

Quand la confiance des clients ne peut souffrir aucun compromis

Comment un grand cabinet d'avocats du Magic Circle a modernisé sa communication sécurisée — tout en préservant l'intégralité de ses processus clients.

Points de preuve techniques

Architecture

- SaaS natif sur AWS, entièrement conçu selon une approche cloud first
- Intégration à l'environnement Mimecast existant
- Aucun remplacement complet de la pile actuelle
- Parité fonctionnelle totale avec l'appliance PGP Universal héritée

Contrôle

- S/MIME sortant avec sélection automatique des clés
- PGP optionnel via mot-clé déclencheur dans l'objet du message
- Signature appliquée à chaque message sortant
- Publication des clés dans LDAP pour un partage à l'échelle du cabinet
- Requêtes externes via l'agrégateur Global TrustPoint

Remise

- Déchiffrement des messages entrants S/MIME et PGP au niveau de la passerelle
- Collecte automatique des clés publiques à partir des messages signés
- Suppression des clés après collecte pour préserver la lisibilité des boîtes de réception
- Alignement avec les politiques entrantes de Mimecast
- Remise via portail en cours d'évaluation pour des cas d'usage plus larges

Résumé exécutif

Pour un cabinet au cœur de transactions transfrontalières, de contentieux à forts enjeux, d'enquêtes internationales et de missions réglementaires complexes, la communication sécurisée n'est pas un simple support : elle fait partie intégrante de la pratique. Pour des clients qui confient certains de leurs sujets les plus sensibles, la discrétion du cabinet compte autant que son expertise juridique, et chaque message chiffré doit refléter cette exigence.

Mais son chiffrement reposait sur des fondations vieillissantes. Une appliance PGP Universal héritée continuait de prendre en charge les workflows fondés sur les certificats attendus par les clients, tout en devenant plus difficile à maintenir et plus compliquée à aligner sur une posture de sécurité moderne, cloud first. Pour un cabinet gérant des échanges d'une extrême confidentialité, ce décalage faisait peser un risque croissant sur la confiance.

Le cabinet s'est tourné vers Echoworx pour un remplacement à parité fonctionnelle : une plateforme cloud native capable de préserver les flux PGP et S/MIME existants, de s'intégrer proprement à son environnement de messagerie sécurisée, et de respecter les processus stricts qui encadrent les communications juridiques à forts enjeux.

Le résultat : un socle de chiffrement moderne, fondé sur des standards reconnus, qui a permis de moderniser les workflows sans perturbation, de renforcer la gouvernance des échanges et de préserver la promesse de confiance numérique du cabinet.

Le défi

01 | Une réputation qui ne laisse aucune place au compromis

Dans la pratique juridique de très haut niveau, la confiance est la véritable monnaie d'échange, et une seule communication mal gérée peut fragiliser une relation client construite au fil des années. Les partenaires et interlocuteurs les plus importants du cabinet imposaient des processus de chiffrement précis et bien établis — des étapes PGP et S/MIME spécifiques, avec très peu de marge de négociation. Toute plateforme de remplacement devait respecter exactement ces exigences, car pour ce cabinet, la protection des communications confidentielles n'est pas une fonctionnalité supplémentaire. Elle fait partie intégrante de la pratique elle-même.

02 | Un chiffrement hérité qui ne pouvait plus suivre

L'appliance PGP Universal du cabinet avait rempli son rôle, mais elle devenait de plus en plus difficile à maintenir et de plus en plus décalée par rapport à une approche de sécurité moderne, résolument cloud first. En tant que client Mimecast, le cabinet avait besoin d'une couche de chiffrement capable de s'intégrer proprement à l'environnement auquel il faisait déjà confiance — et non d'une refonte perturbatrice obligeant ses équipes à réapprendre leurs méthodes de travail. L'exigence était précise : préserver chaque workflow qui fonctionne, tout en modernisant l'infrastructure qui le sous-tend.

03 | Une gouvernance à travers un réseau complexe de contacts externes

Ce cabinet échange des informations sensibles avec des partenaires, des clients et des conseils à travers le monde, chacun avec ses propres clés, ses propres annuaires et ses propres attentes. Gérer cette complexité au moyen d'une infrastructure vieillissante introduisait de la friction et laissait place à l'incohérence. Il fallait un socle unique, gouverné et fondé sur des standards reconnus, capable de localiser les bonnes clés, d'appliquer la bonne protection et d'apporter une preuve de contrôle sur chaque message quittant le périmètre du cabinet.

La Solution

Le cabinet a retenu Echoworx à l'issue d'une évaluation complète en preuve de concept — une évaluation qui a mis à l'épreuve chaque workflow et a produit un résultat concluant sur toute la ligne. Ce qui a rendu la décision simple, c'est ceci : Echoworx était capable d'égaliser l'appliance héritée, fonctionnalité par fonctionnalité, puis de la faire évoluer vers un socle résilient et cloud native, tout en s'intégrant proprement à l'environnement de messagerie sécurisée déjà en place au sein du cabinet.

« Ce cabinet s'est adressé à nous avec un besoin très précis : préserver sans compromis chaque workflow PGP et S/MIME dont dépendent ses clients les plus importants », explique un responsable de mission chez Echoworx. « Nous avons validé chaque cas d'usage dans la preuve de concept, migré chacun d'eux sans friction, et intégré la solution à l'environnement de messagerie sécurisée auquel le cabinet fait déjà confiance. C'est à cela que ressemble, en pratique, une véritable migration à l'identique — et c'est cette base qui permet ensuite à la relation de continuer à se développer. »

Parité fonctionnelle PGP et S/MIME, préservée avec précision

Au cœur de la migration se trouvait le remplacement exact du chiffrement par certificats du cabinet. Les messages sortants utilisent désormais S/MIME avec sélection automatique des clés selon les clés destinataires disponibles, avec un déclenchement PGP optionnel via un mot-clé dans l'objet du message — de sorte que les personnes qui dépendent de la communication sécurisée ont conservé exactement les étapes qu'elles connaissaient déjà. Rien à réapprendre, rien à renégocier. Les workflows attendus par les clients du cabinet se sont poursuivis sans interruption ; seule la plateforme sous-jacente a changé.

Une signature sur chaque message sortant, pour rendre la confiance visible

Parce que S/MIME et PGP sont au cœur de la manière dont ce cabinet communique, tous les e-mails sortants transitent désormais par Echoworx afin que chaque message soit signé. Cette signature est bien plus qu'un détail technique — c'est une marque d'authenticité apposée sur chaque échange, qui donne aux destinataires l'assurance qu'un message provient bien du cabinet et qu'il leur parvient exactement tel qu'il a été envoyé. Pour une institution dont le nom a un poids considérable, cette authenticité démontrable rend la confiance numérique concrète.

Déchiffrement entrant et gestion des clés simple, propre et sans effort

Echoworx prend en charge le déchiffrement entrant S/MIME et PGP au niveau de la passerelle, en coordination avec les politiques de sécurité de la messagerie du cabinet, afin que chaque message entrant soit à la fois lisible et sécurisé. La plateforme collecte également automatiquement les clés publiques à partir des messages signés — puis retire ces clés une fois capturées, afin qu'elles n'apparaissent jamais dans les boîtes de réception et ne créent aucune confusion pour les utilisateurs finaux. Tout se passe de manière invisible au niveau de la passerelle, pour préserver une expérience fluide pour celles et ceux qui s'y fient au quotidien.

De la marge pour évoluer, au rythme du cabinet

Désormais appuyé sur un socle moderne pour son chiffrement par certificats, le cabinet évalue la remise via portail d'Echoworx comme canal complémentaire — une manière concrète d'étendre la communication sécurisée à des cas d'usage plus larges et de favoriser une adoption naturelle au sein de ses équipes et de ses bureaux. L'infrastructure est en place ; le cabinet peut désormais évoluer selon ses propres priorités et son propre calendrier.

Suite...

Découverte globale des clés via des annuaires de confiance

La sécurité commence dès l'enregistrement. Echoworx a imposé une vérification sécurisée automatisée des utilisateurs pour chaque nouveau destinataire : un code généré par le système, transmis hors bande par téléphone ou par SMS, relie directement l'inscription au portail aux propres standards de vérification d'identité de la banque. À partir de là, les utilisateurs gèrent eux-mêmes leurs identifiants en libre-service. Mais intégrer, le jour de la migration, des milliers de contacts déjà approuvés ne pouvait pas signifier des milliers d'étapes de vérification simultanées. La banque a donc utilisé sa plateforme existante pour envoyer les messages de bienvenue, et Echoworx a prévu une exception contrôlée et délibérée pour ces utilisateurs existants, déjà vérifiés. Tous les nouveaux utilisateurs intégrés par la suite sont, eux, soumis au standard complet et permanent de vérification. Une sécurité élevée là où elle compte ; une intégration fluide là où elle était pertinente.

Les résultats

La migration a tenu sa promesse essentielle : chaque workflow sur lequel les clients du cabinet comptaient a été préservé, désormais gouverné, modernisé et conçu pour durer.

Continuité complète des workflows, confirmée.

Chaque capacité de chiffrement par certificats — S/MIME sortant avec sélection automatique, PGP optionnel déclenché par mot-clé, déchiffrement entrant et collecte des clés — a été migrée vers le cloud sans perdre une seule étape, de sorte qu'aucune relation client n'a ressenti la transition.

Une réputation protégée, échange après échange.

La signature appliquée à tous les e-mails sortants confère à chaque communication une authenticité démontrable, renforçant la confiance que le nom du cabinet a su bâtir au fil des décennies.

Des processus clients respectés sans exception.

Les étapes PGP et S/MIME exactes sur lesquelles s'appuient les partenaires les plus exigeants du cabinet sont restées inchangées, permettant aux relations les plus sensibles de se poursuivre sans rupture dans la chaîne de confiance.

Une intégration fluide à la pile existante.

Echoworx fonctionne directement aux côtés des politiques de sécurité de la messagerie du cabinet, en renforçant la couche de communication sécurisée sans perturber l'environnement déjà en place.

Une portée mondiale, gouvernée avec précision.

L'intégration à des annuaires externes — dont l'agrégateur Global TrustPoint — permet au cabinet de localiser les bonnes clés à l'échelle internationale, tout en assurant une gestion des clés automatique et propre au niveau de la passerelle.

Une plateforme conçue pour évoluer.

Avec la remise via portail actuellement à l'étude, le cabinet dispose d'une voie claire et peu contraignante pour étendre la communication sécurisée à de nouveaux cas d'usage, selon son propre calendrier.

Vue d'ensemble

Ce cabinet s'est tourné vers Echoworx pour remplacer une appliance vieillissante. Ce qu'il en a retiré est bien plus durable : un socle de chiffrement cloud native au sein duquel chaque workflow de confiance a traversé la transition intact — ainsi qu'une plateforme conçue pour évoluer au rythme d'une pratique située à la frontière même de la complexité juridique internationale, là où les dossiers sont sans précédent, les clients mondiaux, et la marge d'erreur nulle.

L'enseignement réel va bien au-delà de la technologie. Pour un cabinet dont la réputation repose sur la gestion de dossiers qui ne peuvent se permettre aucun faux pas — transactions transfrontalières, litiges internationaux, missions réglementaires faisant jurisprudence — la discrétion n'est pas un principe. C'est la pratique elle-même. La mesure la plus exigeante d'une modernisation réussie ne se trouve pas dans ce qui a été ajouté, mais dans ce qui n'a jamais été mis en risque. En choisissant une plateforme capable de reproduire avec précision ses capacités héritées, de respecter les processus exacts exigés par ses clients les plus exigeants, et de s'intégrer proprement aux outils déjà utilisés dans l'ensemble de ses bureaux mondiaux, le cabinet a mené à bien l'une des migrations les plus sensibles possibles sans la moindre concession sur la continuité. La parité exacte n'était pas l'ambition — c'était la condition non négociable. Ce qui a été accompli est plus rare encore : une transition complète que les clients du cabinet n'ont jamais eu de raison de remarquer.

Echoworx rend cela possible : une sécurité pensée dès la conception, une résilience à grande échelle, et une fidélité totale aux workflows que celles et ceux qui en dépendent connaissent déjà.

Vos communications sécurisées sont-elles prêtes pour la suite ?

Si une appliance de chiffrement héritée peine à suivre le rythme d'une pratique moderne, résolument cloud first — ou si elle se dresse entre votre cabinet et les processus de confiance qu'exigent vos clients — il existe une manière d'avancer sans rien laisser derrière vous.

[Parlez dès aujourd'hui à un expert Echoworx.](#)