Forcepoint

Solution Brief

Protect WhatsApp Conversations with Forcepoint and Tuvis

Challenge

- Organizations struggle to prevent sensitive data from leaking via methods such as high-velocity chat and file sharing
- When sensitive data travels across unmonitored channels or resides on unmanaged devices, it is impossible to apply full visibility and governance to it
- A patchwork of national and industry-specific regulations raises the burden of compliance for organizations and makes it difficult to expand operations

Solution

- Forcepoint DLP integrates with Tuvis to capture sensitive chat messages and media in WhatsApp in real time
- Set the solution to automatically enforce DLP policies to data-in-motion, inspecting and guarding sensitive data as it moves through WhatsApp
- Log incidents and trigger instant alerts for policy violations to facilitate rapid admin response to data threats

Outcome

- Achieve visibility and governance over sensitive data by continuously monitoring it as it travels across messaging channels
- Simplify compliance to global data regulations by identifying and protecting sensitive data-in-motion and reporting incidents
- Enforce data security policies without compromising the WhatsApp native user experience or hindering employee productivity

WhatsApp Business is no longer just a convenience. It's a critical channel for customer engagement and internal collaboration. But while adoption soars, so do the risks. Sensitive data, financial details and regulated information now flow through a platform never built for enterprise-grade security.

To stay ahead, organizations need more than visibility. They need unified governance and seamless policy enforcement across every communication channel. With the right controls in place, you can embrace modern messaging without sacrificing compliance, security or speed.

Business Challenge

→ Sensitive data leaks through high-velocity chat and file sharing

→ Limited visibility and governance across unmanaged channels

→ Increasing regulatory pressure (GDPR, LGPD, FINRA, SEC, HIPAA)

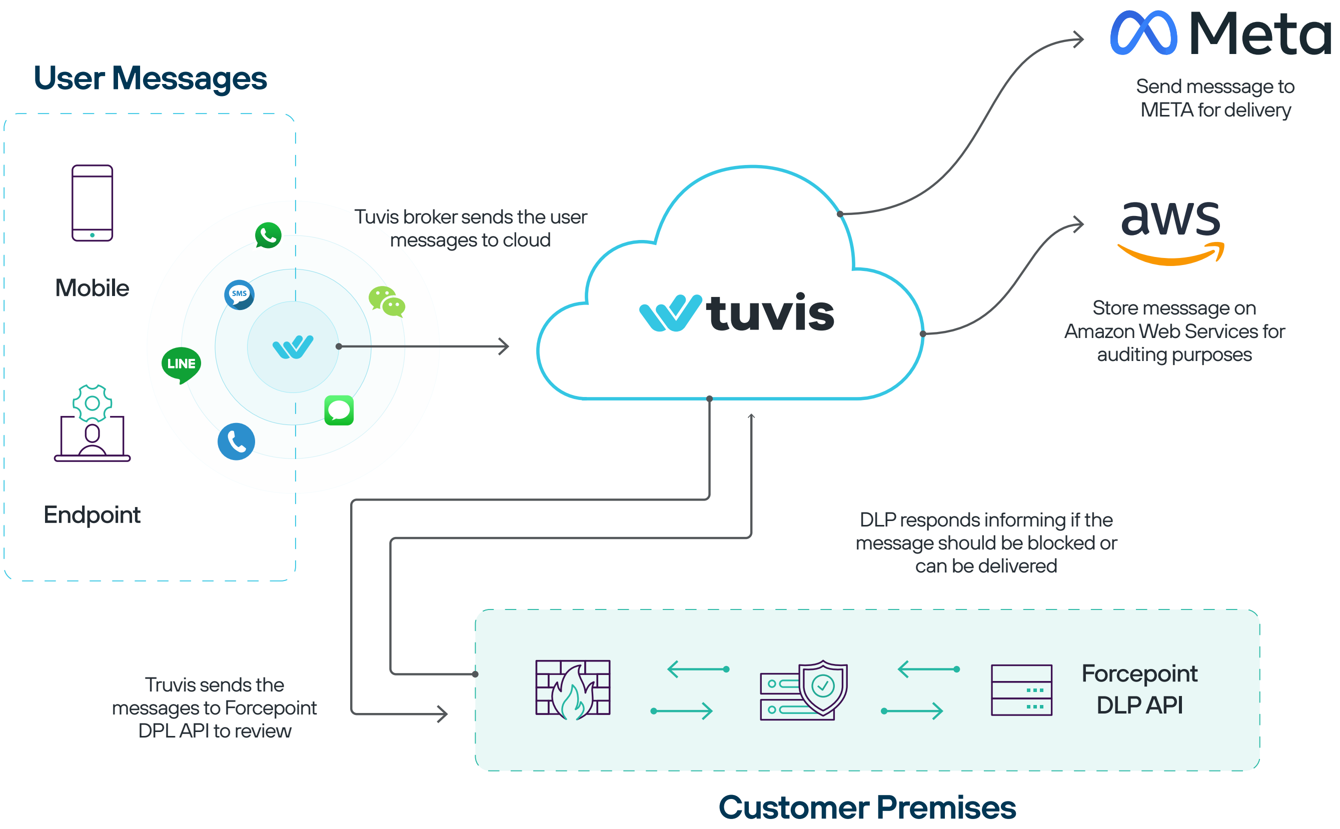
The Solution

Forcepoint has partnered with Tuvis, a leader in secure, compliant messaging, to close the data protection and governance gap in WhatsApp. Applying Forcepoint's advanced Data Loss Prevention (DLP) policies directly within WhatsApp via the Tuvis platform ensures that every message, file or media is monitored, blocked or recorded according to the company's rules without affecting the end-user experience. This joint solution empowers organizations to:

→ Capture sensitive chat messages and media in WhatsApp in real time

→ Automatically enforce DLP policies to inspect and protect content in motion

→ Capture incidents and send instant alerts for policy violations to speedresponse


User Messages
Mobile
Endpoint
Tuvis broker sends the user messages to cloud
tuvis
Meta
Send messsage to META for delivery
aws
Store messsage on Amazon Web Services for auditing purposes
DLP responds informing if the message should be blocked or can be delivered
Truvis sends the messages to Forcepoint DPL API to review
Forcepoint DLP API
Customer Premises

Organizations today face constantly changing risks to data, rapidly evolving regulatory requirements, increased scrutiny,

→ **Real-Time Capture of Communications**
Tuvis acts as the secure bridge between WhatsApp and your security ecosystem. Every message, attachment, image, video and voice note shared through WhatsApp is captured in real time. This ensures that no communication bypasses your organization's security and compliance controls.

→ **Automatic Enforcement of Forcepoint DLP Policies**
Once captured, the content is immediately analyzed by Forcepoint's advanced Data Loss Prevention (DLP) engine. Using contextual analysis and classification, Forcepoint evaluates the data against your organization's policies, whether that means detecting regulated information (like PCI, PHI or PII), intellectual property or sensitive keywords.

→ **Policy Actions in Flow**
Based on the policy evaluation, Forcepoint can automatically block or restrict risky actions before data leaves the organization. For example, it can prevent the sharing of confidential files, financial records, patient information or sensitive contract terms. These controls are applied seamlessly within the messaging workflow, so employees can continue collaborating without friction.

→ **Incident and Alert Generation**
If a policy violation occurs, whether it's an attempt to share regulated data or a breach of internal rules, the system generates an incident in real time. Security teams receive alerts immediately, complete with context and audit trails, enabling rapid investigation and response.

→ **Continuous Governance and Compliance**
This integration ensures ongoing visibility into unmanaged messaging channels, helping organizations maintain compliance with global and industry-specific regulations such as GDPR, LGPD, HIPAA, FINRA and SEC. It also supports audit readiness by logging all relevant interactions and enforcement actions.

Solution Benefits

- → **Proactive risk prevention:** Security policies applied directly within communication flows
- → **Simplified compliance:** Adherence to global data protection laws and industry regulations
- → **Visibility and governance:** Continuous monitoring of interactions in messaging channels
- → **Immediate response:** Automatic alerts and incident creation for rapid action
- → **WhatsApp native user experience:** Policy enforcement without impacting employee workflows

Cross-industry Use Cases

Financial Services

Automatically block the sharing of card numbers, account statements or sensitive financial documents through messaging apps. Generate real-time alerts whenever employees attempt to transmit regulated data, ensuring compliance and protecting customer trust.

Healthcare

Prevent the transfer of medical reports, lab results or patient identifiers through WhatsApp or other messaging applications. Detect and stop attempts to share sensitive data outside authorized systems to maintain patient privacy and reduce liability risks.

Telecommunications and Service Providers

Restrict the use of sensitive keywords such as contract terms or pricing information and block attachments that contain confidential commercial documents. This helps safeguard competitive intelligence and maintain compliance with internal policies.

Retail

Block the sharing of card data, exclusive discount coupons, customer lists or internal promotions via messaging apps. Detect and prevent attempts to share strategic data with unauthorized third parties to protect customer information and brand reputation.

Government and Public Sector

Apply strict DLP policies to prevent the transmission of classified documents or sensitive keywords through personal or corporate messaging applications. This ensures confidentiality of state data and compliance with public sector security standards.

The Forcepoint and Tuvis integration delivers enterprise-grade security for WhatsApp Business, ensuring compliance, preventing data leaks and enabling fast, secure collaboration.

forcepoint.com/contact