Seald vous permet de crypter tous vos messages, sur n’importe quelle plateforme

---

Chiffrer vos mails et diverses messageries instantanées sans qu’aucun intermédiaire entre vous et votre contact n’y accède est désormais possible avec Seald ! Son CEO, Timothée Rebours, présente sa pépite.

Seald est une solution de chiffrage de messages électroniques (mails, messageries instantanées, etc.) qui garantie une absence totale d’intermédiaire entre l’expéditeur et le destinataire d’un message. Partiellement gratuit, ce service s’adresse à tous en raison de sa compatibilité avec la grande majorité des outils de communication quotidiens.

Pouvez-vous nous présenter votre outil ?

Seald propose d’ajouter une couche de chiffrement de bout-en-bout à tous vos outils usuels (GMail, Slack, Office 365, ou n’importe quoi d’autre) extrêmement simplement. Notre technologie permet de s’assurer que seuls les destinataires d’un message ou d’un fichier pourront le lire, c’est-à-dire qu’aucun intermédiaire (y compris Seald) ne possède de moyen de déchiffrer le contenu. Ainsi, même si le compte en ligne utilisé pour envoyer le contenu, ou si les serveurs relayant ce contenu venaient à être compromis par un pirate ou un employé mal intentionné, ce qui est chiffré par Seald ne peut être déchiffré que par les destinataires choisis au moment du chiffrement. Seald est une application (compatible Windows 7, 8, et macOS) que vous installez sur votre ordinateur en quelques étapes simples. Une paire de clés asymétriques est générée sur l’ordinateur, elle est associée à une ou plusieurs adresses e-mail

par le biais d'un e-mail de validation. Une fois validé, vos destinataires peuvent vous ajouter à leurs contacts en connaissant votre e-mail. Une extension est automatiquement installée par l'application dans les outils avec lesquels Seald est compatible (aujourd'hui navigateurs et Slack desktop). Pour chiffrer un message, il suffit alors de sélectionner le texte « sensible », de faire un clic droit et de cliquer sur Seald pour le chiffrer pour le destinataire de votre message. Une fois envoyé, le message apparaît comme une bulle, qui ne peut être déchiffrée que par les destinataires en cliquant dessus. Plus de 2500 messages et documents ont déjà été protégés avec Seald.

Qui sont vos principaux concurrents actuellement sur votre marché ?

La concurrence se divise en trois types d'acteurs :

- Des outils de chiffrement sans intégration tels que Symantec PGP, GnuPG, AxCrypt ou Zed. Ceux-ci permettent de chiffrer des documents avec une myriade d'options et d'étapes qui perdent souvent l'utilisateur néophyte.
- Des moyens de communication chiffrés tels que Symphony, ProtonMail ou Telegram qui doivent remplacer vos outils du quotidien, et empêchent vos employés de choisir les outils qui les rendent le plus productif.
- Des plugins ou reverse proxy proposant une intégration avec quelques outils de communications mais qui ne sont pas universels comme Virtru ou CipherCloud et qui limitent la palette d'outils à disposition de vos employés. Notre solution vous permet d'offrir à vos employés un moyen de sécuriser leurs échanges de données en interne et avec l'extérieur en toute simplicité. Notre chiffrement est réellement de bout-en-bout, ce qui veut dire qu'aucun serveur intermédiaire ne détient à un quelconque moment du protocole des clés permettant le déchiffrement des données échangées. Seules les clés enregistrées sur les postes – et une éventuelle clé de sauvegarde générée par un administrateur dans la version payante – ont la capacité de déchiffrer les données.

Quel est votre business model ?

La version gratuite de notre application permet de chiffrer/déchiffrer des messages et des fichiers sans limitation, ce qui permet d'échanger avec n'importe qui gratuitement. La version payante (en cours de développement) permettra aux entreprises y souscrivant d'ajouter des fonctionnalités de sauvegarde, de journalisation des accès, une révocation d'accès, de gestion centralisée des utilisateurs dans l'entreprise, des intégrations avec l'infrastructure d'entreprise – par exemple un serveur LDAP – et un support prioritaire. L'entreprise est destinée à être cross-border, la R&D est basée à Paris, et l'opérationnel sera effectué depuis San Francisco. L'équipe vise à maximiser son nombre de partenariats en intégrant Seald à l'outillage déjà présent sur le marché professionnel et en s'alliant avec des cabinets de conseil

en cyber-sécurité, permettant d’avoir une image de solution à la fois sécurisée et adaptée au milieu professionnel.

Une actualité financière ?

Nous sommes actuellement en levée de fond et essayons de réunir 500 000 euros.

Qui sont les fondateurs ?

Le projet Seald a débuté en 2015 en Californie, dans le cadre du Master 2 d’entrepreneuriat de l’École Polytechnique, un programme dans lequel 40 étudiants sont envoyés à UC Berkeley, dans la Silicon Valley pour 4 mois afin de créer leur startup. Timothée Rebours, CEO, diplômé de l’Ecole Polytechnique et Berkeley. Développeur, il s’intéresse tout particulièrement aux problématiques business. Mehdi Kouhen, CTO, diplômé de l’Ecole Polytechnique et Berkeley. Développeur et expert réseau, il travaille surtout sur les problématiques d’architecture logicielle. Maxime Huber, CPO. Diplômé de l’université Paris-Dauphine et de Berkeley, il s’occupe du développement produit. Dan Lousqui, CSO. Diplômé de l’Ensimag, développeur et expert en cyber-sécurité, on peut le considérer comme un hacker légal (White Hat).

https://www.youtube.com/watch?v=83ZeB2GEE4A&feature=youtu.be