ECHOWORX™

TÉMOIGNAGE CLIENT

Deux banques. Une plateforme Aucun compromis.

Comment une grande institution allemande a centralisé le chiffrement à travers des unités d'affaires souveraines

Points de validation technique

Modèle de déploiement
Natif AWS, multirégion : Irlande + Allemagne.

Résidence des données
Données hébergées dans la juridiction concernée

Gestion des clés
Gestion des clés validée FIPS 140-3

Gestion du cycle de vie des certificats
Cycle de vie S/MIME automatisé par DigiCert

Intégration DLP
Intégration à Mimecast DLP

Point de chiffrement
Le chiffrement à la passerelle remplace le ZIP sur poste de travail

Formats fondés sur des normes
PDF natif, Microsoft Office et ZIP

Remise sans portail
Remise par phrase secrète partagée

Modules complémentaires Microsoft 365
Menu à options multiples + bouton unique

Résumé de la direction

Dans la région DACH, peu d'enjeux sont aussi étroitement surveillés que la manière dont une banque protège les données qu'elle fait circuler. L'Allemagne, l'Autriche et la Suisse portent parmi les exigences de sécurité les plus profondes et les plus anciennes au monde — des exigences inscrites dans la réglementation, renforcées par la gouvernance et ressenties dans chaque relation avec les partenaires et les clients. Pour une grande institution financière allemande, répondre à ces attentes n'était pas un projet. C'était une obligation permanente.

Or, le chiffrement de la banque s'exécutait au mauvais endroit. Un système Totemo sur poste de travail assurait le chiffrement sécurisé des fichiers ZIP au point d'extrémité, ce qui signifiait que des fichiers sensibles échappaient aux contrôles d'analyse de sécurité et de sauvegarde exigés dans la région. Plus encore, l'institution n'était pas un seul acheteur avec un seul besoin. Sa banque principale et sa branche d'investissement fonctionnaient comme des organisations distinctes, chacune avec sa propre stratégie, ses propres exigences en matière de résidence des données et sa propre vision du cloud.

La banque s'est tournée vers Echoworx pour résoudre ces deux problèmes à la fois : déplacer le chiffrement hors du poste de travail et vers le cloud, tout en offrant à deux unités d'affaires très différentes les environnements sur mesure dont chacune avait besoin, sans se fragmenter en deux outils déconnectés.

Le résultat : une plateforme de chiffrement unique, fondée sur des normes, qui a recentralisé un contrôle auparavant fragmenté, respecté des exigences strictes de souveraineté des données à travers des régions AWS distinctes, et permis à chaque unité d'affaires d'opérer selon ses propres modalités — le tout sous un même toit.

Le défi

01 | Un chiffrement effectué au mauvais endroit.
L'approche de la banque, fondée sur le chiffrement sécurisé de fichiers ZIP au point d'extrémité, pouvait sembler pratique, mais elle comportait une faille structurelle invisible. Lorsque les fichiers sont chiffrés d'un poste à l'autre, ils ne passent jamais par les processus d'analyse de sécurité et de sauvegarde de l'entreprise, alors même que la conformité dans la région DACH les considère comme non négociables. Chaque fichier ZIP qui quittait le poste d'un employé quittait en même temps le cadre de gouvernance de la banque. Pour une institution soumise à un tel niveau d'examen réglementaire, une communication sécurisée qui contourne ses propres contrôles n'est pas véritablement sécurisée — c'est une faille en attente d'être découverte.

02 | Une habitude manuelle incompatible avec une banque moderne.
Les employés exécutaient eux-mêmes chaque étape : regrouper les fichiers dans des archives ZIP, définir des mots de passe et transmettre ces mots de passe échange par échange. Aussi répandu que ce modèle puisse encore être, même dans les grandes organisations, il reposait sur la capacité des personnes à exécuter chaque étape correctement et sur les TI à maintenir en fonctionnement des logiciels de chiffrement sur les postes de travail à l'échelle de l'entreprise. C'était un effort consacré au maintien d'un flux de travail, plutôt qu'à l'avancement du virage cloud de la banque.

03 | Une seule institution, deux mandats très différents.
La véritable complexité allait bien au-delà d'un simple outil. Au sein d'une même banque, différentes parties prenantes et unités d'affaires avaient tracé des trajectoires distinctes. La banque principale voulait un chiffrement proprement intégré à ses processus existants de DLP et d'analyse de sécurité, livré d'une manière simple et fluide pour ses contacts externes. Sa branche d'investissement — la division des services financiers — avait une vision entièrement différente : une approche cloud-first, cloud-only, fondée sur S/MIME, et soumise à des exigences strictes de résidence des données en Allemagne. Chacune de ces unités avait de bonnes raisons d'agir ainsi. Le défi consistait à répondre aux besoins des deux sans fragmenter de nouveau le contrôle du chiffrement dans les silos mêmes que la banque cherchait à quitter.

La Solution

La banque a choisi Echoworx précisément parce que la plateforme pouvait concilier deux stratégies à la fois — standardiser la sécurité tout en respectant la souveraineté de chaque unité d'affaires. Ce qui unifiait l'ensemble de l'approche, c'était l'étendue des modes de remise : une seule et même plateforme offrait un éventail suffisamment large de méthodes de chiffrement pour remplacer les outils hérités des deux divisions, chacune selon ses propres modalités.

« Deux unités d'affaires, deux visions très différentes — l'une voulait des phrases secrètes partagées et le chiffrement ZIP, l'autre du S/MIME avec son propre environnement DigiCert », explique Derek Christian, gestionnaire de l'engagement chez Echoworx. « Notre rôle consistait à respecter ces deux approches, à maintenir les données de chaque unité dans sa propre région et à ramener un chiffrement fragmenté sous un même toit — sans qu'aucune des deux équipes perde sa façon de travailler. »

La souveraineté numérique, tracée selon les lignes régionales.

Dans la région DACH, la résidence des données n'est pas une simple case à cocher — c'est une exigence, et elle peut varier d'une unité d'affaires à l'autre. Echoworx y a répondu de front grâce à des déploiements AWS propres à chaque région. La banque principale opérait depuis une région AWS basée en Irlande, adaptée à ses besoins, tandis que la branche d'investissement, tenue de conserver ses données en Allemagne, était déployée dans une région distincte basée en Allemagne. En s'appuyant sur les régions AWS et les zones de disponibilité pour ancrer chaque empreinte, la plateforme a maintenu les données de chaque entité exactement là où sa gouvernance l'exigeait. En pratique, la souveraineté signifiait que chaque unité conservait la maîtrise de ses données, dans sa propre juridiction.

Le chiffrement a été ramené à la passerelle.

Le changement le plus important a consisté à retirer le chiffrement du poste de travail pour le replacer dans la passerelle cloud. Là, il s'est réintégré directement aux flux qu'il contournait jusque-là — DLP, analyse de sécurité, sauvegarde — de sorte que chaque message sécurisé passe désormais par les contrôles censés le gouverner. Pour la branche d'investissement, cette discipline s'est aussi appuyée sur l'alliance de longue date d'Echoworx avec Mimecast pour le DLP, alignant une sécurité pensée pour le cloud sur une stratégie elle aussi résolument cloud-first. La faille ne s'est pas refermée en ajoutant davantage de supervision, mais en replaçant le chiffrement là où la supervision existait déjà.

Le chiffrement fondé sur des normes, dans des formats familiers pour tous les destinataires.

Echoworx a sécurisé les fichiers dans les formats que les contacts externes connaissent et utilisent déjà — PDF, Microsoft Office et ZIP. Aucun élément propriétaire ne s'interposait entre la banque et ses partenaires, de sorte que les destinataires pouvaient continuer à travailler selon les mêmes processus que ceux auxquels ils étaient habitués. Pour une institution dont la réputation repose sur des échanges fluides et dignes de confiance, l'approche fondée sur des normes n'était pas un simple détail technique. C'était l'essentiel.

Un chiffrement fondé sur des normes, familier pour tous les destinataires.

Echoworx sécurisait les fichiers au moyen de formats que les contacts externes connaissent déjà et auxquels ils font confiance — PDF, Microsoft Office et ZIP. Aucun élément propriétaire ne s'interposait entre la banque et ses partenaires, de sorte que les destinataires pouvaient continuer à travailler selon les mêmes processus que ceux auxquels ils étaient déjà habitués. Pour une institution dont la réputation repose sur des échanges fluides et dignes de confiance, le recours à des standards n'était pas un simple détail technique. C'était l'essentiel.

Suite...

Une approche sur mesure pour la banque principale.

La branche d'investissement voulait autre chose. Sa priorité : le S/MIME, via son propre abonnement DigiCert. Echoworx en a automatisé le cycle de vie des certificats — génération, collecte, vérification et signature — tout en préservant la parité fonctionnelle avec l'environnement Totemo quitté. La migration s'est ainsi inscrite dans la continuité. Et lorsqu'aucune clé n'était disponible chez le destinataire, un portail sécurisé prenait automatiquement le relais. Là où la banque principale privilégiait le choix, la branche d'investissement a opté pour la simplicité : un module complémentaire à bouton unique, avec un acheminement géré en arrière-plan.

Les résultats

Le chiffrement ramené dans un cadre gouverné.

En déplaçant le chiffrement sécurisé des fichiers ZIP et des pièces jointes du poste de travail vers la passerelle cloud, chaque message transite désormais par les contrôles d'analyse de sécurité et de DLP exigés par la conformité dans la région DACH — refermant ainsi une faille que l'approche au point d'extrémité avait laissée largement ouverte.

La souveraineté respectée, unité par unité.

Des déploiements AWS distincts en Irlande et en Allemagne ont permis de maintenir les données de chaque unité d'affaires dans la juridiction requise, satisfaisant ainsi à de strictes exigences de résidence des données sans imposer à une division les règles de l'autre.

Deux stratégies, une seule plateforme.

La banque principale et sa branche d'investissement ont chacune utilisé le modèle de chiffrement qui leur convenait — remise sans portail par phrase secrète partagée pour l'une, S/MIME automatisé pour l'autre — tandis que l'institution retrouvait un contrôle centralisé et fondé sur des normes sur l'ensemble des deux environnements.

Rien n'est resté exposé.

Le repli automatique vers le portail sécurisé garantissait une remise protégée même lorsqu'un destinataire ne disposait d'aucune clé, de sorte qu'un certificat manquant ne devenait jamais un compromis de sécurité.

Un cycle de vie S/MIME sans intervention manuelle.

L'intégration à DigiCert a automatisé la génération des clés, la collecte des certificats et la vérification des signatures pour la branche d'investissement, remplaçant la gestion manuelle des clés tout en préservant une pleine parité fonctionnelle avec sa solution précédente.

Une expérience fluide pour les destinataires.

Les phrases secrètes partagées permettaient aux contacts externes de la banque principale d'ouvrir les messages sécurisés directement dans leur boîte de réception — sans portail, sans inscription — tandis que les formats fondés sur des normes permettaient à chaque destinataire de continuer à travailler dans les outils auxquels il faisait déjà confiance.

Une migration adaptée à la réalité de chaque unité.

Les deux divisions ont quitté Totemo sans abandonner les habitudes ni les capacités sur lesquelles leurs équipes s'appuyaient — parité fonctionnelle pour la branche d'investissement, souplesse dans le choix des méthodes pour la banque principale.

Vue d'ensemble

Au départ, cette institution faisait face à un problème de positionnement : le chiffrement s'exécutait dans un endroit où la gouvernance ne pouvait pas l'atteindre. Ce qu'elle a construit, en revanche, est quelque chose de plus durable : un socle centralisé, fondé sur des normes, qui respecte — plutôt qu'il n'efface — les différences entre ses unités d'affaires.

C'est là le cœur de l'histoire. Dans une grande organisation réglementée, la partie la plus difficile de la modernisation n'est que rarement la technologie elle-même — c'est la capacité à répondre à des mandats réellement différents sans se fragmenter en un patchwork d'outils déconnectés. En choisissant une plateforme assez vaste pour offrir du S/MIME à une division et un chiffrement sans portail par phrase secrète partagée à une autre, tout en étant déployée dans les régions exigées par chacune, la banque a transformé cette complexité en avantage. Un contrôle décentralisé est devenu une gouvernance centralisée, sans qu'aucune unité ne perde l'autonomie dont elle avait besoin.

Echoworx rend cela possible pour les organisations de toute structure : unifiée là où c'est essentiel, souveraine là où ça compte, et fondée sur des normes d'un bout à l'autre.

Prêt à unifier le chiffrement sans effacer ce qui distingue vos unités d'affaires?
Si un chiffrement lié au poste de travail échappe à vos contrôles, ou si des divisions distinctes tirent votre stratégie de sécurité dans des directions différentes, il existe une façon de centraliser la gouvernance tout en respectant le mandat de chaque unité.
Échangez dès aujourd'hui avec un expert Echoworx.