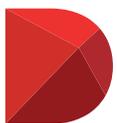




Sécurisation des communications du conseil et des dirigeants Guide d'achat de logiciel



Diligent

Sécurisation des communications du conseil et des dirigeants, pour une gouvernance moderne

Les communications électroniques entre les membres du conseil et les cadres supérieurs font partie intégrante de la gouvernance des entreprises. Lorsqu'un dirigeant ou un membre du conseil doit aborder un sujet sensible, on s'attend généralement à le voir décrocher son téléphone. Cependant, en réalité, il choisira le moyen le plus facile et le plus pratique, comme l'e-mail ou le message électronique. Pour de nombreuses entreprises, ces communications ne sont ni protégées ni administrées correctement. Il est donc essentiel de leur fournir une solution de communication qui offre une sécurité « automatique » à ses utilisateurs. L'erreur humaine nourrit cette demande : elle entraîne souvent des fuites de données ou une divulgation involontaire d'informations sensibles.

Les communications sécurisées, indispensables à une gouvernance moderne et au service de l'entreprise, sont souvent négligées. Plutôt que de déployer une solution de messagerie spécifiquement conçue pour renforcer une gouvernance dans l'air du temps, grâce à des capacités de collaboration et de sécurisation améliorées, les entreprises utilisent diverses applications grand public et des services de messagerie traditionnels qui ne peuvent pas respecter les normes recommandées aujourd'hui aux membres du conseil et aux cadres dirigeants.

Les entreprises sont tenues de fournir aux membres du conseil et aux cadres dirigeants un environnement de communication sécurisé qui réduise les vulnérabilités à l'erreur humaine. Il est temps de bouleverser le statu quo et de mettre un terme à l'utilisation de ces outils de communication personnels ou non sécurisés. Si nous ignorons ce défi, c'est la porte ouverte au vol d'informations sensibles. Sans action, votre entreprise sera menacée et souffrira d'un grave manque de gouvernance.



Les pirates informatiques savent qu'ils peuvent obtenir un gain financier en subtilisant les informations échangées entre membres du conseil et dirigeants. Selon l'étude Verizon 2019 sur la compromission des données, les cadres supérieurs sont six fois plus susceptibles d'être la cible d'une attaque. Dans cette même étude, on apprend que 94 % des incidents concernent les e-mails. Le vol d'identifiants de messagerie est répandu et personne n'est à l'abri d'un gestionnaire informatique malveillant. Selon l'étude Verizon, plus d'un tiers des violations de données impliquent des acteurs internes à l'entreprise.

Les systèmes de messagerie d'entreprise comme Outlook ne sont pas suffisamment sécurisés pour protéger efficacement les communications des membres du conseil et des cadres dirigeants. Par exemple, lors de la négociation des contrats, les membres du conseil et les dirigeants ont besoin d'un outil de collaboration facile à utiliser. Si une contre-offre doit être présentée en urgence, les entreprises se tourneront davantage vers des systèmes de messagerie d'entreprise. Au-delà du risque de vulnérabilité zero-day (une faille n'ayant aucun correctif connu, et découverte par des attaquants avant la disponibilité d'un correctif de sécurité), les utilisateurs qui ne sont pas à jour des derniers correctifs et des dernières mises à jour peuvent être exposés aux menaces.

Les stratégies de conservation des données incohérentes et défaillantes entravent également les communications du conseil. L'utilisation de la messagerie d'entreprise peut également être problématique en cas de litige avec une autre société. En effet, si un membre du conseil siège dans plusieurs conseils d'administration, son adresse e-mail devient accessible. Dans ce cas, des communications sensibles de votre conseil peuvent être exposées. Et dans certains déploiements vers le cloud, une suppression accidentelle peut être définitive. Si vous ne limitez pas l'accès aux e-mails ou aux transferts de fichiers et pièces jointes, vous risquez des divulgations qui vous mettraient dans une situation délicate.

Les services de messagerie grand public comme Gmail sont une alternative encore moins sécurisée. Les systèmes publics et les services de messagerie d'entreprise rencontrent généralement les mêmes problèmes, mais les entreprises n'ont pas de contrôle sur les comptes de messagerie grand public. Les fichiers et les données qu'ils reçoivent doivent être considérés comme perdus définitivement. De plus, la sécurité dépend entièrement de l'utilisateur. Les mots de passe enregistrés dans un navigateur sont une vulnérabilité répandue ; toute personne ayant accès à l'appareil peut consulter, envoyer, retransmettre ou subtiliser n'importe quel message de ce compte. Très peu d'utilisateurs utilisent le chiffrement des données, qui sont alors exposées au vol.

Les services de messageries grand public ne font guère mieux. De nombreuses vulnérabilités connues touchent les services de messagerie instantanée. **Les récents incidents liés à WhatsApp en sont un bon exemple.** Il est donc d'autant plus important de trouver des solutions éprouvées en matière de sécurité et de conformité. L'élimination des outils de communication exposés aux vulnérabilités connues, réduisant la zone à risque, est un grand pas en avant dans la sécurisation des systèmes de communication utilisés par les membres du conseil et les cadres supérieurs.

Un guide d'achat pour évaluer les services de communication des membres du conseil et des dirigeants

Une fois qu'une entreprise comprend la nécessité de posséder un système de messagerie sécurisé et complet au service d'une gouvernance moderne, la recherche de la solution adaptée à ce défi devient un processus critique. Vous trouverez ci-dessous une liste détaillée des fonctionnalités et des capacités requises par les entreprises à la recherche d'une solution de communication sécurisée. Trois questions sont essentielles pour trouver une solution optimale : la gouvernance, la sécurité et la facilité d'utilisation.

Gouvernance : l'impact des communications sécurisées

Pour offrir une solution inégalée en matière de communication sensible aux membres du conseil et aux dirigeants, il faut tenir compte des exigences juridiques et de conformité. Ceci pose plusieurs questions :

- **Tous les types de communication du conseil d'administration et des données sensibles (textes, messages et e-mails) sont-ils gérés dans un même système ?**
- **L'intégralité des informations, y compris les fichiers et les pièces jointes, reste-t-elle dans le système pour éviter les fuites de données ?**
- **Le système assure-t-il des communications transparentes entre les dirigeants et les membres du conseil ?**
- **Votre fournisseur dispose-t-il d'une équipe interne formée aux enjeux de gouvernance et de conformité ?**
- **Les services proposés par ce fournisseur sont-ils conformes aux exigences en matière d'accessibilité et de réglementation ?**
- **La solution permet-elle d'effacer ou de désactiver rapidement les appareils perdus ou volés ?**
- **Le fournisseur est-il réputé pour ses solutions de conformité ?**
- **Le système gère-t-il les documents de manière appropriée ?**



Les qualités indispensables d'un système de communication sécurisé pour les dirigeants et les membres du conseil :

- **Un outil unique pour plusieurs modes de communication :** en matière de gouvernance et de conformité, le contrôle est essentiel. Cependant, lorsque des membres du conseil ou des dirigeants utilisent plusieurs outils de messagerie, il n'y a plus de contrôle. La solution idéale vous fournit un outil unique à la fois pour les e-mails et vos messages sécurisés.
- **Prévention des fuites de données :** outre les e-mails et les messages, les fichiers et les pièces jointes contiennent eux aussi de nombreuses informations sensibles. Diligent Messenger protège votre message et s'assure que les documents joints ne quittent jamais votre système sécurisé.
- **Une transparence garantie :** la transparence est une autre exigence clé pour les stratégies juridiques, de conformité et de gouvernance. Bien trop souvent, le manque de transparence n'est pas un défaut de conception, mais est dû à la multiplicité des outils de communication utilisés. La centralisation de toutes vos communications en une solution unique facilite la transparence.
- **Des interlocuteurs expert en gouvernance :** de nombreux systèmes de communication et de messagerie sont accessibles au grand public, ce qui signifie que les équipes de ces fournisseurs n'ont pas de compétence en matière de gouvernance. L'outil Diligent Messenger s'accompagne d'une équipe dont l'expertise en gouvernance n'est plus à prouver et qui parle le même langage que les dirigeants.
- **Conformité aux exigences de conservation/accessibilité des données :** les systèmes de messagerie d'entreprise et grand public échouent à ce test. Les systèmes d'entreprise pratiquent généralement des périodes de conservation génériques et ne proposent que peu d'assistance en matière d'accessibilité des données. Les services grand public n'offrent aucun contrôle. Lorsqu'un e-mail est supprimé accidentellement, il est disparu à jamais.
- **Gestion des documents pour les appareils perdus/volés :** les régimes de conformité appliquent des règles strictes en cas de perte ou de vol d'un appareil d'une personne clé, et nécessitent souvent son effacement ou sa désactivation. Sans cette fonctionnalité, vous pouvez être certain de ne pas être conforme à la législation.
- **Une réputation solide en matière de conformité :** tous les fournisseurs n'ont pas pour mission d'offrir une meilleure gouvernance, dans l'air du temps et au service de la compétitivité de l'entreprise. Diligent Messenger a une excellente réputation et répond aux dernières exigences en matière de gouvernance.
- **Une capacité à assurer une bonne gestion des archives :** l'utilisation d'une solution conçue spécifiquement pour vos communications permet d'assurer plus facilement la gestion de vos archives. Vous n'avez plus besoin de lier plusieurs systèmes ou de gérer les archives dans des logiciels qui ne disposent pas de fonctionnalités adaptées.

Sécurité : Comprendre les processus de sécurité supportant les communications sécurisées

La cybersécurité est devenue l'une des priorités essentielles dans les entreprises. Les cyberattaques nuisent à la réputation de votre entreprise, causent des dommages financiers et vous exposent à de lourdes sanctions. Les communications sensibles entre les cadres supérieurs et les membres de conseil sont une cible de choix. Les questions clés en matière de sécurité sont les suivantes :

- **S'agit-il d'une plateforme de communication fermée qui n'est pas accessible au public ?**
- **Toutes les communications sont-elles chiffrées ?**
- **L'équipe du fournisseur de la solution a-t-elle suivi une formation rigoureuse en matière de sécurité ?**
- **Existe-t-il un service d'assistance pour la messagerie et le courrier électronique sécurisés ?**
- **Le fournisseur utilise-t-il les technologies les plus récentes en matière de sécurité ?**
- **L'équipe du fournisseur se soumet-elle à des audits réguliers qu'elle réussit ?**
- **Le fournisseur a-t-il une solide réputation en matière de solutions de messagerie sécurisées ?**
- **La solution protège-t-elle les pièces jointes et applique-t-elle une restriction sur les couper/coller ?**
- **Le fournisseur effectue-t-il des tests de vulnérabilité et d'intrusion sur son produit ?**

Les qualités essentielles en matière de sécurité du système de communication idéal pour les dirigeants et les membres du conseil :

- **Une plateforme de communications inaccessible au public :** la plupart des applications de messagerie sont accessibles au grand public. Il suffit aux pirates de s'y inscrire pour avoir accès à un compte, ce qui facilite les attaques. Diligent Messenger est un service de messagerie fermé et autonome inaccessible au public.
- **Chiffrement des communications :** la première étape nécessaire à la sécurisation de vos échanges consiste à chiffrer les e-mails, les messages et autres types de communications sensibles. La plupart des systèmes de messagerie permettent d'activer le chiffrement, mais le chiffrement par défaut fournit une sécurisation de base des communications. Diligent Messenger chiffre par défaut toutes les communications.
- **Une équipe fournisseur formée à la sécurité :** la conception de produits sécurisés est au cœur du travail de chaque salarié de Diligent Messenger. Votre fournisseur doit investir du temps et des ressources pour s'assurer que les salariés impliqués dans le développement et la relation client disposent des compétences nécessaires en matière de sécurité. Les membres de l'équipe d'assistance doivent être formés aux questions de cybersécurité pour fournir une assistance adaptée à vos besoins.
- **Une assistance pour la messagerie et les e-mails sécurisés :** lorsque vous utilisez plusieurs applications, les pirates informatiques chercheront la plus vulnérable pour s'introduire dans votre système. Avec une plateforme unique pour toutes vos communications, vous déployez plus facilement une sécurité plus cohérente.



- **Engagement du fournisseur à sécuriser son exploitation et à utiliser les dernières technologies :** un fournisseur qui se soucie de la sécurité utilisera les dernières technologies de sécurisation dans sa propre organisation. Il devrait être capable de documenter aisément son propre usage des outils et technologies les plus efficaces.
- **Résultats positifs aux audits de sécurité :** un fournisseur doit être en mesure de fournir des détails précis sur ses précédents audits de sécurité et de conformité. Diligent est fier de présenter ses derniers audits de sécurité et de conformité, notamment SOC2, HIPAA AT101, SSAE 16/ISAE 3402 et ISO 27001.
- **Une solide réputation de conception de solutions sécurisées :** le fournisseur doit être reconnu pour offrir aux membres du conseil et aux dirigeants des solutions sécurisées en matière de communication. Malheureusement, une simple recherche sur Google vous démontrera que de nombreux produits de communication ont déjà rencontré des problèmes dans le passé.
- **Contrôle des pièces jointes et du copier/coller :** le plus souvent, la perte des données est due à des lacunes dans la sécurité des pièces jointes aux e-mails, ou à un manque de contrôle sur les informations qui peuvent être coupées et collées en dehors du système. Cela concerne également la gestion des captures d'écran susceptibles de divulguer des informations sensibles. Diligent Messenger fournit une solution complète pour restreindre les pièces jointes et la fonction couper/coller.
- **Les tests d'intrusion et de vulnérabilité du service du fournisseur :** pour garantir la sécurité du service de communication, le fournisseur doit se soumettre à des tests de vulnérabilité et d'intrusion, qui garantissent l'absence de faille exploitable par les pirates informatiques souhaitant accéder aux informations sensibles.

Facilité d'utilisation : l'outil s'adapte-t-il facilement ?

Il ne suffit pas de choisir une plateforme de communication sécurisée qui réponde à tous les critères de gouvernance et de sécurité. Elle doit également être attractive pour les utilisateurs. Si la solution de communication est difficile à utiliser et nécessite une formation poussée, les membres du conseil et les dirigeants auront tendance à la délaïsser. En matière de facilité d'utilisation, il faut se poser les bonnes questions :

- **Existe-t-il un environnement facile à utiliser qui centralise les e-mails et la messagerie ?**
- **Le fournisseur offre-t-il une assistance hors pair aux membres du conseil et aux dirigeants d'entreprise ?**
- **L'utilisateur peut-il rappeler des messages ou des e-mails envoyés par erreur ?**
- **Offre-t-il un affichage en écran partagé pour davantage d'ergonomie ?**
- **Le fournisseur a-t-il une excellente réputation en matière d'ergonomie ?**
- **La solution permet-elle d'entrer en relation instantanément avec les autres membres de l'équipe ?**
- **Existe-t-il un contrôle de version pour s'assurer que tous disposent des mêmes documents ?**
- **Le système automatise-t-il la gestion de l'accessibilité et de la conservation des données à des fins juridiques ?**

Les qualités essentielles en matière de sécurité du système de communication idéal pour les dirigeants et les membres du conseil :

- **Un environnement unique pour les e-mails et les messages :** pour une convivialité optimale, vous souhaitez utiliser un outil qui centralise toutes vos communications et accessible sur tous vos appareils pour une plus grande facilité d'utilisation. Cette solution unique favorise une utilisation continue, facile à apprivoiser, pour un gain d'efficacité certain. Cet avantage de Diligent Messenger est particulièrement apprécié par les utilisateurs.
- **Une assistance utilisateur hors pair :** il est essentiel que le fournisseur bénéficie d'une excellente réputation en matière d'assistance utilisateur. Par exemple, Diligent dispose de nombreuses références client et d'études de cas illustrant la qualité de son service client. L'équipe d'assistance apporte immédiatement des réponses adaptées aux problèmes et a une interaction appropriée avec les dirigeants.
- **Rappel des messages et des e-mails :** le rappel des messages et des e-mails est une fonctionnalité essentielle pour les cadres supérieurs et les membres du conseil, puisque les messages erronés ou obsolètes peuvent devenir un problème et faire perdre du temps aux dirigeants et aux membres du conseil.
- **Affichage en écran partagé :** l'accès simultané aux fichiers et aux informations favorise la collaboration. En outre, la possibilité de consultation des informations clés en temps réel pendant la conversation permet d'améliorer la productivité.

- **Une réputation solide en matière d'ergonomie :** le fournisseur doit être capable de présenter des preuves internes et externes de l'ergonomie de sa plateforme de communication. Les membres du conseil et les cadres supérieurs ont des besoins spécifiques en matière d'ergonomie. Le fournisseur se doit de fournir une formation continue à tous les utilisateurs, et à tout moment.
- **Une connexion instantanée aux membres de l'équipe :** dans de nombreux scénarios, les membres du conseil et les cadres supérieurs exigent une communication en temps réel pour s'adapter au contexte des affaires en accélération permanente. Diligent Messenger est particulièrement appréciée des entreprises pour ses communications instantanées.
- **Un contrôle de version pour assurer la cohérence des informations :** les informations et les données changent constamment. Il est essentiel de fournir aux membres du conseil et aux dirigeants une plateforme de communication garantissant l'homogénéité et la validité des informations. Nul ne devrait être obligé à se plonger dans les archives pour trouver la bonne information.
- **Automatisation de l'accessibilité et de la conservation des données à des fins juridiques :** pour garantir la facilité d'utilisation, il est essentiel d'éliminer le fardeau de la gestion du statut d'accessibilité et de conservation à des fins juridiques des messages et des e-mails. En outre, l'automatisation garantit une application homogène des politiques internes en place. C'est une fonctionnalité très appréciée des utilisateurs de Diligent Messenger.



Diligent Messenger garantit des communications sécurisées et faciles à utiliser pour une gouvernance moderne

La réussite de l'entreprise repose essentiellement sur une communication efficace entre les cadres supérieurs. Diligent Messenger offre une solution complète, sécurisée et facile d'utilisation qui rend plus efficace la collaboration des conseils et des dirigeants. Ce produit permet à l'équipe de partager des informations de propriété intellectuelle, d'accéder à des fichiers confidentiels et de partager leurs points de vue sans limite et sans craindre que les données soient interceptées. Le chiffrement et la sécurité permettent aux membres du conseil de travailler sans problème au-delà du pare-feu. Grâce à notre plateforme qui centralise les e-mails et la messagerie, les membres du conseil et les dirigeants peuvent choisir leur mode de communication favori.

Diligent Messenger est étroitement lié aux dernières innovations en matière de gouvernance moderne. Diligent propose aux membres du conseil et aux dirigeants une plateforme technologique adéquate pour les communications sensibles, et facilite les échanges tout en répondant à vos besoins en matière de gouvernance et de sécurité. Diligent Messenger propose bien plus de fonctionnalités que les systèmes d'e-mails et de messagerie instantanée publics et privés. Messenger est également intégré à Diligent Boards, la solution technologique la plus performante du marché en matière de gouvernance moderne pour les conseils d'administration. Cet ensemble de fonctionnalités et de capacités fait de Diligent Messenger la plateforme de communication optimale au service d'une gouvernance dans l'air du temps. En tant que composant intégré du Governance Cloud de Diligent, Messenger est un élément indissociable de notre plateforme complète.

La solution Diligent Messenger vous permet de respecter plus facilement les exigences de conformité et de gouvernance. Les demandes de conformité les plus importantes et les plus répandues sont celles d'un environnement unique et sécurisé pour les communications du conseil et des dirigeants, qui garantit la confidentialité des informations sensibles. Une assistance est également fournie pour une transparence optimale. La capacité de rappeler des e-mails ou d'effacer le contenu d'un appareil perdu ou volé vous aide à respecter vos obligations clés en matière de gouvernance et de conformité.

Diligent Messenger est également une solution hautement sécurisée qui protège vos communications sensibles. Diligent Messenger est certifiée ISO 27001, la référence absolue en matière de sécurité informatique. Elle permet l'autorisation de l'appareil sur les systèmes iOS et Android, avec plusieurs niveaux de sécurité. Grâce à cette solution réservée aux entreprises, vos communications sont sous contrôle. Le chiffrement complet empêche les pirates informatiques de consulter la moindre information interceptée. Vous contrôlez pleinement les pièces jointes et la fonction couper/coller, et êtes en mesure de rappeler des messages pour éviter la fuite de données.

La garantie d'un haut niveau de convivialité est l'un des principaux objectifs de conception de Diligent Messenger. La solution vous offre une plateforme de communication complète mais épurée pour toutes les activités du conseil d'administration. Les notifications push préviennent instantanément les membres du conseil et les dirigeants dès la réception d'un message. Grâce à l'affichage en écran partagé, les membres du conseil peuvent interagir tout en consultant les

dernières informations. Les membres du conseil peuvent également se concentrer sur des tâches clés : Diligent Messenger automatise de nombreuses tâches logistiques, comme la définition d'une politique de conservation des données à des fins juridiques. Pour permettre aux membres du conseil et aux dirigeants de tirer le meilleur parti de Messenger, chaque client bénéficie d'une formation, de tutoriels et d'une assistance 24 h/24 et 7 j/7.

Cas d'utilisation courants pour Diligent Messenger

La capacité à communiquer en toute sécurité entre des groupes spécifiques n'est pas limitée aux membres du conseil et aux dirigeants. Elle peut également être utilisée dans d'autres scénarios : Diligent Messenger convient parfaitement à d'autres scénarios d'utilisation courants en entreprise :

- **Groupes de travail ou équipes dirigeantes** : la modification ou le développement d'une nouvelle stratégie d'entreprise, ou encore le lancement d'un produit, exigent une solution de communication complète et plus sécurisée qui n'est pas sujette aux vulnérabilités et au manque de contrôle couramment constatés dans les solutions d'e-mails d'entreprise ou les systèmes de messagerie sur smartphone.
- **Équipes de projet de fusions-acquisitions** : il est essentiel de garantir la sécurité des communications pour l'équipe chargée des fusions-acquisitions. La fuite d'informations n'est pas qu'un simple désagrément : la divulgation accidentelle des plans de fusions-acquisitions peut entraîner l'annulation de la transaction et offrir un avantage considérable aux concurrents. Avec la plateforme de communication Diligent Messenger, vous évitez les problèmes de communication susceptibles d'entraver vos projets de fusions-acquisitions.
- **Des équipes stratégiques de développement produit** : dans de nombreuses entreprises, les feuilles de route et les plans de développement produit sont des éléments de propriété intellectuelle précieux. Il est essentiel de veiller à ce que toutes les communications les concernant, y compris les pièces jointes des fichiers, soient les plus sécurisées possible.
- **Enjeux juridiques internes** : dans notre environnement très procédurier, les poursuites judiciaires et les actions en justice sont monnaie courante. La capacité à contrôler et à sécuriser les communications des litiges, ainsi qu'à empêcher les divulgations, est une nécessité absolue. Pour empêcher les fuites accidentelles d'informations sensibles, vous pouvez délaissier les outils de messagerie grand public et opter pour une plateforme de communication sécurisée.
- **Gestion de crise** : la direction et les conseils sont responsables de la continuité des activités. En temps de crise, c'est une mission particulièrement difficile, notamment après une cyberattaque ou lorsque la réputation de l'entreprise est en jeu. Diligent Messenger offre aux dirigeants des outils de messagerie instantanée hautement sécurisés pour gérer la crise en temps réel jusqu'à sa résolution.

Ce qu'il faut retenir

Les entreprises numériques s'appuient sur des communications numériques. Même si la plupart des systèmes de messagerie les plus connus suffisent pour les processus métier courants, ils n'offrent pas la sécurité, la conformité et la facilité d'utilisation nécessaires pour des scénarios plus risqués, comme les communications au niveau du conseil. L'utilisation de systèmes de messagerie externes et de systèmes d'e-mails d'entreprise ou accessibles au public vous expose à des risques bien trop importants, comme les vulnérabilités, le manque de contrôle et les problèmes juridiques potentiels soulevés par la gouvernance.

Ce sont les raisons qui poussent les entreprises à déployer Diligent Messenger, une solution conçue pour répondre aux exigences des communications au niveau du conseil ou comportant des informations sensibles. Avant de faire un choix définitif, l'entreprise doit exiger des réponses aux questions clés énumérées dans ce Guide d'Achat. Diligent Messenger est conçu pour répondre à une demande de solution de communication sécurisée, conforme et conviviale pour le conseil d'administration et les projets sensibles, dans le cadre de notre vision globale au service d'une gouvernance moderne.



Diligent est une marque de Diligent Corporation, déposée aux États-Unis. Toutes les marques tierces sont la propriété de leurs propriétaires respectifs. ©2019 Diligent Corporation. Tous droits réservés.

Pour en savoir plus, contactez-nous aux coordonnées suivantes :

E-mail : info@diligent.com
Appelez le +33 (0)1 86 76 70 80
Visitez : www.diligent.com/fr