Sécuriser les flux documentaires grâce au format PDF

Création, édition et archivage sécurisés de documents

La gestion d'importants volumes de documentation est inhérente à la vie de toutes les sociétés. Mais lorsque des documents sensibles tombent entre de mauvaises mains, une entreprise s'expose à des problèmes majeurs qui peuvent, dans les cas les plus graves, provoquer sa disparition. Le format PDF offre un cadre sécuritaire qui assure une gestion fiable des flux de documents, de leur création à leur archivage ou à leur suppression, en passant par leur édition.

NUANCE

Table des matières

Présentation

Une récente étude menée par Ponemon Institute a révélé que la perte de données sensibles avait coûté aux entreprises plus de 3,4 millions d'euros au cours des deux dernières années. Mais en plus des pertes financières, les entreprises risquent de voir leur réputation entachée – et de perdre grand nombre de leurs clients – lorsque leurs informations internes tombent entre de mauvaises mains. Et les conséquences peuvent être désastreuses en cas de non-respect de leurs obligations légales ; les tribunaux n'hésitant pas à infliger de lourdes sanctions aux entreprises et à leurs dirigeants. Il paraît illusoire de vouloir assurer une surveillance permanente de l'ensemble des documents qu'une compagnie produit, distribue, manipule et stocke au cours de ses activités. Une fois des documents imprimés et distribués, il devient totalement impossible d'en suivre le cheminement. Toutefois, une gestion électronique des documents, basée sur le format PDF, offre une alternative judicieuse, tant en termes d'efficacité que de sécurité. Différentes solutions PDF intègrent des fonctions de protection qui peuvent être combinées à d'autres outils pour mettre en place un environnement sécurisé. Par exemple, le format PDF autorise des mots de passe couplés à un chiffrement, ainsi que la définition de droits d'accès définissant les actions que les utilisateurs peuvent réaliser sur des fichiers.

Ce livre blanc explique comment le format PDF et la solution Power PDF de Nuance permettent de mettre en place, rapidement, efficacement et à moindre coût, des flux qui garantissent l'intégrité de vos documents tout au long de leur cycle de vie.

Vos documents : un risque pour votre sécurité

Il devient de plus en plus difficile pour les entreprises d'assurer la protection de leurs données, particulièrement à une époque où les employés réclament toujours plus de mobilité. Les équipes passent en effet toujours plus de temps en dehors de leur bureau, accédant à leurs documents de travail depuis les quatre coins du monde, souvent à l'aide de leurs périphériques personnels. Cette tendance de fond, dénommée BYOD (pour « Bring your own Device » - « Apportez vos appareils personnels ») pose de réels problèmes de sécurité. Ces risques ont été soulignés par une étude menée par Ponemon Institute en 2014, auprès de 2.300 professionnels de l'informatique et de la sécurité, dans 18 secteurs d'activité et huit pays. Pour 58 pour cent des personnes interrogées, l'utilisation de périphériques personnels présente des risques pour la sécurité. Les experts estiment en effet que ces périphériques limitent l'efficacité des initiatives de protection de données, et entravent la mise en place de politiques de sécurité. Une mobilité accrue et le recours au Cloud pour stocker et échanger des données facilitent et accélèrent la distribution et l'exploitation de documents.

Mais cette indispensable flexibilité fait peser un risque accru sur la sécurité des données. En cas d'erreur d'impression ou de distribution, des documents peuvent finir entre de mauvaises mains, ou être supprimés accidentellement ou délibérément par des employés négligents ou mal intentionnés. La fuite à la concurrence de projets de développement, de devis, de contrats ou d'informations confidentielles porte un préjudice évident à une entreprise. Mais la perte et le vol de données peuvent également nuire gravement à son image et à sa réputation, ou l'exposer à de lourdes sanctions pénales et financières. De nombreuses réglementations (notamment plusieurs directives européennes sur la vie privée et la conservation des données, et la loi française « Informatique, fichiers et liberté ») prévoient des amendes, voire des peines de prison, en cas de manquement aux obligations de protection des données personnelles d'usagers et de consommateurs.

Mais les données ne gagnent pas seulement en accessibilité. Elles sont diffusées toujours plus rapidement, et s'accumulent à un rythme vertigineux. Près de 90 % des sociétés allemandes ayant participé à une étude menée en 2014 par Bitkom (l'association allemande des acteurs de l'économie numérique) ont déclaré que le volume de données qu'elles produisaient était en progression par rapport à l'année précédente (hausse de 22 %, en moyenne). En pratique, des sociétés qui disposaient l'année passée d'un pétaoctet de données devront ajouter 220 To de d'espace complémentaire. Et selon la technologie choisie (disques durs traditionnels ou support flash), les investissements nécessaires au stockage de ces données s'élèvent à des dizaines, voire des centaines de milliers d'euros. Mais il n'y a pas que les dépenses en matériels qui explosent. La protection de ces informations contre une utilisation non autorisée, qu'elle soit interne ou externe, demande des moyens croissants. Et comme l'indique le rapport annuel « Cost of Data Breach » (Le coût des fuites de données) publié par Ponemon Institute, les conséquences des pertes de données sont de plus en plus lourdes. Celui-ci a montré qu'en l'espace de deux ans, le préjudice subi par les entreprises suite à la perte de données avait augmenté de 23 %, pour culminer à 3,4 millions d'euros. Derrière les États-Unis, l'Allemagne occupe la deuxième position au classement des pays où la perte d'un document est la plus coûteuse (190 euros par document, en moyenne). Et ce chiffre ne couvre pas les coûts indirects en matière d'altération de l'image de marque. Selon Ponemon, environ 3 % des consommateurs allemands disent ne plus vouloir traiter avec une entreprise qui connaît un incident impliquant la perte de données. Et ce risque de perte de clientèle est d'autant plus fort dans les secteurs de la santé, de la pharmacie et des services financiers. Le rapport de Ponemon indique également qu'entre 2014 et 2015, la perte de revenus causée par de tels incidents avait augmenté de près de 8 %, pour atteindre environ 1,4 million d'euros.

L'étude « Wirtschaftskriminalität in Deutschland » (Criminalité en cols blancs en Allemagne) menée par KPMG indique que les entreprises allemandes ont clairement conscience de ce danger. 87 % des participants à cette étude estiment que leur entreprise est exposée à un risque « élevé » ou « très élevé » de pertes ou de fuites de données. 34 % avouent avoir déjà subi des pertes supérieures ou égales à 300.000 euros, et pour 35 %, les coûts d'investigation et de correction de ces incidents se sont élevés à 75.000 euros ou plus.

Et contrairement aux idées reçues, les documents papier n'offrent pas plus de sécurité que leurs homologues électroniques, bien au contraire. Dès qu'un document a quitté le bac de collecte d'une imprimante, la route qu'il emprunte devient impossible à suivre. Plus personne n'est en mesure de savoir qui le lit, et qui en fait des copies. Et les déconvenues risquent de se multiplier lors du transport ou de la mise au rebut de documents.

Mais les pertes financières ne sont pas la seule conséquence grave d'une fuite de données. Toute société qui ne pourrait pas prouver qu'elle a pris toutes les mesures pour protéger ses données ou que sa responsabilité ou sa négligence ne sont pas engagées en cas de perte ou de vol de ces données s'exposerait à de lourdes sanctions juridiques.

La gestion de documents contenant des données à caractère personnel est réglementée par différents textes, dont la loi française « Informatique et libertés » et la directive européenne 95/46/EC. En Europe, chaque pays dispose de son arsenal de règlements régissant la collecte, le traitement et la diffusion des données d'usagers ou de clients. Ces textes visent à garantir que toute opération de consultation, de modification et de distribution d'informations peut être enregistrée et retracée.

Le rôle du format PDF dans la sécurisation des flux documentaires

Même s'il est en principe plus facile d'assurer le contrôle de fichiers numériques que de documents imprimés, les formats numériques représentent toujours un risque de sécurité pour les entreprises. Comme le montre l'étude citée précédemment, la sécurité documentaire est un composant essentiel que les entreprises doivent placer au cœur d'une stratégie de sécurité globale. Selon cette étude, 72 % des experts interrogés déclarent qu'un environnement documentaire sécurisé contribue à garantir la confidentialité, l'intégrité, l'authenticité, l'accessibilité, la disponibilité et la facilité d'exploitation des données.

Le format PDF est devenu le standard incontesté pour la diffusion et l'archivage de documents. En vous dotant d'une solution PDF complète, vous pouvez protéger vos documents en définissant des paramètres de protection, qui représentent un aspect important selon les participants à l'étude Ponemon. Avec un score moyen de 1,65 (sur une échelle de 1 à 4, allant du facteur le plus important au moins important), l'utilisation de techniques de protection de documents paraît plus essentielle que la formation et la sensibilisation des employés, que la destruction sécurisée des documents ou que la conformité réglementaire.

En pratique, les PDF peuvent être protégés à différents niveaux :

Protection par mot de passe, pour limiter la consultation et l'édition de PDF

Une solution PDF doit offrir différents niveaux d'autorisation pour la création, l'édition, l'enregistrement, l'impression ou la consultation du PDF. L'idéal est de pouvoir définir ces droits individuellement, pour chaque fichier (manuellement ou à l'aide de profils de sécurité prédéfinis) ou par la définition de rôles et de groupes d'utilisateurs dans des systèmes tels qu'Active Directory Rights Management de Microsoft.

Dans le cadre d'une protection par mot de passe, deux options sont possibles :

Autorisation d'ouverture – Lorsqu'un PDF est protégé par mot de passe (et surtout si ce mot de passe est couplé à un chiffrement), il bénéficie d'une bonne protection contre des consultations non autorisées.

Autorisation d'édition – Même si le format PDF a été à l'origine conçu pour l'échange de documents, il autorise toutefois les modifications. Les solutions PDF professionnelles comme Power PDF permettent à leurs utilisateurs d'apporter facilement des modifications aux textes, images et mises en page de PDF. Pour interdire ces modifications, vous pouvez définir un mot de passe complémentaire, dit « de permissions », qui vous permettra notamment de déterminer si :

- Votre document peut être imprimé et si oui, à quelle résolution.
- des pages peuvent être supprimées, ajoutées, insérées ou pivotées ;
- vos destinataires seront autorisés à remplir des formulaires et apposer leur signature numérique dans les champs correspondants ;
- vos destinataires seront autorisés à ajouter des commentaires.

La protection contre l'ouverture n'est pertinente que si vous avez clairement identifié les destinataires qui sont autorisés à consulter votre document. En pratique, si vous envoyez un document confidentiel par e-mail sans chiffrement PGP ou S/MIME, quiconque aura accès à votre message pourra consulter votre document. En revanche, si votre document est protégé par un mot de passe d'ouverture, seules les personnes à qui vous aurez communiqué le mot de passe (par téléphone ou par SMS, par exemple) pourront le consulter.

Les mots de passe de permissions jouent un rôle complémentaire lorsque vous devez collaborer avec des partenaires internes ou externes, ou avec des clients. Si vous supervisez un projet, vous pourrez par exemple souhaiter que les membres de votre équipe puissent consulter, imprimer et annoter vos documents de travail, mais pas y ajouter ou en supprimer des pages. Et si vous envoyez un contrat à un client, vous pourrez faire en sorte que celui-ci puisse uniquement remplir des champs de formulaire et signer le document, mais pas en modifier le contenu.

Intégration à un SGD, pour une protection au niveau d'un groupe ou d'un projet

La mise en place de flux documentaires standardisés permet aux entreprises de se protéger contre les risques financiers et juridiques, et de bénéficier d'une base stable pour un suivi précis. Mais il ne s'agit pas là des seuls avantages. Les sociétés qui ont l'habitude de classer et d'archiver leurs documents de manière organisée ont un avantage indéniable sur leurs concurrents. Par exemple, un atelier de fabrication pourra suivre plus facilement et précisément les modifications apportées à ses produits, un cabinet d'architecture pourra accéder à des plans et les retravailler à tout moment, et un avocat pourra consulter en quelques clics l'ensemble des pièces d'un cas sur lequel il travaille. En outre, le travail en équipe est grandement facilité, car chaque collaborateur peut savoir qui a créé ou modifié un document, et à quel moment. Et le contrôle des versions permet d'annuler des modifications non pertinentes, et d'évaluer facilement l'impact des différentes versions d'un document.

À une époque où les PDF jouent un rôle toujours plus important, il paraîtrait judicieux qu'une entreprise puisse intégrer sa solution PDF à son système de gestion documentaire existant, tel que HP WorkSite, Microsoft SharePoint ou OpenText eDocs. Cette intégration se fait généralement par l'utilisation de connecteurs qui permettent l'ouverture directe de fichiers depuis ces systèmes. Lors de ces échanges, il devrait être possible de convertir en PDF des fichiers aux formats d'applications comme Microsoft Office ou WordPerfect, des images ou des fichiers XPS (le format d'échange XML de Microsoft), et de convertir directement des PDF dans des formats éditables.

Bien évidemment, une solution PDF doit également fonctionner dans le sens inverse, et permettre l'enregistrement de fichiers vers ces systèmes. Elle doit également permettre l'intégration de documents au SGD, et la création directe de PDF en dehors et au sein même du SGD. En pratique, l'utilisateur doit pouvoir :

- Sélectionner au sein de l'interface du SGD un fichier qui n'est pas au format PDF, et le convertir au format PDF sans quitter le SGD. Le fichier source reste inchangé. Le PDF prend le nom du fichier source et est enregistré par défaut dans le même dossier.
- Sélectionner sur son ordinateur un fichier qui n'est pas au format PDF, le convertir en PDF et l'enregistrer dans le SGD, dans le dossier en cours ou à un emplacement défini.

Dans les deux cas, la conversion se fait sans qu'il soit nécessaire de définir des paramètres additionnels.

Création de PDF protégés depuis Microsoft Office

Lorsqu'ils créent des PDF, les utilisateurs doivent être en mesure de définir leurs paramètres de protection directement depuis leur application Microsoft Office. Au moment d'enregistrer un courrier, par exemple, un directeur commercial pourra indiquer que son destinataire pourra imprimer, mais pas éditer le document.

Une solution PDF doit permettre d'ajouter des mots de passe (d'ouverture et de permissions) aux PDF générés depuis Microsoft Office, mais également d'interdire certaines actions telles que l'impression, l'extraction de contenu ou l'édition. Lors de la définition de droits, des profils de paramètres prédéfinis peuvent aider à répondre rapidement aux cas de figure les plus courants, et d'appliquer les paramètres appropriés selon qu'un document est partagé avec un collègue, envoyé à un partenaire externe, ou diffusé au grand public.

Algorithme de cryptage

Pour interdire totalement la consultation de fichiers par des personnes non autorisées, il convient de leur appliquer un cryptage. En pratique, une solution PDF doit prendre en charge le standard AES (Advanced Encryption Standard) avec une longueur de clé de 256 bits, un algorithme de cryptage défini par le NIST (American National Institute of Standards and Technology) et utilisé mondialement. Les fichiers doivent également pouvoir être chiffrés selon les standards définis par RSA Security.

Mais même avec les plus hauts niveaux de sécurité, des problèmes peuvent survenir, car le cryptage pourra ne pas être reconnu par les applications PDF les plus anciennes. C'est pourquoi la solution retenue doit prendre en charge des standards plus anciens, qui sont certes moins sécurisés, mais compatibles avec d'anciens logiciels. Idéalement, l'utilisateur doit avoir le choix entre les options suivantes :

- Cryptage RC4 40 bits – Prise en charge par les versions 1.1 et ultérieures du format PDF (révision de sécurité n°2)
- Cryptage RC4 128 bits – Prise en charge par les versions 1.4 et ultérieures du format PDF (révision de sécurité n°3)
- Cryptage AES 128 bits – Prise en charge par les versions 1.6 et ultérieures du format PDF (révision de sécurité n°3)
- Cryptage AES 256 bits – Prise en charge par les versions 1.7 et ultérieures du format PDF (révision de sécurité n°3)

Suppression définitive d'informations confidentielles d'un PDF

Il est impératif d'effacer les données personnelles ou confidentielles que contiennent vos documents avant de les diffuser. Ce procédé porte le nom de « biffure ». Mais il ne suffit pas de placer un cadre noir sur les informations que vous souhaitez masquer, car celles-ci figureront toujours dans le document et pourront facilement être récupérées par un utilisateur aguerri. Ces informations doivent être masquées et supprimées de manière totale et irréversible. Les biffures sont couramment utilisées par l'administration et les organismes publics, que la loi oblige à protéger les données personnelles de leurs usagers, et à informer ceux-ci que des sections des documents qu'ils consultent ont été biffées.

De la même manière, toutes les entreprises privées qui manipulent des données personnelles doivent en assurer la protection pour éviter qu'elles ne soient transmises à des tiers. Ces données peuvent comprendre des numéros de sécurité sociale ou de cartes bancaires, des adresses e-mail, des dates de naissance, ou des informations personnelles concernant les convictions religieuses ou politiques, ou l'orientation sexuelle. Une solution PDF doit donc permettre de supprimer définitivement ces informations, manuellement ou automatiquement, et d'une manière qui peut faire l'objet d'un suivi. Mais en plus de ces informations directement visibles, le programme doit également être en mesure d'effacer les métadonnées associées, qui sont souvent masquées.

Idéalement, il doit permettre de traiter aussi bien des PDF individuels que des lots, des porte-documents ou des répertoires complets. En complément, des masques de recherche pourront s'avérer très utiles pour rechercher et biffer automatiquement des informations répondant à un format standard, tels que numéros de carte bancaire, des numéros de téléphone ou des adresses e-mail. Mais quelle que soit la technique utilisée, l'utilisateur devra toujours parcourir son document pour s'assurer que toutes les informations sensibles ont bien été masquées, particulièrement sur les pages constituées d'images.

Comparaison de deux versions d'un document

Une solution PDF doit permettre de comparer deux versions d'un document, afin d'aider l'utilisateur à savoir rapidement si des corrections ont été apportées à son fichier, ou si celui-ci a été manipulé à son insu. Et la comparaison doit permettre d'afficher distinctement les modifications apportées aux textes, aux objets et aux graphiques. Le programme doit pouvoir fournir les informations de comparaison suivantes :

- Nombre de mots ajoutés ou supprimés, et nombre de mots inchangés
- Nombre de mots présentant uniquement des différences de mise en forme
- Nombre de pages identiques
- Nombre de pages présentant des différences
- Nombre de pages ajoutées ou supprimées

En cas de différences entre les documents, leurs pages doivent pouvoir être affichées côte à côte pour être inspectées rapidement, et les différences doivent être clairement visibles. Par exemple, les mots supprimés doivent être barrés, ceux ajoutés soulignés, et les graphiques modifiés entourés, etc. Pour les besoins de la comparaison, des pages blanches sont ajoutées au document le plus court pour que les deux documents aient le même nombre de pages.

Signatures couplées à des certificats

Les documents peuvent être signés à l'aide d'une identité numérique, ce qui équivaut à une signature manuscrite sur un document papier. Dès lors que des modifications non autorisées ont été apportées à un document après qu'il ait été signé, sa signature numérique devient « non valide ». Un document peut être signé plusieurs fois, et par des personnes différentes. Au moment de choisir une solution PDF, préférez une application qui permet non seulement de signer numériquement vos documents, mais également d'y apposer un « tampon horodaté » authentifié numériquement. Un tel tampon établit l'existence d'un contenu donné à une date et à une heure précises, et permet de garantir que ce contenu n'a pas été modifié depuis. En général, les tampons horodatés émanent d'une autorité tierce et s'accompagnent d'un certificat approuvé par cette autorité.

Mais en plus de l'authentification des documents, une identité numérique permet également de les protéger. Ce procédé, connu sous le nom de « certification », permet au propriétaire d'un document d'y appliquer en une opération une signature et une protection. Il pourra verrouiller complètement le document, ou autoriser uniquement certaines actions, comme le remplissage de formulaires ou l'ajout de commentaires. De nombreuses organisations ont recours à cette fonctionnalité avant de distribuer des documents officiels.

Au moment de créer votre signature numérique, vous pouvez choisir entre l'utilisation d'une ID numérique existante ou la création de votre propre identité. Chaque ID numérique comprend une « clé privée » et une « clé publique ». Pour permettre à d'autres utilisateurs de vérifier l'authenticité de votre signature et l'intégrité de votre document, vous devrez leur envoyer votre clé publique, qu'ils pourront stocker dans leur magasin d'identités approuvées.

Six bonnes raisons d'utiliser Nuance Power PDF

Nuance Power PDF regroupe au sein d'une interface conviviale l'ensemble des outils de sécurité pour la création, la diffusion et l'édition de fichiers PDF. Power PDF offre de nombreux avantages pour la mise en place de flux numériques sécurisés :

1. Définition simple et rapide d'autorisations de lecture, d'édition et d'impression – Power PDF permet de définir des droits d'accès pour chaque fichier, par le biais de profils de sécurité, ou par l'affectation de droits d'accès individuels via un système de gestion de droits numériques (DRM), tel que Microsoft Active Directory Rights Management. Power PDF Advanced est également compatible avec l'ensemble des paramètres de protection FileOpen. **Fonctionnalités exclusives de Power PDF Advanced** : Prise en charge du service de gestion des droits numériques AD RMS (Active Directory Rights Management Services) de Microsoft. Cette fonction permet aux administrateurs de définir des droits d'accès dans l'interface AD RMS, et de les appliquer à des fichiers PDF. Ces droits d'accès peuvent être appliqués directement avec Power PDF, mais aussi au sein de flux de travail SharePoint. Il s'agit là d'une méthode efficace pour protéger vos PDF contre un accès non autorisé.

2. Chiffrement renforcé – Power PDF utilise le standard de chiffrement industriel AES, avec des longueurs de clés de 128 ou de 256 bits, ainsi que le standard PKCS#12 (Public Key Cryptography Standard), tout en garantissant une rétrocompatibilité avec les standards plus anciens, jusqu'à la version 1.1 du format PDF. Power PDF permet également de protéger des documents Word au moment de leur enregistrement en PDF.

3. Suppression manuelle ou automatique de données sensibles – Avec Power PDF, des données sensibles, telles que des dates de naissance, des adresses e-mail, des numéros de sécurité sociale ou de carte bancaire, peuvent être recherchées et automatiquement noircies lors de la numérisation de documents papier. D'autres informations sensibles et souvent masquées peuvent également être supprimées avant la diffusion de PDF.

4. Signatures numériques et certificats – Power PDF permet de signer et d'authentifier des documents afin d'en garantir l'intégrité. Il prend en charge les standards de cryptographie PKCS#7 et CAdES pour la signature et la certification de documents.

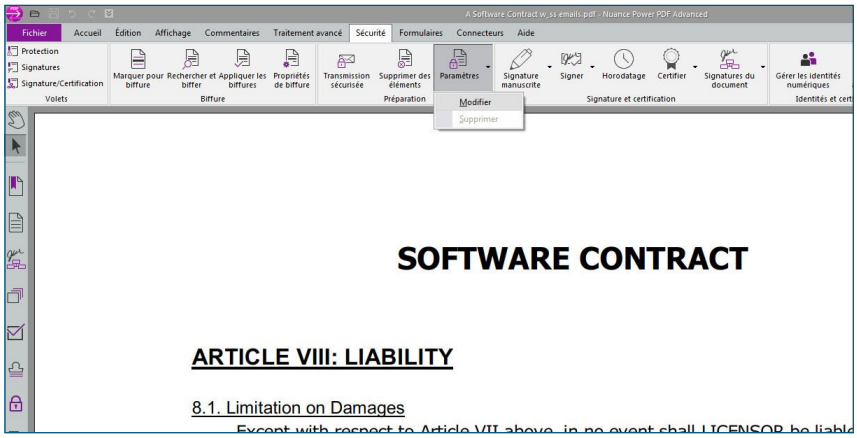
5. Déploiement rapide et intégration directe à des systèmes existants – Power PDF permet de produire des PDF sécurisés depuis des applications bureautiques comme Microsoft Office, et il s'intègre en toute transparence aux flux de travail des systèmes de gestion documentaire les plus récents, comme HP WorkSite, Microsoft SharePoint ou OpenText eDOCS.

6. Comparaison de deux versions d'un document – Power PDF permet de comparer différentes versions d'un même document, en affichant clairement les modifications apportées.

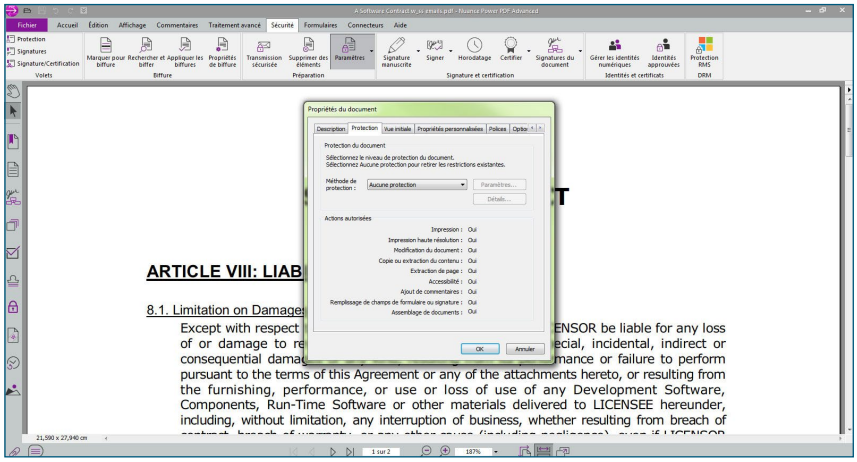
Mise en pratique

Protection d'un document
Voyons comment protéger un document contre un accès non autorisé.

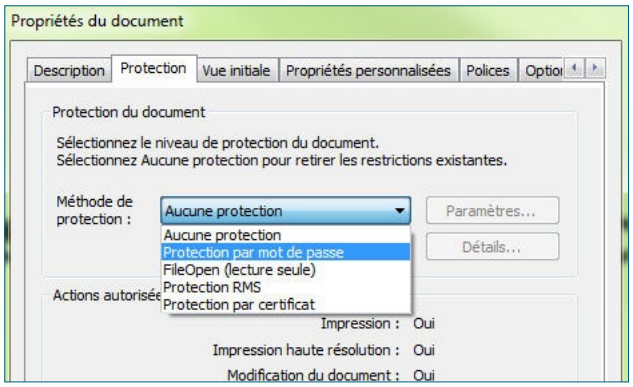
Ouvrez un document dans Power PDF et affichez le ruban Sécurité. Cliquez sur Protection du document, puis sélectionnez Propriétés de protection.



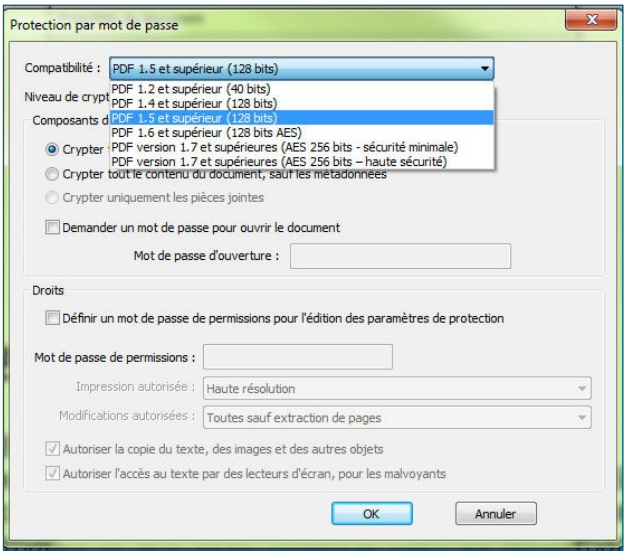
La boîte de dialogue Propriétés du document apparaît.



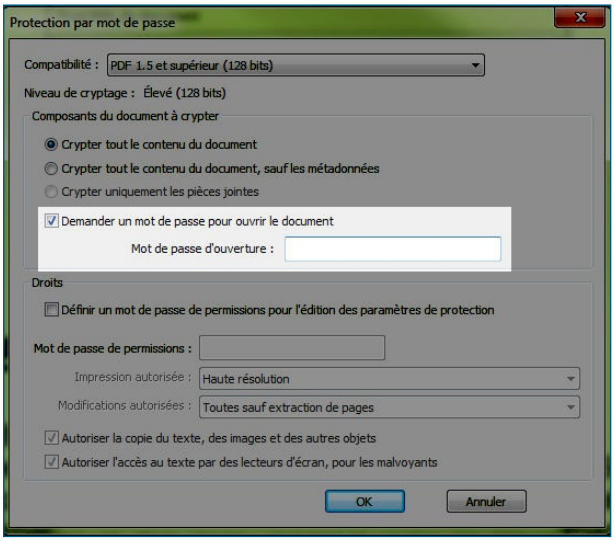
La liste des actions autorisées sur le document s'affiche.



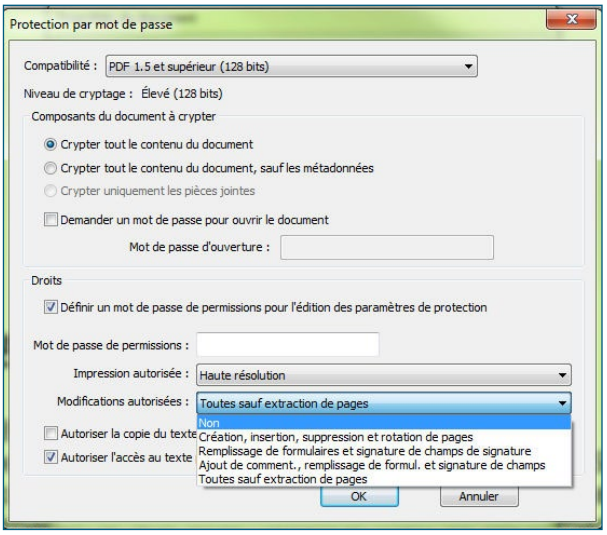
Choisissez un des modes de protection proposés dans la liste déroulante Méthode de protection. Vous pouvez bien évidemment créer un PDF sans aucune protection. Mais si vous préférez opter pour une protection par mot de passe :



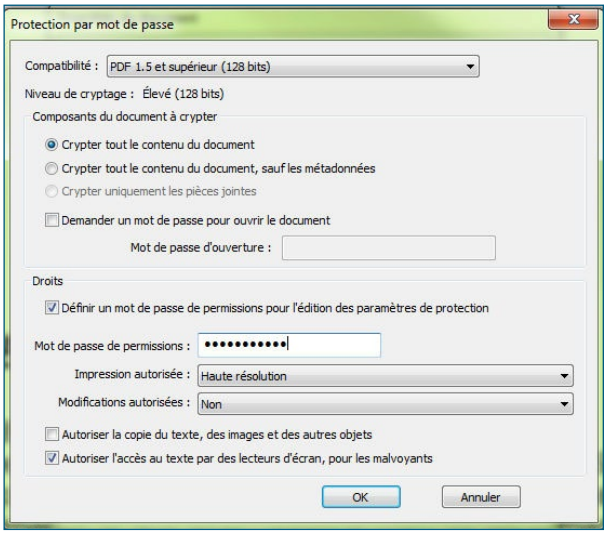
Power PDF prend en charge l'ensemble des niveaux de protection PDF, jusqu'à la version 1.7 du format PDF avec cryptage AES 256 bits.



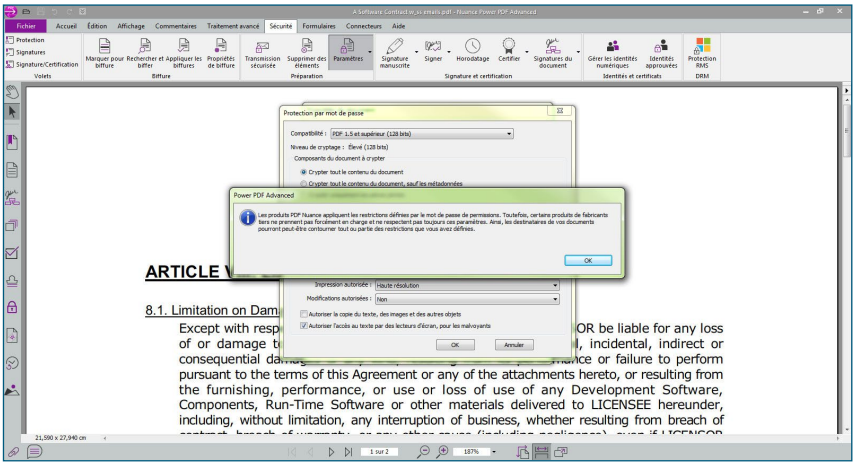
Vous pouvez définir un mot de passe qui sera exigé pour ouvrir le document. Mais soyez prudent, si vous le perdez, vous ne pourrez plus rouvrir le document !



Vous pouvez en plus définir un mot de passe de permissions, qui contrôle l'accès aux paramètres de protection. Dans notre exemple, nous choisirons "Non" pour indiquer qu'aucune modification n'est autorisée tant que le mot de passe de permissions n'a pas été saisi.

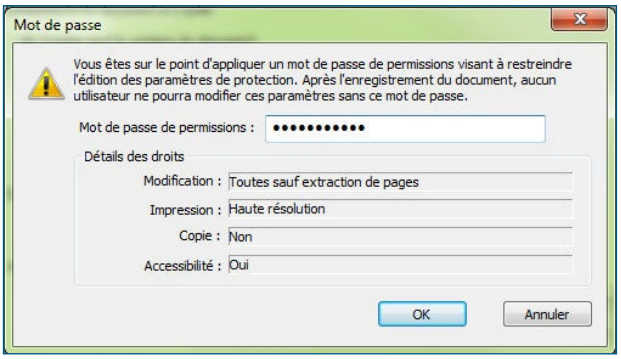


Nous allons définir un mot de passe de permissions, de sorte que le document et les permissions qui lui sont appliquées ne puissent être modifiés que par les personnes qui disposent de ce mot de passe.

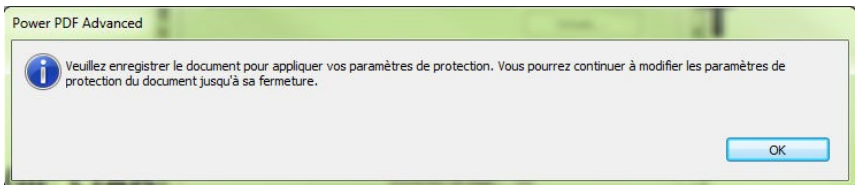


Pour protéger le document à l'aide d'un mot de passe de permissions, cliquez sur OK.

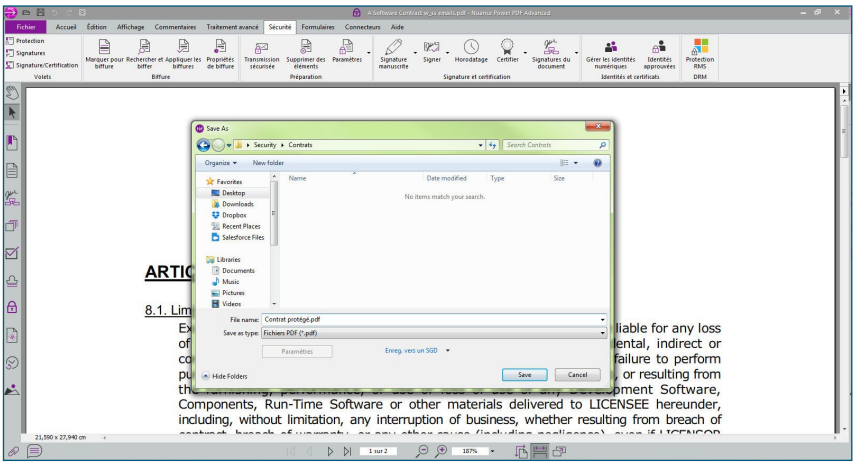
Une fenêtre apparaît pour que vous puissiez confirmer le mot de passe précédemment défini. Entrez le mot que vous avez choisi, puis cliquez sur OK.



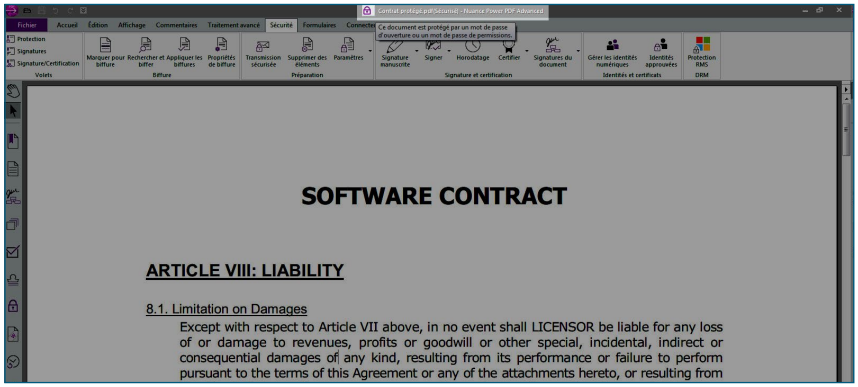
Une fenêtre vous invite à enregistrer le document pour appliquer vos paramètres de sécurité. Cliquez sur OK.



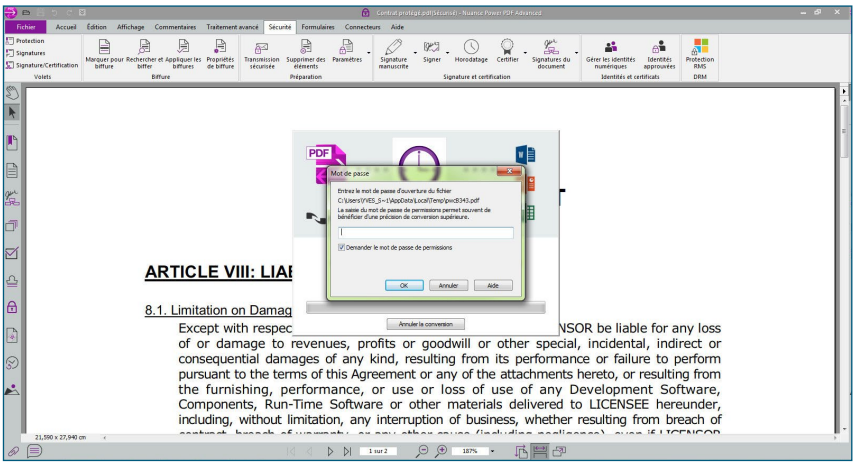
Enregistrez le document sous un nom indiquant qu'il s'agit d'une version protégée, par exemple « Contrat_protégé.pdf ».



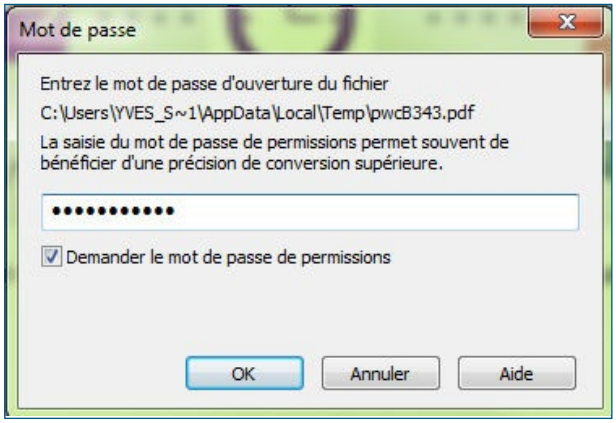
Ouvrez le document que vous venez d'enregistrer en cliquant deux fois dessus. Ce document étant protégé, il ne pourra être modifié qu'après saisie d'un mot de passe.



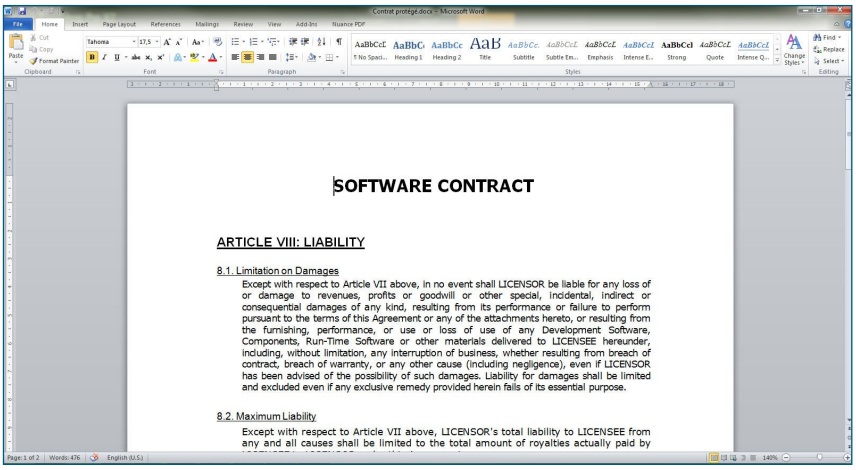
Ainsi, si vous tentez de l'éditer (par exemple, en le convertissant en document Word), une fenêtre vous invitant à saisir son mot de passe apparaîtra.



Entrez le mot de passe, puis cliquez sur OK pour pouvoir travailler sur le document.



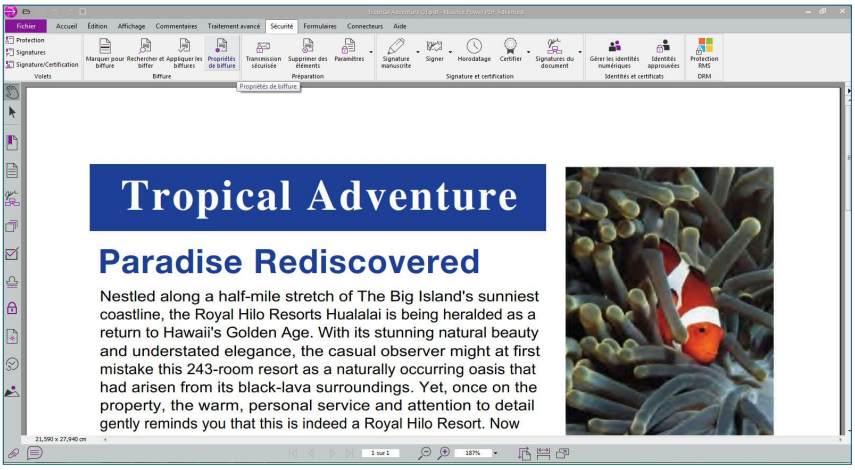
Le document s'ouvrira dans Word. Vous pouvez le consulter et le modifier selon vos besoins.



Biffure
Power PDF propose différentes méthodes permettant de masquer de façon totale et irréversible certaines informations de vos documents. Vous pouvez marquer manuellement des sections à biffer, ou utiliser l'outil de recherche pour trouver et biffer automatiquement certaines expressions.

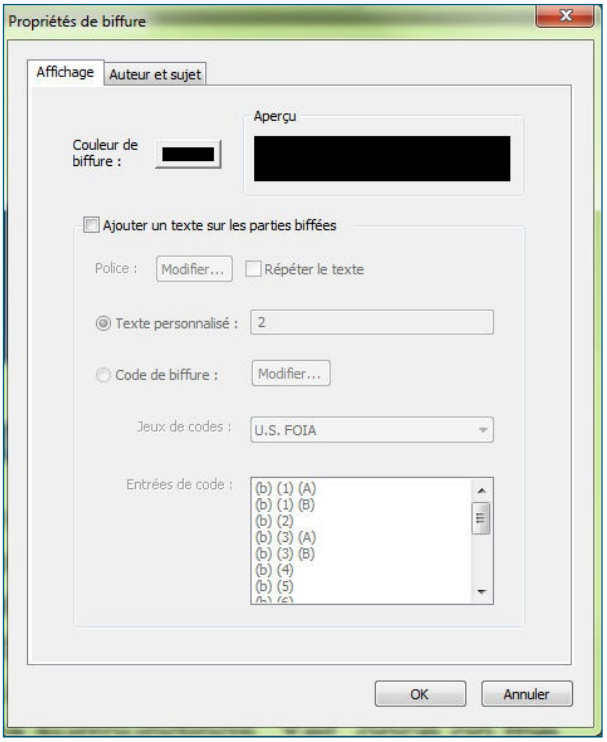
Attention : la fonction de biffure de texte (par sélection manuelle ou par recherche) ne fonctionne que sur des PDF « standard » ou autorisant les recherches. Si votre PDF est constitué uniquement d'images, utilisez l'outil de biffure manuelle de zones.

Pour marquer des parties d'un document et les biffer définitivement, affichez le ruban Sécurité, puis cliquez sur Propriétés de biffure dans le groupe Biffure.

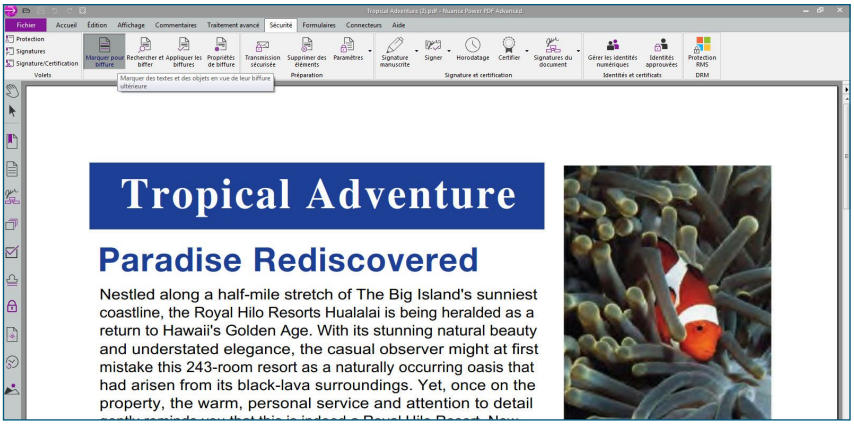


La boîte de dialogue Propriétés de biffure apparaît.

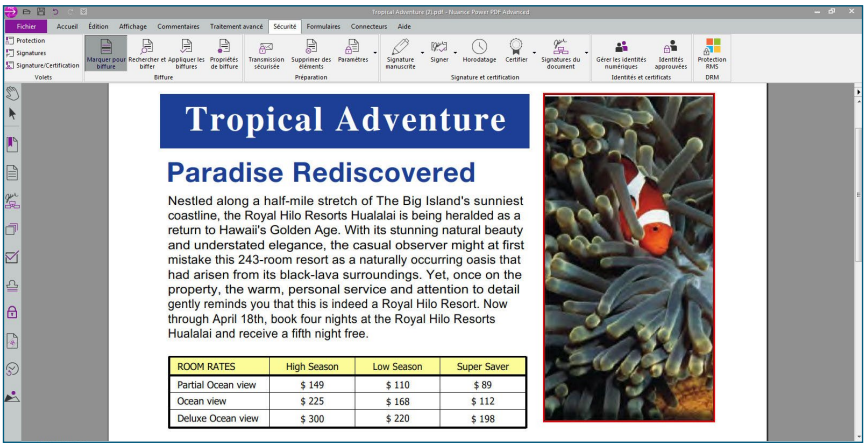
Vous pouvez y définir les couleurs utilisées pour biffer le texte. Dans cet exemple, nous avons utilisé la couleur standard : le noir. Cliquez sur OK.



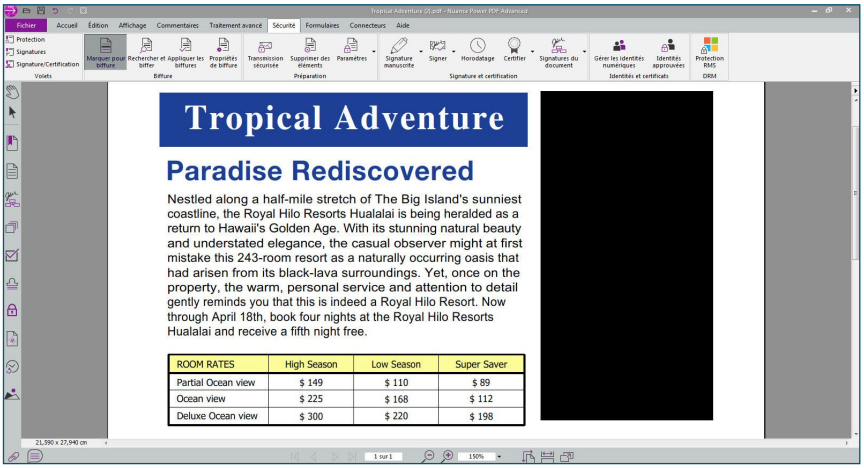
Sélectionnez à présent l'outil Marquer pour biffure. Cet outil vous permet de sélectionner le contenu que vous souhaitez masquer définitivement.



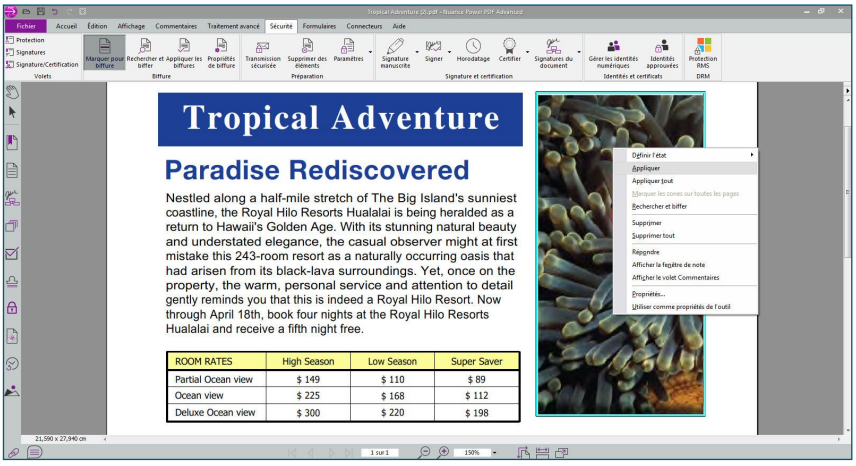
Il peut s'agir de texte sélectionné à l'aide de la souris, ou de n'importe quel autre élément sur une page. Dans notre exemple, nous avons indiqué qu'une image devait être biffée. Pour ce faire, il suffit de placer le curseur sur cette image. Lorsque le symbole + apparaît à la place du curseur, tracez un rectangle couvrant la zone à biffer.



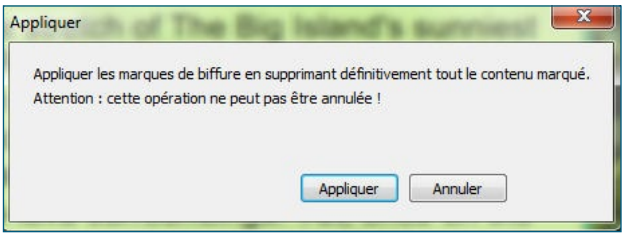
Positionnez le pointeur sur la zone marquée pour biffure afin de visualiser l'apparence de votre biffure une fois appliquée.



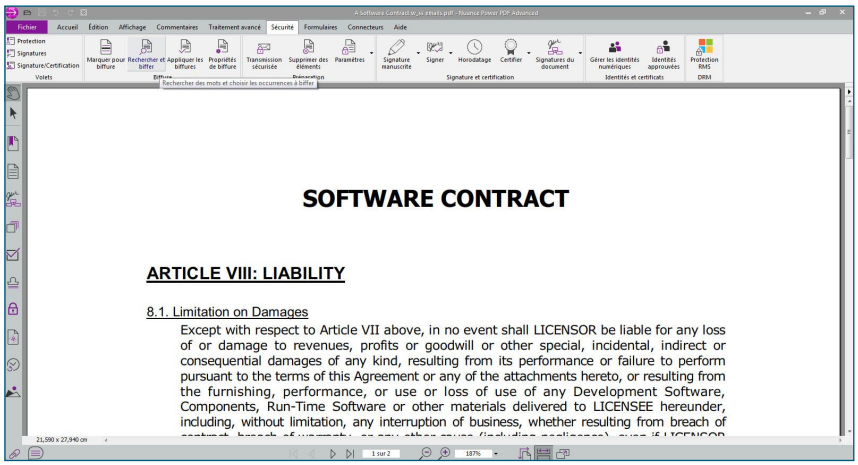
Cliquez avec le bouton droit sur une zone marquée pour biffure, puis sélectionnez Appliquer dans le menu contextuel pour appliquer définitivement la biffure. Pour biffer définitivement tous les contenus marqués pour biffure, sélectionnez Appliquer tout.



Une boîte de dialogue vous invite à confirmer votre intention. Cliquez sur Oui.

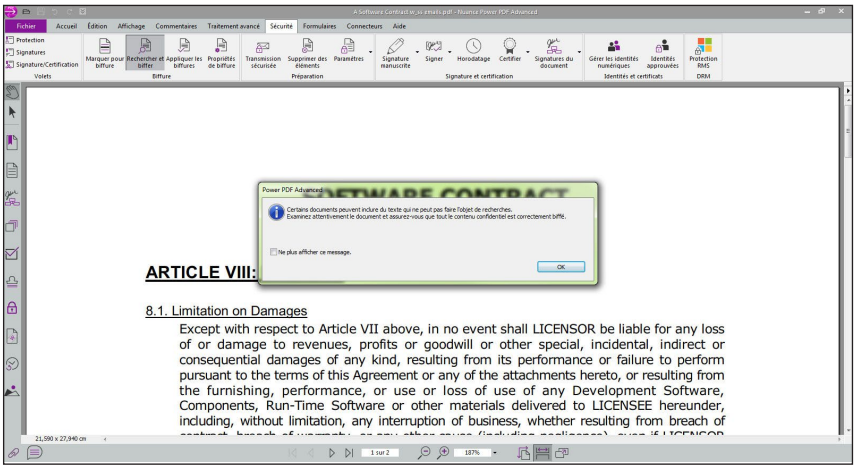


Il est impossible d'annuler une opération de biffure, et de récupérer des zones biffées. Pour éviter toute erreur, effectuez une copie du PDF d'origine avant d'appliquer des biffures, ou enregistrez le PDF biffé dans un nouveau fichier, sous un autre nom et/ou emplacement.

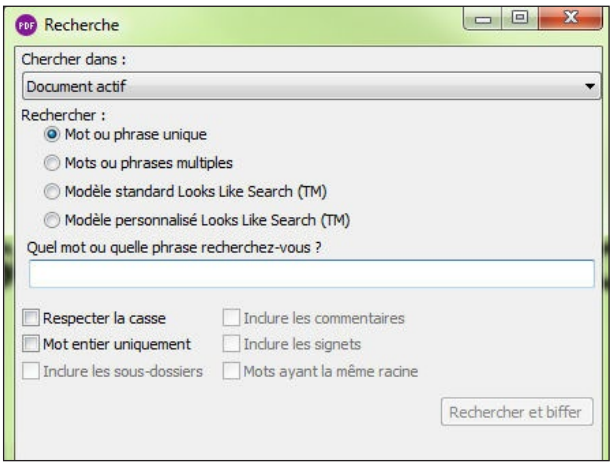


Power PDF vous permet de marquer manuellement des informations à biffer, mais vous pouvez utiliser l'outil de recherche pour biffer automatiquement des mots ou des expressions spécifiques.

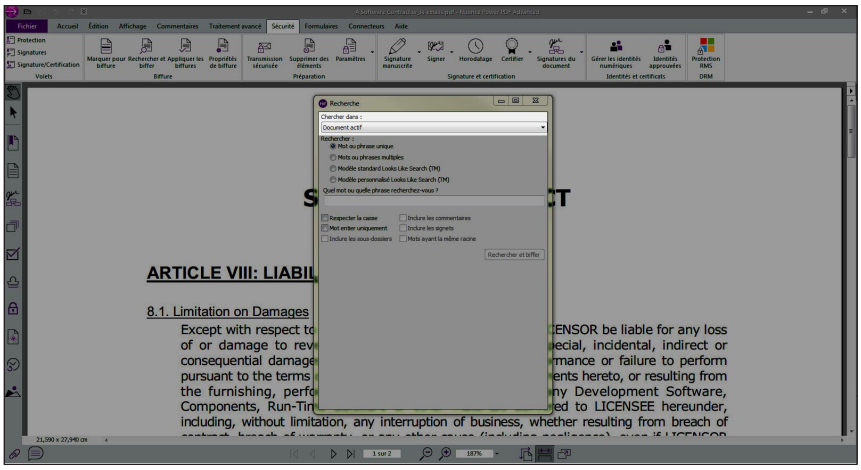
Ouvrez le document contenant les parties que vous souhaitez biffer. Dans notre exemple, nous allons noircir tous les numéros de sécurité sociale qui apparaissent dans un contrat.



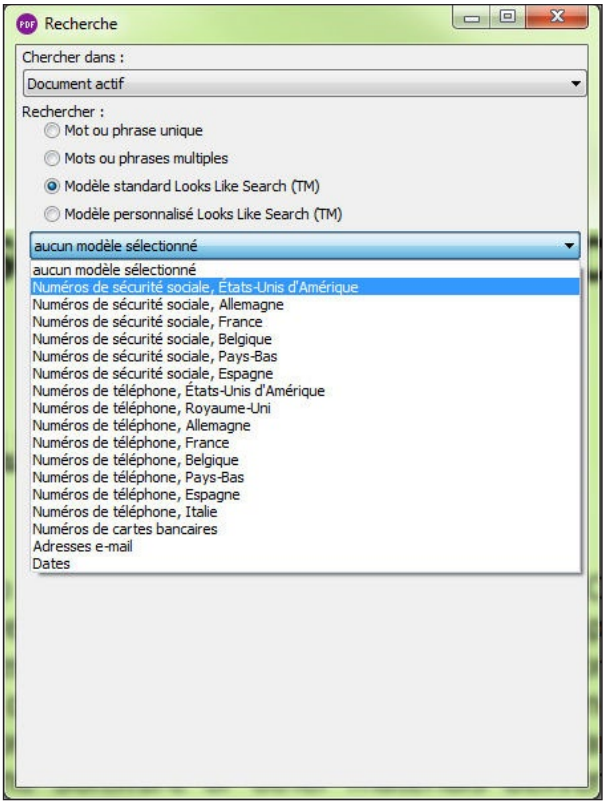
Pour retrouver automatiquement les informations à biffer, ouvrez le ruban Sécurité, et sélectionnez Rechercher et biffer dans le groupe Biffure.



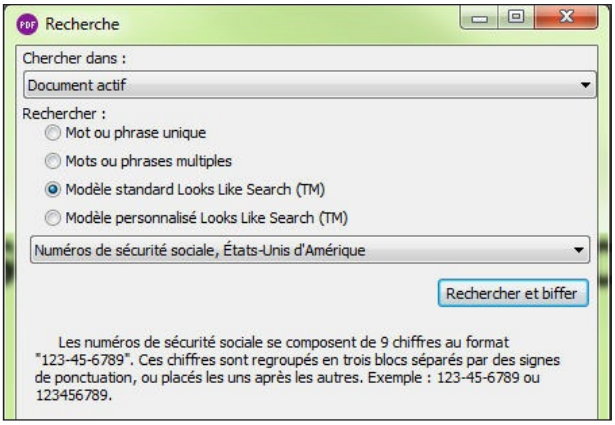
Power PDF vous rappelle que certains documents contiennent du texte qui ne peut pas faire l'objet de recherches, et qui ne peut donc pas être biffé. Avant de diffuser votre document, examinez-le attentivement pour vous assurer que tout le contenu confidentiel a correctement été biffé. Cliquez sur OK.



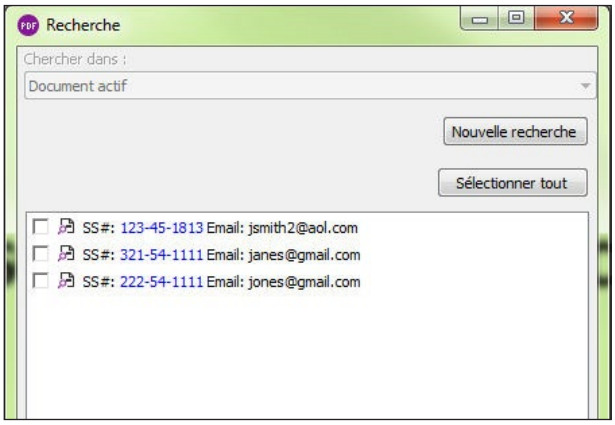
Une boîte de dialogue vous invite à indiquer le document, le porte-documents ou même le dossier sur lequel doit porter votre recherche.



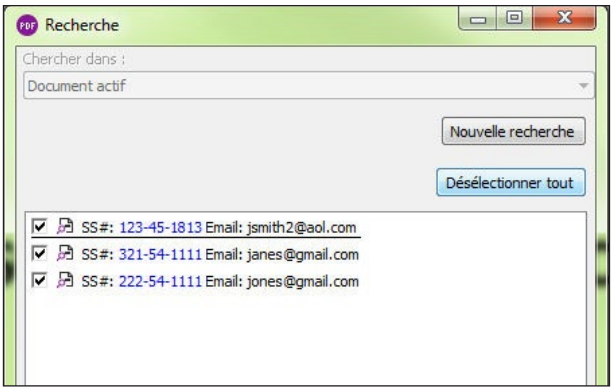
Sélectionnez Numéros de sécurité sociale, États-Unis d'Amérique.



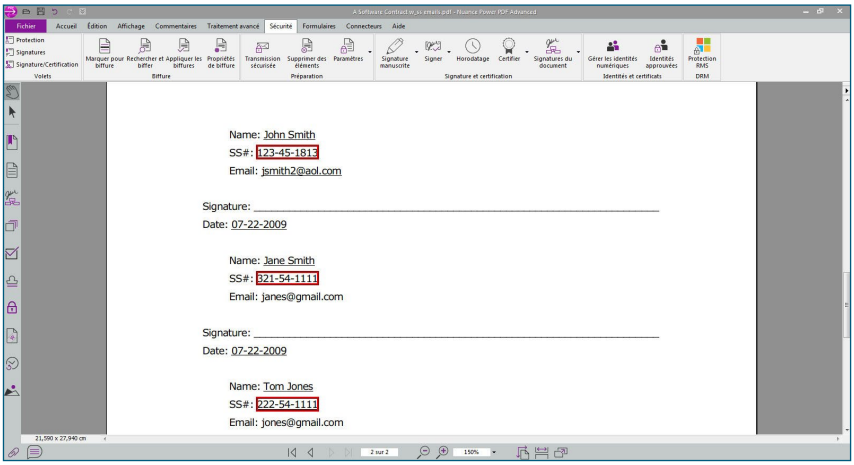
Cliquez sur Rechercher et biffer. La liste de tous les numéros de sécurité sociale trouvés dans le document est affichée.



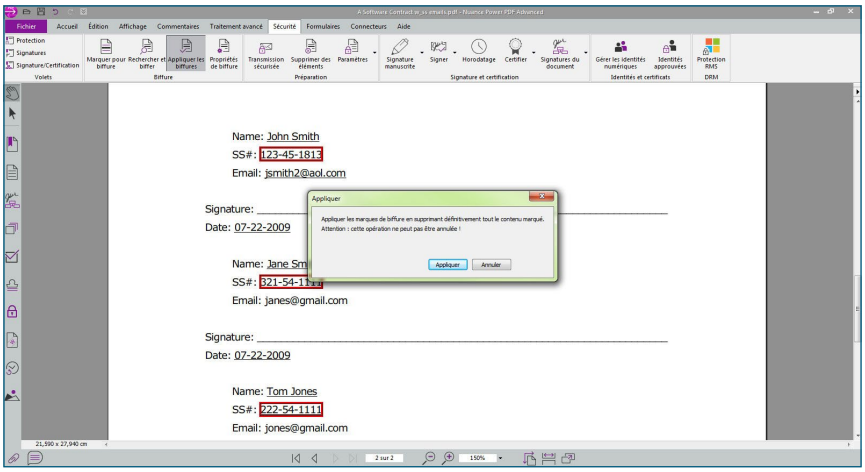
Cliquez sur Sélectionner tout. Toutes les occurrences trouvées sont sélectionnées.



Cliquez sur Marquer les occurrences sélectionnées pour biffure. Les occurrences sont marquées comme devant être biffées.

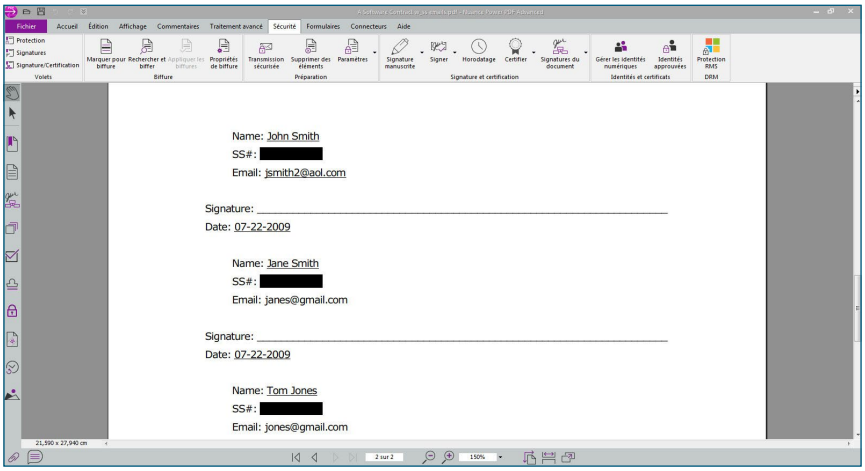


Un message vous informe que les biffures ne peuvent pas être annulées une fois appliquées.



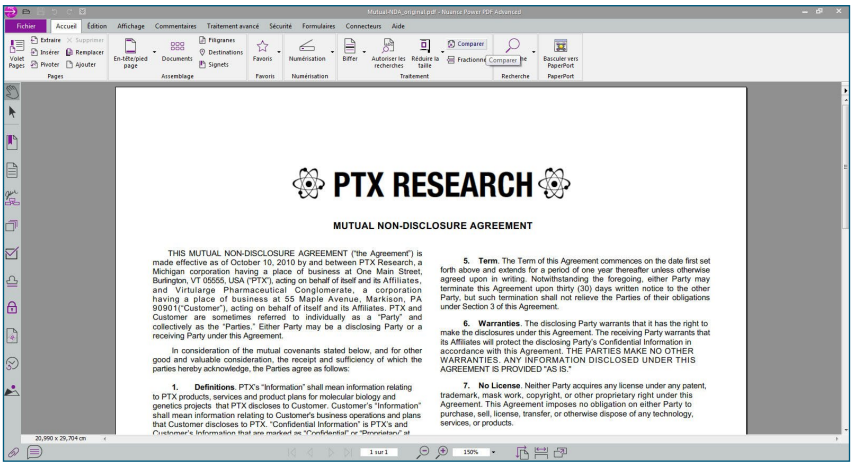
Une fois les biffures appliquées, Power PDF vous demandera si vous souhaitez supprimer d'autres éléments du document.

Cette procédure permettra de supprimer d'autres éléments qui peuvent toujours être liés en arrière-plan aux numéros de sécurité sociale, et qui doivent également être protégés. Cliquez sur OK. Toutes les informations associées aux numéros de sécurité sociale ont à présent été supprimées du document.

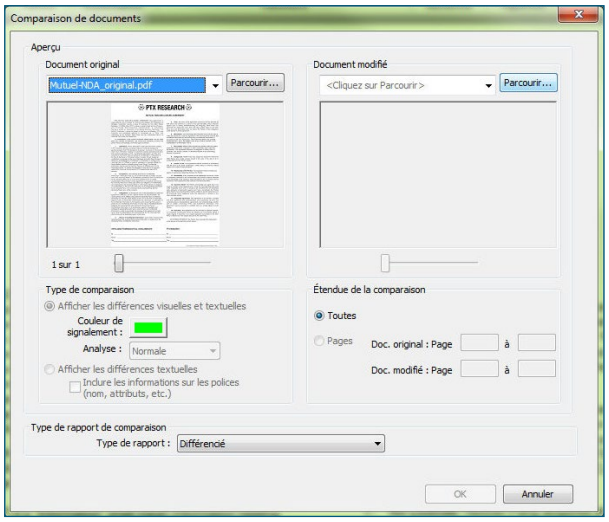


Comparaison de documents

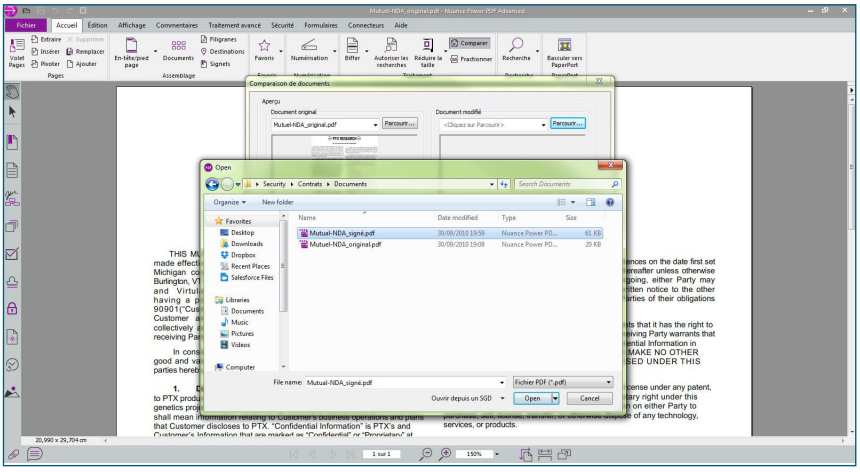
Pour comparer deux documents, ouvrez votre document original dans Power PDF, puis cliquez sur le bouton Comparer du ruban Accueil.



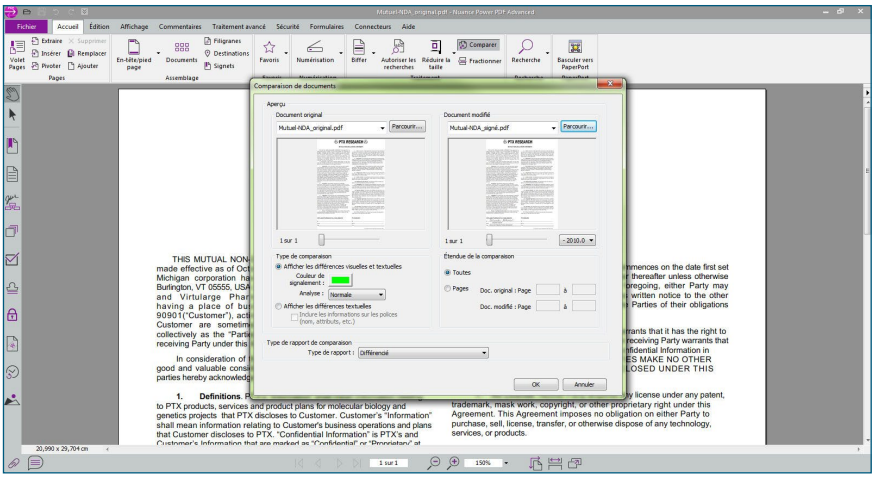
La boîte de dialogue Comparaison de documents apparaît.



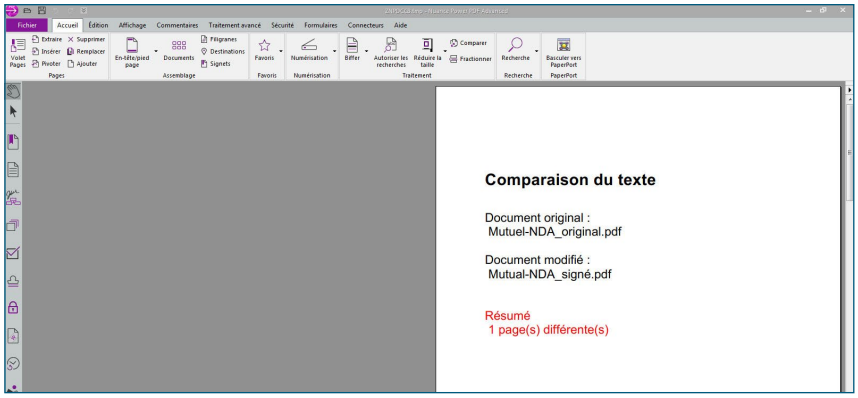
Sélectionnez le document modifié que vous souhaitez comparer à votre original. Pour ce faire, cliquez sur le bouton Parcourir sous Document modifié. La boîte de dialogue Ouvrir apparaît.



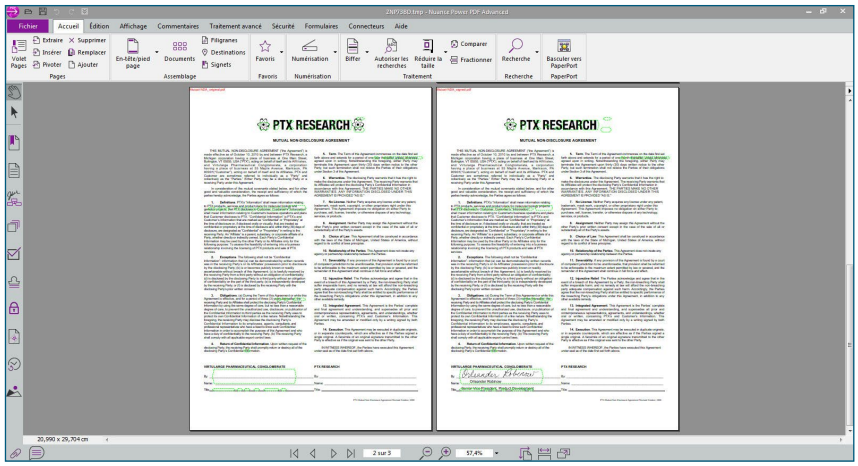
Recherchez la nouvelle version du document à comparer, puis cliquez sur Ouvrir. Les deux documents sont affichés côte à côte : la version originale à gauche, celle modifiée à droite.



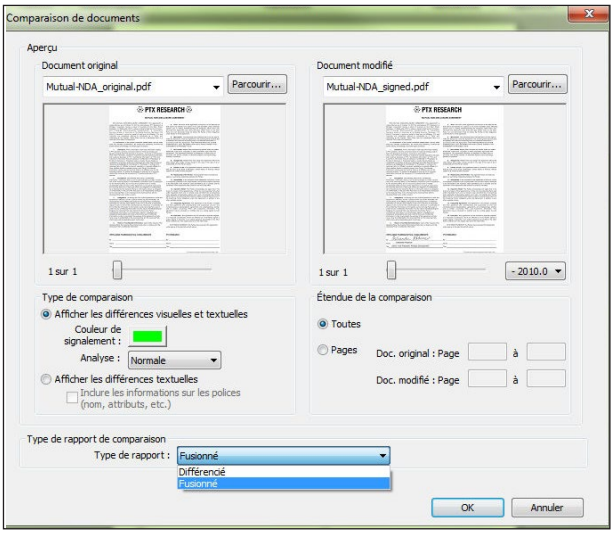
Les documents peuvent être comparés de manière différenciée (l'un à côté de l'autre), soit de manière fusionnée (au sein d'un même document composite). Dans la liste Type de rapport, conservez l'option Différencié sélectionnée, puis cliquez sur OK. La première page du document de comparaison présente un résumé des différences relevées.



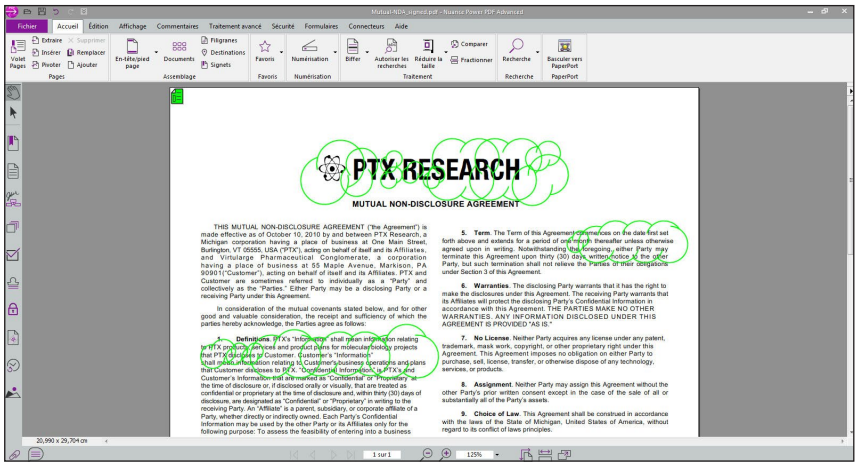
Faites défiler le document de comparaison. Les pages suivantes répertorient en détail les différences entre les deux versions du document. Les sections modifiées sont mises en surbrillance.



Si vous préférez afficher un document de comparaison fusionné (avec marques de révision), sélectionnez Fusionné dans la liste Type de rapport.



Cliquez sur OK. Les modifications sont à présent affichées au sein d'un document unique, et non côte à côte.



À propos de Nuance Communications, Inc.
Nuance Communications réinvente la relation entre l'homme et la technologie. Avec son portefeuille unique de solutions vocales, Nuance permet des interactions plus naturelles et intuitives entre les utilisateurs et de nombreux systèmes, périphériques, appareils électroniques, applications et services. Chaque jour, des millions d'utilisateurs et des milliers d'entreprises vivent l'expérience Nuance par le biais de systèmes intelligents capables d'écouter, de comprendre, d'apprendre et de s'adapter à leur style de vie et leurs méthodes de travail. Pour plus d'informations, rendez-vous sur nuance.fr.