Présentation de la solution

# WithSecure™ Cloud Protection for Salesforce

salesforce PARTNER SINCE 2016

# Sommaire

# 1. Présentation générale

WithSecure™ Cloud Protection for Salesforce est une solution de sécurité cloud conçue pour compléter la sécurité native des plateformes Salesforce. Avec cette solution, les entreprises peuvent assumer leur part de responsabilité en matière de sécurité, conformément au modèle de responsabilité partagée utilisé dans les écosystèmes cloud.

WithSecure™ Cloud Protection for Salesforce vous permet de compléter efficacement votre stratégie globale de sécurité en sécurisant les services cloud. Cette solution fournit des composants de sécurité dédiés permettant de maîtriser les risques liés aux fichiers, URL et e-mails uploadés dans Salesforce, sans entraver l'utilisation de votre plateforme. Cloud Protection fournit des rapports détaillés, des analyses de sécurité avancées et des pistes d'audit complètes, pour garantir une réponse rapide et efficace aux cyberincidents.

Grâce à l'intégration cloud-to-cloud native entre Salesforce et WithSecure™, Cloud Protection constitue une option particulièrement pertinente, tant du point de vue de la sécurité que du point de vue des ressources.

Avec cette solution, vous n'avez pas besoin de consacrer de temps au déploiement ou à la maintenance de middlewares comme les serveurs ou proxys. Vous n'avez pas non plus besoin de modifier les configurations réseau.

Avec sa conception sans proxys, WithSecure™ Cloud Protection se distingue des solutions comme les CASB (Cloud Access Security Brokers) traditionnels qui doivent casser le chiffrement HTTPS de Salesforce à mi-chemin, rendant de ce fait le système moins sûr et beaucoup plus vulnérable.

WithSecure™ Cloud Protection offre une intégration étroite avec Salesforce, avec un déploiement simplifié via AppExchange. Ce déploiement ne prend que quelques minutes, pour vous faire gagner du temps et de l'argent.

## WithSecure™ Cloud Protection for Salesforce offre les avantages suivants :

**Protection cloud :** Avec cette solution, votre stratégie de sécurité couvre les services cloud et répond aux exigences du modèle de responsabilité partagée utilisé dans les écosystèmes cloud.

**Sécurité nouvelle-génération :** Plus qu'un simple produit antivirus, cette solution comprend des fonctionnalités avancées comme les renseignements sur les menaces en temps réel et le sandboxing cloud intelligent.

**Analyses avancées :** Les rapports détaillés, les analyses de sécurité avancées et les pistes d'audit complètes vous offrent une visibilité à 360 degrés sur les contenus de Salesforce. Grâce à cette visibilité, vous répondez rapidement et efficacement aux cyberincidents.

**Solution conçue en partenariat avec Salesforce :** Cette solution a été créée en collaboration avec Salesforce, pour garantir une intégration et une fiabilité sans faille, avec une expérience utilisateur optimale.

**Architecture cloud-to-cloud :** Grâce à l'intégration cloud-to-cloud entre Salesforce et WithSecure™, aucun middleware ou travail informatique coûteux n'est nécessaire.

**Cette solution est disponible à l'essai et en téléchargement sur Salesforce AppExchange.**



# 2. La société WithSecure™

WithSecure™, société leader dans le monde de la cybersécurité, œuvre depuis plus de 30 ans dans la protection des entreprises et des consommateurs. Nous les protégeons contre tous les cyber-risques, depuis les infections opportunistes par ransomware jusqu'aux cyberattaques avancées.

Nos 1 600 professionnels travaillent dans 30 bureaux à travers le monde et génèrent ensemble 170 millions de dollars de revenus annuels.

Nous avons participé à plus d'enquêtes européennes sur la cybercriminalité que n'importe quelle autre entreprise du secteur. Nous travaillons en étroite collaboration avec plus de 70 partenaires de la filière, et avec des entités internationales telles qu'Interpol, afin d'offrir à nos clients le plus haut niveau de sécurité.

Des millions d'utilisateurs sont protégés, chaque jour, par nos solutions. Nous les accompagnons par le biais d'un réseau de milliers de partenaires de confiance et via 200 opérateurs, dont des leaders comme Vodafone, Telefonica et Unity Media.

Année après année, des tests d'experts et d'analystes indépendants viennent confirmer que notre protection est plus efficace et plus consistante que celle offerte par nos concurrents.

WithSecure™ a obtenu l'award Best Protection d'AVTEST à 7 reprises depuis la création de ce prix il y a 8 ans. Les multiples récompenses 'Best Protection' et 'Top-Rated' d'AV-Test et AV-Comparatives viennent également prouver le haut niveau de protection que nous proposons.

Nos solutions utilisent une approche multi-niveaux de la sécurité. Elles s'appuient sur diverses technologies pionnières comme l'analyse heuristique et comportementale des menaces, et les renseignements sur les menaces en temps réel fournis via notre WithSecure™ Security Cloud.

Fondée en 1988, WithSecure™ est cotée au NASDAQ OMX Helsinki Ltd.

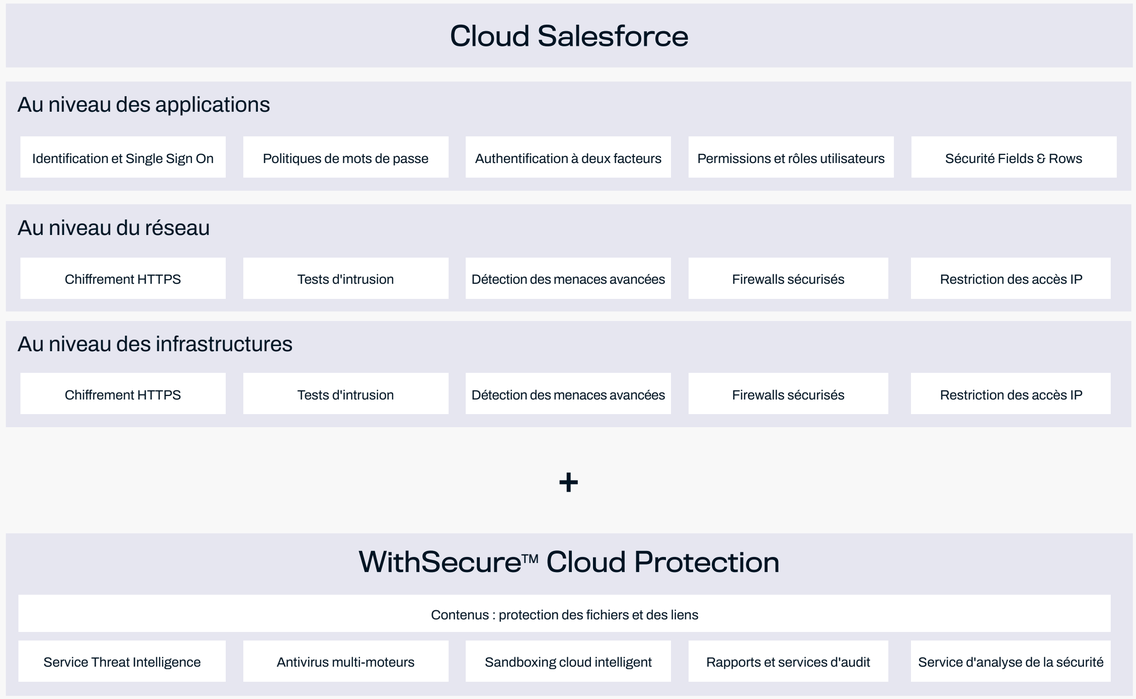
# 3. Modèle de responsabilité partagée

Les fournisseurs de services cloud et leurs clients assument généralement une responsabilité partagée en matière de sécurité dans les écosystèmes cloud.

Salesforce, par exemple, couvre divers aspects de la sécurité au niveau du système et des applications. La plateforme contrôle notamment les authentifications, les règles, les autorisations utilisateurs et les profils.

Mais il incombe aux entreprises de sécuriser les fichiers et les liens uploadés sur leur plateforme Salesforce par les utilisateurs. Pourtant, elles sont souvent dans l'incapacité de contrôler la sécurité des contenus partagés par des utilisateurs externes tels que des partenaires ou des clients.

Par ailleurs, de nombreuses entreprises fournissent un accès direct aux applications cloud via leurs firewalls et via d'autres fonctions de sécurité réseau : la protection contre les malwares, ransomwares et liens malveillants est donc souvent assurée uniquement au niveau des endpoints.




## Il est, par conséquent, nécessaire de mettre en place certaines mesures de sécurité supplémentaires pour maîtriser les risques. Les organisations doivent notamment :

- Empêcher les attaques ciblées visant les équipes du service clientèle utilisant le Service Cloud de Salesforce.
- Bloquer le partage de contenus indésirables ou malveillants comme la pornographie ou les ransomwares dans le Community Cloud. Si de tels contenus sont partagés, l'image de l'entreprise risque d'en pâtir.
- Empêcher la propagation de malwares au sein de l'entreprise par le biais de pièces jointes malveillantes partagées, par exemple, dans Sales Cloud ou Chatter.

WithSecure™ Cloud Protection for Salesforce a été spécialement conçu pour maîtriser ces risques. Cette solution complète les fonctionnalités de sécurité natives de Salesforce avec des composants de sécurité dédiés. Elle permet aux entreprises de satisfaire au modèle de responsabilité partagée utilisé dans les écosystèmes cloud.

# 4. La solution

WithSecure™ Cloud Protection for Salesforce est une solution de sécurité cloud conçue pour compléter la sécurité native des plateformes Salesforce. Elle fournit des composants de sécurité dédiés permettant de maîtriser les risques liés aux URL et fichiers partagés par les utilisateurs.

Cette solution prend en charge la plupart des clouds Salesforce, notamment : Sales Cloud, Community Cloud ou encore Service Cloud. Elle prend en charge les éditions suivantes de Salesforce : Professional, Enterprise, Unlimited et Developer.

WithSecure™ Cloud Protection for Salesforce a été conçu et développé en étroite collaboration avec Salesforce pour assurer une fiabilité maximale et une compatibilité optimale avec leurs différents clouds.

WithSecure™ Cloud Protection for Salesforce utilise une architecture cloud-to-cloud : il n'est donc pas nécessaire de déployer de middlewares comme les proxies, ni d'implémenter des configurations réseau supplémentaires. Vous bénéficiez d'un déploiement simplifié avec AppExchange.

# 4.1 Fonctionnalités

## 4.1.1 Fichiers, URL, e-mails

WithSecure™ Cloud Protection monitore en continu tous les fichiers, liens et e-mails utilisés via les plateformes Salesforce.

## 4.1.2 Le cloud Salesforce

Chaque fois qu'un utilisateur final utilise, uploade ou télécharge des contenus via Salesforce, le trafic est intercepté et soumis à un processus breveté d'analyse et de détection des menaces dans le WithSecure™ Security Cloud. Nous savons que l'expérience utilisateur constitue pour les clients une importance toute particulière : notre solution est donc conçue pour minimiser les temps de latence et compléter l'expérience intuitive et conviviale offerte par Salesforce.

## 4.1.3 Le Security Cloud de WithSecure™

WithSecure™ Security Cloud assure une analyse en plusieurs étapes, selon un processus par paliers, adapté au profil de risque du contenu. Les fichiers jugés à haut risque font l'objet d'une analyse plus approfondie avec notre technologie de Sandboxing cloud intelligent. Cette fonctionnalité est conçue pour prévenir les attaques de malwares 0-day et d'autres menaces avancées.

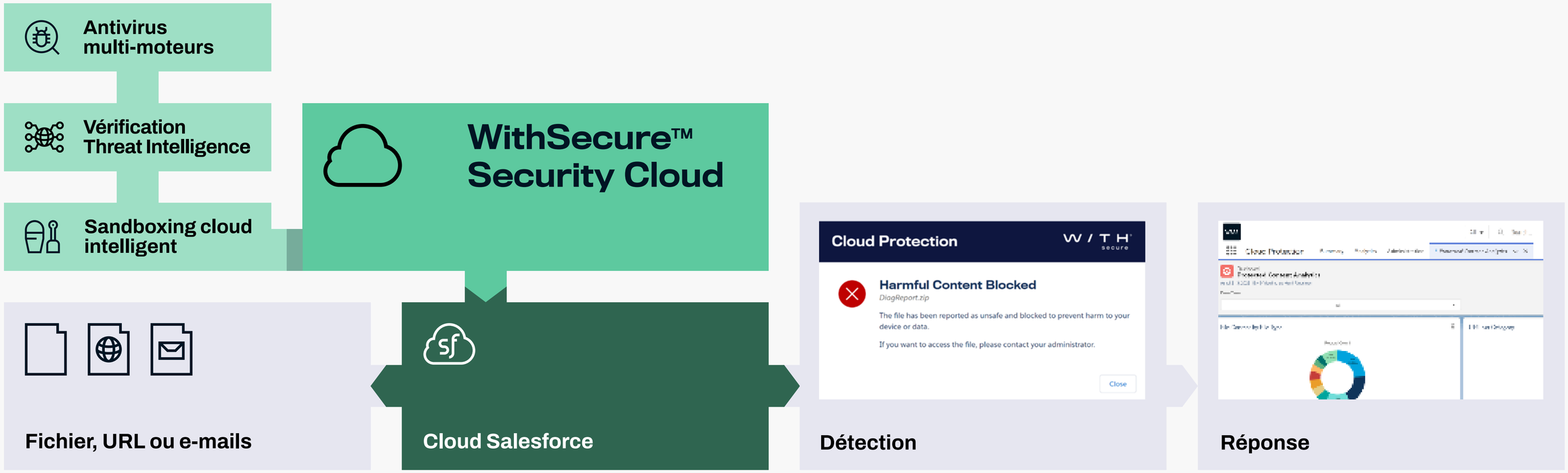
## 4.1.4 Détecter

Les contenus détectés comme étant malveillants ou bien interdits sont automatiquement supprimés ou bloqués. L'utilisateur final est informé du blocage du contenu et est conseillé sur la marche à suivre. Tout accès ultérieur au contenu est refusé. Une alerte de sécurité est envoyée à l'administrateur de la solution et à l'équipe de sécurité. Une politique de filtrage de contenus permet de bloquer les fichiers selon leur type ou extension : par exemple, l'administrateur peut choisir de bloquer tous les exécutables tels que les fichiers .com, .exe, .bin et .bat.

## 4.1.5 Répondre

Grâce aux rapports détaillés, aux analyses de sécurité avancées et aux pistes d'audit complètes, il devient facile pour les administrateurs système de réagir à une attaque se déroulant via Salesforce et d'enquêter sur des attaques provenant de source inconnue.

Voici un aperçu global de notre processus de sécurisation complémentaire des clouds Salesforce :



# 4.2 Protection des fichiers

WithSecure™ Cloud Protection utilise une plateforme de sécurité multi-niveaux propriétaire permettant de détecter et prévenir les virus, chevaux de Troie, ransomwares et autres malwares avancés. Cette solution offre une protection nettement supérieure à celle proposée par les technologies traditionnelles :

- Cette solution détecte un plus large éventail de caractéristiques, de tendances et de modèles malveillants, ce qui permet une détection plus fiable et plus précise, même pour des variants de malwares jusqu'alors inconnus.
- En exploitant les renseignements sur les menaces en temps réel recueillis auprès de dizaines de millions de clients de sécurité, elle offre une protection plus rapide et plus efficace contre les menaces nouvelles et émergentes.
- L'émulation permet de détecter les malwares qui utilisent des techniques d'obscurcissement.

Notre logique d'analyse brevetée garantit un processus transparent de détection des menaces, chaque fois que les utilisateurs uploadent ou téléchargent des fichiers.

## 4.2.1 Protection des uploads

Chaque fois qu'un utilisateur uploade un fichier vers Chatter, Salesforce Files ou Attachments, un processus d'analyse multi-niveaux débute en arrière-plan :

### Analyse initiale

Une checksum (SHA1) du fichier est calculée et stockée dans un cache de détection des menaces dans Salesforce Cloud, avec le contenu du fichier et ses métadonnées. Cette checksum est comparée à celles enregistrées dans le cache de détection des menaces existant, pour voir si le fichier a déjà été analysé auparavant. Ce fonctionnement permet de limiter les requêtes au cloud et donc d'améliorer l'expérience utilisateur. Les résultats de détection des menaces existants sont périodiquement mis à jour et les résultats expirés sont automatiquement effacés afin de garantir une protection actualisée. Si des résultats d'analyse sont disponibles dans le cache, ils sont automatiquement utilisés.

### Vérification Threat Intelligence

Si aucun résultat n'est trouvé dans le cache, une vérification Threat Intelligence est effectuée via le WithSecure™ Security Cloud en utilisant la checksum SHA-1. Le service renvoie la réputation de sécurité des fichiers, la prévalence et les éventuelles menaces détectées, pour bloquer automatiquement tout fichier malveillant. En fonction des paramètres spécifiés, le système peut remplacer les fichiers malveillants par un fichier .txt expliquant pourquoi le fichier original a été supprimé, ou bloque simplement tout accès ultérieur au fichier malveillant.

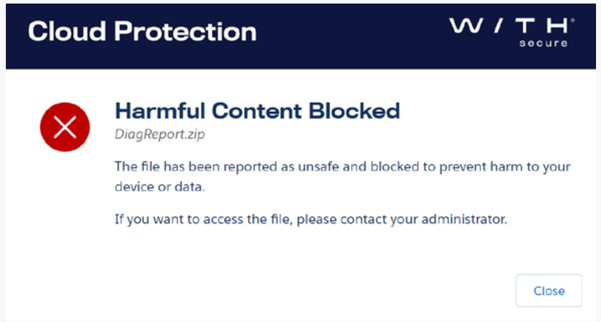
### Anti-malware multi-moteurs

Si la réputation du fichier est inconnue, son contenu est uploadé vers le WithSecure™ Security Cloud pour une analyse plus approfondie des menaces. Le fichier est alors soumis à plusieurs moteurs anti-malware complémentaires afin de détecter les malwares, les exploits 0-day et les modèles de menaces avancées. À ce stade, le processus d'analyse utilise l'ensemble des données et renseignements sur les menaces collectés par WithSecure™ Labs.

### Filtrage des contenus

Avant d'effectuer une analyse des menaces, l'appli Cloud Protection vérifie le fichier par rapport à la liste des extensions ou types de fichiers interdits dans les paramètres. S'il s'agit effectivement d'une extension ou d'un type de fichier non-autorisé, le fichier est bloqué. Une alerte de sécurité peut être envoyée à l'administrateur en fonction des paramètres de notification spécifiés.

Avec le filtrage des contenus, l'entreprise peut empêcher les utilisateurs d'uploader des contenus inappropriés ou dangereux. Par exemple, pour minimiser le risque de propagation des malwares, Cloud Protection peut être configuré pour bloquer tout exécutable (tel que EXE, COM) ou script (tel que VBS, PS1) uploadé vers Salesforce Cloud.




### Sandboxing cloud intelligent

Le système utilise des techniques de machine learning affinées pour décider s'il faut envoyer le fichier dans notre Smart Cloud Sandbox pour analyse approfondie. Si le fichier présente des indicateurs de risque, il y est effectivement envoyé et est exécuté dans plusieurs environnements virtuels pour analyser son comportement. En concentrant l'analyse sur le comportement malveillant du fichier plutôt que sur les identifiants statiques, le sandboxing cloud intelligent permet d'identifier et de bloquer les malwares et les exploits les plus sophistiqués ou 0-day.

### Résultats d'analyse

En fonction du verdict final, le fichier uploadé est classé comme étant soit nuisible, soit sans danger. Selon les paramètres spécifiés, le fichier est supprimé s'il est nuisible/suspect ; et l'expéditeur du fichier et les administrateurs sont informés de l'incident. À l'inverse, si aucune menace n'est détectée, le fichier est accessible à l'emplacement où il a été uploadé, et un événement de détection est enregistré dans le log d'analyse pour mener, en cas de besoin, une analyse et un audit. Le verdict final, la réputation du fichier et les autres détails de l'analyse des menaces sont stockés dans le cache de détection des menaces pour une utilisation ultérieure. Les données de détection des fichiers malveillants sont envoyées au service de Threat Intelligence de WithSecure, pour que, lors de la prochaine requête, les menaces déjà rencontrées puissent être identifiées et bloquées directement.

## 4.2.2 Protection des téléchargements

La protection des téléchargements permet de veiller à ce que les utilisateurs ne puissent pas télécharger de contenus nuisibles ou non-autorisés à partir de Chatter, de fichiers Salesforce ou de pièces jointes. WithSecure™ Cloud Protection passe par le même processus que celui décrit pour les uploads. Si le verdict du fichier est déjà disponible dans le cache de détection des menaces, le fichier est autorisé ou bloqué en conséquence. Dans le cas contraire, le processus d'analyse est enclenché. Si le fichier est sûr, l'utilisateur peut le télécharger sans difficulté. S'il est détecté comme nuisible ou interdit, l'application bloque l'accès de l'utilisateur au fichier et, selon les paramètres spécifiés, envoie une alerte à l'administrateur. Les vérifications pour l'upload et le téléchargement sont toutes deux essentielles pour veiller à ce que les renseignements de sécurité les plus récents soient toujours utilisés. Les malwares qui auraient pu contourner le processus finissent pas être repérés lorsque de nouvelles données sont disponibles.

## 4.2.3 Analyses manuelles

L'analyse manuelle peut être utilisée pour analyser les fichiers et pièces jointes Salesforce qui ont été ajoutés à Salesforce Cloud avant l'installation de WithSecure™ Cloud Protection ou qui ont été exclus de l'analyse. Une analyse programmée peut, par ailleurs, être définie pour analyser l'ensemble du système à intervalles réguliers. Les analyses sont exécutées en arrière-plan, sans interférence avec l'expérience utilisateur ou les performances.

# 4.3 Protection des URL

La protection des URL est une fonction de sécurité essentielle. Elle empêche les utilisateurs de Salesforce d'accéder à des contenus malveillants ou indésirables via des liens web ajoutés aux messages et commentaires Chatter, aux descriptions et commentaires Case, ainsi qu'au corps des messages reçus via la fonction Email-To-Case.

Cette fonction proactive constitue un composant de sécurité particulièrement efficace : l'intervention précoce réduit considérablement l'exposition globale aux contenus malveillants, et donc aux attaques. La protection des URL empêche notamment les utilisateurs de cliquer sur des sites de phishing apparemment légitimes, sur des sites malveillants, ou sur des contenus inappropriés tels que des sites pour adultes ou des sites de jeux d'argent.

Cette fonctionnalité a été conçue pour traiter efficacement les milliards de sites web présents sur internet dont le statut de sécurité évolue constamment. Elle repose sur des requêtes de recherche en temps réel sur le Security Cloud de WithSecure. Toutes ces requêtes passent par plusieurs couches d'anonymisation pour garantir le plus haut degré de confidentialité.

La requête récupère la réputation la plus récente pour les sites web et leurs fichiers. Cette réputation se base sur plusieurs éléments : les adresses IP, les mots-clés des URL, les modèles de sites, les métadonnées extraites des sites web comme les iframes et les types de fichiers, et le comportement des sites web comme les tentatives d'exploitation, les redirections ou les scripts malveillants.

## 4.3.1 Contrôle de sécurité des URL

Notre solution intercepte les URL que les utilisateurs publient sur Chatter et celles intégrées au corps d'un e-mail (Email-to-Case), puis les remplace par des liens de redirection spéciaux. Le lien original est inclus entre parenthèses à des fins de reconnaissance, mais l'utilisateur ne peut pas cliquer dessus. Toute copie est évitée via obscurcissement de l'URL.

Si le lien est jugé malveillant sur la base des informations obtenues à partir de la requête, l'accès au site web est bloqué avant le chargement de tout contenu, et l'utilisateur final reçoit un avertissement.

Lorsque l'utilisateur clique sur le lien de redirection, WithSecure™ Cloud Protection envoie l'URL d'origine au WithSecure™ Security Cloud pour une vérification Threat intelligence. En fonction des renseignements sur les menaces obtenus concernant l'URL, l'accès est soit autorisé, soit bloqué.

## 4.3.2 Classification URL

La classification des URL permet aux administrateurs de contrôler les pages web auxquelles les utilisateurs de Salesforce peuvent accéder. Ils peuvent, par exemple, refuser l'accès à des sites non liés aux processus de travail, comme les réseaux sociaux, pour éviter les pertes de temps. Les sites appartenant à des catégories à haut risque, comme les sites pour adultes ou les sites de jeux d'argent, peuvent être bloqués pour éviter les malwares et empêcher la consultation de contenus inappropriés.

Les administrateurs de la solution peuvent appliquer des règles d'utilisation dans 28 catégories différentes, dont les suivantes : Avortement, Services publicitaires, Adultes, Alcool et tabac, Anonymiseurs, Enchères, Banque, Blogs, Chat, Rencontres, Drogues, Divertissement, Jeux, Piratage, Haine, Recherche d'emploi, Service de paiement, Escroquerie, Shopping, Réseaux sociaux, Téléchargement de logiciels.

# 4.4 Protection des e-mails

L'Email-to-Case de Salesforce crée automatiquement des "cases" et remplit automatiquement les champs lorsque les clients envoient des messages à des adresses e-mails. WithSecure™ Cloud Protection intercepte les e-mails entrants et lance la détection des menaces pour toutes les pièces jointes et URL. Lorsque le verdict d'un fichier malveillant est déjà connu et que le Time-To-Live (TTL) de la détection des menaces est encore valide, le fichier est supprimé et/ou les administrateurs sont informés de l'incident. Toutes les URL sont réécrites.

Si le fichier est nouveau ou si le TTL a expiré, WithSecure™ Cloud Protection lance le même processus de détection des menaces que celui utilisé pour la sécurisation des uploads. Voir la section 4.2 Protection des fichiers.

Lorsqu'un utilisateur clique sur une URL, WithSecure™ Cloud Protection lance le même processus de détection des menaces que celui utilisé dans la vérification de la sécurité des URL. Voir la section 4.3 Protection des URL.

# 4.5 Gestion

Grâce aux rapports détaillés, aux alertes flexibles, aux analyses de sécurité avancées et aux pistes d'audit complètes, les administrateurs système peuvent répondre efficacement aux menaces. La visibilité totale à 360 degrés vous permet de connaître les schémas d'utilisation de Salesforce. Grâce à ces fonctionnalités, vous pouvez répondre à une attaque menée via Salesforce, enquêter sur une attaque provenant d'une source inconnue ou encore vérifier si Salesforce est impliquée dans un incident.

## 4.5.1 Analyses

WithSecure™ Cloud Protection offre une visibilité à 360 degrés sur les contenus de Salesforce. Toutes les actions d'upload et de téléchargement de fichiers, ainsi que les clics d'URL, sont stockés dans un log d'analyse.

Grâce à l'historique, les administrateurs peuvent identifier tous les utilisateurs ayant accédé à un contenu Salesforce. De nombreux départements informatiques ignorent quels types de contenus leur entreprise stocke dans Salesforce. Une telle visibilité peut pourtant s'avérer utile : elle permet de repérer des fichiers exécutables qui ne devraient pas y être stockés.

Mieux comprendre les besoins des clients internes et les cas d'utilisation permet par ailleurs de gagner en efficacité. Enfin, grâce à une puissante fonctionnalité de recherche, les administrateurs peuvent enquêter sur les attaques de contenus en quelques secondes, pour :

- Confirmer ou exclure Salesforce comme vecteur d'attaque
- Obtenir des informations sur l'auteur d'une attaque, comme l'adresse IP
- Identifier les utilisateurs ayant accédé au contenu malveillant.

Le log analytique comprend les informations suivantes :

- Horodateur
- Action
- Verdict + Prévalence du fichier
- Raison
- Direction
- (Upload/Download/Post/Clic)
- Nom d'utilisateur
- Nom de fichier
- Type de fichier
- Version du fichier
- Taille du fichier
- URL
- Catégorie d'URL
- Emplacement (du fichier/de l'URL)
- Checksum SHA-1 du fichier
- Adresse IP

## 4.5.1 Alertes

Toutes les alertes de sécurité et tous les événements d'audit sont écrits dans le log des alertes de sécurité. Les administrateurs Salesforce peuvent permettre aux administrateurs de Cloud Protection et au personnel de sécurité informatique de recevoir des alertes dans les cas suivants :

- Contenu dangereux détecté
- Contenu dangereux bloqué lors de l'upload (alerte envoyée à l'uploadeur s'il s'agit d'un utilisateur interne)
- URL malveillante détectée
- URL malveillante détectée lors de l'upload (alerte envoyée à l'uploadeur s'il s'agit d'un utilisateur interne)
- URL non-autorisée détectée (alerte envoyée à l'uploadeur s'il s'agit d'un utilisateur interne)
- Si les résultats de l'analyse d'un fichier ou d'une URL sont passés de sûrs à dangereux
- Type de fichier non-autorisé détecté
- Type de fichier non-autorisé détecté lors de l'upload (alerte envoyée à l'uploadeur s'il s'agit d'un utilisateur interne)

## 4.5.3 Rapports

WithSecure™ Cloud Protection offre une visibilité accrue sur vos contenus Salesforce :

### Tableau de bord général :

- Upload des fichiers protégés + tendances
- Téléchargement des fichiers protégés + tendances
- Publication des URL protégées + tendances
- Clics sur des URL protégées + tendances
- Événements Threat Intelligence + tendances
- Utilisateurs protégés + tendances

### Analyse des contenus protégés - Tableau de bord :

- Utilisateurs protégés
- Utilisateurs actifs de la Protection des fichiers
- Utilisateurs actifs de la Protection des URL
- Uploads de fichiers
- Téléchargements de fichiers
- Événements relatifs aux fichiers, par utilisateur
- Contenu des fichiers, par emplacement
- Contenu des fichiers, par type de fichier
- Événements liés aux renseignements sur les menaces
- Publications d'URL
- Clics d'URL
- Événements URL, par utilisateur
- URL par emplacement
- URL par catégorie

### Protection des fichiers - Tableau de bord :

- Alertes de sécurité des fichiers, par degré de gravité
- Fichiers malveillants utilisés
- Fichiers malveillants utilisés, par emplacement
- Fichiers malveillants utilisés, par type de fichier
- Fichiers malveillants utilisés, par utilisateur
- Principaux fichiers malveillants (infections)

### Protection des URL - Tableau de bord :

- Alertes de protection des URL, par degré de gravité
- URL malveillantes utilisées
- URL malveillantes utilisées, par emplacement
- URL malveillantes utilisées, par utilisateur
- Principales catégories d'URL

WithSecure™ Cloud Protection prend également en charge les rapports personnalisés via Salesforce Reports.

### Les attributs suivants sont proposés pour les rapports sur la protection des fichiers :

- **Créé par :** Nom complet, Date de création, Date/Heure, Extension de fichier, Nom du fichier, ID d'analyse du fichier, Taille du fichier, Type de fichier, Adresse IP
- **Dernière modification par :** Nom complet, Date de dernière modification, Nom
- **Propriétaire** : Nom complet, ID d'enregistrement, Type d'analyse, SHA1, Emplacement
- **Utilisateur :** Nom complet, Verdict, Propriétaire (Prénom, Nom de famille), ID du propriétaire, Téléphone
- **Profil :** Nom
- **Règle :** Nom, Titre, Nom d'utilisateur, Email, Alias, Actif), Raison, Prévalence du fichier, Evaluation de la réputation du fichier.

### Les attributs suivants sont proposés dans les rapports sur la protection des URL :

Analyse URL : ID, Analyse URL : Nom, Action, Catégories, Date/Heure, Direction, Adresse IP, Emplacement, Raison, Réputation, Description de la réputation, URL, Utilisateur, Verdict, Nom du propriétaire, Alias du propriétaire, Rôle du propriétaire, Créé par, Alias du créateur, Date de création, Dernière modification par, Alias de la dernière modification, Date de la dernière modification.

## 4.5.4 Administration

L'administrateur de la solution peut activer ou désactiver les fonctionnalités de protection en fonction des politiques de sécurité de l'entreprise. Par exemple, si des exigences strictes en matière de conformité ou de confidentialité empêchent l'upload de fichiers vers le cloud pour analyse, les paramètres peuvent être modifiés.

## 4.5.5 Déploiement

WithSecure™ Cloud Protection combine une application native Salesforce et le WithSecure™ Security Cloud. Ce dernier fournit des services de réputation et de sécurité utilisés dans d'autres produits WithSecure™ et produits tiers. La solution est installée sur la plateforme Salesforce et protège tous les clouds Salesforce que votre entreprise utilise comme Sales, Service ou Community Cloud. Aucun autre changement de logiciel ou de configuration réseau n'est nécessaire.

## 4.5.6 Personnalisation

WithSecure™ Cloud Protection permet aux administrateurs de Salesforce de personnaliser tous les messages destinés aux utilisateurs finaux. Il est possible d'utiliser une bannière personnalisée dans les pages d'analyse et de personnaliser les messages suivants :

- Contenu dangereux détecté (alerte pour les administrateurs)
- Contenu dangereux détecté lors de l'upload (Alerte pour les utilisateurs internes)
- Le fichier malveillant est remplacé par un fichier texte (Contenu du fichier)
- URL malveillante détectée (Alerte pour les administrateurs)
- URL malveillante détectée lors de l'upload (Alerte pour les utilisateurs internes)
- URL non-autorisée détectée (Alerte pour les administrateurs)
- URL non-autorisée détectée lors de l'upload (Alerte pour les utilisateurs internes)
- Si le résultat de l'analyse d'un fichier ou d'une URL passe de sûr à dangereux (Alerte pour les administrateurs)
- Contenu non-autorisé détecté (Alerte pour les administrateurs)
- Contenu non-autorisé détecté lors de l'upload (Alerte pour les utilisateurs internes)

# 5. WithSecure™ Security Cloud

WithSecure™ Security Cloud est un système cloud d'analyse des menaces numériques exploité par WithSecure™. Il abrite une base de données des menaces numériques alimentée en permanence par les systèmes clients et les services d'analyse automatisée des menaces. L'infrastructure du Security Cloud est hébergée sur des serveurs situés dans plusieurs data-centers Amazon Web Services, à travers le monde. Security Cloud reçoit plus de 8 milliards de requêtes chaque jour.

Nous ne collectons que le minimum de données clients nécessaires pour fournir nos services. Chaque bit transféré se justifie du point de vue de la prévention des menaces, et les données ne sont jamais collectées pour des besoins futurs hypothétiques. Avec les paramètres par défaut, Security Cloud ne collecte ni adresse IP, ni fichier, ni autre information privée. Les clients peuvent donner à WithSecure™ la permission de stocker des fichiers exécutables suspects et/ou des fichiers non-exécutables suspects.

Grâce aux métadonnées, aux bases de données internes et à diverses autres sources, les systèmes d'analyse automatisés peuvent fournir une évaluation complète et actualisée, pour bloquer immédiatement les menaces déjà identifiées par tout autre service ou appareil connecté au Security Cloud.

Security Cloud permet également aux analystes de WithSecure™ Response Labs d'intégrer leur point de vue humain à la plateforme, pour compléter les systèmes automatisés et la technologie d'analyse onhost. En plus de créer et d'adapter les règles qui sous-tendent les bases de données et les systèmes d'analyse automatisés, ils monitorent activement les menaces récentes et recherchent les caractéristiques et schémas de comportement malveillants, pour trouver les moyens les plus efficaces d'identifier les malwares.

**Le tableau suivant présente en détail nos principes de confidentialité :**

| | |
|---|---|
| **Minimiser l'envoi de données techniques** | WithSecure™ Security Cloud emploie une analyse de contenu multi-étapes. Les données des fichiers ne sont pas envoyées à Security Cloud, sauf si cela est nécessaire pour assurer une protection efficace et si le client l'a autorisé. |
| **Ne pas envoyer de données personnelles** | Aucune information sur les utilisateurs qui publient ou accèdent aux Fichiers/URL analysés n'est envoyée à WithSecure™ Security Cloud. L'emplacement de ces utilisateurs n'est pas non plus communiqué. |
| **Ne pas faire confiance au réseau** | Toutes les métadonnées, tous les fichiers et tous les autres contenus sont transférés vers Security Cloud de manière sécurisée, soit par HTTPS, soit par HTTP chiffré et signé séparément. |

### Les principes du Security Cloud :

| | |
|---|---|
| **Sécurité dès la conception** | La sécurité ne peut pas être ajoutée après coup. Un système n'est sûr s'il n'a pas été conçu d'emblée pour être sécurisé. Le Security Cloud et ses systèmes connexes ont été conçus en gardant toujours ce principe à l'esprit. |
| **Trafic réseau chiffré** | Les données ne sont jamais transférées en clair sur internet. Le chiffrement est utilisé pour assurer l'intégrité des divers objets. WithSecure™ utilise des bibliothèques et protocoles cryptographiques largement disponibles ainsi que du code cryptographique personnalisé. |
| **Environnements de malwares cloisonnés** | Nous possédons plus de 20 ans d'expérience dans le stockage et le test de malwares. Toutes les manipulations de malwares sont effectuées dans des réseaux séparés d'internet et des autres réseaux WithSecure™. Les réseaux de stockage et de test sont isolés les uns des autres, et les fichiers sont transférés à l'aide de méthodes strictement contrôlées. |
| **Monitoring professionnel** | Tous les systèmes critiques de Security Cloud sont monitorés par le personnel de WithSecure™. Tous les systèmes stockant ou testant des malwares sont hébergés par l'entreprise WithSecure™. |
| **Accès contrôlés** | Seul un nombre limité d'employés WithSecure™ a accès aux systèmes critiques du Security Cloud. Cet accès est accordé et révoqué selon un processus documenté et contrôlé. |
| **Ouverture d'esprit** | Dans le domaine de la sécurité, il est capital d'adopter un état d'esprit empreint d'ouverture et d'humilité. Nous avons déployé d'importantes ressources pour sécuriser notre Security Cloud, mais un tel travail n'est jamais terminé. Un système sécurisé ne peut le rester que si ses concepteurs restent toujours prêts à analyser et à corriger les problèmes lorsque ceux-ci sont signalés. Cette approche d'ouverture implique également de rendre des comptes au public si un incident met en péril la sécurité des clients. |

Pour en savoir plus sur WithSecure™ Security Cloud, consultez notre livre blanc Security Cloud et notre politique de confidentialité Security Cloud.

## 5.1 Service Threat Intelligence

En exploitant les renseignements sur les menaces en temps réel recueillis à partir de dizaines de millions de sondes, nous pouvons identifier les menaces nouvelles et émergentes dans les minutes qui suivent leur apparition. Ce fonctionnement permet de garantir une sécurité exceptionnelle contre les cybermenaces en constante évolution. Le service Threat Intelligence permet à WithSecure™ Cloud Protection d'interroger la réputation des objets comme les fichiers et les URL. Les fichiers sont vérifiés en calculant leur hachage cryptographique SHA-1 et en l'envoyant à notre service de réputation.

## 5.2 Antivirus multi-moteurs

L'antivirus multi-moteurs utilise plusieurs niveaux de sécurité pour détecter les exploits et les malwares inconnus utilisés dans les attaques ciblées. Le système combine analyse comportementale, détection heuristique et machine learning pour identifier les malwares spécifiques, les familles de malwares présentant des caractéristiques communes, mais aussi les attributs et comportements malveillants. Suite à cette analyse, un fichier peut être marqué comme suspect : il est alors envoyé vers la Smart Cloud Sandbox pour un traitement plus poussé.

## 5.3 Sandboxing cloud intelligent

Notre Smart Cloud Sandbox exécute les fichiers suspects dans plusieurs environnements virtuels et analyse leur comportement. Si le comportement d'un fichier est jugé suspect, l'information est envoyée à l'antivirus multi-moteurs et au service Threat Intelligence, pour que lors de la prochaine requête de détection, la menace soit directement bloquée.

# Qui sommes-nous ?

WithSecure™ est le partenaire européen de référence en matière de cybersécurité depuis plus de 30 ans. Nous accompagnons les fournisseurs de services informatiques, les MSSP et des multinationales, qui nous font confiance, à travers des modèles commerciaux flexibles et adaptés au marché. Nous leur fournissons une cybersécurité axée sur les résultats, pour les protéger en toutes circonstances et garantir le bon fonctionnement de leurs activités. Notre protection basée sur l'IA sécurise les endpoints et protège les environnement cloud. Nos outils intelligents de détection et de réponse sont pilotés par des experts qui identifient les risques, assurent une recherche proactive des menaces et neutralisent les attaques en temps réel. Un service de consulting expert est également disponible pour les entreprises qui souhaitent renforcer leur résilience.

WithSecure™, anciennement F-Secure Corporation, a été fondée en 1988 et est cotée au NASDAQ OMX Helsinki Ltd.

W / T H™
secure