ECHOWORX™

Customer Success

German Bank Builds Digital Sovereignty with Cloud-Native Encryption

Challenge

- **Desktop encryption:** Didn't align with compliance needs.
- **Security checks** and backups.
- **Decentralized solutions:** Made encryption control difficult.

Solution

- **Shifted to cloud-based:** Integrated with existing DLP.
- **AWS region-specific deployments:** Met data residency needs.
- **Flexible delivery options:** Filled compliance gaps.
- **Made it simple:** Enabled web-based Outlook add-in.
- **Integrated with DigiCert:** Automated S/MIME lifecycle.

Result

- **Frictionless delivery:** Dramatically improved experience.
- **Less manual effort:** Automated key and certificate management.
- **Better oversight:** Built-in tracking and easier compliance audits.

Executive Summary

A major German financial institution, navigating the complex regulatory landscape of the DACH region, executed a strategic migration from a legacy endpoint encryption system to the Echoworx cloud-native platform. The project's mandate was to eliminate the compliance risks of their existing Totemo desktop solution, centralize security at the gateway, and support the distinct needs of two separate business units, including one requiring strict data residency in Germany.

By leveraging Echoworx's flexible, standards-based architecture and deep integration with partners like Mimecast and DigiCert, the bank achieved a seamless migration, fortified its security posture, and ensured compliance with evolving regional mandates.

The Challenge

Overcoming Legacy Endpoint Risk

The bank's reliance on a Totemo-based desktop solution for ZIP encryption created significant compliance and security gaps. This endpoint-to-endpoint process bypassed essential corporate hygiene scanning and backup protocols, leaving the institution exposed to risk and misaligned with modern regulatory requirements. As different business units pursued their own security strategies, the bank required a unified yet adaptable solution that could centralize encryption at the cloud gateway, integrate with existing DLP processes, and offer feature parity to ensure a frictionless transition for users.

The core problem was clear: their decentralized, legacy encryption was a barrier to true regulatory resilience.

The Solution

A Strategically-Architected Migration

Echoworx was chosen to engineer a comprehensive replacement, delivering a solution built on three pillars of flexibility, integration, and absolute security.

1. **Cloud-First Gateway Encryption:** The bank transitioned from disparate endpoint applications to a centralized, cloud-based solution. This move immediately integrated encryption with their existing hygiene and DLP workflows, closing critical compliance gaps. The platform's use of standards-based encryption—including PDF, Microsoft Office, and ZIP—ensured that external recipients could interact with secure communications without needing proprietary software.

2. **Multi-Region and Multi-Strategy Deployment:** Echoworx's platform accommodated the bank's complex structure. The main bank deployed its solution in an Ireland-based AWS region to meet its operational needs. Concurrently, its investment arm, which required a cloud-only approach and strict data residency, was deployed in a separate Germany-based AWS region. This division also leveraged Echoworx's strong alliance with Mimecast for DLP and a robust S/MIME integration with DigiCert for automated key management.

3. **Frictionless User Enablement:** To drive adoption and meet diverse needs, Echoworx provided tailored user experiences. One business unit received a custom Microsoft 365 add-in with multiple delivery options, including attachment-only and full message encryption. The investment arm opted for a simple, single-button add-in for maximum ease of use, with all complex routing—whether S/MIME or portal delivery—managed automatically on the back end.

Results

Measurable Compliance and Operational Gains

The migration delivered transformative results across security, compliance, and user experience.

- **Portal-less, Frictionless Delivery:** A key requirement was met by enabling secure, portal-less delivery. Using shared passphrases, external contacts could access encrypted messages and attachments directly in their inbox without needing to register for an account or manage new passwords, dramatically improving the user experience.

- **Automated S/MIME and Certificate Management:** For the investment arm, the integration with DigiCert automated the entire S/MIME lifecycle. The system seamlessly generated, managed, and utilized public-private key pairs, while inbound certificate harvesting and signature verification ensured feature parity with their previous Totemo solution.

- **Flexible and Resilient Delivery:** The solution guaranteed secure delivery for every recipient. While S/MIME was the primary method for the investment arm, a secure web portal served as an automatic fallback for any contacts without keys, ensuring no message was ever sent in the clear.

Conclusion

From Disjointed Systems to Digital Sovereignty

This project proves that migrating from legacy encryption in a complex regulatory environment can be a strategic triumph. By partnering with a vendor capable of supporting multifaceted organizational needs, the bank replaced its high-risk endpoint solution with a resilient, cloud-native asset.

The ability to deploy in multiple data regions, integrate with key technology partners, and deliver a frictionless user experience allowed the bank to fortify its security, achieve digital sovereignty, and confidently meet the stringent compliance demands of the DACH market.

Learn more about our technical integrations, visit echoworx.com