LIVRE BLANC SUR LA SÉCURITÉ

Sécurité des services de stockage dans le Cloud dans PaperCut MF

par PaperCut Software – Mars 2020

Le risque zéro n'existe pas **4**

L'importance de l'emplacement **5**

Coût 5

Sécurité 6

Évolutivité 7

Fiabilité 7

Accessibilité 7

Intérêt d'une approche multicouche **7**

Couche physique 8

Couche administrative 8

Couche technologique 9

Service Cloud de PaperCut MF **10**

Traitement des documents 10

Trajet des documents 11

Actions depuis l'appareil multifonction 11

Serveur d'applications PaperCut MF 11

Service Cloud de PaperCut 12

Stockage crypté 12

Livraison au fournisseur de services de stockage dans le Cloud 12

Conservation des données 13

Autorisation utilisateur 13

Actions depuis l'appareil multifonction 13

Serveur d'applications PaperCut MF 14

Service Cloud de PaperCut 14

Utilisateur non autorisé 14

OAuth 14

Utilisateur autorisé 15

Prêt à partir 15

Arrivée à destination 15

Réponses aux questions fréquemment posées **16**

Processus opérationnels 16

Développement des logiciels 16

Détection des vulnérabilités 16

Processus et procédures 17

Conclusion **17**

Glossaire **18**

Auteurs 20

Contributeurs 20

Siège PaperCut 20

Un environnement de Cloud pensé pour optimiser la sécurité

La protection des données stratégiques ne date pas d'hier.

En 1586, un noble anglais, Anthony Babington, correspondait secrètement par écrit avec Marie Stuart, reine d'Écosse, alors qu'elle était derrière les barreaux. L'essentiel des communications portait sur un complot visant à assassiner la reine Elizabeth et à installer Mary sur le trône d'Angleterre. Les faits de trahison étant sévèrement punis à l'époque, Babington avait recours à différentes techniques pour garder le plus grand secret sur sa correspondance.

Dans le cyberespace d'aujourd'hui, cela s'apparenterait à une sécurité multicouche. Il prenait soin de coder ses messages, puis il les dissimulait dans les bouchons de fûts de bière et les faisait parvenir à la reine par différents intermédiaires de confiance. Malheureusement pour Babington, le code utilisé n'était pas suffisamment sophistiqué et son réseau de complices fut aussi démasqué. Son stratagème ne dura que quelques mois et Babington paya le prix fort pour son imprudence.

L'aspect sécuritaire est au cœur de tout ce que nous concevons à PaperCut et revêt différents aspects. Pour en savoir plus sur la sécurisation de votre système d'impression, nous vous invitons à consulter le livre blanc Securing your Print System (disponible en anglais).

Le risque zéro n'existe pas

La protection des biens ou actifs précieux comporte toujours une part de risque. Tout l'intérêt d'un système de sécurité efficace est justement de réduire cette part de risque à un niveau acceptable, tout en veillant à préserver les objectifs de l'entreprise et à contenir les coûts. Il est donc essentiel de toujours prendre en compte ces trois paramètres : risques, objectifs et coûts.

Dans l'absolu, on pourrait imaginer un système de sécurité sans faille (ou « zéro risque »), en faisant en sorte que personne ne puisse accéder aux données, quitte à ce que cela fasse grimper la facture et nuise aux objectifs de l'entreprise.

L'avènement des données électroniques introduit un niveau de risque supplémentaire. Alors qu'il était nécessaire autrefois d'être sur place pour faire main basse sur un butin, le voleur peut se contenter aujourd'hui de faire une copie des données électroniques qui aura autant de valeur que l'original dans bien des cas. Pire encore, comme ce type de méfait laisse peu d'indices, vous ne vous rendrez même pas compte qu'on a vous a dérobé des données.

En 1980, une série de vols commis à bord d'avions commerciaux aux États-Unis fit grand bruit. C'est totalement par hasard que l'affaire fut résolue le 14 mai à l'aéroport d'Atlanta dans l'état de Géorgie, lorsqu'une malle s'ouvrit par accident lors du chargement de la soute. L'équipage découvrit alors un passager clandestin à l'intérieur de la malle avec de la nourriture et une bouteille d'oxygène. Le voleur s'extirpait de la malle en cours de vol, raflait un maximum d'objets de valeur, puis les rapportait avec lui dans sa planque. Si on devait comparer ce type de forfait à un vol de données électroniques, on considérerait qu'il s'agit d'une attaque classique de type « *Man in the Middle* », technique permettant d'intercepter des données en transit. Alors que le vol d'actifs physiques a fini par trahir la présence d'un passager clandestin, dérober des actifs numériques peut passer longtemps inaperçu.

L'analyse des objectifs à atteindre en matière de sécurité des données peut prendre un certain temps. Outre les obligations légales (GDPR, HIPAA, etc.) et l'efficacité opérationnelle (plan de continuité d'activité, chaîne d'approvisionnement, etc.), d'autres aspects du problème méritent également réflexion : qui a besoin d'accéder aux données ? dans quel délai ? Il serait possible évidemment de répondre à certains de ces objectifs en plaçant l'ensemble des données de l'entreprise, sans aucun chiffrement, sur un serveur Web public. Cela serait certainement bénéfique aux affaires, mais pourrait avoir des répercussions catastrophiques en termes d'image, de confidentialité et d'intégrité des données. De ce fait, il est indispensable de tenir compte de ces paramètres lors de l'élaboration des objectifs d'entreprise.

Les actifs électroniques comme les informations de santé protégées (PHI), les informations nominatives (PII), les données de cartes de crédit ou la propriété intellectuelle, doivent être sécurisées de façon à minimiser le risque de perte, d'exposition ou de copie des données.

L'importance de l'emplacement

Le choix du lieu de stockage des données est un élément prépondérant d'une stratégie de sécurisation des données électroniques. Deux solutions sont possibles en général : héberger les données localement (c'est-à-dire sur site) ou dans le Cloud. Les dernières avancées en matière de sécurité des données sur le Cloud ont compliqué la donne.

Étudions cinq facteurs pouvant avoir un impact déterminant sur le choix du mode de stockage des données.

Coût

Les investissements de départ et les coûts d'exploitation des centres de données hébergés

localement sont largement supérieurs à ceux de centres de données hébergés dans un Cloud privé (dans le cadre d'une infrastructure en tant que service[1]). Il faut, en effet, se doter des serveurs, disques, licences, équipements du réseau, sources d'alimentation électrique et systèmes de refroidissement nécessaires, et prévoir les ressources informatiques en nombre suffisant pour gérer, entretenir et mettre à jour l'ensemble de l'infrastructure. Le ticket d'entrée d'un centre de données dans un Cloud privé est, à l'inverse, beaucoup moins élevé. Le tarif est généralement calculé en fonction du kilo-octet de disque utilisé et de la puissance de traitement souscrite, auquel il faut ajouter la plupart des frais de licence, de gestion et de mise à niveau logicielle. Cela peut faire gonfler la facture au fil du temps. Le seuil de rentabilité (coût au-delà duquel un Cloud privé revient plus cher qu'un centre de données local) se chiffre généralement en années. Les critères d'évolutivité du matériel, de conformité légale, de trésorerie peuvent également faire pencher la balance d'un côté ou d'un autre.

Remarque : les services de stockage dans le Cloud de PaperCut MF sont compris dans la licence si vous disposez d'un contrat Maintenance et Support actif.

Sécurité

Le temps où la sécurité des données n'était qu'une simple formalité pour les centres de données hébergés localement est révolu. Ceux-ci offrent, néanmoins, un contrôle total sur le lieu et le mode de sécurisation des données, condition non négociable pour certaines organisations manipulant ou gérant des données sensibles et devant se plier aux réglementations en vigueur en matière de protection des données (RGPD, HIPAA ou FERPA, par exemple). En effet, la conformité réglementaire ne peut pas toujours être garantie pour les tierces parties ayant accès aux données d'un Cloud public.

Alors qu'avec des données hébergées sur site, c'est vous qui choisissez le lieu de destination des données et les personnes et systèmes autorisés à y accéder, à moins évidemment que vous ne les stockiez sur un disque ou sur un réseau. Le risque de violation de données est d'autant plus important dès lors que celles-ci sont visibles et accessibles par tous. Voici quelques statistiques éloquentes à ce sujet :

- 22 % des violations de données en 2017 tirent profit d'identifiants volés[2] (Rapport d'enquête de Verizon sur les violations de données en 2018)
- Le courrier électronique est le point d'entrée de 93 % des logiciels malveillants (malware)
- Les attaques perpétrées contre les chaînes d'approvisionnement ont augmenté de 78 % en 2018[3]
- 27 % des violations de données résultent d'une erreur humaine, 25 % de problèmes techniques au niveau du système, et 48 % d'attaques malveillantes (nombre d'entre-elles provenant d'initiés)[4]

1 IBM, Learn IaaS
2 Rapport d'enquête de Verizon sur les violations de données en 2018
3 Rapport de Symantec sur les menaces en matière de sécurité sur Internet en 2019
4 Étude IBM sur le coût d'une violation de données en 2018

La plupart des organisations qui hébergent leurs propres données n'ont plus les moyens de faire face au développement de ces menaces, à la fois en termes de quantité et de sophistication. Rares sont celles prêtes à se défendre contre les failles de sécurité matérielles des puces, les attaques de type « zero-day », les attaques multivectorielles ou les logiciels malveillants polymorphes. Nous en sommes arrivés à un point où la plupart des solutions de stockage dédiées sur le Cloud s'avèrent, en fin de compte, plus sûres que les solutions d'auto-hébergement. La sécurité des données sur le Cloud, notamment en ce qui concerne la façon dont le Cloud est utilisé, reste encore une source de préoccupation importante. On a constaté, par exemple, que des millions d'enregistrements de données avaient été exposés au cours des deux dernières années, en raison d'espaces de stockage de données Amazon S3 mal configurés[5]. Mise en garde importante : dès lors que vous omettez de configurer l'authentification et le chiffrement des données, rien n'empêche les autres personnes de les consulter.

La chaîne d'approvisionnement constitue une autre source potentielle de violation des données en ligne. Les tiers intervenant d'une façon ou d'une autre dans vos activités et ayant accès à vos données peuvent en être les victimes. Or, très peu d'organisations ont mis en place, aujourd'hui, des procédures de contrôle adéquates des tierces parties[6]. Vos obligations en matière de protection des données s'étendent aussi à ceux avec lesquels vous partagez des données. Un établissement scolaire qui fournit des informations sur ses étudiants à une société de restauration collective est aussi vulnérable que le maillon le plus faible de la chaîne d'approvisionnement. Un hôpital qui partage les dossiers de ses patients avec un prestataire de recouvrement des frais médicaux expose les informations de santé protégées (PHI) à des risques de violation et met en jeu sa responsabilité. Avant de confier la responsabilité de ses données à un fournisseur de services de stockage dans le Cloud, mieux vaut donc s'assurer que celui-ci garantit la sécurité de toutes les tierces parties.

Évolutivité

Le stockage dans le Cloud a clairement l'avantage dans ce domaine par rapport à une infrastructure auto-hébergée, sauf si on prend en compte le facteur fiabilité et que l'on ajoute les réseaux dans l'équation. Il est impératif, dans ce cas, que votre réseau offre un niveau de performance et de fiabilité supérieur à Internet. Tout l'intérêt des architectures Cloud est de pouvoir allouer, à la demande, des ensembles de ressources colossaux aux consommateurs. Le service de stockage dans le Cloud n'aura donc aucune difficulté à s'adapter à la demande et à absorber les pics de trafic sur le Web, les hausses des transactions et des demandes de rapport, etc. Le stockage dans le Cloud est le champion incontestable en termes d'évolutivité.

Fiabilité

La fiabilité des services de stockage dans le Cloud (hormis le délai de connexion à Internet) est généralement exprimée en pourcentage de temps de disponibilité. Il convient, pour ce faire, de calculer la durée totale annuelle des mises à jour matérielles et logicielles, réparations, applications de correctifs, pannes, opérations de migration, ou autres raisons pour lesquelles les

5 Bitdefender, Business Insights Blog
6 Help Net Security, Third Party Cyber Risk Management

services ont été interrompus, puis de diviser ce chiffre par 8 760 (nombre d'heure dans une année) pour obtenir le temps de disponibilité en pourcentage. Les services de stockage dans le Cloud ont un temps de disponibilité minimal de 99,95 %, ce qui équivaut à seulement quatre heures et vingt-trois minutes de temps d'arrêt par an. Encore un domaine où le Cloud s'impose haut la main.

Accessibilité

Les données présentent un intérêt à condition de pouvoir y accéder au moment voulu et depuis l'emplacement désiré. À quoi bon disposer, par exemple, d'une source d'informations indispensable sur votre smartphone si vous oubliez celui-ci à la maison ? Si vous avez besoin d'un accès continu aux données (24 heures sur 24 et 7 jours sur 7, par exemple), le stockage dans le Cloud est la solution qui s'impose. En revanche, si vous souhaitez bénéficier d'un haut niveau de contrôle sur l'accessibilité aux données (pour des raisons de confidentialité, de responsabilité, de conformité, etc.), les stockages hébergés localement seront certainement plus adaptés.

L'intérêt d'une approche multicouche

Après avoir décrit les principales différences entre les données hébergées sur site et celles stockées sur le Cloud, approfondissons le sujet de la sécurité. La protection des données met en jeu non pas une, mais plusieurs couches de sécurité :

- *couche physique* : barrières, coffres-forts, agents de surveillance, etc.
- *couche administrative* : procédures de formation, audits de sécurité, rotation de postes, etc.
- *couche technologique* : mots de passe, chiffrement, pare-feu, etc. (première ligne de défense qui nous vient à l'esprit en général). Les choses sont un peu plus complexes dans la pratique, mais cela permet de comprendre le principe général.

Le concept est comparable à des actifs non virtuels (des pierres précieuses, par exemple) que l'on enfermerait dans un coffre-fort à l'intérieur d'un bâtiment où tous les accès sont verrouillés et surveillés régulièrement par des gardes. Dans la plupart des cas, la multiplication des mesures de protection a un effet dissuasif.

De 2011 à 2017, la région du Sud-Est des États-Unis (et majoritairement la Floride) a été le théâtre d'une série de braquages de bijouteries de haut vol[7]. La bande de cambrioleurs avait mis au point des techniques de vol sophistiquées pour passer au travers des différents contrôles de sécurité. Ils ne revenaient jamais deux fois dans le même district pour éviter tout recoupement d'indices. Ils portaient des dispositifs de brouillage électronique pour perturber les systèmes d'alarme. Les bijouteries auxquelles ils s'attaquaient dans les galeries marchandes étaient situées à côté de boutiques mal protégées ou dépourvues de systèmes de sécurité (alarmes, barres anti-intrusion ou caméras). Ils s'introduisaient par effraction dans les boutiques en question, puis faisaient une ouverture dans le mur contigu à la bijouterie à l'aide d'une simple scie pour cloison sèche. Une fois à l'intérieur de la bijouterie, il leur suffisait souvent de percer un trou à un endroit précis avec un foret, pour forcer les coffres-forts « supposés inviolables » en un temps record. La bande ciblait tout particulièrement les boutiques les plus vulnérables.

7 *The Atlantic*, Décembre 2019, The Rise and Fall of an All-Star Crew of Jewel Thieves

Comme les services de numérisation vers un espace hébergé sur le Cloud (Scan to Cloud Storage) et de traitement de documents (Document Processing) de PaperCut MF ont été conçus spécialement pour le Cloud, la sécurité des données occupe une place fondamentale. La plateforme de cloud computing fournie par Google (Google Cloud Platform) sur laquelle sont hébergées les données PaperCut MF intègre, en effet, plusieurs couches de sécurité de pointe et même des sous-couches imbriquées[8]. Avant de choisir un fournisseur de services de stockage dans le Cloud, mieux vaut s'assurer qu'il propose des mesures de sécurité comparables.

Voici un bref aperçu des couches de sécurité mises en œuvre pour le service Scan to Cloud Storage de PaperCut MF sur la Google Cloud Platform.

Couche physique

L'identification biométrique, les détecteurs de métal, les caméras, les barrières de contrôle des véhicules et les systèmes de détection laser sont autant de moyens physiques différents pour assurer la protection des centres de données. Les serveurs et les périphériques du réseau, conçus sur mesure par Google, intègrent des puces de sécurité permettant d'identifier et d'authentifier les appareils légitimes au niveau matériel. Détail étonnant : une grande partie du Cloud est installée sous terre.

Le service de stockage dans le Cloud de PaperCut est basé sur la Google Cloud Platform. Tous les centres de données de cette plateforme possèdent une liste de certifications impressionnante : ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, SOC 1, SOC 2, SOC 3, PCI DSS, CSA STAR, HITRUST CSF, FedRAMP, IRAP, principes de sécurité du Cloud du Royaume-Uni, NIST 800-53, HIPAA, RGPD, exigences en matière de gouvernance des informations commerciales tierces de NHS Digital.

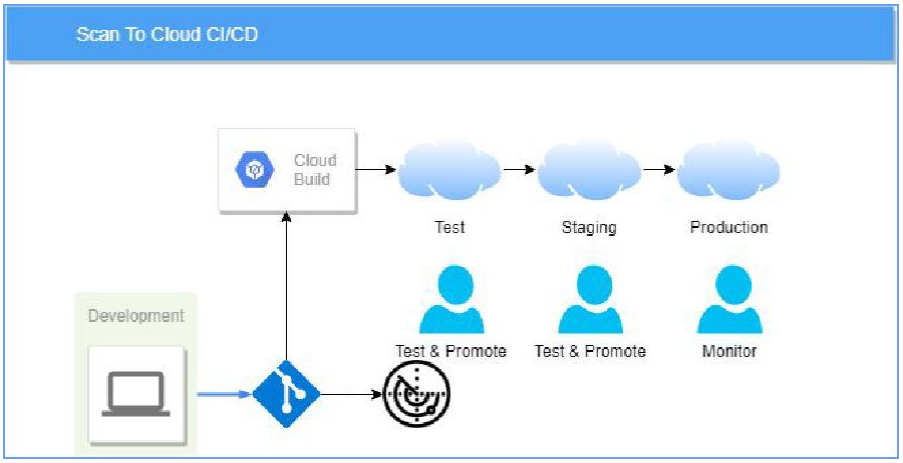
Couche administrative

Les hommes sont les premiers coupables en matière de violations de données. On estime, en effet, que 75 % des violations de données[9] leur sont imputables si on additionne les erreurs humaines, les délits d'initiés et les attaques malveillantes. C'est la raison pour laquelle seul un petit pourcentage des employés de Google et PaperCut ont le droit d'accéder aux données clients dans l'exercice de leur mission. La vérification des antécédents des employés, l'organisation de formations régulières en sécurité et la génération systématique de pistes d'audit prouvent que nous prenons la sécurité de nos clients très au sérieux.

8 Google Infrastructure Security Design Overview

9 Étude IBM sur le coût d'une violation de données en 2018

PaperCut a également mis en place un ensemble de bonnes pratiques de développement logiciel visant à éliminer les failles de sécurité et veille à ce que les meilleures pratiques en matière d'intégration et de livraison continues soient scrupuleusement respectées. PaperCut a prévu, en outre, différentes étapes de suivi et des tests continus (réalisés de façon automatique ou manuelle) entre le moment où un logiciel entre en phase de développement et le moment où le client commence à l'utiliser. Le risque qu'une erreur parvienne à subsister dans la version finale est donc d'autant plus faible.



Programme de développement et de test en plusieurs étapes pour optimiser l'intégration et la livraison continues (CI/CD)

Si cela permet indubitablement d'améliorer le code produit par PaperCut, qu'en est-il des bibliothèques et packages provenant de tierces parties ? Pour s'assurer de leur fiabilité, PaperCut procède à des analyses de code et des tests d'intrusion et participe activement aux travaux du NIST, du CVE, et de divers autres groupes.

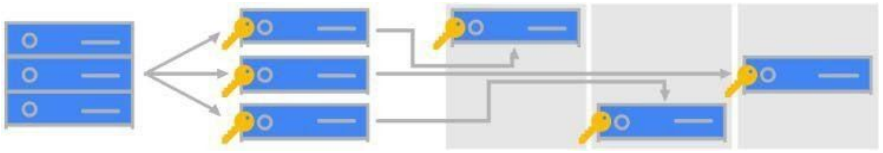
Couche technologique

Du point de vue technologique, plusieurs niveaux ou couches de sécurité entrent également en jeu. La Google Cloud Platform est elle-même protégée contre les accès frauduleux (personne mal intentionnée essayant de se connecter à l'API PaperCut), les intrusions sur le réseau, le vol de données et diverses autres menaces telles que les logiciels malveillants (même au niveau matériel) et les attaques par déni de service (DoS). Prenez le temps de consulter le livre blanc complet rédigé par Google[10]. Ces mesures de protection permettent de neutraliser pratiquement toutes les attaques survenant au niveau de la couche réseau.

10 Google Infrastructure Security Design Overview

Diverses autres couches de protection des données sont déployées, comme le chiffrement des données en transit et le chiffrement des données au repos. « Google chiffre et authentifie toutes les données en transit sur une ou plusieurs couches réseau lors de transferts en dehors des limites physiques qui ne sont pas contrôlées par Google. »[11]. Autrement dit, vos données n'apparaissent jamais en texte clair quand elles sont transférées de votre site au service Scan to Cloud Storage de PaperCut MF. Le niveau de chiffrement le plus élevé du protocole de sécurité de la couche transport (TLS) leur est appliqué.

Les données sont également chiffrées au repos. Le processus de chiffrement se déroule lui aussi en plusieurs étapes. Chaque fichier de données est d'abord subdivisé en plusieurs blocs, puis chaque bloc est chiffré au moyen d'une clé différente. Chacun des blocs chiffrés est ensuite stocké sur des lecteurs indépendants qui ont eux-mêmes été cryptés. C'est un peu comme si vous deviez reconstituer toutes les pièces un puzzle sans savoir où elles se trouvent, ni connaître le nombre total de pièces[12].

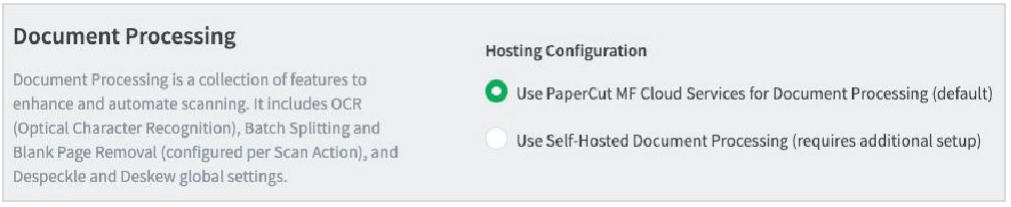


Mode de chiffrement de fichier multicouche de Google

Le service Cloud de PaperCut MF

Examinons, à présent, le flux des données et la sécurité aux différents stades du service Scan to Cloud Storage de PaperCut MF. Nous étudierons plus précisément le mode de traitement des documents, le trajet des documents ainsi que le rôle des autorisations utilisateur.

Si le traitement des documents est configuré pour tirer parti des services du Cloud PaperCut MF, chaque numérisation empruntera le chemin défini pour le document. Même la fonction de numérisation vers des e-mails (Scan to Email) transmettra l'image numérisée vers le Cloud en vue de procéder au traitement du document, à condition d'avoir sélectionné ces options dans la console d'administration de PaperCut MF.



Traitement des documents de PaperCut MF configurable pour le Cloud ou l'auto-hébergement

11 Google's Encryption in Transit

12 Encryption at Rest in Google Cloud Platform

Avant d'aller plus loin, il est important de rappeler que les utilisateurs PaperCut MF peuvent uniquement numériser des documents vers des destinations autorisées. L'administrateur PaperCut MF bénéficie d'un contrôle total sur les destinations des numérisations et les options de traitement des documents. Le recours au service Cloud de PaperCut (PCS) est entièrement facultatif pour chacun des clients PaperCut MF. Aucun document ou aucune métadonnée ne peut être transmis au service Cloud de PaperCut sans la configuration explicite de l'administrateur PaperCut MF.

Pour déterminer ce à quoi chaque utilisateur a accès sur l'appareil multifonction (MFD), l'administrateur est tenu de créer une action de numérisation (Scan Action). Si l'administrateur n'a défini aucune action de numérisation pour les fonctions de numérisation vers un espace hébergé sur le Cloud (Scan to Cloud Storage) ou de traitement de documents (Document Processing) dans le Cloud, les images numérisées ne sont pas transmises au Cloud. Pour configurer les actions de numérisation de façon plus fine, l'accès peut être accordé au niveau de l'utilisateur ou du groupe.

Traitement des documents

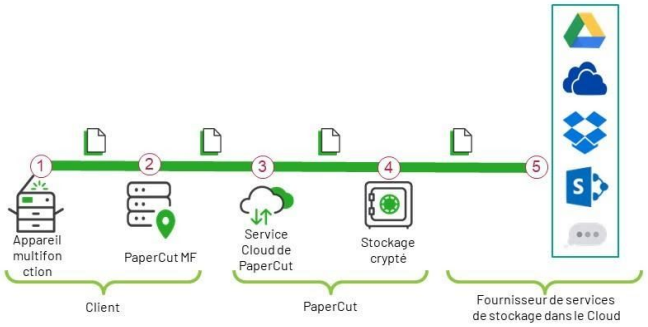
Le service Cloud de PaperCut offre des fonctions avancées de traitement de documents telles que la reconnaissance optique de caractères (OCR), le déparasitage et le redressement. Celles-ci nécessitent, toutefois, le déchiffrement du document pendant un laps de temps très bref. Ces fonctions sont facultatives et peuvent être désactivées par votre administrateur PaperCut MF.

Votre administrateur peut également configurer le traitement de documents dans le service Cloud de PaperCut de façon à maintenir les documents au sein d'une région géographique donnée. Trois régions sont disponibles actuellement : Australie, Allemagne et États-Unis. Les documents ne quittent la région sélectionnée, au moment de la livraison à la destination, que si l'action de numérisation (Scan Action) désigne un fournisseur de services de stockage dans le Cloud hébergé ailleurs (Evernote, par exemple).

Trajet des documents

Le cycle de vie d'un document numérisé vers un espace hébergé sur le Cloud (Scan to Cloud Storage) commence au niveau de l'appareil multifonction (MFD), et plus précisément au niveau de la fonction de numérisation intégrée de PaperCut MF. Nous tirons parti des fonctionnalités intégrées à l'appareil multifonction pour créer une image du document.

Remarque : sauf indication contraire, les communications établies tout au long du cycle de vie du document numérisé utilisent le protocole TLS 1.2.



Trajet du document numérisé en cas de sélection de l'option Scan to Cloud Storage dans PaperCut MF

1. **Actions depuis l'appareil multifonction**

    a. L'utilisateur s'authentifie auprès de PaperCut MF.
    b. L'utilisateur sélectionne une action de numérisation (Scan Action) et une destination sur le Cloud.
    c. L'utilisateur lance la numérisation du document.
    d. L'appareil multifonction crée l'image du document numérisé.
    e. L'appareil multifonction envoie le document image au serveur PaperCut MF.

    Remarque : il est possible de désactiver les algorithmes de chiffrement faibles dans PaperCut MF pour obliger l'appareil multifonction à recourir à des algorithmes de chiffrement plus puissants et plus sûrs.

2. **Serveur d'applications PaperCut MF**

    a. PaperCut MF reçoit le document image et les métadonnées de l'appareil multifonction.
    b. PaperCut MF crée une connexion sécurisée vers le service Cloud de PaperCut. PaperCut MF utilise uniquement les suites de chiffrement PFS (Perfect Forward Secrecy) conformes avec le protocole TLS 1.2.
    c. Le serveur PaperCut MF est authentifié et autorisé auprès du service Cloud grâce à une clé unique composée de l'identifiant d'installation de PaperCut MF et de sa clé de licence.
    d. PaperCut MF envoie le document image et les métadonnées qui s'y rapportent (l'adresse e-mail de l'utilisateur, par exemple) au service Cloud de PaperCut.

    Remarque : la sécurisation du serveur d'applications et du système de fichiers PaperCut MF, la formation du personnel informatique, les pare-feu et les autres considérations de ce genre sont de la responsabilité de l'organisation hébergeant PaperCut MF.

3. **Service Cloud de PaperCut**

    a. Le service Cloud de PaperCut reçoit le document et les métadonnées transférés par le serveur d'applications PaperCut MF. Et c'est là que la magie opère.
    b. En fonction des options sélectionnées par l'administrateur de PaperCut MF, le document transféré est ouvert en vue d'être traité. Plusieurs traitements sont possibles : reconnaissance optique de caractères (OCR), déparasitage et redressement.
    c. Le service Cloud de PaperCut écrit le document sur le stockage crypté.
    d. Le service Cloud de PaperCut est hébergé sur la plateforme Cloud sécurisée de Google (Google Cloud Platform).
    e. Le service Cloud de PaperCut s'exécute en intégralité dans la région sélectionnée par le client (Australie, Allemagne ou États-Unis).

4. **Stockage crypté**

    ○ Grâce au chiffrement au repos de Google, mentionné plus haut, le document est chiffré, puis placé sur des lecteurs cryptés.

- Tous les documents sont différenciés au moyen d'un identifiant client unique.
- Seul un petit nombre d'employés PaperCut ont accès aux documents dans le stockage.
- L'accès est géré à la demande conformément aux règles d'accès IAM[13] de Google.
- Une piste d'audit est générée à chaque accès au stockage des données, y compris par le personnel d'exploitation.
- Si le service Cloud de PaperCut n'est pas en mesure de traiter ou de livrer le document, il recommence l'opération pendant une durée maximum de 24 heures.
- Une fois la livraison effectuée ou le délai de 24 heures atteint, le document est supprimé de façon sécurisée.

5. **Livraison au fournisseur de services de stockage dans le Cloud**

    - À peine une ou deux minutes après que l'utilisateur a appuyé sur la touche de numérisation de l'appareil multifonction, le service Cloud de PaperCut transmet le document numérisé au fournisseur de services de stockage dans le Cloud sélectionné (OneDrive ou G Drive, par exemple)
    - Le service Cloud de PaperCut demande toujours l'autorisation minimum requise pour livrer les documents (écriture seule). Cependant, tous les fournisseurs de services de stockage dans le Cloud n'offrent pas une telle souplesse d'accès.
    - Une fois le document arrivé à destination, il est supprimé de façon sécurisée du service Cloud de PaperCut.
    - Si la livraison échoue, le document peut être conservé dans le stockage crypté pendant 24 heures supplémentaires, la suppression sécurisée n'intervenant qu'à l'issue de ce délai.

Conservation des données

Aucune partie du contenu du document numérisé n'est préservée par PaperCut MF ou le service Cloud de PaperCut. Le service Cloud de PaperCut conserve, cependant, les informations suivantes au sujet de chaque document numérisé :

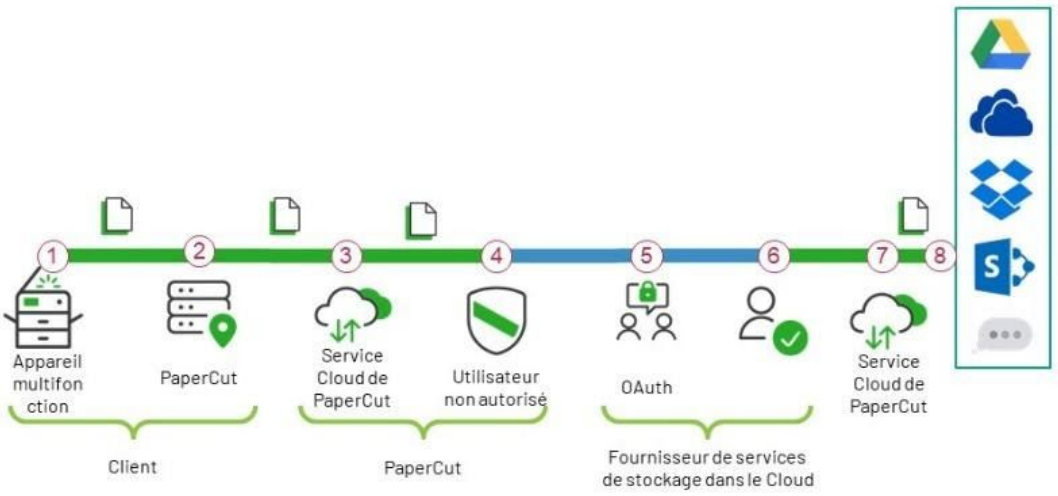
- Adresse e-mail de l'utilisateur
- Nom d'utilisateur ou nom complet
- Paramètres régionaux utilisateur
- Nom de fichier du document numérisé

La conservation des données est soumise aux dispositions législatives et réglementaires en matière de confidentialité (RGPD, par exemple).

13 Cloud Identity and Access Management

Autorisation utilisateur

La première fois qu'un utilisateur numérise un document à destination d'un service de stockage dans le Cloud, PaperCut MF lui demande sa permission pour transférer le document (ainsi que les prochains documents) vers le fournisseur de services de stockage dans le Cloud sélectionné. Cette autorisation peut être révoquée à tout moment par l'utilisateur.



Trajet de l'autorisation utilisateur en cas de sélection de l'option Scan to Cloud Storage dans PaperCut MF

1. Actions depuis l'appareil multifonction

Les opérations à effectuer au niveau de l'appareil multifonction lors de l'autorisation utilisateur sont identiques à celles décrites à la section Trajet du document ci-avant.

a. L'utilisateur s'authentifie auprès de PaperCut MF.
b. L'utilisateur sélectionne une action de numérisation (Scan Action) et une destination sur le Cloud.
c. L'utilisateur lance la numérisation du document.
d. L'appareil multifonction crée l'image du document numérisé.
e. L'appareil multifonction envoie le document image au serveur PaperCut MF.

Remarque : il est possible de désactiver les algorithmes de chiffrement faibles dans PaperCut MF pour obliger l'appareil multifonction à recourir à des algorithmes de chiffrement plus puissants et plus sûrs.

2. Serveur d'applications PaperCut MF

Actions identiques à celles répertoriées pour le serveur d'applications PaperCut MF dans la section Trajet du document ci-avant.

a. PaperCut MF reçoit le document image et les métadonnées de l'appareil multifonction.
b. PaperCut MF crée une connexion sécurisée vers le service Cloud de PaperCut. PaperCut MF utilise uniquement les suites de chiffrement PFS (Perfect Forward Secrecy) conformes avec le protocole TLS 1.2.
c. Le serveur PaperCut MF est authentifié et autorisé auprès du service Cloud grâce à une clé unique composée de l'identifiant d'installation de PaperCut MF et de sa clé de licence.
d. PaperCut MF envoie le document image et les métadonnées qui s'y rapportent (l'adresse e-mail de l'utilisateur, par exemple) au service Cloud de PaperCut.

Remarque : la sécurisation du serveur d'applications et du système de fichiers PaperCut MF, la formation du personnel informatique, les pare-feu, et les autres considérations de ce genre sont de la responsabilité de l'organisation hébergeant PaperCut MF.

3. Service Cloud de PaperCut

Actions identiques à celles répertoriées dans la section Trajet du document ci-avant.

a. Le service Cloud de PaperCut reçoit le document et les métadonnées transférés par le serveur d'applications PaperCut MF. Et c'est là que la magie opère.
b. En fonction des options sélectionnées par l'administrateur PaperCut MF, le document transféré est ouvert en vue d'être traité. Plusieurs traitements sont possibles : reconnaissance optique de caractères (OCR), déparasitage et redressement.
c. Le service Cloud de PaperCut écrit le document sur le stockage crypté.
d. Le service Cloud de PaperCut est hébergé sur la plateforme Cloud sécurisée de Google (Google Cloud Platform).
e. Le service Cloud de PaperCut s'exécute en intégralité dans la région sélectionnée par le client (Australie, Allemagne ou États-Unis).

4. Utilisateur non autorisé

- Le service Cloud de PaperCut détecte si l'utilisateur est autorisé à accéder au fournisseur de services de stockage dans le Cloud sélectionné.
- Si ce n'est pas le cas, le service Cloud de PaperCut lui envoie un e-mail contenant un lien sécurisé (TLS) vers la page d'autorisation du fournisseur de services de stockage dans le Cloud.
- Le service Cloud de PaperCut conserve le document de l'utilisateur pendant une durée maximale de 24 heures, pour lui laisser le temps d'obtenir l'autorisation requise.

5. **OAuth**
    - La communication est établie entre l'utilisateur et le fournisseur de services de stockage dans le Cloud via le protocole OAuth2[14]. Les communications OAuth (y compris le lien de l'e-mail initial) utilisent systématiquement le protocole TLS 1.2.
    - Si l'autorisation utilisateur est validée, le fournisseur de services de stockage dans le Cloud envoie un jeton (au nom de l'utilisateur) au service Cloud de PaperCut.
    - Il est inutile de recommencer le processus d'autorisation pour les numérisations suivantes destinées au même fournisseur de services de stockage dans le Cloud.
    - Si l'autorisation échoue ou si elle n'est pas validée dans un délai de 24 heures, le service Cloud de PaperCut supprime, de façon sécurisée,[15] le document de l'utilisateur.

6. **Utilisateur autorisé**
    - Le service Cloud de PaperCut stocke le jeton OAuth (chiffrement AES256-GCM) de l'utilisateur, mais n'accède jamais à ses identifiants de connexion.
    - Le jeton sert uniquement à transmettre les documents d'un utilisateur donné à un fournisseur de services de stockage dans le Cloud spécifique.
    - Le jeton ne quitte jamais le service Cloud de PaperCut.
    - Le jeton possède une date d'expiration.
    - Le service Cloud de PaperCut stocke les clés de chiffrement du jeton grâce au service KMS (Cloud Key Management) de Google.
    - Les clés ne quittent jamais le service Cloud de PaperCut.
    - L'utilisateur peut à tout moment révoquer le jeton en se rendant sur le site du fournisseur de services de stockage dans le Cloud et en supprimant l'autorisation pour le service Cloud de PaperCut.

7. **Prêt à partir**
    a. Le service Cloud de PaperCut utilise le protocole TLS le plus sûr pour transmettre le document de l'utilisateur au fournisseur de services de stockage dans le Cloud.
    b. Le document est ensuite supprimé de façon sécurisée du service Cloud de PaperCut.
        - Si la transmission échoue, le document peut être maintenu dans le service Cloud de PaperCut pendant 48 heures supplémentaires (24 heures pour l'autorisation utilisateur, et 24 heures pour le traitement et la livraison).
        - Si le document ne parvient pas à destination après plusieurs tentatives, il est supprimé de façon sécurisée.

14 https://auth0.com/docs/protocols/oauth2

15 https://cloud.google.com/security/deletion/

8. **Arrivée à destination**

   Il suffit généralement d'une à deux minutes pour acheminer, en toute sécurité, un document numérisé jusqu'au fournisseur de services de stockage dans le Cloud.

Réponses aux questions fréquemment posées

L'examen des questions portant sur sécurité fait partie du processus normal d'évaluation de PaperCut MF et de la fonction Scan to Cloud Storage. Voici les réponses aux questions les plus courantes.

Processus opérationnels

- Le service Cloud de PaperCut (PCS) est conforme à la réglementation HIPAA. Pour les services basés sur le Cloud, nous avons conclu un accord de partenariat (BAA) avec Google pour nous assurer que les informations nominatives (PII) transitant par l'instance du Cloud seront traitées conformément aux prescriptions légales de l'HIPAA (Health Insurance Portability and Accountability Act). Si vous comptez utiliser le service Cloud de PaperCut (PCS) pour y stocker des informations nominatives (PII), signez le même type d'accord avec la société PaperCut pour qu'elle s'engage à respecter les mêmes prescriptions (HIPAA) lors de la manipulation des informations nominatives (PII) transitant par le PCS.
- PaperCut MF (PMF) et le service Cloud de PaperCut (PCS) sont conformes au Règlement général sur la protection des données (RGPD). Selon les modalités du RGPD, vous avez le droit de configurer PaperCut MF (PMF) et le service Cloud de PaperCut (PCS) pour l'édition de données utilisateur.
- PaperCut désigne une personne qui sera chargée de l'examen et de la mise en œuvre du plan de continuité/reprise d'activité (PCA/PRA).
- Les dispositions du plan PCA/PRA sont examinées une fois par an et révisées si cela s'avère nécessaire.
- Le plan PCA/PRA a été testé pendant l'année écoulée.

Développement des logiciels

- PaperCut propose à ses employés des programmes de formation continue en vue d'expliquer les rôles et responsabilités de chacun en temps de crise.
- PaperCut MF (PMF) et le service Cloud de PaperCut (PCS) suivent un cycle de développement logiciel (SDLC) documenté.
- PaperCut MF (PMF) et le service Cloud de PaperCut (PCS) ont été développés en utilisant des techniques de codage sécurisées.
- Le cycle de vie de PaperCut MF (PMF) et du service Cloud de PaperCut (PCS) respecte les principes en matière de sécurité de l'information.
- Le code source de PaperCut MF (PMF) et du service Cloud de PaperCut (PCS) fait l'objet d'une analyse statique et d'un test de sécurité des applications statiques avant publication.
- PaperCut MF (PMF) et le service Cloud de PaperCut (PCS) ont été soumis à une batterie de tests automatisés avant publication.

Détection des vulnérabilités

- Un prestataire externe a été chargé d'analyser PaperCut MF (PMF) et le service Cloud de PaperCut (PCS) en vue de détecter des éventuelles vulnérabilités avant publication.
- PaperCut MF (PMF) et le service Cloud de PaperCut (PCS) ont fait l'objet de chasse aux bogues dans le cadre de programmes « Bug Bounty ».
- PaperCut accepte l'envoi direct des problèmes de sécurité[16].
- L'outil de vérification automatique des dépendances d'OWASP (nommé Dependency-Check) a été appliqué à PaperCut MF (PMF)[17].
- PaperCut étudie tous les problèmes de sécurité soumis et utilise l'algorithme DREAD pour calculer la valeur du risque[18].
- PaperCut prend en charge la base de données CVE et publie ses rapports sur la base de données américaine sur les vulnérabilités (NVD)[19].

Processus et procédures

- PaperCut dispose d'un protocole de réponse aux incidents.
- PaperCut s'engage à se soumettre pleinement aux lois en matière de notification des atteintes à la protection des données.
- PaperCut vérifie systématiquement les antécédents des employés chargés de l'exploitation des données, avant de les recruter.
- PaperCut exige que les nouvelles recrues adhèrent aux politiques en matière d'exploitation des données.
- PaperCut a mis en place une politique documentée en matière de protection des données.
- PaperCut examine et met à jour régulièrement les stratégies en matière de protection et d'accès aux données conformément aux règles d'accès IAM.
- PaperCut a instauré des procédures d'audit internes et des pistes d'audit complètes[20] pour l'accès aux données du Cloud.

Conclusion

Grâce à la fonction de numérisation vers un espace hébergé sur le Cloud (Scan to Cloud Storage) de PaperCut MF, vous avez l'assurance que vos documents sont parfaitement protégés à tous les stades de leur cycle de vie. La satisfaction de nos clients est l'une de nos principales priorités. C'est pourquoi nous prenons soin de protéger ce qui compte pour eux. Nous avons mis en œuvre les technologies les plus sophistiquées pour maintenir les plus hauts niveaux d'accessibilité, de confidentialité et de protection des informations client.

16 https://www.papercut.com/solutions/security/report/
17 https://owasp.org/www-project-dependency-check/
18 https://wiki.openstack.org/wiki/Security/OSSA-Metrics
19 https://nvd.nist.gov/
20 https://cloud.google.com/logging/docs/audit/

Glossaire

Terme	Description
Amazon Web Services (AWS)	Série de services de cloud computing (informatique dématérialisée dans le Cloud) proposés par Amazon.com.
Plan de continuité d'activité/Plan de reprise d'activité (PCA/PRA)	Ensemble de meilleures pratiques et de procédures permettant à une entreprise de poursuivre ses activités à la suite d'une crise.
Cloud Security Alliance Security Trust Assurance and Risk (CSA STAR)	Initiative visant à encourager les principes de transparence, d'audit rigoureux et d'harmonisation des normes.
Common Vulnerabilities and Exposures (CVE)	Référence mondiale en matière de failles et vulnérabilités informatiques.
Données au repos	Informations stockées sur un appareil ou un support de sauvegarde sous une forme quelconque.
Données en transit	Informations qui se déplacent sur un réseau d'un endroit à un autre (câble, Wi-Fi, mobile, etc.).
Attaque par déni de service (DoS)	Cyberattaque tirant profit des limites de capacité d'un ordinateur ou d'un réseau pour bloquer son fonctionnement.
Family Educational Rights and Privacy Act (FERPA)	Loi du gouvernement américain visant à protéger la confidentialité des dossiers scolaires des élèves et étudiants.
Règlement général sur la protection des données (RGPD)	Directive permettant d'harmoniser les lois sur la confidentialité des données en Europe.
Health Insurance Portability and Accountability Act (HIPAA)	Loi qui impose à tous les intervenants du secteur des soins de santé aux États-Unis de protéger les informations nominatives (PII) des patients contre les risques de fraude et de vol.
Health Information Trust Alliance Common Security Framework (HITRUST CSF)	Cadre de certification en matière de conformité réglementaire et de gestion des risques pour tous les secteurs.
Information Security Registered Assessors Program (IRAP)	Processus complet pour l'évaluation de la sécurité d'une organisation par rapport aux stratégies et directives australiennes.

Terme	Description
Organisation internationale de normalisation et Commission électrotechnique internationale (ISO/IEC)	Organismes chargés du développement, de la gestion et de la promotion des normes dans le secteur informatique.
Attaque de type « Man in the Middle » (MitM)	Attaque consistant à espionner illicitement la communication entre deux parties et à l'altérer parfois, tout en s'assurant que l'échange paraisse normal.
Appareil multifonction (MFD)	Imprimante pouvant également faire office de photocopieuse, de fax et de scanner.
National Health Service (NHS)	Système de la santé publique du Royaume-Uni.
National Institute of Standards and Technology (NIST)	Organisme public américain chargé de développer des normes, des mesures et des directives en matière de cybersécurité.
Open Authorization (OAuth)	Protocole libre de délégation d'autorisation pour accorder à une application tierce un accès limité sur une ressource, avec l'accord du propriétaire.
Reconnaissance optique de caractères (OCR)	Conversion électronique des images de texte dactylographié, manuscrit ou imprimé sous une forme lisible par ordinateur.
Open Web Application Security Project (OWASP)	Organisation à but non lucratif ayant pour objectif d'améliorer la sécurité des logiciels.
Informations de santé protégées (ou PHI pour Protected Health Information)	Ensemble des informations portant sur l'état de santé, les prestations de soins de santé ou le paiement de ces prestations, pouvant être liées à un individu spécifique.
Informations nominatives (ou PII pour Personally Identifiable Information)	Toutes les données pouvant servir à identifier un individu.
Amazon Simple Storage Service (abrégé S3)	Service de stockage d'objets hébergé par AWS.
System and Organization Controls (SOC)	Référentiel utilisé par les professions comptables pour réaliser des audits au niveau système d'une société de service ou des audits au niveau entité pour les autres organisations.
Transport Layer Security (TLS)	Protocole de sécurité de la couche transport assurant l'authentification, la confidentialité et l'intégrité des données entre les applications informatiques.

Remerciements

Auteurs

David O'Hara (Architecte de solutions, PaperCut Software)

Contributeurs

Amir Khassaia (Ingénieur produit senior, PaperCut Software)
Bryce Smith (Chef de produit, PaperCut Software)
Geoff Smith (Ingénieur produit éminent, PaperCut Software) Sonja
McShane (Designer produit, PaperCut Software)

---

sales@acd-inc.com

acd-inc.com

Support

support@acd-inc.com

acd-inc.com/support