ECHOWORX™

Customer Success

Top Bank Mandates 2FA in Cloud-Native Encryption Overhaul

Challenge

- **Legacy system was rigid:** Couldn't enforce 2FA or work with Proofpoint.
- **User friction:** Complex steps slowed people down.
- **Compliance gaps:** Missing key authentication standards.

Solution

- **Moved to cloud:** Switched to Echoworx on AWS for full key control.
- **Proofpoint in sync:** Rolled out encryption with their Proofpoint migration.
- **Made it simple:** Enabled web-based Outlook add-in for easy use.

Result

- **Stronger security:** 2FA required for all contacts.
- **Better oversight:** Real-time tracking with Splunk.
- **Less manual effort:** Automated certificate management.

Executive Summary

A top-tier Canadian financial institution, encumbered by an inflexible legacy Zix solution, executed a complete "Big Bang" migration to the Echoworx cloud-native encryption platform. The project's core mandate was to replace their existing system with a modern architecture that could enforce mandatory 2FA, integrate seamlessly with their active Proofpoint migration, and provide data sovereignty.

By leveraging Echoworx's deep integration with AWS and its flexible APIs, the bank achieved a frictionless cutover, enhancing security posture and operational efficiency without business interruption.

The Challenge

Overcoming Legacy Inflexibility

The bank's existing Zix deployment presented significant operational and security roadblocks. It lacked the capability to mandate Two-Factor Authentication (2FA) for external contacts—a critical compliance requirement. Furthermore, the system was a source of considerable user friction and could not integrate effectively with other strategic IT projects, most notably a company-wide migration to Proofpoint. They required a solution that could not only solve the S/MIME certificate management chaos but also provide the technical agility to support diverse business units, from shared mailboxes to high-security teams.

The fundamental problem was clear: their security infrastructure was reactive, not resilient.

The Solution

A Strategically-Architected Migration

Echoworx was selected to engineer a full-scale replacement. The solution was built on three core technical pillars designed for seamless integration and absolute security.

1. **Cloud-Native Architecture on AWS:** The entire solution was deployed on Echoworx's AWS-native platform. The most critical security requirement—key sovereignty—was met by integrating with AWS CloudHSM for Key Management Service (KMS). This provided hardware-backed, FIPS 140-3 validated key generation and storage, ensuring that the bank retained absolute, auditable control over their encryption keys. This architecture gave them the power of the cloud without compromising on data ownership.

2. **Seamless Proofpoint Integration:** A hard requirement was to find a vendor with proven expertise in large-scale Proofpoint deployments. Echoworx's platform was architected to work in parallel with the bank's existing Proofpoint migration. Policies were configured to ensure a unified and streamlined defense perimeter, eliminating the need for complex re-engineering or creating security gaps between systems.

3. **Frictionless Transition & User Enablement:** To avoid disruption, the migration was executed as an instant "Big Bang" cutover.

   Legacy Keyword Retention: The original keyword used to trigger encryption in Outlook was maintained, creating a zero-learning-curve transition for all employees.

   Microsoft 365 Add-in: For modern workflows, a web-based M365 Outlook add-in was deployed. This eliminated software installs and provided a consistent, cross-platform experience on Windows, Web, and macOS, giving users a simple button to control encryption and notifications.

Results

Measurable Security and Operational Gains

The migration delivered tangible results across security, compliance, and user operations.

- **Mandatory, Flexible 2FA:** The bank successfully enforced 2FA for all external contacts using a combination of SMS-based codes (via an existing Sinch integration) and TOTP authenticator apps, providing users with a secure choice.

- **Real-Time SIEM Integration:** A mission-critical requirement for Splunk integration was achieved. The bank leveraged Echoworx's web APIs to pull real-time, granular audit data directly into their SIEM, enabling immediate event correlation and threat analysis.

- **Simplified Certificate Management:** The new system automated certificate lifecycles, effectively ending the "S/MIME nightmare." It provided multiple delivery methods—from a secure portal to direct-to-inbox encrypted attachments—that could accommodate even complex use cases like shared mailboxes.

- **Empowered Senders:** The platform's sender notifications provided deep visibility into message status, including read receipts and attachment download tracking. It also included an instant, user-initiated message recall function that actually works, reducing help desk dependency.

Conclusion

From Technical Debt to Technical Advantage

This project demonstrates that migrating from a first-generation encryption provider does not have to be a high-risk, multi-year endeavor. By partnering with a vendor that specializes in complex, regulated environments, the bank transformed its greatest security liability into a strategic asset.

The combination of a cloud-native AWS architecture, seamless Proofpoint integration, and a focus on user experience allowed them to fortify their security posture, meet stringent compliance mandates, and simplify operations in a single, decisive move.

Learn more about our technical integrations, visit echoworx.com