Sécurité des documents, contrats et identités dématérialisés

Protégez vos actifs numériques et gardez le contrôle

yousign × HEXATRUST CYBERSECURITY & DIGITAL TRUST

Sommaire

Introduction

Page 3

Du papier au digital : s'adapter aux défis d'un environnement dématérialisé

Page 4

> Les cyberrisques d'aujourd'hui et de demain : quelles stratégies pour les contrer ? Insights d'Hexatrust.
>
> Page 8

Les tactiques pour sécuriser son intégrité numérique

Page 12

Faire de son intégrité numérique un levier stratégique

Page 22

Conclusion

Page 27

Introduction

Depuis plusieurs années, la dématérialisation des documents, contrats et identités s'est affirmée comme un **levier stratégique**, permettant aux entreprises plus d'efficacité et de flexibilité.
La pandémie de COVID-19 a joué un rôle d'accélérateur dans cette transformation, ancrant le digital au cœur de nos pratiques professionnelles.

Cependant, **les enjeux et les risques associés à cette digitalisation massive demeurent largement sous-estimés**. En effet, si la protection de l'intégrité physique et morale des individus est aujourd'hui une évidence, son extension à l'univers numérique reste encore imparfaite. Qu'il s'agisse d'organisations publiques ou privées, tout comme des individus, garantir l'intégrité numérique n'est pas encore un réflexe pour tous, comme en témoigne l'application parfois difficile du règlement RGPD en Europe. Pourtant, il s'agit là d'un enjeu crucial puisqu'elle touche directement à la sécurité de données stratégiques.

Pour faire face à ce défi, il est donc crucial d'adopter des pratiques robustes pour **protéger vos actifs numériques**.
Des bonnes pratiques peuvent aider à limiter les risques, sans perdre en efficacité. Ce livre blanc regroupe ces conseils pour vous guider vers une approche proactive et de **maximiser les bénéfices de la digitalisation**.

Nous sommes ravis de nous associer à **Hexatrust**, une association reconnue qui rassemble les entreprises françaises et européennes innovantes spécialisées dans la cybersécurité, le cloud, le digital workplace et la confiance numérique. Notre partenariat incarne une vision commune : **renforcer l'intégrité numérique des entreprises et les guider vers une protection accrue de leurs données et opérations essentielles**.

Bonne lecture !

Du papier au digital : s'adapter aux défis d'un environnement dématérialisé

Aujourd'hui, presque toutes les entreprises ont adopté la digitalisation de leurs activités. Essentielle pour attirer de nouveaux clients, les fidéliser et améliorer leur efficacité au quotidien, cette transformation a cependant entraîné l'apparition de nouveaux risques.

Un contexte ultra-digitalisé

La digitalisation désigne tous les processus par lesquels une société intègre les technologies numériques dans ses activités, tant externes qu'internes.

Elle transforme les méthodes de travail, favorise la collaboration et facilite la prise de décision grâce aux données. Cette transition a aussi permis de moderniser des processus traditionnels, comme la gestion documentaire et la relation client.

71 % des professionnels considèrent que leur entreprise est digitalisée en France. 29 % la considèrent comme "très digitalisée".

D'après une étude réalisée par Ipsos et Yousign, en février 2024.

"

La pandémie a poussé les entreprises à adopter la dématérialisation à marche forcée. Elles ont massivement recouru à la signature électronique pour signer les contrats avec leurs contreparties entreprises ou particuliers. Après la pandémie, l'habitude était prise. En termes d'accompagnement, cela s'est traduit par une demande croissante d'évaluation de la qualité technico-juridique des procédés proposés par les prestataires de confiance et, dans certains secteurs, de sécurisation de la vérification d'identité à distance en termes de conformité au règlement eIDAS et au RGPD.

Isabelle Renard, Avocat au Barreau de Paris, Docteur Ingénieur

Les actifs numériques sensibles

Bien que la digitalisation ait permis de formidables opportunités, les risques auxquels sont confrontées les entreprises n'ont jamais été aussi nombreux. Ils concernent notamment :

Les contrats dématérialisés

Qu'il s'agisse d'accords signés avec vos clients, prestataires ou salariés, les contrats dématérialisés peuvent être falsifiés en l'absence d'une protection adéquate. Au même titre que les accords papier "traditionnels", leur validité peut être contestée devant les tribunaux.

Les documents électroniques

Factures, bulletins de paie, notes de frais, comptes annuels... Ces documents peuvent être altérés et manipulés. Ils s'exposent particulièrement à ces risques quand ils transitent par plusieurs outils ou plateformes.

Les identités numériques

Pour toute relation commerciale, vous devez vous assurer d'avoir affaire à la bonne personne ou la bonne entreprise. Malheureusement, les méthodes d'authentification sont souvent peu développées, ce qui entraîne des cas d'usurpation d'identité.

Les techniques couramment utilisées incluent l'hameçonnage (phishing), où des messages ou des e-mails sont envoyés pour tromper les victimes, accéder à du contenu sensible et signer illégalement des documents. On observe aussi la multiplication des cas d'usurpation d'identité synthétique, qui créent de nouvelles identités à partir d'informations réelles et fausses. Ce type d'attaques conduit à des fraudes au faux président, IBAN ou fournisseur.

Tous ces risques peuvent avoir un impact direct sur les résultats de l'entreprise

La manipulation des contrats et documents, tout comme l'usurpation des identités, peut avoir des conséquences directes sur les résultats de votre entreprise, à travers différents aspects.

Pertes financières

Transactions frauduleuses, paiements non autorisés, engagements non respectés... Ces incidents occasionnent des coûts importants, en termes d'opportunités manquées, de dédommagements et de frais juridiques.

Poursuites judiciaires

En cas de contestation ou de falsification des contrats, votre entreprise s'expose à des litiges longs et coûteux. En effet, le non-respect des normes de sécurité et de protection des données, telles que le RGPD (Règlement Général sur la Protection des Données) en Europe, peut entraîner des amendes importantes et des sanctions qui pèsent lourdement sur les résultats financiers.

Avec l'augmentation de la communication par voie électronique uniquement, la fraude à l'identité pour tenter d'obtenir frauduleusement des paiements, comme la "fraude au président" par exemple, ou encore la divulgation d'informations confidentielles, me semble avoir beaucoup augmenté ces dernières années. Ces fraudes prennent des formes très variées qui combinent éléments technologiques et manipulations psychologiques. Elles sont de plus en plus sophistiquées et de nombreuses entreprises n'y sont pas préparées.

Isabelle Renard, Avocat au Barreau de Paris, Docteur Ingénieur

Les cyberrisques d'aujourd'hui et de demain : quelles stratégies pour les contrer ?

Insights d'Hexatrust

Les attaquants continuent de perfectionner des techniques qui leur permettent de s'introduire dans des systèmes d'information, de s'y propager, d'exfiltrer des informations, de se prépositionner (installation d'outils et accès nécessaires avant une attaque) et d'éviter d'être détectés.

Face à cette montée en puissance des cyberattaques, les organisations doivent adapter leurs stratégies de défense.

Parmi les plus répandues, on trouve les **ransomwares**, qui bloquent l'accès aux données en les cryptant, exigeant une rançon pour les déverrouiller. Les **attaques de phishing**, tout aussi courantes, visent à piéger les utilisateurs en les incitant à fournir des informations sensibles, comme des identifiants ou des données bancaires, à travers des e-mails frauduleux ou des sites web imitant des plateformes fiables.

Les salariés, qu'ils agissent de manière malveillante ou non, peuvent aussi constituer une menace majeure. Les **fuites de données** peuvent résulter d'erreurs humaines involontaires ou d'actes intentionnels, comme le vol d'informations sensibles ou la complicité dans des cyberattaques.

Les **attaques DDoS**, en augmentation, sont souvent utilisées comme outils de chantage ou de sabotage. Les **cybercriminels** exploitent également les failles de sécurité dans les logiciels pour accéder aux systèmes, les vulnérabilités non corrigées étant souvent exploitées pour des attaques à grande échelle. Cela souligne l'importance d'anticiper, tester et surveiller en continu pour corriger les failles sans délai.

Si on se projette dans le futur, **l'émergence de nouvelles technologies et tactiques nécessite une vigilance accrue**. C'est notamment le cas de **l'Intelligence Artificielle** qui offre de nombreux avantages mais pose également des défis considérables en matière de sécurité.

Focus sur l'IA

Avec **Garance Mathias**, Avocat Associé - Fondatrice Mathias Avocats

Falsification de documents

Les différents modèles d'IAG peuvent être utilisés pour créer des documents falsifiés, ce qui peut compromettre l'intégrité des contrats.

Violation des droits de propriété intellectuelle

L'IAG peut utiliser des données protégées par des droits de propriété intellectuelle sans autorisation, d'où l'intérêt d'adopter des politiques appropriées pour l'utilisation des données d'entrée et de sortie des systèmes d'IA.

Collecte massive de données personnelles

Les systèmes d'IAG peuvent collecter et analyser de grandes quantités de données, avec des risques potentiels en matière de confidentialité et de sécurité des données en cas d'absence de conformité au RGPD.

Usurpation d'identité

Les technologies d'IA, comme les deep fakes, peuvent créer des vidéos ou des enregistrements audios très réalistes de personnes, facilitant ainsi l'usurpation d'identité.

Pour y faire face, **une approche par les risques est nécessaire**.
Il faut notamment prendre en compte :

La sécurisation des usages

Déployer des outils de sécurité adaptés aux usages de l'IA capables de détecter les deep fakes et autres formes de falsification numérique, en intégrant notamment des analyses de risques et d'impact sur la vie privée (RGPD, RIA...).

L'authentification renforcée

Vérifier l'identité des utilisateurs et/ou choisir des prestataires de services de confiance selon les exigences de confidentialité (eIDAS 2) et de sécurisation des échanges (signatures, archivages électroniques...).

Approche par les risques + approche par la conformité

L'approche par les risques se concentre sur une protection proactive et personnalisée. Elle s'adapte à ce qui est réellement important pour l'entreprise. Quant à l'approche par la conformité, elle s'assure que l'organisation respecte des règles fixées par des tiers pour éviter sanctions et audits défavorables.

Bien qu'elle soit plus rigide, **cette approche est complémentaire** à la première : la conformité établit une base essentielle, tandis que l'approche par les risques va plus loin en personnalisant la protection.

L'IA ne modifie pas fondamentalement la nature des menaces, mais elle facilite considérablement le travail des attaquants. Les attaques par "deep fake" existent par exemple depuis longtemps, mais elles sont désormais accessibles à un public plus large, sans nécessiter de moyens ou d'expertise significatifs. Cela oblige les entreprises à ajuster le niveau de sécurité en fonction de la sensibilité du document à signer et du type de signature électronique utilisé.

Kevin Dubourg, Director of Engineering, Yousign

Les tactiques pour sécuriser son intégrité numérique

La dépendance grandissante à l'égard des outils digitaux dans les opérations quotidiennes met en évidence la nécessité d'une stratégie globale. Sécuriser ses documents, contrats et identités numériques s'avère essentiel pour protéger les revenus, les activités et la réputation de l'entreprise.

Utilisez une solution de signature électronique certifiée

Les solutions de signature électronique certifiées offrent aux entreprises une sécurité renforcée en garantissant l'authenticité, l'intégrité et la traçabilité des contrats et documents. Grâce à des protocoles d'authentification stricts, elles protègent contre les falsifications et les accès non autorisés.

En plus de simplifier les processus, ces solutions aident à respecter les réglementations sur la protection des données (RGPD, eIDAS), tout en réduisant les risques de litiges et de fraudes pour l'entreprise.

Connaissez-vous les trois niveaux de signature électronique ?

Selon le règlement eIDAS, la signature électronique se décline en trois niveaux :

Niveau de signature	Description	Exemples d'utilisation
Signature simple	La plus simple à mettre en place, elle permet d'identifier l'auteur d'un document.	Engagements de faible risque, tels que l'approbation de devis ou de bons de commande.
Signature avancée	Elle garantit l'identité du signataire et l'intégrité du document, avec une authentification plus poussée.	Contrats d'embauche ou des accords commerciaux, où une sécurité supplémentaire est nécessaire.
Signature qualifiée	Le niveau le plus élevé, juridiquement équivalent à une signature manuscrite. Elle requiert l'utilisation d'un certificat qualifié délivré par un prestataire agréé.	Documents hautement sensibles, comme des contrats financiers ou des accords de fusion-acquisition.

“

En cas de contestation, il est nécessaire, pour prouver la validité d’une signature électronique devant les tribunaux, de fournir au minimum :

- Une copie du document signé électroniquement, comportant une mention claire et explicite de l’utilisation de ce type de signature.
- Un fichier de preuve retraçant les éléments essentiels de la transaction et comportant un lien avec le document signé.
- Les certifications attestant de la conformité aux standards applicables en vertu du Règlement eIDAS.

Isabelle Renard, Avocat au Barreau de Paris, Docteur Ingénieur

Connaissez-vous le “dossier de preuves” ?

Le dossier de preuves, également appelé “audit trail”, est un document renfermant toutes les informations et procédés techniques ayant contribué au bon déroulement d’une opération dématérialisée. Il est essentiel pour garantir l’authenticité, l’intégrité et la non-répudiation des opérations, notamment dans le cas des signatures électroniques.

Optez pour des solutions européennes

Privilégier des solutions européennes garantit la protection des données et la sécurité des documents électroniques. Ces entreprises, opérant dans le même cadre réglementaire que le vôtre, sont souvent exemptées des lois extraterritoriales imposées par des acteurs non-européens. Cela vous garantit un contrôle accru sur l’utilisation et la confidentialité des données qui transitent par leurs plateformes.

Dans le même temps, un cadre réglementaire novateur et rigoureux existe au sein de l'Union européenne pour assurer la cyberprotection des données. Outre le RGPD, d'autres régulations, comme le Data Governance Act ou la Directive NIS2 imposent des standards élevés de sécurité et de gestion des données. Plus récemment, le Digital Markets Act (DMA) et le Digital Services Act (DSA) visent à limiter les abus de position dominante des grandes plateformes.

Enfin, faire le choix d'une solution européenne, c'est favoriser l'émergence d'une filière respectueuse des réglementations en vigueur et digne de la confiance des particuliers et des entreprises. C'est aussi construire un écosystème innovant et capable de se mesurer aux grandes entreprises technologiques internationales tout en renforçant la souveraineté numérique de l'Europe.

“

Favoriser la souveraineté numérique est nécessaire dans un monde où la maîtrise de la donnée devient un enjeu stratégique. De plus, au-delà de l'intégrité numérique, choisir des partenaires européens, c'est s'assurer de coconstruire des chaînes de valeurs expertes et durables, au service de notre économie et in fine de notre modèle social européen.

Dorothée Decrop, Déléguée Générale - Hexatrust

“

Les solutions européennes sont créatrices de confiance pour leurs partenaires, investisseurs et clients car elles intègrent les enjeux de conformité dès la conception de leurs produits et services. En plus de mettre en œuvre un cadre réglementaire ambitieux et innovant, les réglementations comme NIS 2, CRA, eIDAS 2 ou encore DORA et le RIA sont également porteuses d'opportunités business et technologiques.

Garance Mathias, Avocat Associé et Fondatrice - Mathias Avocats et adhérent Hexatrust

55 % des RSSI (Responsables Sécurité des Systèmes d'Information) déclarent être intéressés par les initiatives en matière de souveraineté et de cloud de confiance.

D'après le baromètre CESIN 2024 sur la cybersécurité des entreprises françaises

Protégez les identités numériques

Prévenir les risques d'usurpation d'identités nécessite une approche proactive à l'heure où l'intelligence artificielle et les "deep fakes" se développent à vitesse grand V.

Pour protéger les identités numériques, les solutions d'authentification multifacteurs (MFA) restent l'une des meilleures pratiques pour protéger les identités numériques. Le recours à l'intelligence artificielle peut également jouer en votre faveur en détectant des anomalies.

"

Sur le plan méthodologique, les capacités algorithmiques ont considérablement progressé, permettant aux modèles de lutte contre la fraude de se perfectionner grâce à l'apprentissage à grande échelle sur des ensembles de données importants, sans exposition directe à la fraude. Les solutions de vérification d'identité se développent également en intégrant des fonctionnalités complémentaires qui renforcent la sécurité sans nuire à l'expérience utilisateur. Ces contrôles additionnels, appelés contrôles passifs, peuvent inclure des éléments tels que le contrôle de l'appareil, la géolocalisation, la répétition...

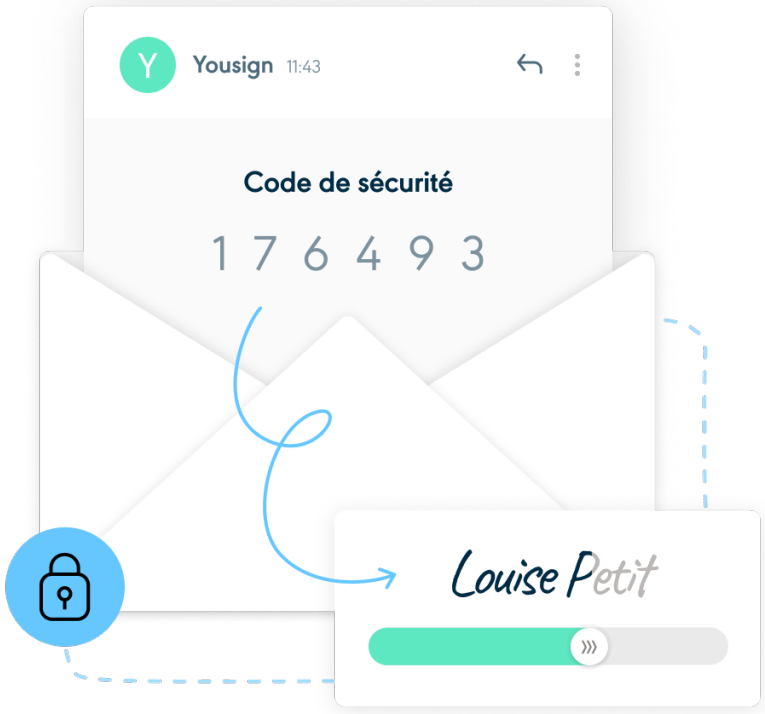
Emilie Lagarde, Product Marketing Senior Manager, Checkout

71 % C’est le pourcentage d’augmentation des cyberattaques exploitant les identifiants des utilisateurs en 2024, par rapport à l’année précédente. Elles sont devenues le principal point d’entrée des attaques.

Selon l’IBM X-Force Threat Intelligence Index

99% C’est le pourcentage d’attaques par mot de passe dans les attaques d’identité quotidiennes.

D’après le Microsoft Digital Defense Report 2024



Cartographiez les risques

Pour commencer, il est essentiel de comprendre d'où vous partez ! C'est pourquoi nous vous conseillons de lister tous les documents que vous manipulez afin de mettre en place les mesures de protection adaptées.

Finance

- Notes de frais
- Factures
- États financiers (bilans, comptes de résultat, flux de trésorerie)
- Rapports de gestion et analyses de performance
- Contrats de financement (emprunts, obligations, lignes de crédit)
- Données fiscales et déclarations d'impôts
- Données de paie et informations sur les salaires des employés...

Ressources humaines

- Bulletins de salaire
- Contrats de travail et avenants
- Dossiers des employés (informations personnelles, coordonnées bancaires, évaluations de performance)
- Plans de rémunération et de primes
- Documents relatifs aux avantages sociaux (assurance, retraite, etc.)
- Procédures disciplinaires et documents de gestion des litiges internes...

Ventes

- Propositions commerciales et devis aux clients
- Contrats clients et accords de partenariat
- Documents de négociation et notes internes sur les conditions commerciales
- Données de tarification et modèles de prix confidentiels
- Rapports de performance commerciale (chiffre d'affaires, pipeline de ventes)...

Juridique

- Accords commerciaux, contrats d'acquisition, partenariats stratégiques...
- Dossiers juridiques et informations sur des affaires en cours.
- Brevets et marques déposées.
- Rapports d'audit, certifications, dossiers réglementaires.
- Accords de non-divulgation (NDA)...

Cryptez vos documents

Le cryptage est une technique qui transforme les données en un code illisible pour quiconque n'ayant pas la clé de déchiffrement appropriée.
En clair, même si un document crypté est intercepté, il restera inaccessible et inutilisable sans cette clé.

Tous vos documents sensibles doivent être cryptés, durant tout leur cycle de vie – de leur création à leur archivage.

Veillez à la sécurité de vos documents tout au long de leur cycle de vie

Utilisez-vous des plateformes sécurisées pour le stockage à long terme ? Détruisez-vous de façon sécurisée les documents obsolètes, par exemple par une suppression cryptographique des données ?

Vous devez garantir la protection des documents à chaque étape de leur vie (création, transmission, stockage et destruction), en vous appuyant sur des mécanismes de contrôle stricts pour prévenir tout accès non autorisé ou altération.

Instaurez une politique de sauvegarde régulière

Une politique de sauvegarde régulière permet de minimiser les risques en assurant la disponibilité des documents importants à tout moment. Opter pour des serveurs sécurisés situés en Europe renforce la protection des informations sensibles.

Ces sauvegardes doivent être testées périodiquement pour s'assurer de leur intégrité et de leur capacité à restaurer rapidement les documents et contrats en cas de besoin.

Utilisez des certificats numériques

Délivrés par des autorités de certifications (tiers de confiance), les certificats numériques garantissent que les documents n'ont pas été modifiés après leur signature, assurant ainsi leur authenticité et leur valeur juridique. Ces certifications reposent sur des algorithmes cryptographiques qui associent l'identité du signataire au document de manière sécurisée.

En plus de prouver l'identité des signataires, elles offrent une traçabilité et un horodatage des actions. En conformité avec des normes légales strictes, comme le règlement eIDAS en Europe, les signatures électroniques certifiées renforcent la sécurité de vos échanges et protègent l'entreprise contre la fraude et les litiges.

Formez toutes vos équipes

Utilisation de mots de passe faibles, phishing, navigation non sécurisée, contournement des contrôles de sécurité perçus comme contraignants, utilisation de l'IA inappropriée... Tous ces comportements peuvent avoir de lourdes conséquences sur l'intégrité numérique de vos transactions numériques.

C'est pourquoi la formation régulière de vos équipes sur les bonnes pratiques de sécurité est indispensable. Cela inclut aussi la création de mots de passe forts, la reconnaissance des tentatives de phishing et la gestion sécurisée des documents sensibles. Vous pouvez aussi encourager l'utilisation de l'authentification à deux facteurs (2FA) pour renforcer la protection des comptes de vos salariés.

Connaissez-vous le principe du Zero Trust ?

"Ne jamais faire confiance, toujours vérifier", c'est la devise du Zero Trust ! Il s'agit d'une stratégie de cybersécurité dans laquelle chaque connexion, que ce soit pour accéder à une application, un service ou via une API, est systématiquement vérifiée et autorisée. Cette stratégie renforce la protection contre les menaces, tout en aidant à respecter les exigences de conformité et de sécurité des données.

Faire de son intégrité numérique un levier stratégique

La sécurisation de vos contrats, documents et identités numériques peut devenir un véritable avantage concurrentiel et renforcer la confiance de vos partenaires et clients. Vous réduisez les risques, accélérez les transactions et améliorez la conformité.

C'est pourquoi il est primordial d'adopter une démarche constante et d'investir dans des solutions adaptées pour protéger efficacement les personnes et les actifs numériques dans ce paysage en mutation technologique constante.

91 % **des dirigeants et professionnels IT/de sécurité disent que la cybersécurité est une question stratégique majeure dans leur entreprise.**

Cependant, moins de la moitié des répondants déclarent que leurs dirigeants ont une compréhension avancée de termes comme la gestion des vulnérabilités

D'après un rapport signé Ivanti

Limitation des risques de non-conformité

Garantir la validité de vos documents, contrats et identités numériques protège l'intégrité de vos données, tout en assurant la conformité avec les différentes régulations. Vous réduisez les risques de falsification ou de manipulation non autorisée, ce qui peut entraîner des pertes financières et des dommages à votre réputation.

Aussi, en collaborant avec des partenaires vérifiés, vous démontrez votre engagement envers des solutions reconnues, ce qui renforce votre crédibilité sur le marché.

2 cas d'usage

Prévenir les fraudes contractuelles grâce à des outils de signature électronique conformes

Une PME décide d'adopter une solution de signature électronique certifiée conforme à la réglementation eIDAS. Un de leurs contrats clés est contesté par un client qui prétend que les termes du contrat ont été modifiés après la signature. Grâce à l'intégrité numérique de la solution utilisée, qui garantit que les documents sont cryptés et infalsifiables, l'entreprise peut prouver la validité du contrat en fournissant un audit détaillé. Cela permet d'éviter un litige juridique coûteux et de préserver leur réputation sur le marché.

Sécuriser les identités numériques pour éviter les usurpations

Une start-up spécialisée collabore avec un partenaire pour le lancement d'un produit. En utilisant une solution de vérification d'identité numérique conforme au RGPD, l'entreprise détecte que l'un des interlocuteurs prétendant représenter un partenaire est en réalité un acteur malveillant tentant d'accéder à des données sensibles. En protégeant l'intégrité numérique des échanges, la start-up évite une potentielle fuite de données qui aurait pu entraîner des sanctions pour non-conformité et ternir leur crédibilité auprès des investisseurs.

Augmentation du chiffre d'affaires

En mettant l'accent sur la sécurisation des documents, vous montrez à vos clients que leurs informations sont protégées. La perception de votre marque s'améliore, ce qui se traduit par une meilleure rétention et une meilleure conversion des prospects en clients.

La sécurisation de vos opérations permet également d'accélérer vos résultats commerciaux, ce qui a un impact direct sur les revenus. En effet, vous réduisez ainsi le temps nécessaire pour signer de nouveaux contrats et améliorez votre réactivité opérationnelle.

2 cas d'usage

Protection des données dans une entreprise internationale

Une entreprise internationale intègre une solution de signature électronique sécurisée et conforme aux réglementations mondiales pour ses contrats. En garantissant la confidentialité et l'intégrité des données des clients, elle améliore leur confiance. Cela renforce la fidélité d'investisseurs importants et accélère la finalisation des contrats, augmentant ainsi ses résultats financiers.

Sécurisation des contrats chez un géant de l'e-commerce

Un leader de l'e-commerce déploie un système de gestion numérique pour sécuriser ses contrats avec les fournisseurs grâce à une solution conforme aux normes eIDAS. Cette initiative réduit les contestations juridiques et améliore la transparence des opérations. Résultat : une optimisation des processus et une meilleure collaboration avec les partenaires, renforçant sa position sur le marché.

Optimisation des coûts

La sécurisation des transactions digitales et leur automatisation permettent à l'entreprise de gagner un temps précieux. Les équipes passent moins de temps à résoudre des problèmes liés aux erreurs humaines et peuvent ainsi se concentrer sur des activités à plus forte valeur ajoutée.

En limitant les pertes dues aux mauvaises décisions ou à diverses inefficacités, l'entreprise est plus productive et améliore la qualité de ses opérations.

2 cas d'usage

Optimisation des processus dans une entreprise logistique

Une entreprise de logistique implémente une solution numérique sécurisée pour automatiser la gestion des contrats avec ses sous-traitants. En réduisant les erreurs humaines et en évitant les litiges liés à des documents falsifiés, elle limite les pertes financières. Les équipes peuvent ainsi se concentrer sur l'optimisation des chaînes d'approvisionnement, ce qui réduit les coûts opérationnels.

Rationalisation des ressources dans une entreprise de consulting

Une société de consulting déploie une plateforme sécurisée pour la gestion des documents sensibles et la signature électronique. Les erreurs administratives sont quasi éliminées. Les équipes passent moins de temps sur des tâches répétitives, ce qui permet à l'entreprise d'allouer plus de ressources à des projets clients à forte valeur ajoutée. In fine, l'entreprise réduit les coûts tout en augmentant la rentabilité.

“

La cybersécurité reste un jeu perpétuel du chat et de la souris, où les méthodes d’attaque ne cessent d’évoluer. Il est donc crucial de s’appuyer sur des prestataires certifiés et qualifiés, capables de proposer des solutions à la pointe de l’état de l’art pour garantir une protection optimale.

Kevin Dubourg, Director of Engineering, Yousign

Conclusion

Dans un monde où les cybermenaces se multiplient et deviennent de plus en plus sophistiquées, **la sécurité numérique n'est plus une option, mais une nécessité urgente**. Les usurpations d'identité, falsifications de documents et attaques ciblées sur les actifs numériques menacent directement la pérennité des entreprises, avec des conséquences financières, juridiques et réputationnelles majeures. Ce livre blanc met en lumière l'ampleur des risques et la vulnérabilité de nombreuses organisations face à ces dangers.

Cependant, au-delà de la protection essentielle qu'elle offre, une sécurité numérique accrue peut également devenir **un puissant levier de compétitivité**. En effet, en adoptant des solutions certifiées et en renforçant leurs pratiques, les entreprises gagnent la confiance de leurs clients, partenaires et investisseurs, et accélèrent leurs processus. Investir dans une cybersécurité proactive, c'est donc non seulement protéger, mais aussi **se positionner comme un acteur fiable et innovant dans un monde numérique en constante évolution**.

À propos de Yousign

Créé en 2013, Yousign est une solution européenne de signature électronique dédiée à la simplification et à la sécurisation des contrats. Yousign accompagne plus de 20 000 organisations, allant des start-up aux grandes entreprises, dans la transformation digitale de leurs processus documentaires.

La plateforme permet de signer, envoyer et gérer des documents de manière 100 % électronique, tout en garantissant la conformité légale selon les normes européennes, notamment eIDAS. Elle propose une interface intuitive pour l'envoi de documents, une gestion des signataires avec suivi en temps réel, ainsi qu'une piste d'audit complète pour chaque transaction.

De plus, l'outil permet une intégration API rapide et flexible, permettant aux entreprises de l'incorporer facilement à leurs systèmes existants, comme des logiciels RH ou des CRM.

Bénéficiez d'une qualité et d'une expertise inégalées

Notre engagement ne se limite pas à vous fournir notre solution de signature électronique : nous nous engageons à vous offrir une expérience inégalée et à vous fournir un accompagnement sur-mesure pour assurer votre succès.

Un modèle flexible

Sélectionnez le modèle de votre choix, en ligne avec votre Business Model, et accédez à des tarifs compétitifs pour générer du profit rapidement.

Partner success program

Bénéficiez d'un accompagnement 360° sur-mesure : de l'assistance technique à l'accès à des ressources marketing et commerciales.

99.9% SLA (uptime)

Reconnu comme Prestataire de Services de Confiance (TSP), Yousign fournit une solution européenne sécurisée, fiable et robuste, conforme à la réglementation eIDAS.

Intégration < 2 semaines

Intégrez rapidement et facilement notre API "developer-friendly" dans votre produit grâce à notre documentation détaillée et à notre assistance premium.

Plus de 20 000 clients en France

SHINE · sellsy · lifen · bpifrance · AGICAP · Konbini · Matera · leocare

Testez Yousign gratuitement pendant 14 jours !

En savoir plus

À propos d'Hexatrust

Hexatrust est une association française qui réunit désormais plus de 140 entreprises européennes incluant des startups, PME, ETI, avocats, assureurs, banques d'affaires, éditeurs de logiciels, fournisseurs de cloud et sociétés de services, véritables pépites de la cybersécurité et de la confiance numérique française. Fondée en 2013, Hexatrust a pour objectif de défendre, représenter et promouvoir l'expertise et l'innovation des entreprises membres. L'association agit comme un réseau d'entreprises pour mutualiser les efforts, développer des synergies, et représenter les intérêts des membres auprès des instances gouvernementales, des institutions européennes, et des grands donneurs d'ordre.

Hexatrust joue également un rôle important dans la sensibilisation aux enjeux de la cybersécurité et dans le développement de solutions souveraines, c'est-à-dire des solutions technologiques françaises ou européennes qui respectent la confidentialité des données et les réglementations locales. Les membres de Hexatrust collaborent souvent pour répondre à des appels d'offres et proposer des solutions intégrées couvrant différents aspects de la cybersécurité et du cloud.

Enfin, Hexatrust et ses membres, acteurs clés des filières "Industries de Sécurité" et "Solutions Numériques de Confiance", promeuvent la souveraineté numérique française. Leurs solutions, alignées sur la directive NIS2 et l'ANSSI, couvrent cybersécurité et cloud de confiance, répondant aux enjeux de conformité, cyberprotection et transformation numérique, avec une ambition européenne.

En savoir plus