



## 7 étapes pour sécuriser vos impressions



### 1. Impliquez la Direction

Étant donné les exigences strictes du RGPD et l'ampleur des dégâts causés par les cyberattaques ou les violations de données, la sécurité de l'impression ne relève plus uniquement du service informatique, mais doit être abordée d'un point de vue stratégique au niveau de la Direction, avec implication du DSI et du responsable de la sécurité des systèmes d'information.



### 2. Menez des audits rigoureux

Les entreprises doivent impérativement identifier toutes les failles de sécurité potentielles dans leur environnement d'impression en contrôlant régulièrement ce dernier dans le cadre d'audits de sécurité. Ce point est particulièrement important si votre société dispose d'équipements nouveaux et anciens. En matière de gestion déléguée des impressions (MPS), la plupart des fournisseurs proposent non seulement une évaluation approfondie, mais aussi un suivi continu des appareils une fois que le parc a été optimisé et sécurisé.



### 3. Modifiez les mots de passe administrateur prédéfinis

Les mots de passe administrateur par défaut ou prédéfinis constituent l'un des points faibles des imprimantes, mais ce problème est heureusement facile à résoudre. Une fois le périphérique installé, il vous suffit de choisir un nouveau mot de passe robuste.



### 4. Mettez à jour vos micrologiciels et installez les correctifs

Vous pouvez réduire considérablement les failles de sécurité potentielles de vos imprimantes en mettant à jour leurs micrologiciels et en activant les mises à jour automatiques. Contactez le fabricant de vos imprimantes pour toute question à ce sujet.



### 5. Sécurisez les tâches d'impression

Vous devez protéger non seulement vos imprimantes, mais aussi les documents envoyés à l'impression. Le chiffrement de bout en bout du trafic réseau garantit un transfert sécurisé des tâches d'impression vers les imprimantes. Étant donné que la plupart des imprimantes stockent temporairement les tâches d'impression, assurez-vous que les données sont chiffrées.



### 6. Monitorer vos périphériques

Bénéficiez d'une vue globale sur votre environnement d'impression en suivant l'état actuel de vos imprimantes. En utilisant des outils logiciels pour surveiller leurs appareils, les entreprises peuvent résoudre les problèmes au plus vite. Les équipements génèrent une quantité importante de données pouvant souvent être utilisées pour identifier d'éventuels événements de sécurité, ce qui permet de répondre rapidement aux attaques. Les utilisateurs de solutions MPS peuvent également obtenir régulièrement des rapports de conformité incluant la surveillance et le signalement des violations de données.



### 7. Formez vos collaborateurs

De nombreuses pertes de données sont non intentionnelles : selon Quocirca, 32 % des incidents de sécurité liés à l'impression sont causés par des actions accidentelles des utilisateurs. Il est donc essentiel que les entreprises sensibilisent leurs collaborateurs à l'importance de protéger les informations sensibles et aux menaces malveillantes. Les prestataires de solutions MPS peuvent aider les sociétés à répondre à leurs besoins en formation.

## Méthodologie de l'enquête

Quocirca a réalisé une enquête en ligne auprès de 250 TPE, PME et grandes entreprises au Royaume-Uni, en France, en Allemagne et aux États-Unis en décembre 2018.