

Wenn Compliance nicht warten kann

Wie eine der fünf größten Banken Kanadas Vertrauen auf einem modernen Fundament neu aufgebaut hat

Auf einen Blick

Branche

Finanzdienstleistungen —
Bankwesen

Wichtigste Ergebnisse

- ✓ Verpflichtende 2FA — vollständig durchgesetzt für jeden externen Kontakt
- ✓ Vollständige Zweisprachigkeits-Compliance gemäß Quebec Bill 101 & 96
- ✓ Audit-Bereitschaft in Echtzeit durch Live-SIEM-Integration und vollständige Transparenz
- ✓ Migration ohne Unterbrechung — Tausende von Nutzerinnen und Nutzern wurden umgestellt, ohne ihre Arbeitsweise zu verändern
- ✓ Echte Datensouveränität auf einer cloud-nativen AWS-Basis

Zusammenfassung für Entscheider

Für eine der „Big Five“-Banken Kanadas war sichere E-Mail nie nur ein technisches Feature. Sie war ein Versprechen gegenüber Millionen von Kundinnen und Kunden, eine gesetzliche Verpflichtung in zwei Amtssprachen und ein stiller, täglicher Beweis dafür, dass Vertrauen verdient wurde. Im Bankwesen ist Vertrauen kein Nice-to-have. Es ist das gesamte Geschäftsmodell.

Dieses Versprechen wurde jedoch immer schwerer einzuhalten. Die bestehende Verschlüsselungsplattform der Bank konnte die starke Authentifizierung, die Regulierungsbehörden inzwischen erwarteten, nicht durchsetzen. Sie konnte nicht mit der Geschwindigkeit einer Cloud-First-Strategie mithalten. Und sie ließ sich nicht sauber in den modernen Sicherheits-Stack integrieren, den die Bank für die kommenden Jahre aufbaute.

Also entschied sich die Bank gemeinsam mit Echoworx für einen neuen Kurs. Das Ergebnis war eine cloud-native Verschlüsselungsplattform, die eine verpflichtende Zwei-Faktor-Authentifizierung durchsetzte, vollständige Compliance in Englisch und Französisch sicherstellte und Tausende von Nutzerinnen und Nutzern ohne einen einzigen Tag Unterbrechung auf eine moderne Architektur migrierte.

Dies ist die Geschichte, wie eine hochregulierte Institution sichere Kommunikation nicht als bloße Pflichtübung verstand, sondern als Teil ihres Betriebsmodells — und ein drohendes Compliance-Risiko in einen nachhaltigen strategischen Vorteil verwandelte.

Die Herausforderung

Ein Altsystem, das seine Versprechen nicht mehr halten konnte

Vertrauen ist die Währung des Bankwesens. Für ein führendes kanadisches Institut, das unter einigen der strengsten Regeln der Welt arbeitet, zählt jede verschlüsselte Nachricht – vom Kontoauszug eines Kunden bis zur vertraulichen Datei eines Partners. Solange dieses Vertrauen hält, nimmt es niemand wahr. Wenn es bröckelt, bemerken es alle.

Das Problem war, dass sich die veraltete Zix-Verschlüsselungslösung der Bank still und leise von einer Schutzmaßnahme zu einer Quelle von Risiken entwickelt hatte.

01 | Es konnte keine verpflichtende Zwei-Faktor-Authentifizierung durchsetzen.

Regulierungsbehörden und interne Sicherheitsteams brauchten eine starke Verifizierung für alle, die sensible E-Mails von außerhalb der Bank empfangen. Die Altplattform war dazu schlicht nicht in der Lage. Dadurch entstand genau in dem Moment eine Lücke, in dem Vertrauen am wichtigsten ist: wenn eine vertrauliche Nachricht im Posteingang einer anderen Person landet.

02 | Es verursachte Compliance-Lücken in einem zweisprachigen Land.

Quebecs Bill 101 und Bill 96 verlangen eine vollständige französischsprachige Unterstützung in der Kundenkommunikation. Alles, was unter einem nahtlosen Service in beiden Sprachen lag, bedeutete regulatorische Risiken und zugleich eine schwächere Erfahrung für genau die Kundinnen und Kunden, die die Bank besonders schützen wollte.

03 | Es stand der Cloud im Weg.

Die Bank befand sich mitten in einer unternehmensweiten Transformation – weg von On-Premises-Systemen und hin zu einem modernen, cloudbasierten Security Gateway. Das alte Verschlüsselungstool ließ sich nicht in diese neue Welt integrieren. Statt die Strategie voranzutreiben, bremste es sie aus.

04 | Es machte das Zertifikatsmanagement zu einer dauerhaften Belastung.

Die Verwaltung von S/MIME-Zertifikaten über viele Geschäftsbereiche, gemeinsame Postfächer und Hochsicherheitsteams hinweg war manuell, fehleranfällig und zeitaufwendig – und band qualifizierte Fachkräfte an Aufgaben, die ihre Zeit an anderer Stelle dringender gebraucht hätten.

Das Fazit war eindeutig: Um Vertrauen zu schützen, Compliance sicherzustellen und die Cloud-Strategie voranzubringen, brauchte die Bank keinen weiteren Patch. Sie brauchte ein Fundament, das für das gebaut ist, was als Nächstes kommt.

Die Lösung

Ein cloud-natives Fundament für Resilienz

Die Bank entschied sich für Echoworx, um ihre sichere Kommunikation von Grund auf neu aufzubauen — auf einer Plattform, die für die realen Anforderungen einer modernen, regulierten und zweisprachigen Institution konzipiert ist.

Dabei handelte es sich nicht um ein Projekt auf Distanz. In enger Zusammenarbeit mit dem Client-Engagement-Team von Echoworx entwickelte die Bank eine Implementierung entlang von drei klaren Prioritäten: compliant bleiben, die Kontrolle behalten und den Geschäftsbetrieb ohne Unterbrechung aufrechterhalten.

„Das Ziel war nie einfach nur, ein Tool gegen ein anderes auszutauschen“, erklärt Derek Christian, Engagement Manager bei Echoworx. „Es ging darum, der Bank eine sichere Kommunikationsschicht zu geben, der sie im großen Maßstab vertrauen kann — in beiden Sprachen, unter realem regulatorischem Druck und ohne Tausende von Menschen dazu zu zwingen, ihre Arbeitsweise zu verändern.“

Cloud-native Architektur mit echter Datensouveränität

Echoworx wurde zu 100 % auf AWS bereitgestellt und mit AWS CloudHSM für das Schlüsselmanagement integriert, um eine nach FIPS 140-3 validierte Schlüsselgenerierung und -speicherung zu erreichen. Mit der Bring-Your-Own-Key-(BYOK)-Funktion behielt die Bank die vollständige Kontrolle über ihre Verschlüsselungsschlüssel. Für eine Institution, die sowohl gegenüber Regulierungsbehörden als auch gegenüber Kundinnen und Kunden rechenschaftspflichtig ist, war dieses Maß an Kontrolle keine Präferenz. Es war nicht verhandelbar.

Nahtlose Integration in den modernen Sicherheits-Stack

Anstatt einen störenden Neuaufbau zu erzwingen, wurde **Echoworx so konzipiert, dass es parallel zur Proofpoint-Migration** der Bank betrieben werden konnte. Der gateway-agnostische Ansatz schuf eine einheitliche, cloudfähige Verteidigungslinie und ermöglichte es, zwei große Initiativen gleichzeitig voranzubringen, statt sie um dieselben Ressourcen konkurrieren zu lassen.

Ein reibungsloser „Big Bang“-Cutover

Echoworx machte die Migration für die Bank nahezu unsichtbar: Der Wechsel erfolgte in einem einzigen Cutover, während Mitarbeitende weiterhin dieselben Outlook-Schlüsselwörter zur Verschlüsselung nutzen konnten, sodass sich im Arbeitsalltag vom ersten Tag an kaum

etwas änderte. Ein webbasiertes Microsoft-365-Outlook-Add-in für Windows, Mac und Web kam zudem ohne Geräteinstallation aus, erhielt roamingfähige Einstellungen und persönliche Benachrichtigungen aufrecht und wurde durch Praxisschulungen sowie Live-Demos zusätzlich reibungslos eingeführt.

Verpflichtende 2FA – fest integriert

Echoworx setzte für jeden externen Kontakt eine verpflichtende Zwei-Faktor-Authentifizierung durch. Verifizierungscode per SMS wurden über das bestehende Sinch-Abonnement der Bank versendet, Authenticator-Apps (TOTP) standen als zweite Option zur Verfügung. So erhielten Empfängerinnen und Empfänger eine starke und zugleich flexible Verifizierung — ohne zusätzlichen Aufwand.

Flexible Zustellung für eine vielfältige Kundenbasis

Da viele Kundinnen, Kunden und Partner mit gemeinsamen Postfächern arbeiten, bot die Plattform Wahlfreiheit: standardmäßig über ein sicheres **Portal oder per direkter „Push Delivery“** verschlüsselter Dokumente in den Posteingang. So konnten alle geschützte Nachrichten auf die für sie passende Weise empfangen.

Fortsetzung...

Vollständige Zweisprachigkeits-Compliance

Die native Unterstützung der französischen Sprache ermöglichte es der Bank, Quebecs Bill 101 und Bill 96 mit einer konsistenten und regelkonformen Nutzererfahrung in beiden Amtssprachen zu erfüllen – ohne Lücken und ohne Interpretationsspielraum.

Auditierbarkeit in Echtzeit und zentrale Kontrolle

Die Web-APIs von Echoworx speisten Live-Auditdaten direkt in das Splunk-SIEM der Bank ein, sodass Ereignisse in Echtzeit korreliert und überprüft werden konnten. Gleichzeitig sorgten SAML Single Sign-on über Entra ID, rollenbasierte Zugriffsrechte, IP-Beschränkungen und ein dedizierter SMTP-Server für sichere, zentrale Kontrolle sowie eine klare Trennung zwischen automatisierten Massenmails und Echtzeit-E-Mails, wodurch die Performance für alle geschützt blieb.

Die Ergebnisse

Compliance erreicht, Vertrauen gestärkt, Unterbrechungen vermieden

Die Migration schloss nicht nur bestehende Lücken. Sie machte sichere Kommunikation zu einem strategischen Vorteil, der sich im Gleichschritt mit der Cloud-First-Zukunft der Bank weiterentwickelt.

Verpflichtende 2FA, vollständig durchgesetzt.

Jede externe Empfängerin und jeder externe Empfänger verifiziert nun vor dem Öffnen sensibler Inhalte die eigene Identität. Damit wurde eine kritische Sicherheitslücke geschlossen und die strenge Authentifizierungsanforderung der Bank erfüllt.

Vollständige Zweisprachigkeits-Compliance, nahtlos erreicht.

Mit umfassender Unterstützung für Englisch und Französisch erfüllte die Bank Quebecs Bill 101 und Bill 96 und schützte damit sowohl ihre regulatorische Position als auch ihre Kundenbeziehungen.

Audit-Bereitschaft in Echtzeit.

Die Live-Integration mit Splunk verschaffte Sicherheits- und Compliance-Teams die Transparenz und Aufsicht, die moderne Regulierung verlangt, und machte sichere Kommunikation von einem blinden Fleck zu einer klar einsehbaren Kontrolllinie.

Effizienterer Mitteleinsatz.

Durch die Nutzung des bestehenden Sinch-Abonnements der Bank für SMS-Verifizierung bot die Lösung starke Authentifizierung, ohne einen zusätzlichen Budgetposten zu schaffen.

Mehr Handlungsspielraum für Absender.

Mitarbeitende erhielten Lesebestätigungen, ein Tracking für Attachment-Downloads und eine Self-Service-Rückruffunktion, die sofort und ohne Unterstützung durch die IT funktioniert. Externe Nutzerinnen und Nutzer konnten sich zudem über eine dedizierte URL selbst registrieren, um eigenständig sichere eingehende Gespräche zu starten.

Vereinfachte Abläufe.

Das automatisierte Management des Zertifikatslebenszyklus beendete langjährige S/MIME-Probleme, entlastete das IT-Team von wiederkehrender manueller Arbeit und verringerte das Risiko von Serviceunterbrechungen.

Migration ohne Unterbrechungen.

Vielleicht das aussagekräftigste Ergebnis von allen: Tausende Nutzerinnen und Nutzer wechselten auf eine moderne, cloud-native Plattform, ohne ihre Arbeitsweise ändern zu müssen. Die Transformation verlief leise im Hintergrund – genau so, wie es sein sollte.

Das große Ganze

Die Bank machte sich ursprünglich daran, ein Compliance-Problem zu lösen. Entstanden ist jedoch etwas Größeres: operative Resilienz, Datensouveränität und digitales Vertrauen — getragen von einem cloud-nativen Fundament, das für alles bereit ist, was als Nächstes kommt.

Diese neue Einordnung ist entscheidend. Sichere Kommunikation ist längst keine IT-Aufgabe mehr, die im Hintergrund mitläuft. Für die am stärksten regulierten Institutionen der Welt ist sie Teil des Betriebsmodells selbst — ein Grundpfeiler von Resilienz und ein täglicher Beleg dafür, dass Vertrauen eingehalten wird.

Die Lehre aus dieser Geschichte ist klar: Mit der richtigen cloud-nativen Plattform und dem richtigen Partner an Ihrer Seite stehen die Modernisierung von Verschlüsselung, die Erfüllung anspruchsvoller regulatorischer Anforderungen und eine bessere Nutzererfahrung nicht im Widerspruch zueinander. All das kann gleichzeitig gelingen — selbst in den komplexesten und am stärksten regulierten Märkten.

Echoworx macht genau das möglich: compliance-konform by design, resilient im großen Maßstab und mühelos für die Menschen, die sich jeden Tag darauf verlassen.

Ist Ihre sichere Kommunikation bereit für das, was als Nächstes kommt?

Wenn veraltete Verschlüsselung Ihre Cloud-Strategie ausbremst, Compliance unnötig erschwert oder dem Vertrauen im Weg steht, das Ihre Kundinnen und Kunden erwarten, ist es Zeit für ein modernes Fundament. Sprechen Sie noch heute mit einer [Expertin oder einem Experten von Echoworx](#).