AWS SECURITY

5 Keys to Secure Enterprise Messaging

Reducing the security and compliance risks of messaging apps

Table of contents

Introduction

The Rise of Messaging Apps

Messaging is a vital part of daily life. Employees routinely use messaging applications (apps) on both personal and corporate devices to chat with friends and family, and boost productivity at work.

While consumer messaging apps are convenient and support real-time communication with colleagues, customers, and partners, they lack the robust security and administrative controls many businesses require.

An estimated 3.09 billion mobile phone users access messaging apps to communicate, and this figure is projected to grow to 3.51 billion users in 2025.[1]

1 - https://www.statista.com/statistics/483255/number-of-mobile-messaging-users-worldwide/

The Risks of Messaging Apps

Consumer messaging apps are often free and simple to use, but they can introduce risks if used in business settings.

Security – The transmission of sensitive and proprietary data—such as personally identifiable information, protected health information, financial records, and intellectual property—through messaging apps and collaboration tools that lack critical encryption and security protocols increases the likelihood of a security incident.

Control – Unlike the oversight organizations have over business email, IT has no control over information transmitted with consumer messaging apps. Account management features that allow administrators to update passwords and remove profiles remotely are often absent, increasing the threat of data exposure stemming from a lost or stolen device.

Compliance – Unapproved and unmonitored use of messaging apps can lead to a failure to preserve business communications in accordance with regulatory requirements that fall under the Federal Records Act (FRA), the National Archives and Records Administration (NARA), as well as Securities and Exchange Commission (SEC) Rule 17a-4 and Sarbanes-Oxley (SOX). This can lead to increased organizational risk.

"It is now logical to assume that most financial services organizations with mobile Bring Your Own Device (BYOD) programs for regulated employees could be fined due to a lack of compliance with electronic communications regulations." [2]

2 - Gartner, "Quick Answer: Are Mobile BYOD Programs Still Viable for Regulated Employees in Financial Services?," Tom Cipolla, Erin Pierre, Pankil Sheth, 20 January 2023.

Keys to Secure Enterprise Messaging

Evolving threats, flexible work models, and a growing patchwork of data protection and privacy regulations have made maintaining secure and compliant messaging a priority for organizations across the globe.

This eBook details five keys to secure enterprise messaging that balance people, process, and technology.

Key #1: Establish Clear Policies

Policies are a vitally important component of any security program. Without a security policy governing the use of unauthorized technologies, each employee or user will be left to decide what's appropriate, and what's not.

Establishing detailed policies and guidelines to make employees aware of the ramifications and restrictions around messaging app use is critical. Policies spelling out the do's and don'ts, along with the actions that will be taken in response to violations should be published from high up in the organization, and communicated clearly. Be sure to detail specific protocols and processes for sharing sensitive data, so employees understand appropriate communication channels.

When developing policies, many organizations choose to restrict messaging apps and specify which can be used. While some companies impose a complete ban of any form of unmonitored messaging, this may not be practical. Work with your HR, legal, and operations teams to develop policies that will be effective for your workforce.

You can build upon existing policies that cover privacy, electronic communication, or social media. Company laptops can be set up to block unapproved messaging apps from running desktop versions, and—if managed Android/iOS devices are in use—mobile device management (MDM) technologies can achieve the same result.

Key #2: Educate Employees

Training and education are critical to strengthening cybersecurity. Even with the most robust and modern tools, security is effective only when people know what to do and how to do it.

The World Economic Forum reports that 95% of cybersecurity issues are traced to human error.[3]

Conduct ongoing security awareness campaigns that cover communication channels including text, voice and video messaging, emails, and file sharing. Policies detailing acceptable software, tools and apps should be highlighted, as well as risks related to improper messaging app usage such as communication interception, adversary-in-the-middle attacks, and organizational fines related to record-keeping lapses.

Ensuring employees know how they can use technology in a way that doesn't leave them—and your organization—open to threats will go a long way to keeping your data safe.

3 - https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf

"Assume positive intent when building security educational programs. The majority of people want to do the right thing, and you need to create opportunities to inform and model what good security hygiene looks like with clear expectations."

- Jenny Brinkley, Director at Amazon Security

"When organizations have a strong security culture and everyone sees security as their responsibility, they can move faster and achieve quicker and more secure product and service releases."

- Clarke Rodgers,
Director of Enterprise Strategy at AWS

Key #3: Build a Culture of Security

Evaluate Your Current State – Consider the strength of your existing security awareness program or security culture. Free resources such as the SANS Security Awareness Planning Kit can help you determine how mature (or immature) your program is, identify short and long-term goals, and communicate your efforts to leadership.[4]

Go All In – Get company-wide buy-in from security leaders and C-level executives, all the way down to individual managers. Update your organization's overall vision or mission statement to clearly communicate that security is non-negotiable. Let employees know what's in it for them; they'll be more invested if they understand security awareness extends beyond corporate concerns to protect against threats to their identity and financial security.

Mind the Culture – Focus on building a strategy that blends your security awareness program with your existing corporate culture. Initiatives that are carefully tailored to your industry as well as workforce demographics, regions, departments, and roles will help your employees see security as part of their story, and give them a sense of ownership.

Make it Engaging – Choose relatable content that is visually and emotionally compelling. Reinforce key messages, but diversify delivery methods to include a mix of presentations, videos, discussions and hands-on labs that appeal to all learning styles. Behavior-related metrics that focus on assessment results, and the performance of high-risk individuals can help you measure progress and determine what drives the most change.

Avoid Punishment – Security events should be treated as learning opportunities, rather than cause for punishment. If users fear they'll be singled out and blamed, reprimanded, or even fired for security-related blunders, they'll be far less likely to report them. Taking a "more carrot, less stick" approach will encourage employees to share their experiences and make them feel like collaborators.

4 - https://www.sans.org/security-awareness-training/demos/security-awareness-planning-kit/

Key #4: Use True End-to-End Encryption

While many messaging apps offer some form of encryption, not all of them use end-to-end encryption (E2EE). E2EE is a secure communication method that protects data from unauthorized access, interception, or tampering as it travels from one endpoint to another.

In end-to-end encryption, asymmetric cryptography—also known as public-key cryptography—is used to encrypt and decrypt data with two separate cryptographic keys. Encryption takes place locally, on the sending device. Every call, message, and file is encrypted with a unique private key. Unauthorized parties cannot access communication content, because they don't have the private key required to decrypt the data.

Encryption in Transit vs. End-to-End Encryption

Encryption in transit encrypts data over a network from one point to another (typically between one client and one server); data may remain stored in plaintext at the source and destination storage systems. End-to-end encryption, by contrast, combines encryption in transit and encryption at rest to secure data at all times, from being generated and leaving the sender's device, to arriving at the recipient's device and being decrypted.

"Messaging is a critical tool for any organization, and end-to-end encryption is the security technology that provides organizations with the confidence they need to rely on it."

- CJ Moses, CISO and VP of Security Engineering at AWS

Key #5: Implement Effective Data Retention

Retaining data in accordance with internal, legal, and regulatory requirements is an important part of secure enterprise messaging. Consumer apps that rely on individual users to back up messages and share records do not support a scalable or reliable method of recordkeeping.

Establish a Data Retention Policy – This requires finding and classifying data, and determining which requirements apply to which data. Directives detailed in the policy should cover the following:

- Where data is stored
- What storage is used
- How long data is preserved
- What happens when data is no longer needed
- How to facilitate compliance

Find the Right Solution – While E2EE is often thought of as incompatible with data retention, enterprise-grade messaging services offer both, providing you with the ability to deploy an encrypted host within your environment, and configure a data store of your choice to retain conversations—without exposing them to outside parties. No one other than the intended recipients and your organization has access to content, giving you full control over your data.

How AWS Wickr Can Help

AWS Wickr was built from the ground up with features designed to help you keep communications secure, private, and compliant.

Messaging – Send private, end-to-end encrypted messages and files either one-to-one or in groups. Default expiration and burn-on-read (BOR) timers can be set for each room or message, allowing you to destroy sent messages and files after a set amount of time (anywhere from 1 minute to 365 days), or automatically delete messages once they have been read by recipients.

Calling – Hold end-to-end encrypted voice or video calls for up to 100 participants within AWS Wickr rooms, or one-on-one calls within direct messages. Securely share video, audio, and screens with up to 500 participants during conference calls.

Security – Protect communications with 256-bit Advanced Encryption Standard (AES) E2EE. User key verification helps confirm digital signatures and protect against adversary-in-the-middle attacks. Open access capabilities provide domain fronting, as well as SSH and VPN technology to direct encrypted traffic around blocking attempts and identify the best path for data in restricted environments.

External Federation – Allow individual users and teams to safely collaborate with outside parties. Groups of users can be assigned to specific federation rules. Access can be restricted to select customers, vendors, partners, and other companies or subsidiaries.

Guest User Access – Wickr administrators can enable or disable the guest user feature for individual security groups in the Wickr admin console. Once the feature is enabled, anyone can sign-up for a Wickr guest account with their email address, and participate in secure conversations that are initiated by licensed Wickr network users.

Data Retention – Retain information in a private data store that you control to help meet legal hold, audit, and compliance needs. Data retention can be implemented as an always-on recipient that is added to conversations, not unlike the blind carbon copy (BCC) feature in email. The data retention process can run anywhere: on-premises, on an Amazon Elastic Compute Cloud (Amazon EC2) virtual machine, or at a location of your choice.[5]

Administrative Controls – Fine-grained administrative controls allow you to organize users into security groups with restricted access to features and content at their level. Passwords can be reset and profiles can be deleted remotely, helping you reduce the risk of data exposure stemming from a lost or stolen device.

5 - https://aws.amazon.com/blogs/aws/aws-wickr-a-secure-end-to-end-encrypted-communication-service-for-enterprises-with-auditing-and-regulatory-requirements/

Getting Started

Are you confident in your ability to secure enterprise messaging?

Employees today depend heavily on messaging tools. Establishing clear policies that cover the use of messaging apps, incorporating a security-first solution that combines end-to-end encryption with data retention capabilities, and increasing awareness of security issues will allow you to accelerate collaboration, while protecting your organization's data.

Keep your communications safe with AWS Wickr. Let us show you how.

Please visit https://aws.amazon.com/wickr/ for more information.

"As former employees of federal law enforcement, the intelligence community, and the military, Qintel understands the need for enterprise-federated, secure communication messaging capabilities. When searching for our company's messaging application we evaluated the market thoroughly and while there are some excellent capabilities available, none of them offer the enterprise security and administrative flexibility that Wickr does."

- Bill Schambura, CEO at Qintel