Achieving 360° Email Protection and Data Residency Compliance with AI-Powered Email Security and XDR

Industry: Public Sector - Financial Services
Size : 2000+ employees
Region: United Arab Emirates

Business Problem

The client faced challenges with their traditional email security solution, which struggled to protect against advanced threats like phishing, ransomware, and BEC. The existing system was reactive, leaving users vulnerable to modern cyberattacks and lacking sufficient visibility and proactive defense.

How Intertec Helped

Intertec collaborated with Trend Micro to deploy a comprehensive, AI-driven email and collaboration security solution tailored for compliance and cyber resilience:

- Deployed UAE-hosted cloud email security to meet regional data residency mandates
- Enabled real-time protection using AI, ML, Computer Vision, and Writing Style DNA for detecting BEC, ATO, phishing, and zero-day threats
- Secured email and collaboration tools (Microsoft 365, Google Workspace, Box, Dropbox) across API, inline, and gateway layers
- Enhanced visibility with centralized dashboards, XDR telemetry, and attack correlation across communication channels
- Introduced native DLP and encryption for protecting sensitive information
- Launched employee awareness programs to improve cyber hygiene and reduce user-targeted risks

Business Outcomes Delivered

The solution significantly elevated the client's security posture and email resilience, resulting in:

- Complete protection of email and collaboration apps with multi-layered defense against BEC, phishing, ATO, and ransomware
- Zero data leakage outside the UAE, ensuring full regulatory compliance
- Improved incident detection and response through XDR-powered visibility and analytics
- Proactive threat identification via AI, sandboxing, and behavioral analysis—detecting both known and unknown attack tactics
- Strengthened user protection with identity-based risk scoring, remediation for high-risk users, and writing-style detection
- Actionable threat insights for leadership via Advanced Security Risk Management (ASRM) and unified reporting