

Quand la conformité ne peut pas attendre

Comment l'une des cinq plus grandes banques canadiennes a rétabli la confiance sur des bases modernes

En bref

Secteur

Services financiers — Banque

Résultats clés

- ✓ **Authentification à deux facteurs obligatoire** — appliquée intégralement à chaque contact externe
- ✓ **Conformité bilingue complète** au titre des lois 101 et 96 du Québec
- ✓ **Préparation aux audits en temps réel** grâce à une intégration SIEM en direct et à une visibilité complète
- ✓ **Migration sans interruption** — des milliers d'utilisateurs migrés sans changer leur façon de travailler
- ✓ **Véritable souveraineté des données sur une infrastructure AWS cloud native**

Résumé exécutif

Pour l'une des « cinq grandes » banques du Canada, le courriel sécurisé n'a jamais été un simple dispositif technique. C'était une promesse tenue envers des millions de clients, une obligation légale dans les deux langues officielles, et une preuve discrète, au quotidien, que la confiance avait été méritée. Dans le secteur bancaire, la confiance n'est pas un simple atout. C'est le fondement même de l'activité.

Or, cette promesse devenait de plus en plus difficile à tenir. La plateforme de chiffrement existante de la banque ne permettait pas d'imposer l'authentification forte désormais attendue par les régulateurs. Elle ne pouvait pas évoluer au rythme d'une stratégie axée sur le cloud. Et elle ne s'intégrait pas proprement à la pile de sécurité moderne que la banque mettait en place pour les années à venir.

La banque s'est donc associée à Echoworx pour changer de cap. Le résultat : une plateforme de chiffrement cloud native qui imposait une authentification à deux facteurs obligatoire, assurait une conformité complète en anglais et en français, et permettait de faire migrer des milliers d'utilisateurs vers une architecture moderne sans une seule journée d'interruption.

Voici l'histoire d'une institution hautement réglementée qui a considéré la communication sécurisée non comme une simple case à cocher, mais comme un élément à part entière de son modèle opérationnel — et qui a transformé un risque de conformité imminent en un avantage stratégique durable.

Le défi

Un système hérité qui ne pouvait plus tenir ses promesses

La confiance est la véritable monnaie du secteur bancaire. Pour une institution canadienne de premier plan soumise à certaines des règles les plus strictes au monde, chaque message chiffré compte, qu'il s'agisse d'un relevé client ou d'un fichier confidentiel envoyé à un partenaire. Lorsque cette confiance est maintenue, personne ne le remarque. Lorsqu'elle vacille, tout le monde le voit.

Le problème, c'est que la solution de chiffrement Zix vieillissante de la banque était passée en silence du statut de protection à celui de source de risque.

01 | Il ne permettait pas d'imposer une authentification à deux facteurs obligatoire.

Les régulateurs comme les équipes internes de sécurité exigeaient une vérification forte pour toute personne recevant des courriels sensibles provenant de l'extérieur de la banque. La plateforme existante n'en était tout simplement pas capable. Cela créait une faille précisément au moment où la confiance compte le plus : lorsqu'un message privé arrive dans la boîte de réception de quelqu'un d'autre.

02 | Il créait des écarts de conformité dans un pays bilingue.

La Loi 101 et la Loi 96 du Québec imposent une prise en charge complète du français dans les communications clients. Toute expérience qui n'était pas parfaitement fluide dans les deux langues exposait la banque à un risque réglementaire et affaiblissait l'expérience des clients mêmes qu'elle cherchait le plus à protéger.

03 | Il freinait la transition vers le cloud.

La banque était en pleine transformation à l'échelle de l'entreprise, abandonnant les systèmes sur site au profit d'une passerelle de sécurité moderne basée sur le cloud. L'ancien outil de chiffrement ne pouvait pas s'intégrer à ce nouvel environnement. Au lieu de faire avancer la stratégie, il la ralentissait.

04 | Il faisait de la gestion des certificats un casse-tête permanent.

Maintenir les certificats S/MIME en ordre à travers de nombreuses unités d'affaires, des boîtes mail partagées et des équipes à haute exigence de sécurité relevait d'un processus manuel, délicat et chronophage, détournant des ressources qualifiées de tâches à plus forte valeur ajoutée.

Le constat était clair. Pour protéger la confiance, rester conforme et libérer sa stratégie cloud, la banque n'avait pas besoin d'un correctif de plus. Elle avait besoin d'une base conçue pour ce qui vient ensuite.

La solution

Une fondation cloud native conçue pour la résilience

La banque a choisi Echoworx pour reconstruire sa communication sécurisée de fond en comble, sur une plateforme conçue pour répondre aux exigences réelles d'une institution moderne, réglementée et bilingue.

Il ne s'agissait pas d'un projet mené à distance. En travaillant étroitement avec l'équipe Client Engagement d'Echoworx, la banque a élaboré une mise en œuvre autour de trois priorités simples : rester conforme, garder le contrôle et assurer la continuité des activités sans le moindre accroc.

« L'objectif n'a jamais été simplement de remplacer un outil par un autre », explique Derek Christian, gestionnaire de l'engagement chez Echoworx. « Il s'agissait de donner à la banque une couche de communication sécurisée en laquelle elle pouvait avoir confiance à grande échelle, dans les deux langues, sous une véritable pression réglementaire — et de le faire sans demander à des milliers de personnes de changer leur façon de travailler. »

Architecture cloud native avec véritable souveraineté des données

Echoworx a été déployé à 100 % sur AWS, avec une intégration à AWS CloudHSM pour la gestion des clés afin d'atteindre une génération et un stockage des clés validés FIPS 140-3. Grâce à la capacité d'apport de vos propres clés (BYOK), la banque a conservé l'entière propriété de ses clés de chiffrement. Pour une institution redevable à la fois aux régulateurs et à ses clients, ce niveau de contrôle n'était pas une préférence. C'était une exigence non négociable.

Intégration fluide à la pile de sécurité moderne

Plutôt que d'imposer une refonte perturbatrice, Echoworx a été conçu pour fonctionner en parallèle de la migration de la banque vers Proofpoint. Cette approche agnostique à l'égard de la passerelle a permis de créer une ligne de défense unique, prête pour le cloud, et de faire avancer simultanément deux initiatives majeures, au lieu de les mettre en concurrence pour les mêmes ressources.

Conformité bilingue complète

Grâce à la prise en charge native du français, la banque a pu respecter les exigences des lois 101 et 96 du Québec en offrant une expérience cohérente et conforme dans les deux langues officielles, sans zone grise ni approximation.

Une bascule « Big Bang » sans friction

Le changement est souvent l'aspect le plus difficile d'une migration, surtout dans des unités d'affaires sensibles; Echoworx a donc rendu la transition presque invisible. La banque a effectué le basculement en une seule étape en conservant le même mot-clé dans Outlook pour déclencher le chiffrement, si bien que rien ne semblait différent au quotidien dès le premier jour. Un module complémentaire Outlook Microsoft 365 basé sur le web, compatible avec Windows, Mac et le web, ne nécessitait aucune installation logicielle et préservait les paramètres itinérants ainsi que les notifications personnelles, tandis que des formations pratiques et des démonstrations en direct ont permis de lever les derniers obstacles.

Authentification à deux facteurs obligatoire, intégrée d'emblée

Echoworx imposait une authentification à deux facteurs obligatoire pour chaque contact externe. Les codes de vérification par texto étaient envoyés via l'abonnement Sinch déjà en place à la banque, avec les applications d'authentification (TOTP) comme deuxième option. Les destinataires bénéficiaient ainsi d'une vérification forte et flexible, sans complexité supplémentaire.

Suite...

Modes de livraison flexibles pour une clientèle diversifiée

Comme de nombreux clients et partenaires s'appuient sur des boîtes mail partagées, la plateforme leur offrait le choix : **un portail sécurisé par défaut, ou une livraison directe dans la boîte de réception « push delivery »** de documents chiffrés. Chacun pouvait ainsi recevoir des messages protégés de la manière qui lui convenait le mieux.

Auditabilité en temps réel et contrôle centralisé

Les API Web d'Echoworx alimentaient directement le SIEM Splunk de la banque en données d'audit en temps réel, ce qui permettait de corréler et d'examiner les événements au fur et à mesure qu'ils se produisaient. L'authentification unique SAML par l'intermédiaire d'Entra ID, combinée à des contrôles d'accès fondés sur les rôles et à des restrictions d'adresses IP, offrait au personnel du centre d'assistance et aux administrateurs un contrôle à la fois simple et sécurisé.

De plus, un serveur SMTP dédié permettait de séparer les envois automatisés en masse des courriels des utilisateurs en temps réel, protégeant ainsi les performances pour tous.

Les résultats

Conformité assurée, confiance renforcée, perturbations éliminées

La migration n'a pas seulement permis de combler des lacunes. Elle a transformé la communication sécurisée en un actif stratégique, capable d'évoluer au rythme de l'avenir cloud first de la banque.

Authentification à deux facteurs appliquée.

Chaque destinataire externe doit désormais vérifier son identité avant d'ouvrir un contenu sensible, ce qui permet de combler une faille de sécurité critique et de répondre aux exigences strictes de la banque en matière d'authentification.

Conformité bilingue complète, obtenue sans friction.

Grâce à une prise en charge exhaustive de l'anglais et du français, la banque a satisfait aux exigences des lois 101 et 96 du Québec, protégeant à la fois sa conformité réglementaire et ses relations avec sa clientèle.

Préparation à l'audit en temps réel.

L'intégration en direct avec Splunk a donné aux équipes de sécurité et de conformité la visibilité et la supervision exigées par la réglementation moderne, transformant la communication sécurisée d'un angle mort en un point de contrôle clair.

Dépenses plus intelligentes.

En s'appuyant sur l'abonnement Sinch déjà en place pour la vérification par texto, la solution a offert une authentification forte sans ajouter une nouvelle ligne au budget.

Expéditeurs outillés et autonomisés.

Les employés ont obtenu des accusés de lecture, le suivi du téléchargement des pièces jointes et un bouton de rappel en libre-service qui fonctionne instantanément, sans intervention du service TI. Les utilisateurs externes pouvaient également s'inscrire eux-mêmes au moyen d'une URL dédiée afin de lancer de leur propre initiative des échanges entrants sécurisés.

Opérations simplifiées.

La gestion automatisée du cycle de vie des certificats a mis fin à des difficultés persistantes liées au S/MIME, libérant l'équipe TI des tâches manuelles répétitives et réduisant le risque d'interruptions de service.

Migration sans perturbation.

C'est peut-être le résultat le plus révélateur de tous : des milliers d'utilisateurs sont passés à une plateforme moderne et cloud native sans changer leur façon de travailler. La transformation s'est déroulée discrètement, en arrière-plan, exactement comme elle le devait.

Vue d'ensemble

La banque s'était donné pour objectif de résoudre un problème de conformité. Ce qu'elle a mis en place allait bien au-delà : une résilience opérationnelle, une souveraineté des données et une confiance numérique, le tout reposant sur une fondation cloud native prête à faire face à la suite.

Ce repositionnement est important. La communication sécurisée n'est plus une tâche informatique reléguée à l'arrière-plan. Pour les institutions les plus réglementées au monde, elle fait désormais partie intégrante du modèle opérationnel lui-même, un pilier de la résilience et une démonstration quotidienne du maintien de la confiance.

La leçon à retenir de cette histoire est simple. Avec la bonne plateforme cloud native et le bon partenaire à vos côtés, moderniser le chiffrement, répondre à des exigences réglementaires strictes et offrir une meilleure expérience aux utilisateurs ne sont pas des objectifs incompatibles. Tout peut se réaliser simultanément, même dans les marchés les plus complexes et les plus fortement réglementés.

Echoworx rend cela possible : conforme par conception, résilient à grande échelle et simple d'utilisation pour les personnes qui en dépendent chaque jour.

Votre communication sécurisée est-elle prête pour la suite?

Si un chiffrement hérité freine votre stratégie cloud, complique la conformité ou s'interpose entre vous et la confiance qu'attendent vos clients, il est temps de passer à une fondation moderne.

Communiquez dès aujourd'hui avec un expert d'Echoworx.