LEAP XPERT

Now More Than Ever

Why Enterprise Messaging Needs a Security-First Architecture

Dima Gutzeit, Founder & CEO
LeapXpert

May 8, 2025

Introduction

“We’ve been hacked.”

Those three words should send chills down the spine of any organization using consumer messaging platforms like WhatsApp, iMessage, SMS, Telegram, Signal, WeChat, or LINE for official communications.

When consumer apps are adapted for enterprise use without security as the foundation, vulnerabilities can be exploited with alarming speed, transforming what should be secure, compliant conversations into public disclosures and triggering organizational crises that unfold in real-time across global headlines.

As the industry leader in responsible business communication, LeapXpert was founded on a critical insight: compliance without security is merely an illusion of protection.

The LeapXpert Communications Platform was built from day one with security-first architecture—not as an afterthought or bolt-on feature.

For financial institutions, government agencies, and regulated industries, enabling proper recordkeeping is essential—but it can’t come at the cost of introducing new security risks. Solving the problem of off-channel communications without oversight must not create a bigger one: vulnerabilities that compromise sensitive data.

And as non-regulated industries begin embracing messaging governance to enable responsible use of modern communication channels, addressing security from day one is critical. Without a security-first foundation, organizations risk trading compliance and governance gains for long-term exposure.

Consumer messaging channels have leapt from personal convenience to mission-critical business tools—without the security infrastructure to match. The consequences of system vulnerabilities are catastrophic:

- Operational paralysis
- Shattered reputation
- Compromised data
- Severe regulatory penalties

Enterprise messaging security is no longer an IT checkbox—it’s a boardroom imperative.

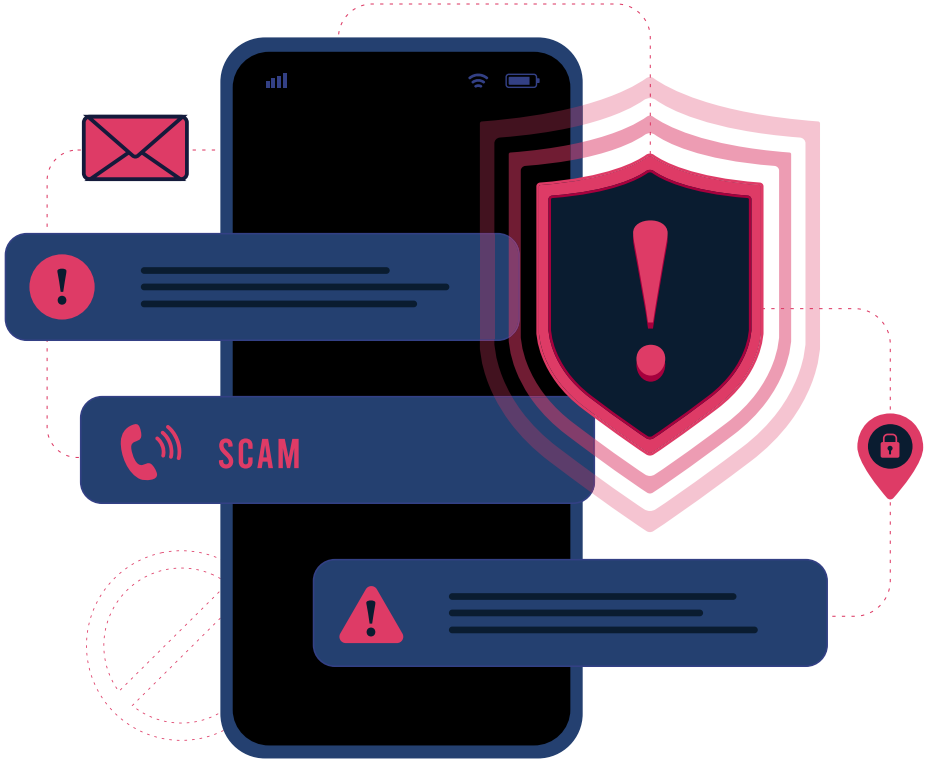
The Evolving Messaging Security Landscape

The enterprise messaging ecosystem faces unique challenges that traditional security approaches struggle to address.

Conventional security models that focus on perimeter defense or basic encryption often fall short when applied to the complex, multi-channel communication needs of modern enterprises.

The stakes are particularly high for organizations in regulated industries. Financial institutions must maintain compliant records of client communications across various channels. Government agencies handle classified information that requires robust protection against both external and internal threats. Healthcare providers need secure communication platforms that protect patient data while enabling efficient collaboration.

Most concerning is the increasing sophistication of attacks targeting messaging platforms. Threat actors recognize these systems as high-value targets that can provide access to sensitive conversations or proprietary information. When organizations deploy messaging solutions with fundamental security weaknesses, they're effectively putting their most sensitive communications at risk.



Security-First Architecture as a Foundation

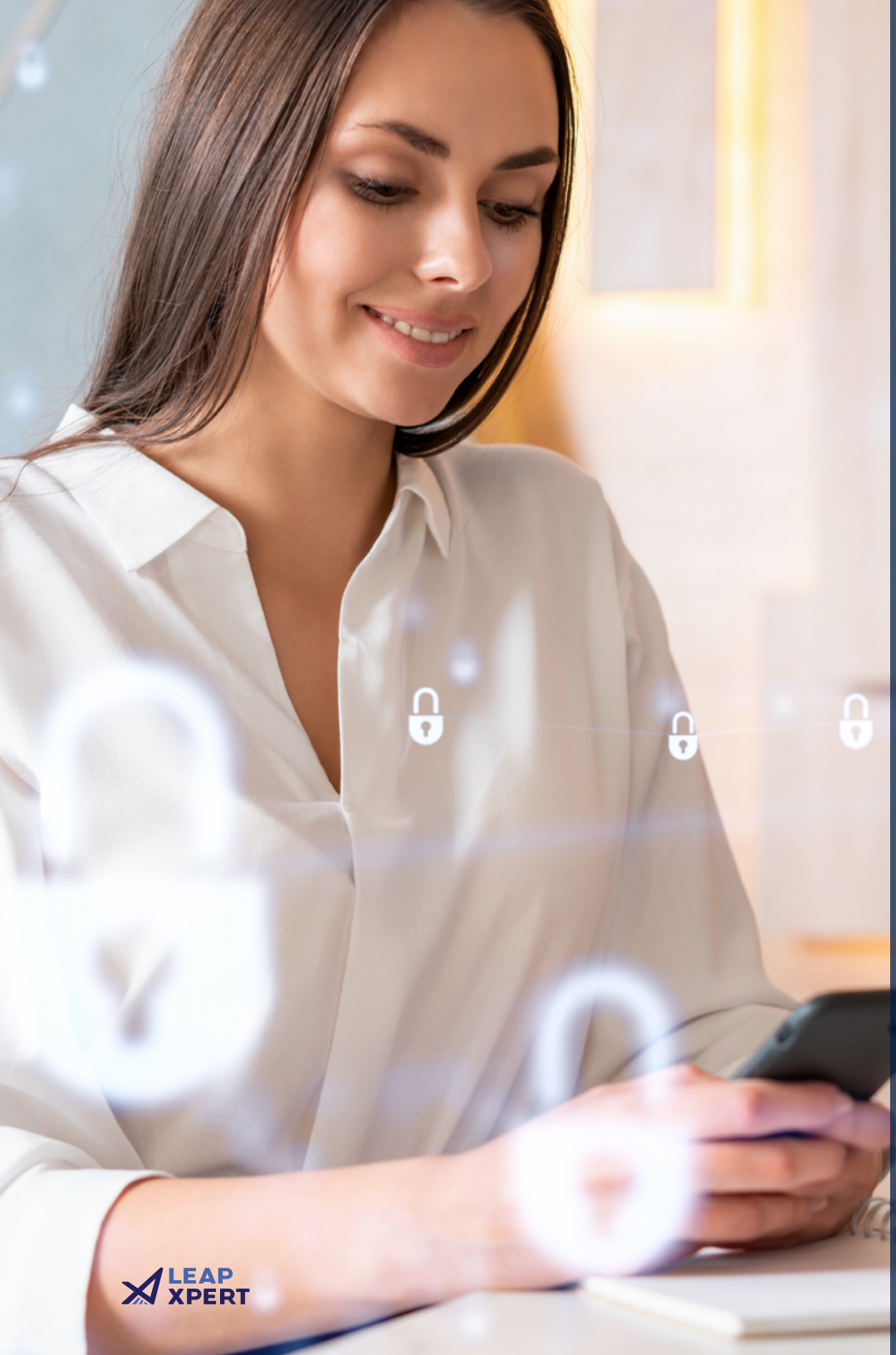
When we founded LeapXpert, we faced a crucial architectural decision that would define our company's future. The market presented two paths: the expedient "wrapper" approach or the more challenging path of building official, authorized integrations from the ground up.

This security-first architecture manifests in several critical ways:

Official channel integrations vs. wrappers

- **The wrapper approach is fragile.** They are unreliable and often break with messaging app updates, require constant compatibility testing, creating a constant liability.
- **The wrapper approach creates operational burden.** These solutions can't be distributed through official app stores, requiring risky sideloading practices.
- **The wrapper approach poses additional security risks.** It deviates the original security of the application and exposes captured communication data to uncontrolled and external systems (e.g, external Wi-Fi networks may be not fully secure)

Instead, we chose the more difficult but only viable path for an enterprise-ready solution—building LeapXpert with official, authorized integrations deployed within secure enterprise environments. Our platform integrates through authorized APIs, methods and features, with data capture mechanisms positioned securely behind enterprise firewalls.



Zero-trust architecture implementation

We implement a comprehensive zero-trust architecture where nothing is trusted by default—even behind traditional firewalls. This security-first approach enforces continuous validation with strict per-request authentication and authorization, regardless of network origin. Our multi-layered protection includes TLS 1.3 encryption for all data in transit, mutual TLS authentication between services, and granular micro-segmentation that prevents lateral movement if a breach occurs. By moving security controls from the network perimeter to each individual resource, we eliminate vulnerabilities inherent to legacy perimeter-based models.

Comprehensive, multi-layered security controls

At LeapXpert, security is systematically integrated across all phases of our platform lifecycle—from development and testing to production and post-deployment. Our approach includes:

- **Granular role-based access control (RBAC)** that prevents unauthorized data exposure by limiting access based on specific roles and responsibilities
- **Comprehensive CI/CD security controls** with segregated access zones and automated security testing to protect the development pipeline
- **Third-party penetration testing** performed by CREST-certified security firms, complemented by continuous internal penetration testing following the OWASP framework
- **SOC 2 Type 2 / ISO 27001 compliant** information security management system, with SOC 2 compliance audited exclusively by one of the big four accounting firms

Customer-controlled encryption

LeapXpert supports Bring Your Own Key (BYOK) encryption so that customers have complete control over their data at rest (AES-256 encryption), allowing you—not us—to secure your sensitive communications.

Enterprise-grade endpoint security

For customers utilizing our Leap Work application, we deliver additional protection by bundling it with either BlackBerry Dynamics or Microsoft Intune, providing enterprise-grade security at the device level.

Beyond security

LeapXpert's foundation provides critical advantages that extend beyond security:

- **Business continuity:** Our official integrations ensure uninterrupted service even when messaging apps update, while wrapper solutions often break with each update cycle.
- **User experience:** LeapXpert delivers consistent performance and reliability that maintains user adoption and satisfaction across teams.
- **Future-ready platform:** Our approach supports rapid integration of new messaging channels and features as business needs evolve, without compromising core platform integrity.

This architectural difference ultimately determines whether your messaging solution will be a sustainable business asset or a potential liability as your communication needs grow and evolve.

Built-in Security Controls and Enterprise Integration

Regulatory compliance alone is insufficient for truly secure enterprise messaging. LeapXpert takes security beyond mere checkbox compliance with robust built-in security controls and seamless integration with enterprise security systems.

Our platform provides:

Advanced threat protection and data security

LeapXpert provides comprehensive security through:

Real-time scanning for malware and viruses

- Scans files using multiple third-party engines
- Reduces outbreak detection times
- Sanitizes and rebuilds files using Content Disarm and Reconstruction technology

Data leakage prevention

- Applies policy rules through built-in DLP module
- Integrates with third-party platforms such as Microsoft Purview
- Issues warnings or blocks in Governed Mode

Information barriers

- Restricts information access to authorized individuals or groups
- Maintains control over chat room participants
- Ensures compliance with corporate communication policies and regulations

Enterprise security integration

Rather than functioning as an isolated system, LeapXpert integrates with your existing security infrastructure. This includes Enterprise Single Sign-On (SSO) integration and connections to enterprise governance systems to enforce existing security policies within the LeapXpert platform.

Comprehensive monitoring

Security events and platform activities are continuously monitored, with the ability to integrate into your security information and event management (SIEM) systems. This extends your security visibility and enables a unified approach to threat detection.

This integration capability enables organizations to maintain consistent security policies across all communication channels, eliminating security gaps that arise when messaging platforms operate outside the enterprise security perimeter.

Data Sovereignty and Control

In an era of increasing data regulation and cross-border concerns, LeapXpert puts organizations in complete control of their messaging data. Unlike alternative solutions that may compromise on data sovereignty, our platform offers:

Flexible deployment options

LeapXpert can be deployed as a dedicated or shared SaaS solution on country-specific clouds, ensuring data sovereignty within specific jurisdictional boundaries. For example, we have some installations in the US, the UK, Switzerland, Germany and other countries on customer-approved cloud service providers.

Complete data ownership

Customers maintain absolute ownership and control over their data, with no third-party access, through our Bring Your Own Key (BYOK) capability.

Geographic control

All data can be stored exclusively within the chosen jurisdiction, preventing inadvertent cross-border data transfers that might violate regulatory requirements or raise sovereignty concerns.

The importance of this control becomes particularly evident when considering international messaging traffic or the potential for foreign access to sensitive communications. Organizations must maintain sovereign control of their most sensitive conversations, especially when they involve matters of national security, strategic business decisions, or regulated information.

"Organizations must maintain sovereign control of their most sensitive conversations, especially when they involve matters of national security, strategic business decisions, or regulated information."

Compliance Without Compromise

For regulated industries or the public sector, recordkeeping requirements are non-negotiable, but compliance need not come at the expense of security. LeapXpert delivers true compliance without compromise:

Comprehensive recordkeeping

Our platform captures all required communications with tamper-proof archiving that meets the strictest regulatory standards. This includes texts, images, files, voice notes, emojis, and a rich set of metadata necessary for regulatory compliance.

Flexible retention policies

LeapXpert enables customers to minimize and customize data retention periods, putting you in control of where and how to keep your data in accordance with your specific regulatory or governance requirements.

Consent management

The platform captures customer consent and delivers custom legal and privacy disclaimers where required by regulations, ensuring compliant operation across various jurisdictions.

This approach ensures that organizations can meet their regulatory obligations while maintaining the highest security standards—a critical balance that inferior solutions often fail to achieve.

The LeapXpert Difference

Recent events have demonstrated that messaging security can no longer be an afterthought. As the use of messaging applications continues to expand across enterprises globally, organizations must adopt solutions built on fundamentally secure architectures.

LeapXpert stands apart through:

- A security-first architecture that builds protection into every aspect of the platform
- Official channel integrations that avoid the inherent vulnerabilities of wrapper approaches
- Zero-trust design principles that minimize attack surfaces and contain potential breaches
- Comprehensive security controls that extend beyond basic compliance
- Enterprise integration that aligns messaging security with broader security strategies
- Complete data sovereignty that puts organizations in control of their communications

In a world where messaging vulnerabilities can quickly escalate to organizational crises, the choice of a secure, governed messaging solution has never been more critical. LeapXpert delivers the robust security architecture that modern organizations require—moving beyond mere compliance to true communication security. When it comes to securing sensitive data, the right foundation matters. You can rely on assumptions, or you can rely on architecture built for integrity, oversight, and resilience. At LeapXpert, that foundation is already in place.

About LeapXpert

LeapXpert, the responsible business communication leader, provides enterprises peace of mind through compliant and secure communication solutions. The LeapXpert Communications Platform enables compliant, governed, and secure communication between enterprise employees and their clients across consumer messaging channels, while leveraging Communication Intelligence to enhance front-office employee productivity and decision-making. LeapXpert, a Gartner Cool Vendor, is headquartered in New York, with offices in London, Tel Aviv, and Asia. Hundreds of enterprise customers, with hundreds of thousands of users in more than 45 countries, depend on LeapXpert daily for Digital Communications Governance and Archiving (DCGA) solutions. For more information, visit **leapxpert.com**