Kitewcrks

Protéger les données sensibles gérées par le service client

5 mesures pour protéger les données personnelles gérées par le service client

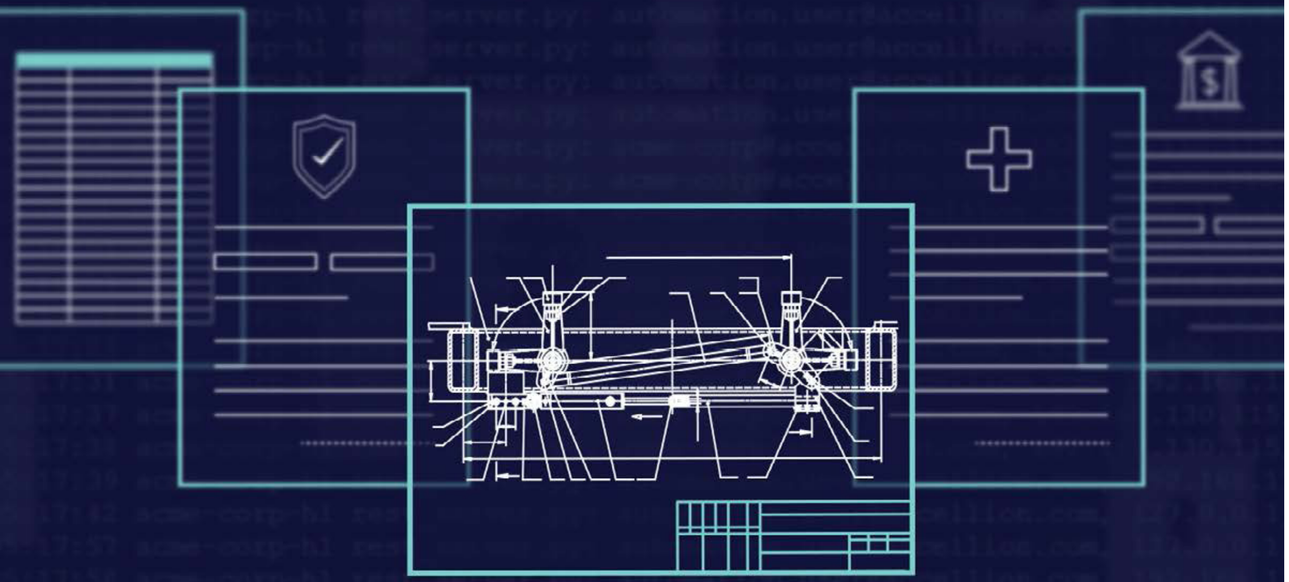
Introduction

Les agents du service client sont obligés d'agir vite pour offrir la meilleure expérience client possible et ainsi limiter les résiliations. Elles tournent parfois en 24/24, tels des pompiers, pour résoudre un cas complexe ou traiter individuellement de nombreux petits dossiers sur la journée.

Pour leurs dirigeants, il est impératif de protéger l'entreprise et ses clients contre les failles de sécurité, les amendes pour non-conformité, ou les atteintes à la réputation. Le tout en assurant une expérience client fluide et efficace.

Dans ce contexte, les données personnelles des clients sont très exposées aux risques de violation. En effet, ces derniers sont amenés à partager des informations personnelles identifiables (PII), des informations médicales protégées (PHI) ou encore leurs données bancaires. Votre RSSI est-il attentif à la manière dont vos agents reçoivent et stockent les informations clients ? Les agents connaissent-ils et respectent-ils vos politiques de confidentialité, même en condition de stress ? Êtes-vous en mesure de le prouver à un auditeur ?

Les organisations les plus performantes sont celles qui garantissent la conformité de leurs activités tout en assurant une expérience client et salariée exceptionnelle. Voici cinq bonnes pratiques pour intégrer les données personnelles de vos clients dans vos politiques de gouvernance, directement là où opèrent vos équipes d'assistance : dans leurs dossiers Salesforce®.



01 Prévenez les risques de non-conformité

Traitez les données clients comme des données confidentielles

Chaque secteur d'activité est amené à manipuler des PHI, des PII, ou des données bancaires de leurs clients. Ce qui implique de respecter les réglementations HIPAA, RGPD et bien d'autres. Vous vous exposez à des atteintes à la vie privée chaque fois qu'un client transmet un document à votre service client.

- Santé et protection sociale : résultats d'examens, demandes de remboursement, dossiers médicaux des patients
- Industrie et ingénierie : conception assistée par ordinateur (CAO), plannings de production, plans budgétaires
- Finance : avis d'imposition, relevés bancaires, affidavits, lettres de recouvrement
- Gouvernement : déclarations fiscales, preuves judiciaires, immatriculations de sociétés, données de santé
- Technologie : journaux, captures d'écran, projets, architectures

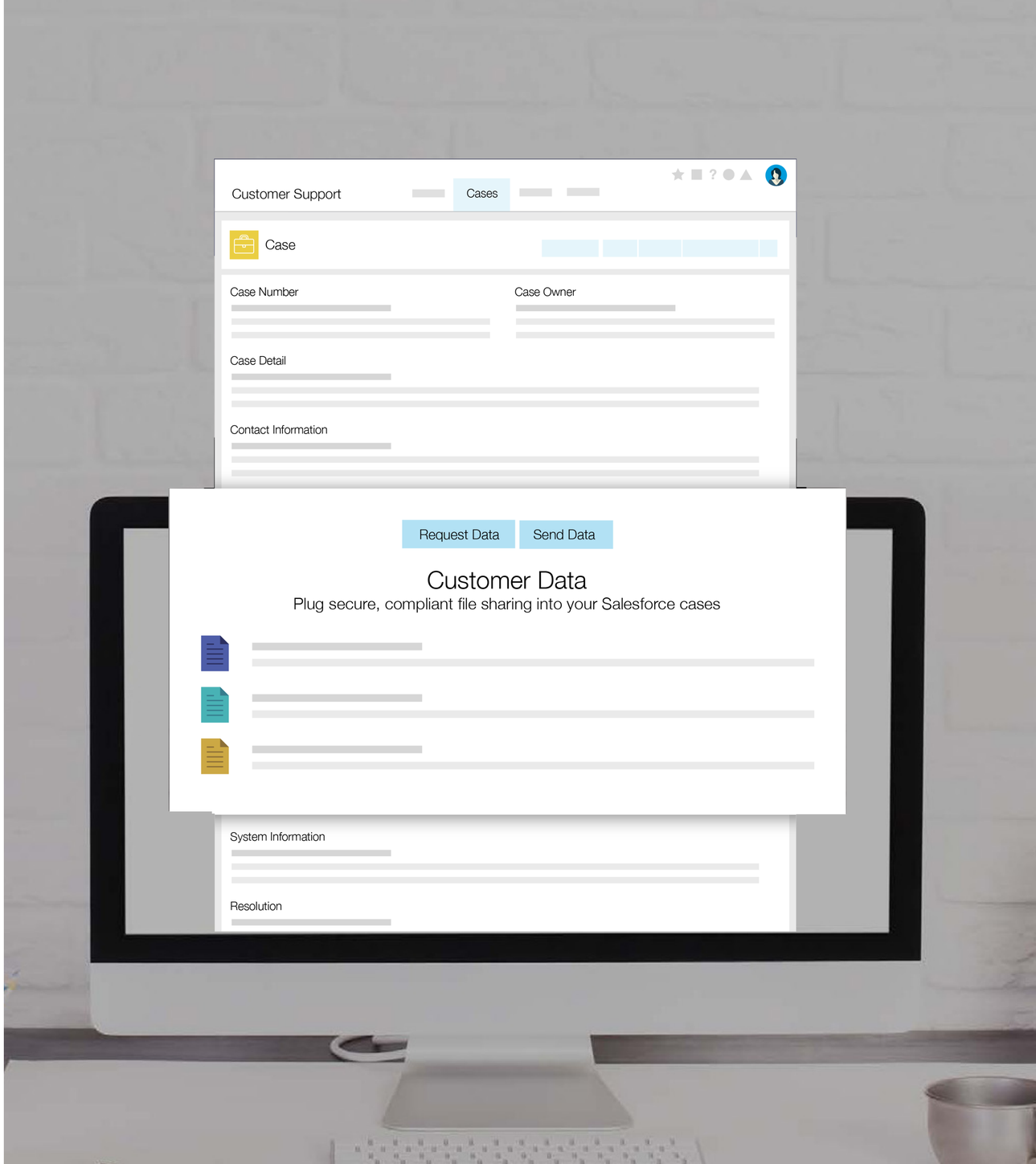
Votre service client doit traiter les données des clients en respectant les lois sur la confidentialité des données, sans pour autant perdre du temps. Respectez tous les critères de conformité en automatisant les procédures de gouvernance, et en vous appuyant sur un système de sécurité qui verrouille vos logiciels de partage de données.

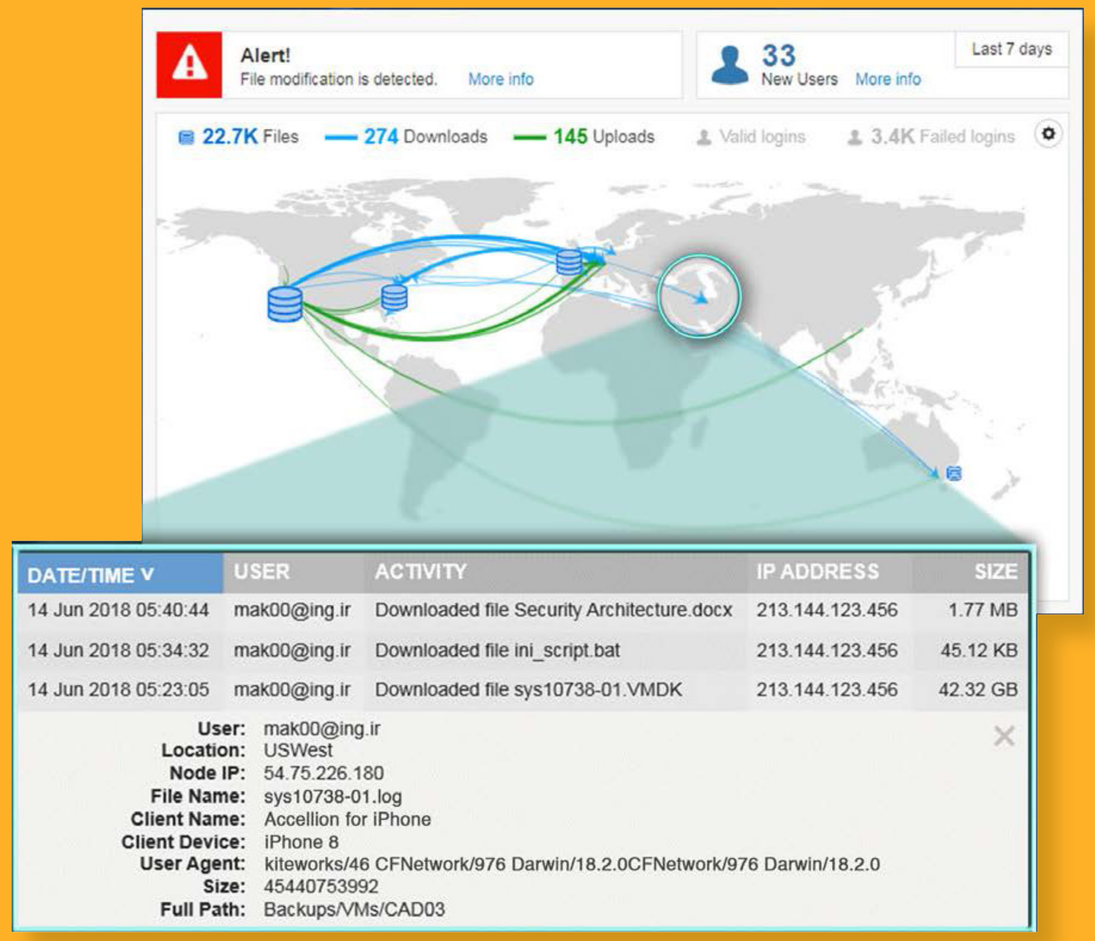
02 Une vision à 360°

Intégrez les informations de chaque client dans un dossier

Les agents ont une visibilité complète et immédiate de chaque dossier client dans la solution Salesforce, qui leur permet de personnaliser la réponse au client.

Par contre, si vous travaillez avec un portail traditionnel ou sur un système de partage de fichiers dans le cloud, les données de vos clients vont se retrouver dans un silo isolé. À la place, fournissez un plugin Salesforce case à vos équipes pour récupérer les fichiers clients. Laissez le plugin rattacher automatiquement les données au dossier correspondant et attribuer les droits d'accès appropriés.





03 Prévenir les violations de données

Garantir la visibilité de tous les dossiers traités par le service client

Se prémunir contre les menaces de sécurité et les risques de non-conformité de vos procédures d'assistance n'est pas chose facile. Il vous faut pouvoir retrouver facilement chaque fichier entrant et sortant des dossiers Salesforce. Et parmi cette montagne de données, les équipes en charge de la sécurité, de la conformité et du service client doivent être en mesure de localiser rapidement d'éventuelles anomalies.

Commencez par mettre en place une traçabilité de tous les transferts de données entre les clients et votre service client. Une fois recueillies, ces métadonnées vous permettront d'avoir en temps réel des informations claires et détaillées sur la sécurité des données du service client. D'où viennent-elles ? Où vont-elles ? Qui les envoie ? À qui sont-elles transmises ? Sont-elles confidentielles ?

04 Supprimez les solutions alternatives

Proposer des outils simples que les usagers auront envie d’utiliser

Les équipes du service client sont prêtes à tout pour régler le problème d’un client. Vos employés n’hésiteront pas à passer par un outil de partage de fichiers grand public pour déjouer les obstacles de votre outil de transfert de données, ou même à envoyer des e-mails non chiffrés. Et alors là, que répondrez-vous aux auditeurs qui demanderont : quelles données personnelles stockez-vous ? Sont-elles chiffrées ? Qui les a interceptées ?

Évitez d’en arriver là, en permettant à vos collaborateurs d’envoyer et de recevoir des fichiers clients très facilement depuis leur interface Salesforce case. Dotez-vous d’une solution capable de prendre en charge n’importe quelle taille de fichiers et d’analyser leur fiabilité, même quand le réseau de vos clients ne le permet pas. Et gardez en tête que vos clients, eux, ne sont pas formés : accompagnez-les jusqu’à la fin du processus de chargement et de téléchargement pour éviter les erreurs.

Face à la menace constante des cyberattaques et aux règles de confidentialité, les RSSI imposent des politiques de stockage de données de plus en plus strictes, obligeant les opérateurs à stocker les dossiers dans des partages de fichiers Windows ou des dossiers SharePoint.

05 Réduire les coûts et garantir la conformité règlementaire

Contrôlez les emplacements de stockage des données

Face à la menace constante des cyberattaques et aux règles de confidentialité, les RSSI imposent des politiques de stockage de données de plus en plus strictes, obligeant les opérateurs à stocker les dossiers dans des partages de fichiers Windows ou des dossiers SharePoint. Cela vous permet de maitriser les coûts. Cependant, cela représente des étapes supplémentaires pour les employés, et donc dégrade l'expérience client et alourdit les procédures de conformité manuelles. À la place, laissez-les gérer les données directement dans les dossiers Salesforce à l'aide d'un plugin connecté au stockage, que vous contrôlerez sur site, dans un cloud privé, ou dans un environnement autorisé par FedRAMP. Ainsi, vous maitrisez vos coûts tout en respectant la conformité règlementaire.

Réseau de contenu privé compatible avec Kiteworks

- Stockage sécurisé
- Traçabilité intégrée
- Tableau de bord RSSI
- Rapports de conformité
- Politiques basées sur les rôles utilisateurs

salesforce appexchange partner

Kiteworks

www.kiteworks.com

Juillet 2022

 Kiteworks s'est donné une mission : aider les organisations à gérer efficacement les risques liés à l'envoi, à la réception, au partage et au stockage d'informations confidentielles. Avec la plateforme Kiteworks, nos clients disposent d'un réseau dédié à leurs contenus privés qui assure à la fois gouvernance, conformité et protection des données. La plateforme unifie, suit, contrôle et sécurise les partages des contenus sensibles, à l'intérieur de l'organisation, mais aussi avec l'extérieur.
Ce faisant, elle améliore considérablement la gestion du risque et assure la conformité réglementaire de toutes les communications d'informations sensibles.