SEARCHINFORM

RISK AND COMPLIANCE MANAGEMENT

# Solution de protection contre les menaces internes

www.searchinform.com

**1995** La compagnie a été fondée

**2 000 000+**

Ordinateurs protégés par la solution de SearchInform

Représentants et partenaires

Plus de **3 000** clients dans 28 pays

**8** produits et services pour la protection complète des données

2019 SearchInform a commencé à fournir des **services** de surveillance

2020 SearchInform a déployé la **solution dans le cloud**

**32** procès pénaux contre des utilisateurs malveillants ont été gagnés par des clients

**2017** Le logiciel SearchInform a été inclus dans le **Magic Quadrant de Gartner**

## 2018-2020

La série de conférences

**Road Show SearchInform**

a eu lieu

en **Amérique latine,** au **Moyen-Orient** et en **Afrique** du **Nord,** en **Afrique du Sud,** en **Inde** et en **Indonésie**

**2010**

**Le centre de formation** s'est lancé

**Radicati Group** a inclus SearchInform dans la recherche **«Marché de la prévention des pertes de données, 2017-2021»**

# Produits et services

**SearchInform DLP**
*Page 4*

**SearchInform Risk Monitor**
*Page 4-11*

**SearchInform ProfileCenter**
*Page 12-13*

**SearchInform SIEM**
*Page 14-15*

**SearchInform FileAuditor**
*Page 16-17*

**SearchInform TimeInformer**
*Page 18-19*

**SearchInform Services**
*Page 20-21*

# SearchInform DLP

Renforce la protection d'une entreprise contre les fuites de données confidentielles, le contrôle des données au repos et en transit.

Facilite la surveillance de presque tous les canaux de transfert de données, l'analyse des informations, la détection des violations et leur prévention, aide à fournir des rapports à un responsable.

## SearchInform aide les entreprises en répondant à tous leurs besoins :

- La protection des informations confidentielles contre les fuites pendant le stockage, l'utilisation et le transfert
- Le contrôle des outils d'accès à distance et de virtualisation (TeamViewer, RAdmin, RDP)
- La facilitation de l'inventaire des logiciels et du matériel
- Le cryptage des données pour éviter leur utilisation en dehors de l'entreprise
- Le signalement d'événements irréguliers au sein du réseau, tels que la copie de données sur des périphériques de stockage amovibles ou la suppression d'un grand nombre de fichiers

# SearchInform Risk Monitor

SearchInform propose une approche complète de la surveillance interne en déployent une solution DLP et en combinant deux concepts puissants : la prévention des incidents et l'atténuation des menaces internes.

Les instruments d'atténuation des menaces internes et d'identification des risques internes protègent votre entreprise contre les pertes financières et de réputation causées par les menaces internes.

### SearchInform **solution en cloud**

Les entreprises ne doivent pas choisir entre sécurité, convivialité et coût car la solution peut être déployée dans un cloud. Aucun équipement particulier n'est requis : le système collecte, traite et conserve les données dans un environnement virtuel.

Un tel modèle de déploiement conviendra aux entreprises qui ne disposent pas de leur propre infrastructure informatique, ou si leurs bureaux sont situés dans différentes villes, ou encore s'ils ont un grand nombre d'employés travaillant à distance.

## Solution étendue :

- Détecte les incidents d'utilisateurs malveillants impliquant des fraudes et des profits d'entreprise
- Facilite les processus de conformité réglementaire et d'enquête
- Contrôle le facteur humain et anticipe les risques RH
- Fonctionne comme un système d'alerte précoce découvrant une menace potentielle ou une condition préalable à une violation et alertant sur les risques possibles

# Capture d'informations

La solution SearchInform se compose de modules, chacun d'eux contrôle son propre canal de données.

## MailController

Capture tous les courriels sortants et entrants envoyés via les clients de messagerie et les services Web, y compris Gmail, Yahoo, Hotmail, etc. Détecte l'envoi de messages aux boîtes courriels privés et aux adresses électroniques des concurrents et bloque la transmission des messages si leur contenu contient données confidentielles de l'entreprise.

## FTPController

Vérifie le trafic régulier (FTP) et crypté (FTPS) et informe l'exécutif des incidents ou bloque la connexion.

## HTTPController

Capture et indexe les fichiers et les messages envoyés via HTTP/HTTPS. Si nécessaire, le système bloque le trafic Web, y compris les messageries Web, les services de cloud, la messagerie, les blogs, les forums, les réseaux sociaux et les requêtes de recherche. Maintient sa fonctionnalité de surveillance régulière même si les employés utilisent des dispositifs d'anonymisation.

## IMController

Suit les discussions, l'historique des messages, les appels et les listes de contacts dans les messageries : Skype, WhatsApp, Telegram, Viber, Lync, Gadu-Gadu, XMPP, etc. Surveille la correspondance via les services Web sur les réseaux sociaux, tels que Facebook, Google+, LinkedIn, etc.

## ProgramController

Collecte des données sur l'activité des utilisateurs au cours de la journée et sur le temps passé dans les applications, les programmes et sur les sites Web. Détermine automatiquement si des employés travaillent ou viennent de lancer le programme pour prétendre qu'ils travaillent. Catégorise les ressources Web : rencontres, musique, shopping, actualités, etc.

*Vous aide à surveiller les performances des employés à distance*

## PrintController

Inspecte le contenu des documents envoyés à l'impression (les fichiers texte sont simplement copiés et les numérisations de documents sont interceptées en tant qu' « empreintes digitales » numériques avec leur contenu textuel reconnu). Détecte les documents authentifiés par un sceau et surveille l'impression des formulaires à émission contrôlée.

## MonitorController

Prend des captures d'écran et enregistre des vidéos de l'activité surs l'écran. Complète les photos et vidéos séquences avec des informations actuelles sur les applications ouvertes et les processus en cours. Si nécessaire, affiche des informations en temps réel. Prend des clichés instantanés pour identifier l'intru.

## Keylogger

Capture les frappes et les données copiées dans le presse-papier. Intercepte les données de connexion et de mot de passe pour faciliter le suivi des comptes gérés sur des ressources Web potentiellement dangereuses. Identifie les utilisateurs qui ont entré des mots de passe sur leur clavier pour accéder aux documents cryptés.

## CloudController

Contrôle les fichiers reçus, téléchargés et stockés dans des stockages en cloud. Suivi des services de stockage en nuage et de partage de fichiers : Google Docs, Office 365, Evernote, iCloud Drive, SharePoint, Dropbox, Amazon S3, DropMeFiles, etc. Intercepte les fichiers envoyés et reçus via TeamViewer, RealVNC, Radmin, LiteManager.

## DeviceController

Capture et bloque les données transférées vers les lecteurs flash, les disques durs externes, les CD/DVD, via RDP et les caméras. Crypte automatiquement les données écrites sur un lecteur flash. Il détecte et reconnaît les smartphones connectés à un ordinateur (Android, Apple, BlackBerry, Windows Phone), analyse leur contenu. Il contrôle l'accès d'un appareil à un ordinateur.

## MicrophoneController

Utilise un microphone détecté pour enregistrer les conversations à l'intérieur et à l'extérieur du bureau. Active l'enregistrement audio – avant même que l'utilisateur ne se connecte – lorsque la parole est détectée ou lorsque certains processus et programmes, comme spécifié dans la politique de sécurité pertinente, sont lancés. Le flux audio peut être converti en texte, qui est également vérifié par rapport aux politiques de sécurité spécifiées.

# Centre de contrôle

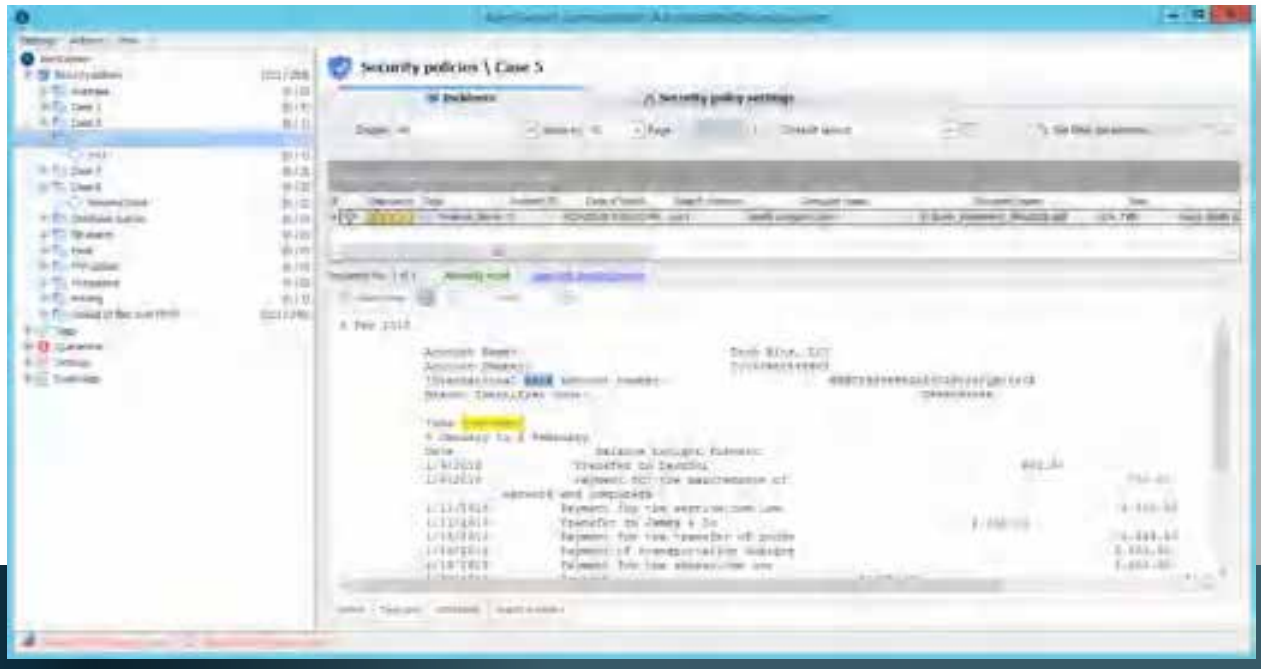
## DataCenter

Gère les index de produits et les bases de données, surveille la santé du système et assure la connectivité aux systèmes tiers, tels qu'AD, SOC, et le serveur de courrier sortant. Les utilisateurs du DataCenter peuvent configurer la différenciation des droits d'accès.

## AlertCenter

C'est le « think tank » du système où les politiques de sécurité sont mises en place. Il comprend plus de 300 politiques de sécurité préconfigurées qui peuvent être modifiées. La solution permet de créer des règles personnalisées d'analyse et de blocage des données capturées, de configurer le calendrier des contrôles et d'envoyer des notifications.

Vous pouvez également visualiser les incidents dans la console AlertCenter sur l'ordinateur d'entreprise d'un responsable ou via l'interface web accessible via un ordinateur portable, une tablette, ou un smartphone.



*Politiques de sécurité et résultats de recherche dans AlertCenter*

## Analytic Console

Ses objectifs sont de parcourir les données capturées et de les analyser ainsi que de surveiller les activités des utilisateurs en ligne. Divers algorithmes de recherche et modèles de rapports prédéfinis sont à la disposition de l'expert.

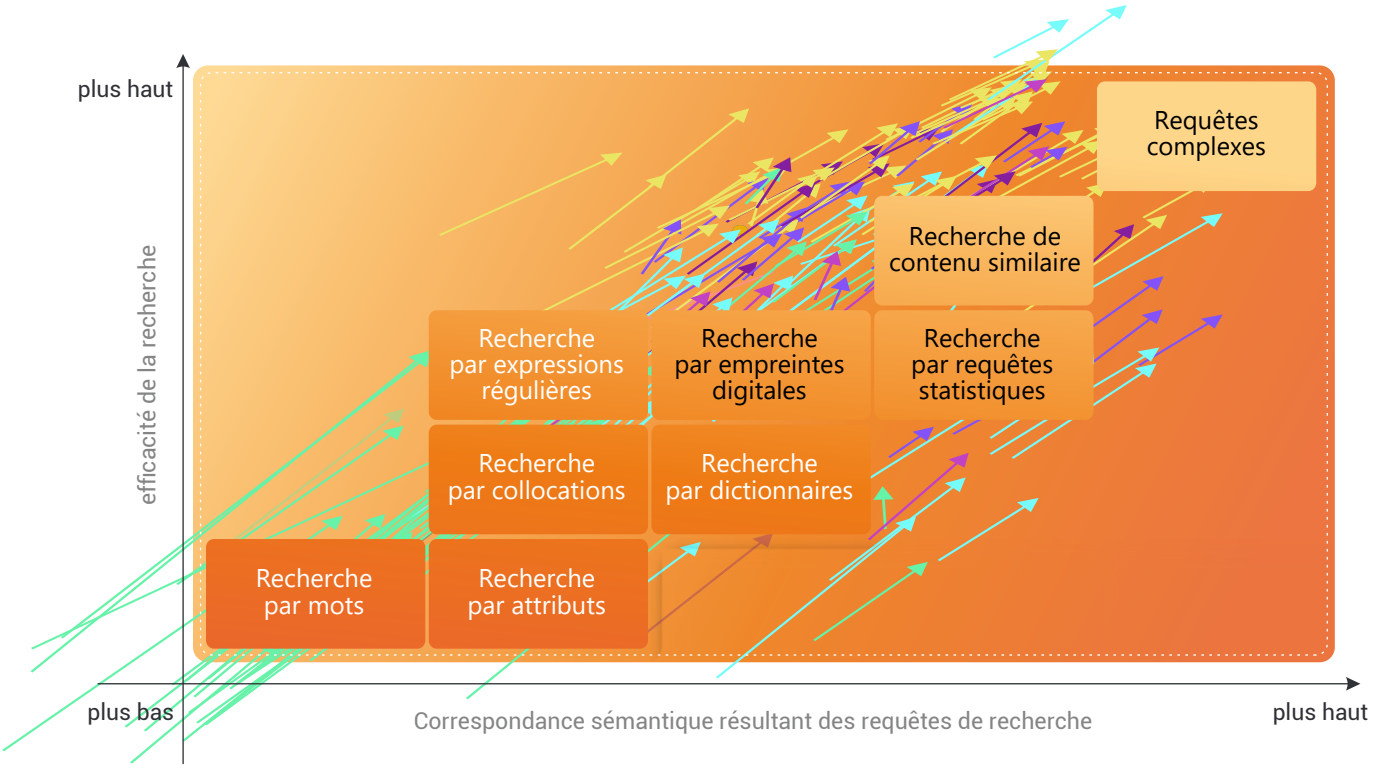
Les rapports créés dans Analytic Console sont disponibles dans la version **Web de la console**.

# Capacités analytiques

Pour remplir efficacement leurs fonctions, les experts doivent disposer de capacités de contrôle complètes sur tous les canaux de communication ainsi que de fonctionnalités adéquates pour rechercher les données capturées et les analyser. Un module analytique puissant, avec diverses options de recherche et des analyses graphiques et audio automatisées permettent à un seul spécialiste d'inspecter le travail de plusieurs milliers d'employés.

## Analyse de texte

Une variété d'algorithmes fournit une vérification approfondie des messages textes et des documents. Le système offre des technologies de recherche uniques telles que la recherche de contenu similaire ou les requêtes complexes. L'algorithme propriétaire de la recherche de contenu similaire identifie les documents confidentiels même s'ils ont été modifiés, ce qui signifie que les résultats de la recherche incluront des documents qui correspondent à la requête sémantiquement plutôt que celle simplement technique. Les requêtes complexes permettent à l'utilisateur de construire des algorithmes de recherche avancés à l'aide de requêtes simples combinées logiquement par des opérateurs ET, OU et NE.




## Analyse graphique

Le système détermine les types d'images circulant au sein de l'entreprise : fichiers PDF, photos ou copies numérisées – et catégorise les fichiers images en conséquence. Le système intégré OCR (Optical Character Recognition/Reconnaissance Optique de Caractères) identifie les documents conformes à des modèles spécifiques : passeports, cartes bancaires, permis de conduire, etc. La technologie permet de retrouver des données personnelles, financières et toute autre donnée sensible dans les archives, même transmises au format de documents numérisés.

## Analyse audio

La solution SearchInform convertit les enregistrements audios en texte et vérifie si une transcription est conforme aux politiques de sécurité. Le système a la possibilité d'activer l'enregistrement audio lorsque la parole est détectée ou lorsque certains processus ou programmes, comme spécifié dans la politique de sécurité pertinente, sont lancés.

# Rapports & UEBA

Le logiciel SearchInform visualise tous les événements et connexions au sein de l'entreprise sous forme de rapports – via la console analytique et l'interface Web. La configuration par défaut comprend plus de 30 modèles de base. L'assistant de rapport permet à l'utilisateur de créer des rapports personnalisés et non limités par aucun critère.

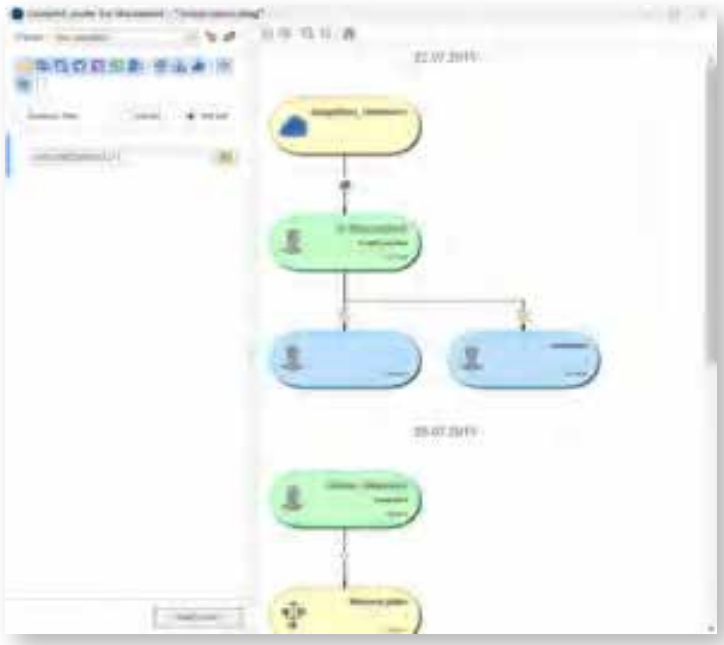
## Rapport Graphique des relations

Démontre les connexions d'employé à employé et d'employé à personne tiers sous la forme d'un graphique relationnel. Visualise les activités des utilisateurs sur tous les canaux de communication ou au sein d'une ligne de communication particulière. Facilite les enquêtes d'entreprise.

*Graphique relationnel de Analytic Console*

## Rapport de routage de contenu

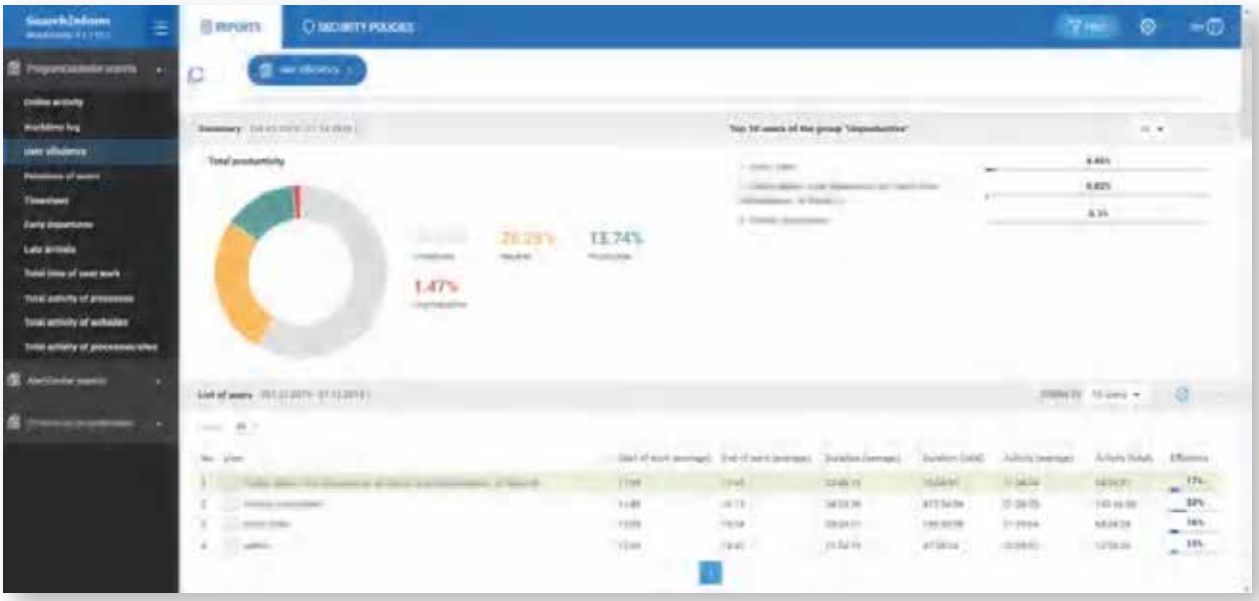
Illustre tous les mouvements de documents entre l'expéditeur et le destinataire via des canaux de communication internes et externes de manière complètement transparente. Permet d'identifier rapidement l'auteur du document ainsi que la source des informations respectives et les chemins de sa distribution.



*Routage de contenu*

## Rapport de productivité des utilisateurs

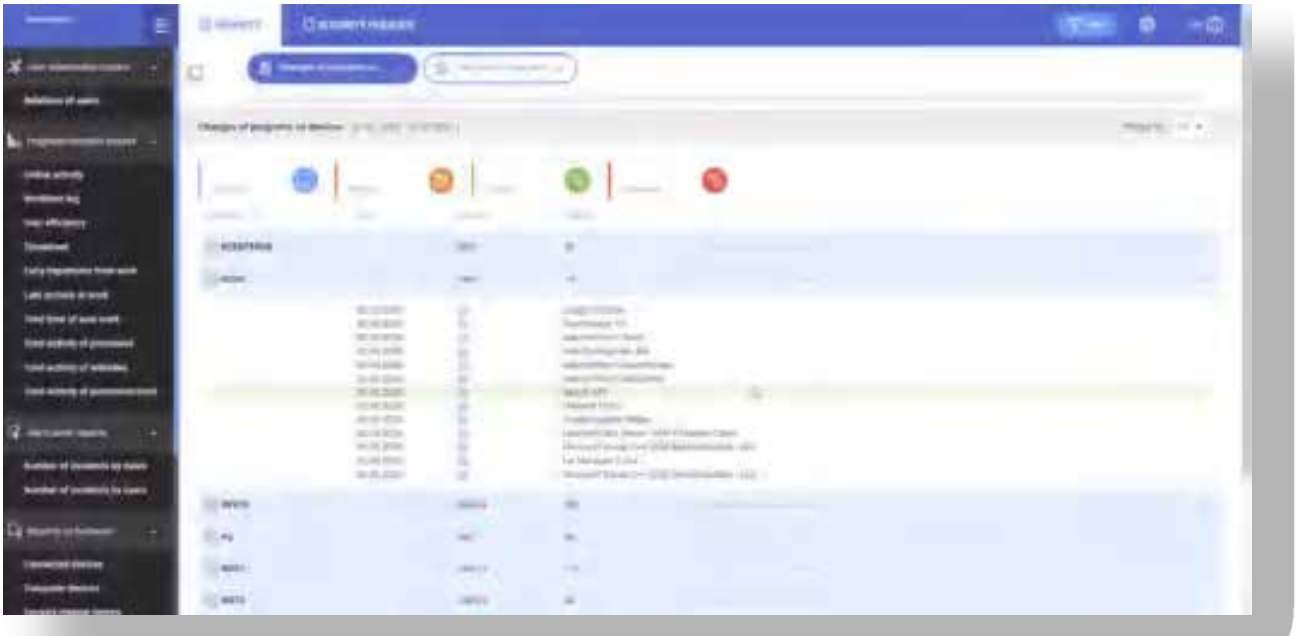
Affiche la productivité globale des employés de l'entreprise via des graphiques et des notes. Le rapport détecte la fréquence à laquelle les employés arrivent et quittent le travail ainsi que ceux qui sont fréquemment en retard au travail. Visualise la performance de l'utilisateur pendant la semaine de travail sous un format de calendrier.



*Rapport de productivité des utilisateurs*

## Rapport logiciel et matériel

Signale toute modification apportée au matériel installé et aux appareils connectés. Cela facilite l'inventaire et les garanties contre le vol d'équipement ou les substitutions d'équipement non autorisées. Les rapports logiciels organisent les données sur les opérations d'installation et de désinstallation des logiciels.



*Rapport logiciel et matériel*

# Avantages

## Le déploiement facile sans modification de la structure du réseau

Les informaticiens du client pourront installer la solution SearchInform en quelques heures. Le processus d'installation n'entrave pas le fonctionnement des systèmes d'information locaux de l'entreprise.

## Solution complète

La structure a plusieurs composants vous fournira des solutions adéquates, que vous souhaitiez poursuivre une surveillance complète sur plusieurs canaux de fuites de données ou simplement combiner un certain nombre de modules de votre choix en fonction de vos besoins – dans ce cas, le coût sera considérablement inférieur.

## Module analytique puissant

Offre des solutions rapides et flexibles pour la configuration des alertes et l'analyse des flux de données sans faire appel à des spécialistes tiers. Avec l'aide du produit SearchInform, un spécialiste peut contrôler le travail de plusieurs milliers d'employés.

## Garanties de sécurité pour les entreprises dispersées géographiquement

Dans les succursales distantes avec un petit nombre d'ordinateurs et un canal de communication en « bande étroite » vers le siège social, où il est impossible de déployer un système à part entière, les données seront filtrées, traitées et cryptées localement avant d'être transférées vers le serveur.

## Outils pour les enquêtes d'incident étape par étape

L'enregistrement des conversations et la capture du contenu à l'écran en temps réel, la surveillance des entrées du clavier et les vidéos avec une webcam – ces composants intégrés du système aident à retracer la violation étape par étape.

## Agents de contrôle pour OS Linux

Le produit SearchInform peut fonctionner sous certaines des distributions les plus populaires.

## Solution déployée en cloud

Tous les composants de Risk Monitor peuvent être déployés en nuage (la plateforme cloud SearchInform ou tout service cloud tiers peut être utilisé) sans interférer avec les fonctionnalités du système. Ce moyen de protection des données est rentable et permet de gagner du temps.

## Intégration avec d'autres produits SearchInform

La solution SearchInform est intégrée de manière transparente à SIEM, ProfileCenter, FileAuditor et Database Monitor, ce qui augmente le niveau de sécurité des informations et de sensibilisation aux risques de l'entreprise, et réduit le temps de réponse à l'incident, permettant d'enquêter pleinement sur les violations.

## Visualisation des connexions entre les employés

Un graphe relationnel interactif est un bon support visuel démontrant les cercles sociaux et les lignes de communication impliquant les salariés de l'entreprise et leurs interlocuteurs tiers.

## Département de mise en œuvre et Centre de formation

Notre expérience pratique avec plus de 3 000 entreprises dans différents secteurs nous permet de créer rapidement des ensembles uniques de politiques de sécurité axées sur les tâches pertinentes et le secteur d'activité spécifique du client.

## Contrôle d'accès à distance

La solution SearchInform protège les données transmises via des environnements virtuels et des outils de contrôle à distance. La surveillance est mise en œuvre au niveau du presse-papiers, via la connexion des périphériques de stockage virtuels, et au niveau des fonctionnalités logicielles spécifiques (par exemple, le transfert via le menu contextuel TeamViewer).

## Une archive des informations interceptées

Facilite considérablement la reconstruction de la chaîne d'événements et permet à une entreprise de mener une enquête rétrospective.

## Parcours du contenu des documents

Il montre le mouvement des documents, indique l'expéditeur et le destinataire, ainsi que les canaux de communication utilisés pour le transfert de données.

## Surveillance des données au repos

Le système fournira des alertes au moment opportun lors de l'enregistrement de la présence d'informations confidentielles dans des emplacements non conçus pour leur stockage.

# SearchInform ProfileCenter

80% des entreprises ont découvert que leurs employés effectuent des activités non liées au travail pendant les heures de travail*

**Selon les statistiques de mise en œuvre de la solution SearchInform 2020.*

L'objectif d'une entreprise est de réduire les risques, de prévoir l'activité des salariés et de prévenir un incident.

Le problème est résolu par ProfileCenter – l'ensemble d'outils de diagnostic sans test qui aide à classer les personnalités, à prévoir le comportement, à mettre en évidence les forces et les faiblesses et à détecter la propension à la criminalité.

## Comment le profilage peut-il aider les entreprises ?

Les méthodes de profilage sont appliquées dans les entreprises pour détecter les activités frauduleuses, améliorer les techniques de gestion du personnel, augmenter les ventes et évaluer les risques causés par des traits de personnalité pouvant nuire à des collègues ou à une entreprise.

**ProfileCenter détecte :**

- Propension à commettre un crime.
- Traits de personnalité clés, forces et faiblesses.
- Comportement en situation de conflit.
- Rôle social des employés au sein d'une équipe.
- Attitudes cachées.
- Émotions simples.

## Comment fonctionne le produit ?

### Étape 1

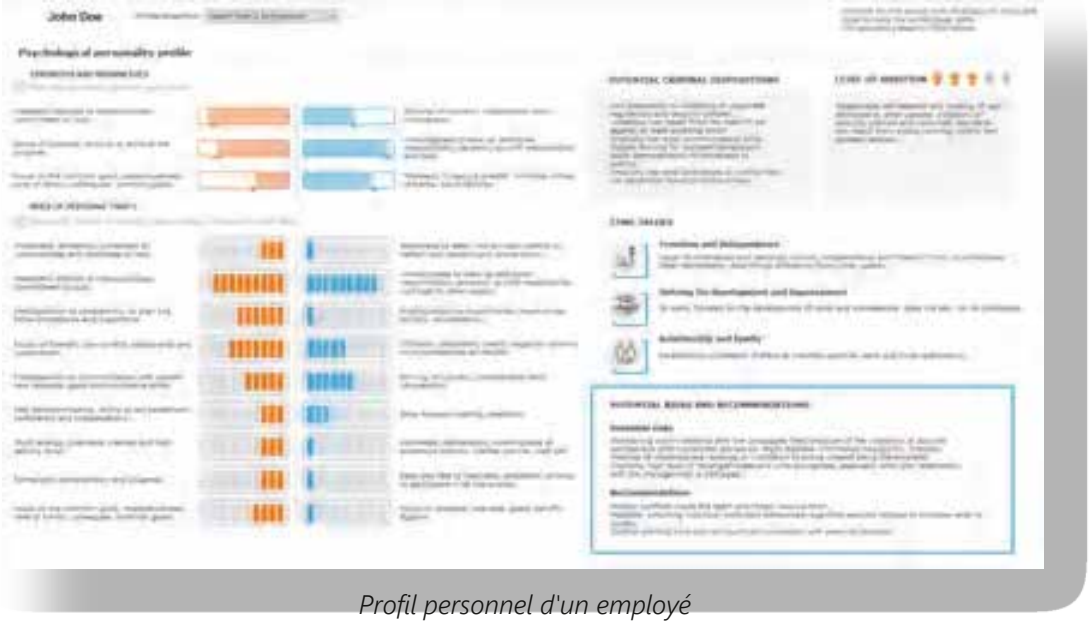
Le système collecte la correspondance des employés (email, messagers, réseaux sociaux).

### Étape 2

Le logiciel effectue l'identification des particularités de comportement et des schémas de pensée sur la base de l'analyse de texte comportant plus de 70 critères.

### Étape 3

Les résultats de l'analyse sont affichés sous forme de rapport avec un commentaire et une approche pratique.

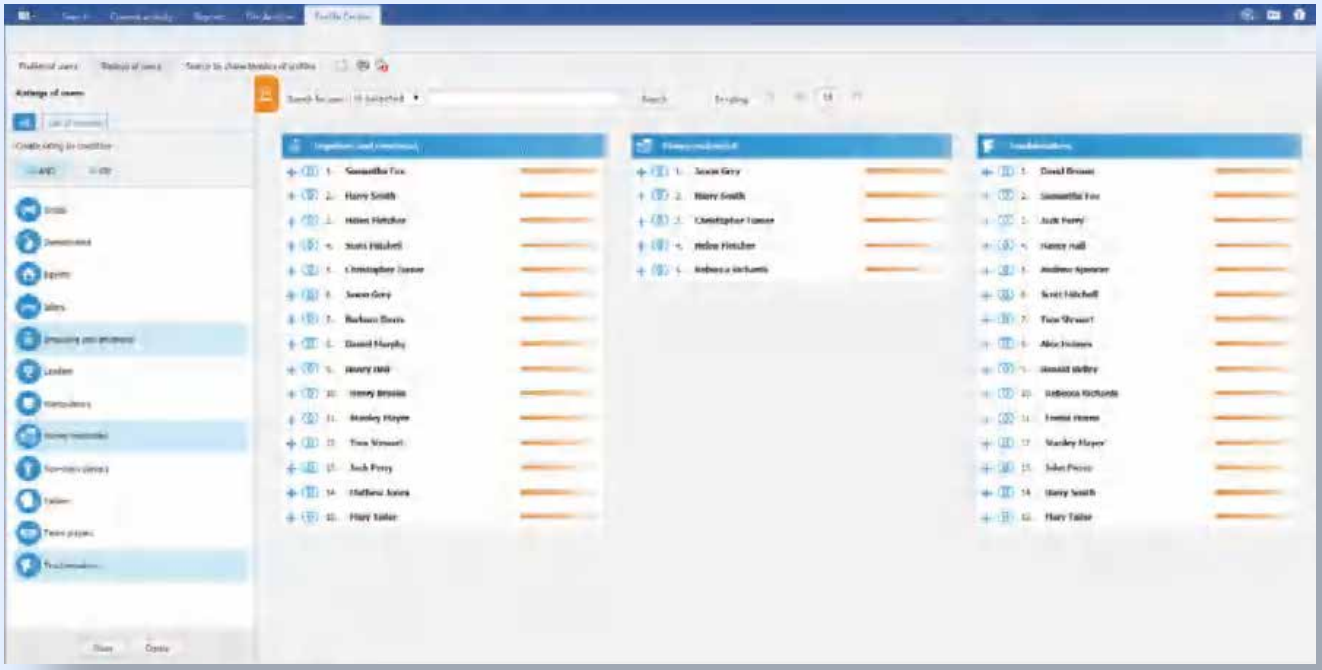


*Profil personnel d'un employé*

# Le produit facilite la prise de decision

**Recevez des recommandations pratiques sur :**

- Quels comportement d'employé doivent attirer votre attention.
- Comment créer une équipe efficace.
- Qui doit être parfois surveillé et qui – doit l'être toujours ou dans des situations spécifiques.
- Est-il sûr de donner accès à des informations confidentielles, des actifs financiers et des sources précieuses ?
- Si un emploi convient à un employé.
- Avec qui communiquer de manière officielle et professionnelle et qui est ouvert à l'établissement d'une amitié.
- Si une réprimande ou une brève instruction est une mesure suffisante ou si certains employés doivent être systématiquement formés ou sanctionnés.



*Note de l'utilisateur*

# Avantages

- La solution automatisée vous fournit des résultats rapidement et permet d'économiser de l'argent sur l'embauche d'un profileur.
- Analyse les données collectées par une solution de protection des données dont la pertinence est supérieure à celle obtenue lors de tests ouverts.
- Surveille la personnalité en dynamique.
- Ne distrait pas le personnel du travail et n'aggrave pas la situation.
- Détecte les changements d'humeur et d'attitude au sein d'une équipe.

# SearchInform SIEM

L'infrastructure informatique d'une entreprise comprend une multitude de systèmes d'entreprise : pare-feu, systèmes d'exploitation, serveurs de messagerie, bases de données, périphériques réseau.

Beaucoup de ces systèmes sont des sources de données qui attirent les contrevenants, ce qui implique la nécessité d'une protection spéciale.

- **Le premier SIEM système prêt à l'emploi**
- **La création de politique en deux clics**

N°1

## Surveillance automatique des événements de sécurité

SearchInform SIEM est un système permettant de collecter et d'analyser les événements de sécurité en temps réel, d'identifier les incidents de sécurité de l'information et d'y répondre. Le système accumule les informations de diverses sources, les analyse, enregistre les incidents et alerte le personnel désigné.

## SearchInform SIEM révèle :

- Des épidémies virales et infections distinctes
- Des tentatives d'accès non autorisé aux données
- Des tentatives de deviner le mot de passe du compte
- Des comptes actifs d'employés licenciés qui ont dû être supprimés
- Des erreurs de configuration matérielle
- Un abus de température de fonctionnement admissible
- Une suppression des données des ressources critiques
- L'utilisation des ressources de l'entreprise pendant les heures de repos
- Une suppression des machines virtuelles et des snapshots
- Une connexion à de nouveaux équipements de l'infrastructure informatique
- Des modifications de la politique du groupe
- L'utilisation de TeamViewer, accès à distance aux ressources de l'entreprise
- Des événements critiques dans les systèmes de protection
- Des erreurs et défaillances dans les systèmes d'information

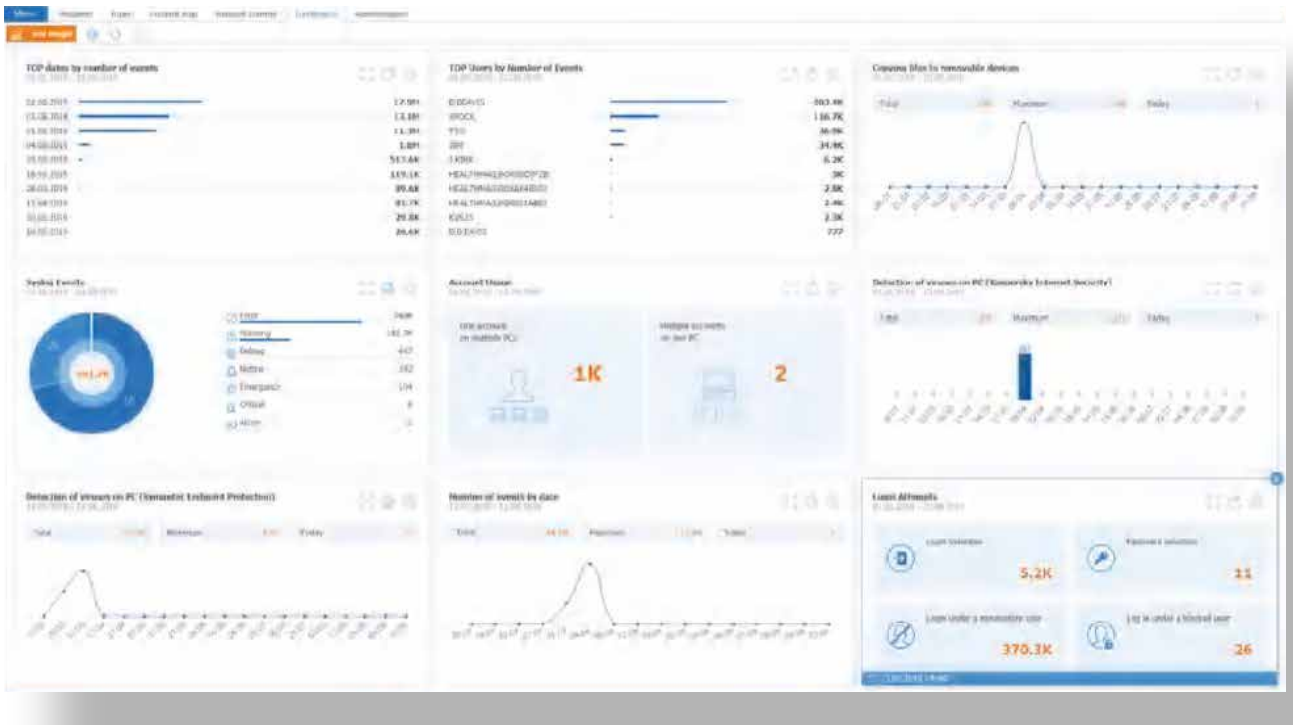



*Tableau de bord des statistiques des événements*

# Politiques de sécurité préconfigurées

Lors de l'installation du système, le personnel de sécurité de l'information a alors accès à plus de 300 règles toutes faites – des politiques de sécurité. Les utilisateurs peuvent modifier et personnaliser les règles existantes et créer leurs propres politiques, c'est-à-dire choisir dans la liste prédéfinie et ajouter leurs propres politiques (fonction connecteur utilisateur).

- Systèmes d'exploitation
- Serveurs de messagerie
- Domaine et poste de travail
- Contrôleurs
- Serveurs et postes de travail Linux
- SGBD
- Systèmes DLP
- Serveurs de fichiers
- Virtualisation
- Environnements
- Antivirus
- Pare-feu et réseau intégré
- Dispositif de sécurité
- Solutions sur la plateforme 1C
- Autres sources Syslog

Les règles de corrélation croisée peuvent être configurées pour rechercher des incidents liés à des événements collectés à partir de diverses sources.

*Écran d'affichage des incidents*

# Avantages

- Le mise en œuvre est rapide sans configuration préalable intensive, le logiciel peut commencer à fonctionner le jour de l'installation.
- L'intégration avec les produits SearchInform augmente le niveau de sécurité des informations d'une entreprise et permet d'enquêter pleinement sur l'incident et de collecter une base de preuves.
- Le système est facile à utiliser, un spécialiste sans compétences informatiques s'occupera du programme car il ne nécessite pas de connaissance des langages de programmation pour créer des règles de corrélation et de corrélation croisée.
- Les exigences matérielles et logicielles sont faibles et le prix est raisonnable même pour les petites entreprises.

# SearchInform FileAuditor

**La quantité de données qu'une entreprise moyenne stocke est énorme. Certaines de ces données contiennent des informations confidentielles : données personnelles et financières, spécifications, dessins, etc. Chaque groupe de données sensibles doit être stocké, traité et diffusé conformément aux règles correspondantes.**

## Les données importantes sont toujours visibles

SearchInform FileAuditor est une solution DCAP (l'audit et la protection centrés sur les données) pour l'audit automatisé des stockages d'informations, la recherche de violations d'accès et le suivi des modifications apportées aux données critiques.

### FileAuditor résout les tâches suivantes :

#### La classification des données vulnérables

Trouve les fichiers dans un flux de documents qui contiennent des informations critiques et attribue un certain type à chaque fichier : données personnelles, secret commercial, numéros de carte de crédit, etc.

#### L'archivage de documents critiques

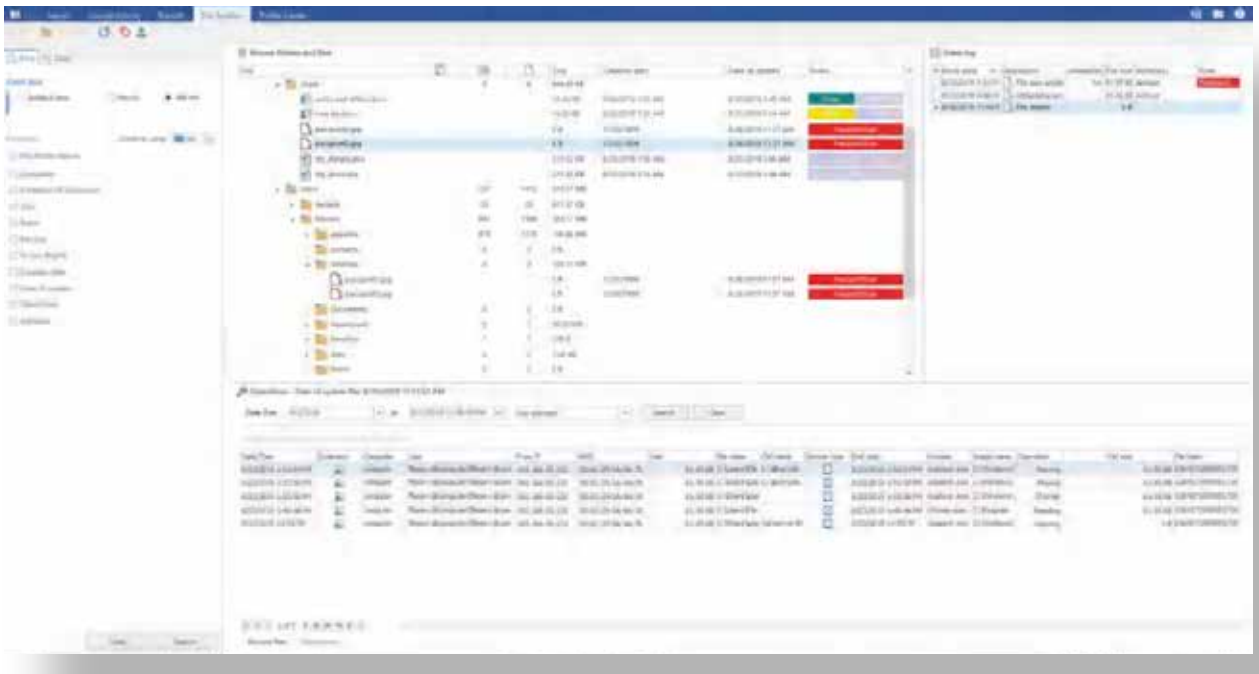
Crée des clichés instantanés des fichiers critiques trouvés sur un ordinateur, un serveur ou des dossiers réseau, enregistre l'historique de leurs révisions. L'archivage des données confidentielles aide à enquêter sur les incidents et assure la récupération des informations perdues.

#### L'audit des droits d'accès

Facilite le contrôle d'accès aux informations confidentielles – surveille automatiquement les ressources ouvertes, les fichiers disponibles pour un utilisateur ou un groupe spécifique, et les comptes privilégiés.

#### La surveillance de l'activité des utilisateurs

Audite les opérations des utilisateurs dans un système de fichiers et leur chronologie. Les spécialistes chargés de l'atténuation des risques ont toujours à jour leurs informations sur les modifications apportées à un fichier (création, édition, déplacement, suppression, etc.).



*Audit d'un dossier contenant des informations confidentielles*

# Analyse des données

Le module analytique FileAuditor visualise les résultats de l'analyse d'un système de fichiers conformément aux règles définies. Les paramètres de règles ont différents types de recherche disponibles (par contenu, attributs, expressions régulières, dictionnaires). Les résultats de la recherche peuvent être visualisés sous forme de rapports visuels (sur les sources, les droits d'accès, les erreurs) ou d'une arborescence.

**Le programme démontre :**

- L'arborescence des dossiers avec indication des droits d'utilisateur sur chaque répertoire ou fichier
- Les opérations sur fichiers critiques, dates de création et de modification
- Le nombre de documents critiques sur un disque ou dans un dossier
- Le marquage des dossiers (accord confidentiel, données personnelles, états financiers)

Les notifications sur les violations de stratégie définies peuvent être configurées dans AlertCenter. Par exemple, si FileAuditor trouve un document sensible sur l'ordinateur d'un utilisateur qui n'a pas le droit de le lire, un spécialiste responsable de l'atténuation des risques sera automatiquement alerté dès qu'une notification sera envoyée par courriel.

*Arborescence des dossiers avec marquage des documents sensibles*

Les informations collectées par les agents et le module d'analyse du réseau sont écrits dans une base de données exécutant Microsoft SQL Server, et des copies des fichiers critiques sont stockées dans le référentiel. C'est ainsi que les documents sont disponibles même après leur suppression.

# Avantages

- L'intégration transparente d'une solution DCAP dans Risk Monitor étend considérablement la fonctionnalité du système pour l'atténuation des risques.
- Contrôle de la charge d'ordinateur et sauvegarde de la mémoire – la surveillance peut être programmée ou provoquée par un événement ou une condition particulière ; le stockage seuls de documents sensibles est possible ; et un système de déduplication permet d'économiser de l'espace de stockage.
- Les paramètres de règles personnalisables évitent aux spécialistes des travaux inutiles, leur permettant de se concentrer uniquement sur la surveillance des données critiques.
- Les modifications apportées aux fichiers peuvent être suivies presque instantanément – le système enregistre un nombre spécifiques de révisions de fichiers, ce qui facilite l'enquête interne.

# SearchInform TimeInformer

Pour certains employés, être au travail ne signifie pas automatiquement s'occuper de leurs responsabilités directes. Il y a toujours des personnes irresponsables qui prennent fréquemment des pauses cigarettes et café, bavardent avec des collègues, passent du temps sur les réseaux sociaux, arrivent au travail tard ou partent tôt.

**TimeInformer est une solution de surveillance des employés qui protège l'entreprise contre le travail inefficace et les pertes financières liées au personnel.**

**TimeInformer analysera les ordinateurs de travail et vous aidera à identifier :**

- **Les contrevenants à la discipline** — du travail qui arrivent plus tard, partent tôt, prennent fréquemment des pauses cigarettes et café
- **Les oisifs** — qui discutent, font des achats en ligne, se tournent vers des jeux et d'autres activités
- **Les indépendants** — qui font du travail annexe dans les heures payées par l'entreprise
- **Les employés insatisfaits** — qui entraînent les autres travailleurs contre l'employeur, ou qui se sont épuisés sous une lourde charge de travail ou des tâches ennuyeuses

Le logiciel détermine le temps d'inactivité et le temps de travail des employés, collecte des données sur les logiciels utilisés par les employés au cours d'une journée, enregistre tous les sites Web visités et les catégorise – sites de rencontres, achats en ligne, actualités, émissions de télévision, etc. et évalue la productivité réelle du personnel selon les paramètres donnés.

SEARCHINFORM
RISK AND COMPLIANCE MANAGEMENT

## Contrôle en temps réel

TimeInformer peut être déployé en cloud, vous offrant la solution sans avoir besoin d'acheter et de maintenir du matériel.

TimeInformer peut être utilisé non seulement à l'arrière-plan, mais aussi dans d'autres modes. Le programme se connecte aux moniteurs et aux microphones des ordinateurs et reproduit en temps réel ce qui se passe.

La solution joue ou enregistre en temps réel les négociations importantes avec les principaux partenaires et clients.

TimeInformer montre en temps réel ce qui est affiché sur les moniteurs de vos employés à un moment donné, jusqu'à 16 ordinateurs simultanément.

# Assistance aux decisions de gestion

33 rapports prédéfinis dans TimeInformer permettent un démarrage en douceur, permettent une détection rapide des utilisateurs, aident à optimiser les processus de travail, à organiser les gens et à atteindre les objectifs.

## L'interface conviviale

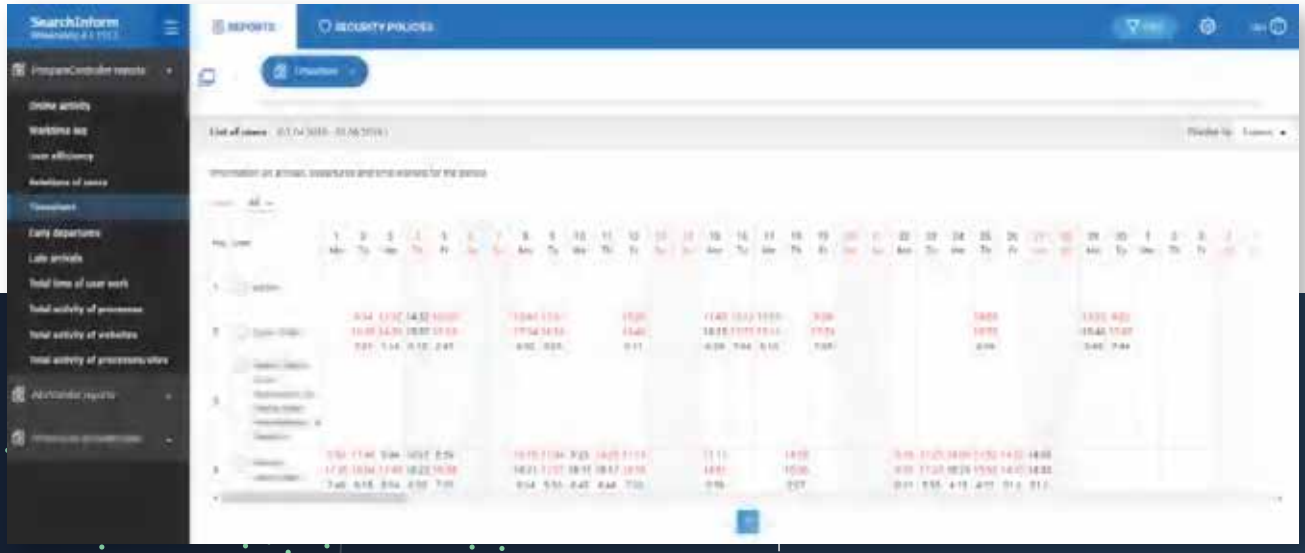
L'interface Web permettra de contrôler les employés de n'importe où dans le monde. Les autorisations pour afficher les rapports et les options d'administration sont différenciées en fonction des tâches et des outils.

**TimeInformer a les groupes de rapports suivants :**

- Des rapports sur l'activité des utilisateurs dans les applications et sur les sites Web
- Des rapports sur les programmes avec l'historique d'installation et de suppression de logiciels
- Des rapports sur les appareils avec des données sur les équipements installés sur un PC et les changements dans leur configuration

Les rapports et les notifications sont facilement personnalisés. Le système enverra une notification automatique en cas de violation.

Des alertes automatiques sur les activités suspectes des employés peuvent être reçues par courriel.



*Feuille de temps dans l'interface Web*

## Avantages

- Sécurisé contre la suppression et alerte sur ces tentatives.
- Suivi de l'activité des utilisateurs même lorsqu'ils travaillent à domicile ou sont en déplacement professionnel.
- Interface Web pour accéder aux résultats du suivi en dehors du bureau.
- Intégration avec les produits SearchInform, qui permet d'effectuer des enquêtes internes.

# Services

SearchInform fournit des services aux entreprises qui ne disposent pas d'un service dédié à l'atténuation des risques ou manquent de ressources pour intégrer un système de protection des données et mettre en œuvre un programme de surveillance.

Nos services permettent à une entreprise de bénéficier de la solution qui nécessite des coûts financiers et de main-d'œuvre minimum d'un client ainsi qu'aucun besoin d'embaucher des spécialistes. Un client obtient le système avec une équipe d'analystes qui ont une vaste expérience dans le domaine. Les experts commencent à travailler immédiatement après le déploiement sans être embarqués – pas de formation, pas de vacances, pas de congé de maladie.

L'option en tant que service est disponible pour chaque produit SearchInform. Certains d'entre eux peuvent être déployés en cloud, ce qui permet d'économiser les finances de l'entreprise, car il n'est pas nécessaire d'acheter du matériel et de dépenser pour sa maintenance.

| | SaaS (logiciel en tant que service) | Déployé en cloud |
|---|---|---|
| DLP | + | + |
| Risk Monitor | + | + |
| ProfileCenter | + | + |
| SIEM | + | - |
| FileAuditor | + | + |
| TimeInformer | + | + |

## Comment ça marche ?

Un spécialiste configure le système en fonction des tâches définies par un client

Un client devient pleinement autorisé à travailler avec le système

Après la détection d'un incident, un spécialiste contacte un client (les moyens de communication sont sélectionnés au préalable)

Un spécialiste fournit à un client des rapports d'incidents qui couvrent une période déterminée (une fois par jour/semaine/mois)

Un client peut travailler avec le système avec un spécialiste ou indépendamment

Un client peut assigner des tâches à un spécialiste

# Tâche – solution

Nos services permettent de détecter les points faibles d'une entreprise en peu de temps (les premiers résultats sont obtenus en 1 à 3 mois).

Les spécialistes qui travaillent avec le client surveillent le déploiement de la solution et prennent également des décisions en fonction des résultats des rapports et des enquêtes sur les incidents.

*Bref rapport sur les incidents*

# Avantages

- Une attitude impartiale et une approche professionnelle – l'équipe d'analystes fournissant nos services ne connaît pas les employés en personne, par conséquent, le facteur humain est exclu lors de l'enquête.
- Partager l'expérience et les connaissances de l'entreprise avec plus de 3 000 clients. Notre équipe sera en mesure d'affiner le logiciel en tenant compte de la portée d'une entreprise, ainsi que d'aider une organisation à tirer le meilleur parti des fonctionnalités du système.

# CONTACTS


**Argentine**
Buenos Aires
Téléphone : +54 9 11 5158 8557
Courriel : r.martinez@searchinform.com

**Brésil**
São Paulo
Téléphone : +55 11 43 80 19 13
+7925 681 1803
Courriel : v.prestes@searchinform.com

**Kazakhstan**
Almaty
Téléphone : +7 727 239 30 36
+7 727 222 17 95
Courriel : d.stelchenko@searchinform.ru

**La région du Moyen-Orient et de l'Afrique du Nord**
Téléphone : +375 25 708 77 69
Courriel : yamen@searchinform.com

**Afrique du Sud**
Centurion
Téléphone : +27 12 683 8816
Courriel : jorina@searchinform.com

**Royaume-Uni**
Londres
Téléphone : +44 0 20 3808 4340
Courriel : uk@searchinform.com