Gespage

Powered by Cartadis

Optimisez et Sécurisez vos Flux d'impression avec Gespage

Livre Blanc

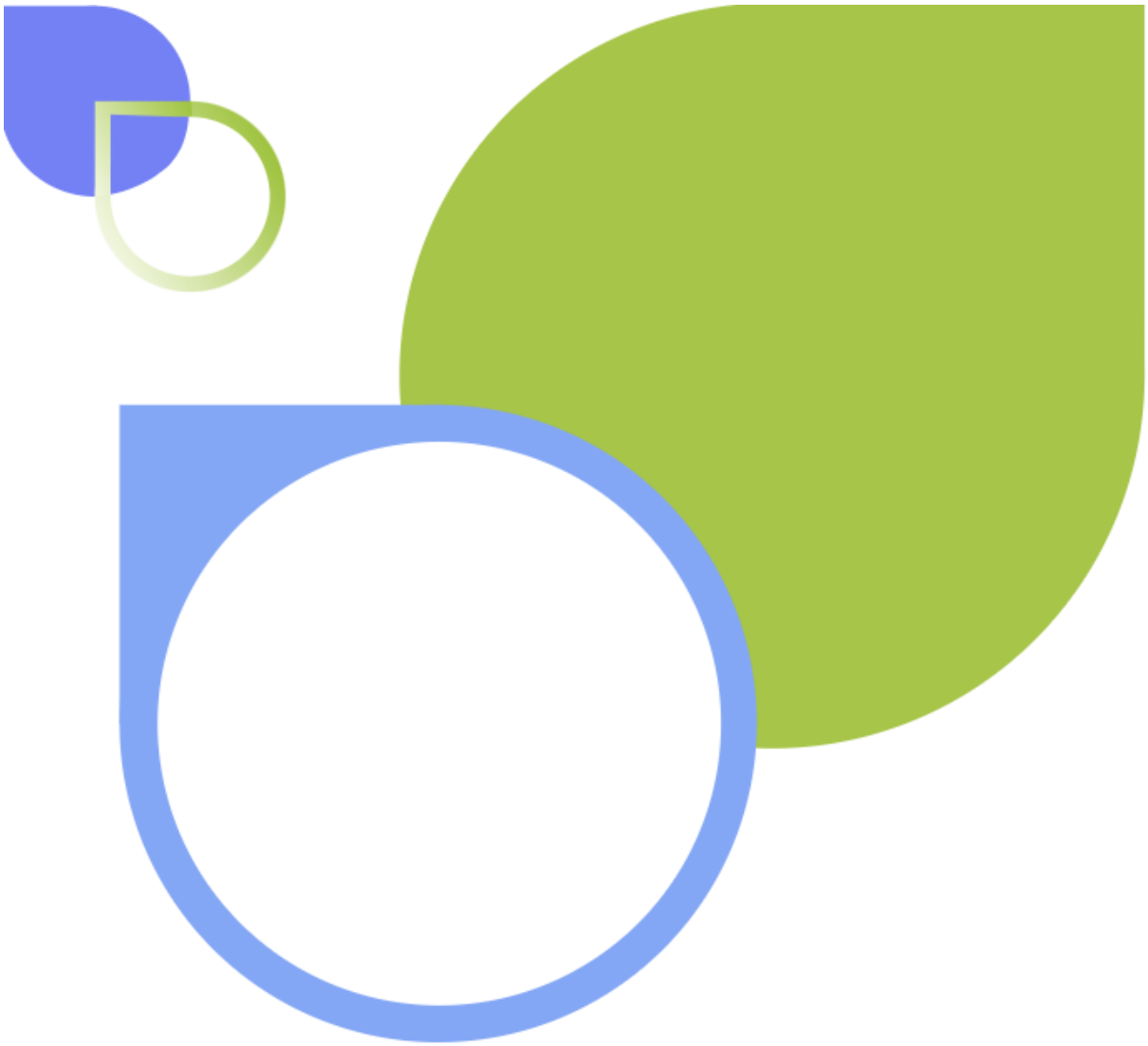


Table des matières

1. Introduction

Saviez-vous que 67% des organisations subissent chaque année des pertes de données dues à des impressions non sécurisées ? Face à ce défi majeur, Gespage sécurise efficacement vos flux d'impression en garantissant une protection complète des informations sensibles tout en optimisant les coûts et en facilitant la conformité aux réglementations internationales telles que le RGPD.

Dans un monde professionnel où les données sont un actif précieux, la gestion et la sécurité des flux d'impression prennent une importance capitale. Trop souvent négligé, l'environnement d'impression peut devenir une porte d'entrée pour des failles de sécurité ou une source d'inefficacités coûteuses.

Gespage, la solution phare de gestion des impressions de Cartadis, répond à ces défis avec une approche complète et innovante.

Ce livre blanc explore comment Gespage vous permet d'optimiser vos flux d'impression tout en renforçant la sécurité et en réduisant les coûts, le tout dans le respect des réglementations telles que le RGPD.

Selon le rapport "Print Security Landscape 2024" de Quocirca, la sécurité des impressions demeure un défi majeur pour les organisations. Nous retenons quelques statistiques clés issues de ce rapport :

- **Violations de données liées à l'impression** : 67 % des organisations ont signalé des pertes de données au cours des 12 derniers mois en raison de pratiques d'impression non sécurisées, en hausse par rapport à 61 % en 2023.
- **Confiance dans la sécurité de l'infrastructure d'impression** : Seules 43 % des organisations se déclarent totalement confiantes dans la sécurité de leur infrastructure d'impression.
- **Coûts des violations de données** : Les entreprises de taille moyenne sont particulièrement touchées, avec des coûts de violation atteignant 1 million de livres sterling.
- **Importance de l'impression pour les activités** : 71 % des entreprises estiment que l'impression sera très importante pour leurs activités au cours des 12 prochains mois.

- **Satisfaction à l'égard de la sécurité d'impression** : Seulement 16 % des entreprises se disent "très satisfaites" de leur sécurité d'impression en 2024, un chiffre en déclin depuis 2022.

Ces données soulignent l'importance cruciale de renforcer les mesures de sécurité autour des infrastructures d'impression pour protéger les informations sensibles des organisations.

2. Sécurisation bas niveau de l'infrastructure complète

Il est important d'identifier que la sécurité du flux d'impression passe par la mise en sécurité de l'intégralité de l'infrastructure d'impression.

Cela commence par l'imprimante puis continue par l'architecture réseau de l'entreprise pour finir par le serveur d'impression.

2.1 Sécurisation des imprimantes

Les imprimantes multifonctions sont dotées d'une multitude de protocoles et de services, elles sont souvent surchargées de fonctionnalités qui ne sont pas nécessaires dans un environnement professionnel spécifique.

Afin de minimiser les vulnérabilités, il est essentiel de les placer dans des lieux surveillés, de mettre en place une configuration sécurisée de l'imprimante, et mettre à jour régulièrement son firmware.

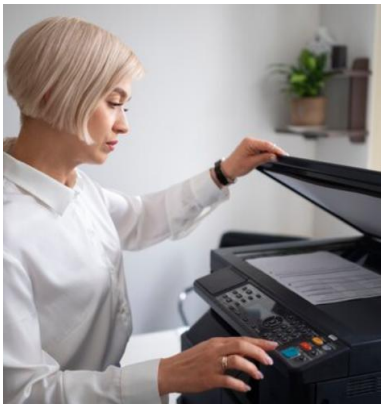
Nous fournissions ci-dessous les recommandations de bonne pratique standards pour la sécurisation des imprimantes. **Nous vous recommandons en complément de contacter votre fournisseur d'imprimante ou MFP pour obtenir leurs recommandations de sécurité spécifiques.**

Sécurisation de l'emplacement

Les risques d'attaques peuvent être considérablement affectés si les imprimantes sont placées dans des zones vulnérables, où elles risquent d'être utilisées à mauvais escient. Installer les imprimantes dans des emplacements sécurisés et accessibles uniquement au personnel autorisé est une solution simple pour réduire les risques liés à la sécurité.

Les institutions éducatives et les campus sont particulièrement exposés, notamment lorsque les imprimantes sont facilement accessibles aux étudiants.

Pour renforcer la sécurité physique, les mesures suivantes peuvent être mises en œuvre :



- **Fixer solidement l'imprimante** au bâtiment pour éviter les vols ou manipulations non autorisées.
- **Désactiver les ports USB** pour empêcher l'accès à des périphériques externes non autorisés.
- **Sécuriser les connexions réseau**, par exemple en fixant les câbles réseau pour prévenir les manipulations.
- **Verrouiller les bacs à papier** afin de limiter le vol ou d'éviter une mauvaise utilisation.

Gestion des mots de passe

Les mots de passe administrateur par défaut sont souvent connus publiquement, exposant les appareils à des intrusions potentielles. Il est donc crucial de remplacer ces mots de passe dès l'installation et de les modifier régulièrement. De plus, optez pour des mots de passe complexes pour protéger les paramétrages critiques, tels que la configuration réseau, contre les tentatives de piratage ou les modifications non autorisées.

Sécurisation des protocoles et services

Au niveau du paramétrage de votre imprimante, il est recommandé de désactiver les protocoles et services qui ne sont pas utilisés dans votre infrastructure. Voici certaines de ceux-ci à titre d'exemple :

- **Protocoles d'impression** : Une imprimante peut supporter divers protocoles d'impression (IPP, JetDirect, LPD, AirPrint, FTP…). Il est recommandé que les protocoles mis en place dans votre infrastructure, les plus fréquemment utilisés sont IPP et JetDirect.
- **Prise en main à distance** : Cette option peut poser des problèmes de sécurité, il est recommandé de l'activer uniquement sur des durées limitées uniquement lorsque cela est nécessaire.
- **Stockage des données d'impression** : Certaines imprimantes permettent de conserver les travaux d'impression sur leur mémoire interne pour une réutilisation ultérieure. Bien que pratique, cette fonctionnalité peut entraîner des risques si des documents confidentiels sont accessibles sans protection adéquate. Une politique stricte devrait définir quels types de documents peuvent être stockés et imposer une protection par mot de passe. Lorsque cette fonctionnalité n'est pas nécessaire, il est recommandé de la désactiver ou d'utiliser une option de suppression automatique des données.

Chiffrement des données sensibles

Les appareils modernes intègrent souvent des fonctionnalités avancées, comme le chiffrement complet du disque dur à l'aide de standards tels que l'AES (Advanced Encryption Standard). L'activation de cette option est recommandée pour assurer que toutes les données enregistrées sur l'appareil soient protégées contre les accès non autorisés.

Solutions dédiées à la sécurité des données

Certains fabricants proposent par ailleurs des ensembles complets de fonctionnalités de sécurité regroupés dans des « kits de protection des données ». Ces kits, incluant des options de suppression sécurisée des données, de chiffrement et de gestion des impressions sensibles, peuvent être indispensables dans des environnements nécessitant un haut niveau de protection. Assurez-vous que ces kits soient installés et correctement configurés si votre organisation traite des données critiques.

Mises à jour du firmware de l'imprimante

Pour finir, il est primordial de s'assurer régulièrement que le firmware de l'imprimante soit à jour.

Les fabricants d'imprimantes et MFPs mettent de plus en plus l'accent sur la sécurité en publiant régulièrement des mises à jour pour corriger les vulnérabilités identifiées. Il est donc indispensable d'instaurer une politique de mise à jour périodique du Firmware de vos imprimantes et MFP pour bénéficier des correctifs essentiels et des améliorations en matière de protection.

En particulier, les protocoles de chiffrement utilisés par les imprimantes évoluent constamment. En mettant régulièrement à jour le Firmware, vous vous assurez que vos équipements utilisent des protocoles de chiffrement modernes et robustes, renforçant ainsi la protection contre les attaques potentielles.

Les systèmes modernes négocient automatiquement le protocole de sécurité le plus performant lors de la communication entre appareils. Par exemple, des solutions comme Gespage sont conçues pour fonctionner avec les algorithmes TLS les plus récents tout en maintenant la compatibilité avec les dispositifs qui n'ont pas encore été mis à jour. Cela garantit un équilibre optimal entre sécurité et fonctionnalité.

Recommandations :

- Planifiez des **vérifications régulières** des versions de firmware de tous vos appareils.
- Identifiez les imprimantes utilisant des protocoles obsolètes et **priorisez leur mise à jour.**
- Si possible, **automatisez** les processus de mise à jour pour minimiser les risques liés à des firmware obsolètes.

En suivant toutes ces bonnes pratiques, vous renforcerez la résilience de votre infrastructure d'impression face aux menaces émergentes tout en optimisant la compatibilité et les performances.

Avec Gespage, vous bénéficiez également d'un support technique dédié et d'une communauté active, garantissant une assistance rapide et efficace.

Par ailleurs, nous vous rappelons qu'il est primordial que vous vous rapprochiez de votre fournisseur d'imprimante et MFP lors de la mise en place de configurations spécifiques.

2.2 Sécurisation du réseau

Les imprimantes multifonctions nécessitent un accès au réseau pour communiquer avec Gespage ou recevoir les impressions. Toutefois, mal configurées, ces connexions peuvent ouvrir des failles dans votre infrastructure. Une gestion prudente des accès et des protocoles est essentielle pour garantir une sécurité optimale.

Isolation des appareils sur le réseau

Créez des sous-réseaux dédiés ou utilisez des VLAN pour isoler vos imprimantes des autres segments de votre infrastructure. Autorisez uniquement le serveur d'impression à communiquer avec les MFP. Ce contrôle peut être renforcé par des listes de contrôle d'accès (ACL) et des règles de filtrage IP. Ainsi, vous réduisez considérablement les possibilités d'exploitation en cas de compromission d'un appareil.

Le détail des flux réseaux utilisés entre Gespage et les imprimantes et MFP est disponible dans la **matrice des flux réseau Gespage** disponible sur la base de connaissance Gespage (lien).

Si cette mise en place n'est pas possible au niveau de votre configuration réseau, il est en général possible de restreindre l'impression à l'adresse IP du serveur d'impression au niveau du paramétrage de l'imprimante. Cette configuration est particulièrement recommandée en environnement payant.

Chiffrement des connexions réseau

Activez les connexions HTTPS sur vos imprimantes pour protéger les transmissions de données sensibles. Configurez vos appareils pour utiliser les dernières versions des protocoles TLS, qui offrent un haut niveau de sécurité. Les anciens standards doivent être désactivés car ils sont vulnérables aux attaques.

Par défaut, Gespage impose l'utilisation au minimum du protocole TLS 1.2 par les imprimantes et MFPs.

Utilisation de certificats pour sécuriser TLS

Pour prévenir les attaques de type "man-in-the-middle", configurez vos appareils pour qu'ils requièrent des certificats valides lors des connexions TLS. Si le risque est faible, un certificat auto-généré peut être suffisant tout en assurant le chiffrement des communications.

Selon le modèle de votre imprimante ou MFP, la mise en place d'un certificat nécessite des paramétrages complémentaires spécifiques au niveau de l'eTerminal Gespage. Les manuels et bases de connaissance Gespage documentent ces spécificités.

En combinant ces mesures, vous pouvez transformer votre infrastructure d'impression en un réseau résilient, capable de répondre aux besoins quotidiens tout en minimisant les risques liés à la sécurité.

2.3 Serveur d'impression Gespage On-Premise

Le serveur d'impression et le serveur applicatif Gespage (qui peuvent être hébergés sur un même serveur) sont des éléments stratégiques de votre infrastructure. Ils centralisent les ressources d'impression.

Mises à jour et protection du système

Il est essentiel que vos serveurs hébergeant le serveur d'application et le serveur applicatif Gespage soient sécurisés. Cette sécurité repose sur les meilleures pratiques IT. Cela inclut :

- **Mises à jour régulières du système d'exploitation** : Assurez-vous que le système d'exploitation soit à jour pour combler les vulnérabilités. Ces mises à jour doivent être effectuées en suivant les bonnes pratiques de sauvegarde préalable.

- **Antivirus et pare-feu** : Activez une protection en temps réel et configurez des pares-feux pour limiter les accès non autorisés.
- **Mises à jour régulières des pilotes d'imprimantes** : Assurez-vous régulièrement que les pilotes d'imprimantes soient à jour en vous rapprochant de votre fournisseur d'imprimantes pour connaitre les pilotes recommandés pour votre environnement
- **Accès administrateur sécurisé** : L'accès administrateur au système d'exploitation doit être strictement réservé aux membres habilités de l'équipe informatique en charge de l'administration du serveur.

Configuration réseau sécurisée

Grâce à Gespage, les serveurs d'impression peuvent être placés dans des sous-réseaux isolés et protégés par des pare-feu. Cela garantit que les adresses IP internes ne sont pas accessibles depuis l'extérieur. Gespage peut également limiter les communications entre le serveur et les imprimantes, réduisant ainsi la surface d'attaque.

Le détail complet des flux réseau utilisés par Gespage ainsi que par votre infrastructure (imprimantes, postes utilisateurs, etc.) est disponible dans la matrice des flux réseau, consultable sur la base de connaissances Gespage (lien).

Chiffrement de bout en bout

Toutes les communications réseaux avec l'application Gespage sont chiffrées via des protocoles sécurisés : aucune donnée ne circule en clair.

Gestion avancée des files d'impression et des droits d'accès

Avec Gespage, la gestion des droits sur les files d'impression est simplifiée :

- **Libération sécurisée des impressions** : Intégrez des fonctions de libération sécurisée après authentification des utilisateurs.
- **Contrôle des accès** : Configurez les permissions pour limiter les fonctions accessibles sur les imprimantes à leurs seuls besoins.
  - **Limitez l'accès** aux imprimantes utilisant des papiers à en-tête de l'entreprise.
  - **Configurez des groupes spécifiques** pour éviter tout abus ou accès non autorisé.

Gestion des mots de passe et accès administrateur personnalisé

Il est fortement recommandé de modifier le mot de passe administrateur Gespage par défaut après la mise en service, puis de le renouveler régulièrement, en respectant les bonnes pratiques en matière de sécurité (mot de passe complexe, unique et confidentiel).

Par ailleurs, l'activation d'identifiants administrateurs personnalisés est conseillée afin que chaque action soit tracée et associée à un utilisateur spécifique. Cette personnalisation permet notamment de créer un accès dédié pour un technicien externe intervenant ponctuellement en maintenance sur le serveur.

Enfin, il est possible de restreindre les droits d'administration par utilisateur, afin de limiter l'accès aux seules fonctionnalités nécessaires selon les responsabilités de chaque administrateur.

Maintenance et mises à jour de sécurité de Gespage

Cartadis fournit régulièrement des mises à jour de l'application Gespage. Ces mises à jour sont mises à disposition sous couvert du contrat de maintenance. Il est important de noter que l'utilisateur doit, à ses frais, télécharger et installer ces mises à jour dans un délai raisonnable.

Ces mises à jour sont essentielles pour corriger les vulnérabilités identifiées tout au long de la vie du produit.

Ces mises à jour doivent être effectuées en suivant les bonnes pratiques de sauvegarde préalable et en ayant lu attentivement les release notes au préalable. En effet, certaines mises à jour majeures peuvent nécessiter la fourniture d'une assistance par un technicien certifié Gespage.

Pour être informé des mises à jour Gespage, nous vous invitons à suivre les actualités publiées sur le site web Gespage ou contacter votre fournisseur de la solution Gespage (lien).

2.4 Serveur d'impression Gespage Stratus (Saas)

Gespage Stratus est la solution de gestion d'impression en mode Saas, hébergée dans un cloud privé sécurisé par Cartadis, conçue pour les petites et moyennes organisations.

Gespage Stratus est une application serveur mono-client, entièrement gérée par Cartadis.

Chaque instance dédiée garantit une sécurité renforcée et des performances optimales.

Localisation des données

Hébergement souverain et sécurisé : La solution est hébergée chez OVHcloud, assurant d'un point de vue de l'architecture, conformité RGPD et sécurité maximale pour les clients en France comme à l'étranger (normes ISO ISO/IEC 27001, 27017 et 27018 et SecNumCloud / Cloud de confiance).

Mises à jour et protection du système

Il est essentiel que vos postes utilisateurs ou serveurs hébergeant localement des services Gespage (Agent Gespage, Connecteur Gespage, etc.) soient sécurisés. Cette sécurité repose sur les meilleures pratiques IT. Cela inclut :

- **Mises à jour régulières du système d'exploitation** : Assurez-vous que le système d'exploitation soit à jour pour combler les vulnérabilités.
- **Antivirus et pare-feu** : Activez une protection en temps réel et configurez des pares-feux pour limiter les accès non autorisés.
- **Mises à jour régulières des pilotes d'imprimantes** : Assurez-vous régulièrement que les pilotes d'imprimantes soient à jour en vous rapprochant de votre fournisseur d'imprimantes pour connaitre les pilotes recommandés pour votre environnement

Configuration réseau sécurisée

Lors du déploiement de Gespage Stratus, il est possible de restreindre les ouvertures réseau aux seules communications strictement nécessaires au bon fonctionnement de la solution. Cette approche permet de réduire significativement la surface d'exposition aux attaques.

Le détail complet des flux réseau utilisés par Gespage Stratus ainsi que par votre infrastructure (imprimantes, postes utilisateurs, etc.) est disponible dans la matrice des flux réseau, consultable sur la base de connaissances Gespage (lien).

Chiffrement de bout en bout

Toutes les communications entre imprimantes, postes utilisateurs et le cloud sont chiffrées via des protocoles sécurisés : aucune donnée ne circule en clair.

Gestion avancée des files d'impression et des droits d'accès

Avec Gespage, la gestion des droits sur les files d'impression est simplifiée :

- **Libération sécurisée des impressions** : Intégrez des fonctions de libération sécurisée après authentification des utilisateurs.
- **Contrôle des accès** : Configurez les permissions pour limiter les fonctions accessibles sur les imprimantes à leurs seuls besoins.
    - **Limitez l'accès** aux imprimantes utilisant des papiers à en-tête de l'entreprise.
    - **Configurez des groupes spécifiques** pour éviter tout abus ou accès non autorisé.

Gestion des mots de passe et accès administrateur personnalisé

Il est fortement recommandé de modifier le mot de passe administrateur Gespage par défaut après la mise en service, puis de le renouveler régulièrement, en

respectant les bonnes pratiques en matière de sécurité (mot de passe complexe, unique et confidentiel).

Par ailleurs, l'activation d'identifiants administrateurs personnalisés est conseillée afin que chaque action soit tracée et associée à un utilisateur spécifique. Cette personnalisation permet notamment de créer un accès dédié pour un technicien externe intervenant ponctuellement en maintenance sur le serveur.

Enfin, il est possible de restreindre les droits d'administration par utilisateur, afin de limiter l'accès aux seules fonctionnalités nécessaires selon les responsabilités de chaque administrateur.

Maintenance et mises à jour de sécurité de Gespage

L'application Gespage Stratus est mise à jour régulièrement à la dernière version applicative. Cartadis se charge des mises à jour pendant des créneaux de maintenance de courte durée.

3. Modèle de sécurité de Gespage : Un cadre en trois phases

Dans un environnement où la sécurité des données est une priorité, la gestion des impressions doit intégrer des mesures rigoureuses pour protéger les informations sensibles et garantir une conformité optimale. **Gespage**, une solution de gestion d'impression de pointe, est conçue pour répondre à ces exigences tout en optimisant vos processus d'impression.

3.1 Sécurisation de l'infrastructure d'impression

Protégez vos communications et vos données

Avec Gespage, toutes les transmissions entre composants, comme les serveurs, les interfaces d'administration, et les imprimantes, sont sécurisées grâce au protocole **HTTPS**. Cette approche garantit que les informations sensibles, telles que les documents imprimés ou les identifiants, restent protégées contre les interceptions.

En ce qui concerne les données stockées, Gespage permet une gestion flexible en utilisant des bases de données compatibles avec vos standards internes, tout en prenant en charge des sauvegardes régulières pour éviter toute perte.

Fonctionnalités avancées pour une sécurité optimale

Gespage intègre des mesures de sécurité robustes pour répondre aux défis actuels :

- **Isolation des processus** : Gespage fonctionne dans des processus isolés pour minimiser les interactions avec le noyau du système. Cela garantit que les tâches critiques ne nécessitent pas d'autorisations excessives, comme l'accès administrateur.

- **APIs sécurisées** : Les appels aux API publiques de Gespage sont protégés par des jetons d'authentification, garantissant une communication fiable et contrôlée.
- **Pages web sécurisées** : Gespage protège ses interfaces contre les attaques telles que l'injection SQL, la falsification de requêtes intersites (CSRF), et le cross-site scripting (XSS).
- **Authentification via services d'annuaire** : Gespage s'intègre aux services comme LDAP, Active Directory, et Entra ID pour authentifier les utilisateurs, évitant ainsi de stocker directement les mots de passe. Les comptes locaux, comme ceux pour l'impression des invités, sont protégés par un chiffrement robuste.

Conformité RGPD avec Gespage

Gespage respecte les normes européennes de protection des données en garantissant que les informations personnelles sont traitées avec le plus haut niveau de confidentialité. Cela comprend la gestion des droits d'accès, le chiffrement des données, et des politiques paramétrables pour leur suppression lorsque cela est nécessaire.

Maintenir un système d'impression sécurisé avec Gespage

Une infrastructure d'impression fiable et sécurisée repose sur l'adoption de bonnes pratiques IT :

- **Audits réguliers** : Effectuez des vérifications périodiques pour identifier les vulnérabilités potentielles.
- **Sauvegardes automatisées**
    - Dans le cas d'un serveur Gespage On-Premise, assurez-vous que les bases de données Gespage soient sauvegardées régulièrement sur un serveur externe sécurisé pour éviter toute perte de données.
    - Dans le cas d'un serveur Gespage Stratus, la sauvegarde automatisée est gérée par Cartadis
- **Mises à jour et correctifs** : Maintenez votre solution Gespage à jour pour bénéficier des derniers correctifs de sécurité.
- **Plan de reprise après sinistre** : Testez régulièrement votre plan de reprise pour garantir la continuité en cas d'incident.

Avec ses fonctionnalités avancées et son accent sur la sécurité, Gespage est bien plus qu'un outil de gestion d'impression : c'est une solution stratégique pour protéger vos données et optimiser vos opérations d'impression.

3.2 Sécurisation des flux d'impression

Dans de nombreux environnements d'impression traditionnels, les travaux sont envoyés directement aux imprimantes pour être immédiatement traités. Cependant, une grande partie de ces impressions est souvent abandonnée, créant non seulement des déchets inutiles, mais également des risques pour la confidentialité lorsque des documents sensibles sont laissés sans surveillance.

Avec Gespage, la fonctionnalité de libération sécurisée des impressions garantit que les travaux restent en attente dans une file jusqu'à ce que l'utilisateur s'authentifie physiquement sur l'imprimante pour les libérer. Cette approche offre plusieurs avantages :

- **Confidentialité renforcée** : Les documents sensibles ne sont imprimés que lorsque l'utilisateur est présent pour les récupérer.
- **Réduction des impressions inutiles** : Les travaux non nécessaires ne sont jamais imprimés, ce qui permet d'économiser du papier et de l'encre.
- **Sécurité accrue** : Les documents sensibles ne restent jamais exposés sur les imprimantes.

Paramétrage de la durée de rétention des impressions

Les impressions abandonnées ne sont pas le seul risque : les impressions en attente sur le serveur peuvent aussi être consultés par des personnes malveillantes si la sécurité n'est pas assurée.

Même si les mesures décrites dans la section « Sécurisation bas niveau de l'infrastructure complète » permettent de limiter ce risque, il est recommandé de supprimer automatiquement les travaux d'impression restés trop longtemps en file d'attente.

Cela permet de protéger les données sensibles et d'alléger la charge du serveur d'impression,

Avec Gespage, vous pouvez définir combien de temps un travail d'impression reste en attente avant d'être automatiquement supprimé.

Impression Print2Me avec Gespage

Pour encore plus de flexibilité, Gespage intègre l'impression Print2Me, une solution mobile qui permet aux utilisateurs d'envoyer leurs travaux dans une file d'attente unique et de les récupérer sur n'importe quelle imprimante du réseau. En s'authentifiant via des méthodes telles que le badge RFID (*sur un lecteur de cartes type Cartadis TCM4*) ou un code d'impression, les utilisateurs peuvent facilement récupérer leurs travaux d'impression vers l'appareil de leur choix.

Pourquoi choisir Gespage pour vos impressions sécurisées ?

Gespage ne se limite pas à offrir des fonctionnalités de base. Son interface intuitive et ses capacités avancées, comme la gestion centralisée et le suivi détaillé des

impressions, font de cette solution un choix stratégique pour optimiser vos flux d'impression tout en assurant une sécurité maximale.

En intégrant des fonctionnalités comme la libération sécurisée et l'impression Print2Me, Gespage aide les entreprises à réduire leurs coûts, améliorer la confidentialité des documents et simplifier la gestion des ressources d'impression.

3.3 Sécurisation des sorties imprimées

Avec Gespage, vous pouvez sécuriser vos impressions tout en garantissant une traçabilité complète grâce à des fonctionnalités avancées comme la gestion des journaux ou les filigranes.

Suivi avancé des impressions avec Gespage

Gespage enregistre chaque détail des travaux d'impression :

- Qui a imprimé (nom d'utilisateur).
- Qu'est-ce qui a été imprimé (nom du document).
- Quand et où (heure, imprimante utilisée).

Ces journaux détaillés sont accessibles via une interface intuitive, permettant aux administrateurs de détecter les comportements inhabituels et de garantir la transparence des activités d'impression. De plus, Gespage offre des rapports programmés qui peuvent être envoyés automatiquement pour assurer un suivi constant.

Filigranes intégrés

Gespage propose des filigranes personnalisés, affichant des informations comme le nom de l'utilisateur ou la date d'impression, directement sur le document. Cette fonctionnalité agit comme un rappel visuel que chaque document est traçable.

Suivi des modifications de configuration Gespage

Gespage met à disposition un journal d'évènement très détaillé qui permet de suivre toutes les modifications de configuration effectuées, et l'identifiant de l'administrateur les ayant effectuées.

Il est également possible de s'abonner à une alerte email administrateur sur certains de ces évènements.

4. Conformité aux réglementations internationales

4.1 Protection des données et conformité RGPD

Le règlement (UE) n° 2016/679, dit **Règlement Général sur la Protection des Données (RGPD)**, constitue le texte de référence européen en matière de protection des données à caractère personnel. Il renforce et unifie la protection des données pour les individus au sein de l'Union européenne. Entré en vigueur le **25 mai 2018**, il s'applique à toute organisation collectant ou traitant des données personnelles de résidents de l'Union européenne, qu'elle soit située au sein ou en dehors de l'UE.

Le RGPD a pour objectif principal de restituer aux citoyens et résidents le contrôle sur leurs données personnelles tout en simplifiant l'environnement réglementaire pour les entreprises opérant à l'international grâce à une réglementation unifiée. Il encadre également l'exportation de données personnelles en dehors de l'Union européenne.

Pour être conforme au RGPD, les organisations doivent respecter plusieurs exigences:

- **Sécurisation des systèmes IT** : Assurer la protection des données personnelles contre tout accès non autorisé.
- **Respect des droits des personnes concernées** : Offrir aux individus la possibilité d'accéder à leurs données, de corriger des informations erronées ou d'exiger leur suppression (droit à l'oubli).
- **Consentement éclairé** : Obtenir un consentement explicite avant toute collecte ou traitement de données.
- **Conception sécurisée** : Mettre en place des systèmes conformes dès leur conception (principe de "privacy by design").

Ces exigences s'appliquent également aux **systèmes d'impression**. Un système d'impression non sécurisé peut représenter un point de vulnérabilité majeur pour une organisation, permettant l'accès non autorisé à des données sensibles ou la perte de documents. Par exemple :

- **Documents imprimés abandonnés** sur les imprimantes.
- **Données stockées sur les disques durs des MFPs** ou dans les files d'attente d'impression des serveurs.

Un système conforme au RGPD doit donc inclure des fonctionnalités de traçabilité, d'authentification sécurisée et de gestion des droits d'accès pour minimiser ces risques.

4.2 La conformité de solution Gespage

Gespage permet de répondre à la directive Européenne RGPD.

Les fonctionnalités suivantes de Gespage permettent cette mise en sécurité :

• La gestion de l'impression est sécurisée. La sécurisation du système d'impression passe par la sécurisation de bout en bout du flux d'impression (à partir du moment où l'utilisateur envoie son job d'impression jusqu'à l'impression du document sur le point d'impression)

• L'authentification et la libération « en pied de machine » (Print2me) évitent les impressions « orphelines » et donc la perte de documents imprimés. Les documents ne sont imprimés qu'au moment où l'utilisateur se présente devant l'imprimante et s'authentifie.

• La purge automatique des « spools » d'impression non imprimés évite également les données perdues.

• Les « spools » d'impression restent en attente sur le serveur d'impression et ne s'enregistrent pas sur le Disque Dur du Multifonction.

• L'information des utilisateurs est disponible immédiatement par l'exportation de données. Une personne peut donc facilement demander et obtenir l'accès à l'ensemble des informations la concernant.

• Les informations d'un utilisateur se suppriment automatiquement (synchronisation d'annuaire) lorsqu'il quitte la structure. Seul l'historique des impressions reste sauvegardé pour le calcul des statistiques.

• Possibilité d'anonymiser les noms d'utilisateurs : Un paramètre est disponible dans l'administration de Gespage pour demander automatiquement l'anonymisation des noms d'utilisateurs, de manière systématique ou après le départ d'un collaborateur. Les personnes disposent donc d'un droit à l'oubli pour les informations les concernant.

• Possibilité de masquer les noms de documents dans les files d'attente d'impression : Gespage offre une option permettant de masquer les titres des documents dans les files d'attente, renforçant ainsi la confidentialité des informations sensibles avant même l'impression.

5. Bonnes pratiques pour intégrer Gespage dans votre organisation

Il est important de bien définir dès le commencement une bonne politique d'impression pour optimiser au mieux le parc machines et afin d'améliorer la qualité de service envers vos utilisateurs.

Lorsque vous souhaitez mettre en place des règles restrictives (limitation des crédits utilisateurs, forçages d'impression en noir et blanc, etc.), nous vous conseillons d'utiliser durant les deux premiers mois Gespage en mode observation. A la fin de cette période d'analyse, il sera alors plus aisé d'opter pour la bonne politique d'impression.

L'emplacement des imprimantes/MFP pourra être revu pour optimiser le taux de fonctionnement de votre parc. De plus les règles de redirection seront mises en place pour favoriser une utilisation de qualité pour votre parc.

Un déploiement favorisant la mise en sécurité de l'infrastructure d'impression se résume sur ces trois points :

- Analyse des volumes d'impression précédents et identification des risques.
- Déploiement par étapes pour minimiser les interruptions.
- Sessions de formation pour garantir une adoption sécuritaire.

6. Conclusion : Un outil stratégique pour l'avenir de votre infrastructure d'impression

Gespage n'est pas seulement une solution logicielle : c'est un levier stratégique pour améliorer la sécurité, réduire les coûts, et aligner votre infrastructure sur les normes actuelles.

La sécurité de l'environnement d'impression est donc une responsabilité partagée, la compréhension du **Contrat de Licence Utilisateur Final** est essentielle pour une utilisation conforme et sécurisée de Gespage.

Mail : support@cartadis.com
1 av. Louison Bobet, 94120 Fontenay-sous-Bois, FRANCE