée des disques locaux et des périphériques externes avec chiffrement BitLocker.	×	✓	✓
Protection des données dans le Cloud	×	✓	✓
Protection contre la synchronisation des terminaux dans le Cloud Protection des données stockées dans le Cloud via OneDrive, Google Drive, Dropbox, Box, etc., à partir des terminaux.	×	✓	✓
Protection avancée des terminaux Microsoft 365 Protection des données pour Microsoft 365 et SharePoint à partir des terminaux. Empêchez le partage ou le téléchargement de données que vous ne souhaitez pas héberger sur le Cloud.	×	✓	✓
Protection des informations Azure Détection des classifications de données provenant de Microsoft Azure Information Protection, même sous forme chiffrée.	×	✓	✓
Protection d'Exchange Online Unifiez les politiques appliquées à la messagerie sur les terminaux et dans le Cloud. Gérez et filtrez les données sortant des terminaux et d'Exchange Online.	×	✓	✓
Fonctionnalités d'Enterprise	×	×	✓
Habillage des notifications à la marque de l'entreprise Personnalisation des notifications envoyées aux utilisateurs finaux (logo).	×	×	✓
Contrôle des flux de travail Politiques applicatives et paramètres des politiques configurés par des experts pour aligner les flux de travail des terminaux aux processus de l'entreprise.	×	×	✓
Prise en charge multidomaine Prise en charge de multiples domaines sur Active Directory.	×	×	✓
Automatisation de la sécurité	×	×	✓
Intégration SIEM Signalement automatisé des incidents aux solutions de SIEM (Splunk, QRadar, LogRhythm, ArcSight, etc.).	×	×	✓
Intégration avec FortiGate Intégration automatisée de la sécurité avec les Appliances réseau FortiGate pour créer une robuste solution de sécurité réseau de bout en bout.	×	×	✓
API de reporting API pour transmettre les données de Safetica à des services d'analyse et de visualisation.	×	×	✓

Spécifications et exigences techniques

Serveur

- Processeur quad-core 2,4 GHz
- 8 Go de RAM ou plus
- 100 Go d'espace disque disponible
- Un serveur partagé ou dédié, prise en charge des machines virtuelles et de l'hébergement dans le Cloud
- Nécessite une connexion au serveur avec MS SQL 2012 ou ultérieur, ou Azure SQL
- Serveur MS Windows 2012 et ultérieur

Base de données

- MS SQL Server 2012 et ultérieur, ou MS SQL Express 2016 et ultérieur, ou Azure SQL.
- MS SQL Express fait partie d'un installateur universel et est recommandé pour protéger jusqu'à 200 terminaux.
- 200 Go d'espace disque disponible (idéalement 500 Go ou plus, en fonction de l'étendue des données collectées).
- Un serveur partagé ou dédié, prise en charge des machines virtuelles et de l'hébergement dans le Cloud. Il peut être hébergé avec le serveur Safetica.

Client Windows

- Processeur dual-core 2,4 Ghz, 2 Go de RAM ou plus
- 10 Go d'espace disque disponible
- MS Windows 7, 8.1, 10 (32 bits [x86] ou 64 bits [x64])
- Programme d'installation MSI
- .NET 4.7.2 et ultérieur

Client macOS

- Processeur quad-core 2,4 GHz, 2 Go de RAM ou plus
- 10 Go d'espace disque disponible
- macOS 10.10 et ultérieur (pour l'ensemble des fonctionnalités de DLP, nous recommandons la version 10.15 et ultérieur).

Client mobile

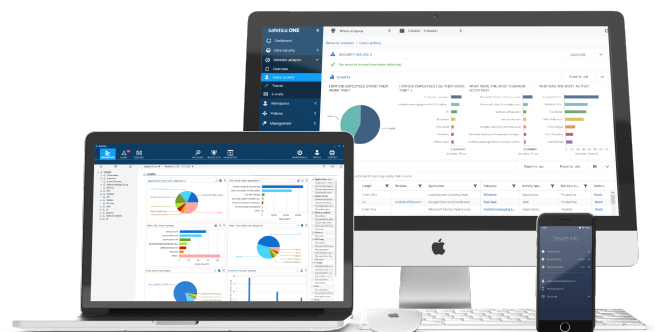
- Android : Android 6+ et Google Play Services
- iOS : iOS 10+

Plateformes de Cloud prises en charge

- Microsoft Azure, Microsoft 365

Certifications

- ISO 9001 et ISO/IEC 27001
- Membre de l'Accord des entreprises de technologies de cybersécurité
- Partenaire Gold Microsoft
- Membre de l'Alliance technologique ESET
- Membre de l'Alliance technologique Fortinet



+ 400 000
appareils protégés

+ 120
pays

+ 80
experts en sécurité

À propos de Safetica

Safetica est un éditeur de logiciels tchèque qui fournit aux entreprises de toute taille et de toute forme des solutions de prévention des pertes de données et de protection contre les menaces internes. Chez Safetica, nous pensons que chacun mérite de savoir que ses données sont en sécurité.

Alliances technologiques



Récompenses et réalisations



THE RADICATI GROUP, INC.
A TECHNOLOGY MARKET RESEARCH FIRM

FORRESTER

Gartner



Excellente
protection des données
en toute simplicité

Essayez une démo de Safetica
dès maintenant !

safetica