rocket.chat

12 things to look for in a **secure business communication platform**

Ensure regulatory compliance and highest security standards while communicating remotely

For most businesses out there, the customer is the king. **Every company wants to keep their customers happy** - and ensuring data privacy is one of the best ways to do it.

Employers want their business to be successful. In order to do that, they **need to foster communication and collaboration among their teams**. At the same time, they need to guarantee to their customers that their data is safe and secure.

Read on to find out **why you should pay attention to the security aspect of your business communication**, and which 12 security features should your communication platform entail.

Why security matters when it comes to communication

It is increasingly important to businesses to facilitate seamless communication among their employees. However, **cybersecurity risks are everywhere**, and business communications are being targeted.

Since the abrupt switch to remote work happened in 2020, there has been an increase in cyberattacks. More specifically, 20% of directors and C-suite executives in IT and cybersecurity roles say they have experienced a security breach as a result of a remote worker since switching to a work-from-home model in 2020.[1]

As the frequency and intensity of data breaches goes up, businesses are looking to strengthen their cybersecurity and protect their sensitive data. These are the specific reasons why businesses prioritize security when it comes to their internal communications.

#1 Employees want to communicate effortlessly

Nowadays, employees expect to exchange information and collaborate without a hassle. **In their private lives, most of them use WhatsApp, Facebook Messenger**, or another popular communication app. They expect the same level of user experience from their business communication platform.

When companies don't deliver a seamless communication experience to their employees, they tend to talk about work-related matters in less secure channels. For example, 53% of remote workers reportedly use consumer messaging apps for work between one and six times per day.[2]

However, consumer messaging apps don't uphold the same security standards as business ones. **Sharing sensitive business information via consumer communication channels is risky**, despite their great user experience. This is why businesses are increasingly looking into communication and collaboration platforms that can ensure safe management and confidentiality of their conversations.

#2 Customers care about safety of their data

Data privacy is becoming increasingly important to customers. In a recent study, 83% of Americans said they would stop buying from a business after it experienced a security breach.[3]
Moreover, 52% of US citizens **refused to use a product or a service due to privacy concerns**.[4]

This is why companies must ensure their communication stays private. Many businesses go over and beyond to ensure they are in total control over all the communication going on between their employees.

In the words of Rocket.Chat's VP of Product:

> ***Compromised data protection is a disqualifying factor when it comes to business communication solutions.***

Christopher Skelly, VP of Product at Rocket.Chat

#3 Avoiding costs

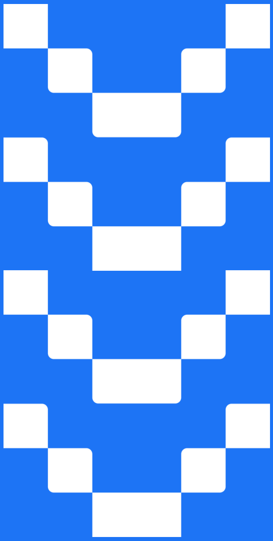
It’s very clear to many businesses that, besides costing them a good reputation, data breaches are also financially very costly. Let us just drop a few numbers here:

- 24% of directors and C-suite executives in IT and cybersecurity roles say that they have paid unexpected expenses to address cybersecurity breaches since switching to remote work model in 2020[5]
- The average cost of a data breach in the US is **$3.8 million** - and it takes 280 days on average to identify and contain it[6]
- In 2020, penalties under GDPR totaled **€158 million**.[7]

With these statistics in mind, businesses should be aware of how important it is to ensure the highest security level of their data and business processes.

12 security features your business communication platform should entail

Secure communication platform is not a myth - and there is no one right way to ensure safety of communication. However, this **checklist of security features** is something you should look for in your communication platform.



#1 Open-source code

Open-source code is our #1 choice when it comes to secure software of any kind, including communication platforms. When an app is open-sourced, it means that its code is publicly available for anyone to see.

It may seem counterintuitive to believe that this feature is safety-friendly. However, the transparency allows anyone to see the code, recognize potential vulnerabilities in it, and propose changes to it to make it more safe.

This is exactly what happens. Members of open-source communities love improving apps' codes' safety, and the sheer number of contributing developers and their different approaches makes the open-source projects as safe as they are.

#2 End-to-end encryption

Encryption was popularized in mass communications when WhatsApp decided to build it in their messaging app. However, end-to-end encryption is nowadays a standard security feature of business communication platforms.

End-to-end encryption ensures that a message cannot be seen from anyone but the sender and the receiver - parties that hold the encryption keys. As such, it prevents eavesdropping from third parties.

However, when it comes to absolute security of communication, encryption doesn't suffice. Why? Because it only ensures message security in transit. You still need to address the security of your devices and servers that store copies of your communications.

#3 On-premise hosting

Although cloud storage has been immensely popular in the last decade, we see companies opting for on-premise hosting more than ever. On-premise hosting allows organizations to have full control over their data, and not risk cybersecurity breaches directed at their communications provider.

Moreover, on-premise hosting is not as lengthy nor complicated as it used to be. 92% of companies report an increase in on-premise software sales, and the demand for it is equal as for public cloud solutions.[8]

Naturally, the same research shows that 65% of buyers want on-premise solutions due to unmatchable security and data protection levels.

#4 Regulatory compliance

Some industries or geographical areas require businesses to comply with specific data protection regulations. HIPAA in the US healthcare industry, CCPA in California, US, or GDPR in the European Union are such examples.

Make sure your communications platform can be adjusted to comply with such regulations in order to protect sensitive data that your employees exchange.

#5 DLP

DLP or Data Loss Prevention technology helps companies to identify and protect their data by making sure no data is misused, lost, or used by unauthorized parties. It works by classifying business critical data (typically driven by regulatory compliance) and prevents end users from accidentally or intentionally sharing data that could put a company at risk.

Data Loss Prevention technology is much needed - since approximately 90% of data breaches happen through human error.[9]

#6 Multi-Factor Authentication

Multi-Factor Authentication or MFA is a staple in enterprise-grade security. The main purpose of multiple authentication is to ensure that the right person is logging in the software. This is why users have to either authenticate with the combination of email, text message, mobile app, and other.

#7 Safe integrations

Communication platforms can expose your data in numerous ways. One of the most common ways is integrating with third-party apps to perform certain functions, but then sharing user data and metadata with them.

Therefore, it is useful to see for which functionalities of your communication platform you need to install third-party apps, and what is the nature of the integration.

#8 LDAP/Active Directory

Lightweight Directory Access Protocol is a protocol used to talk to different types of directories - including Active Directory. Active Directory is used to ease the management of users and computers by storing information about them in a single place.

Moreover, Active Directory has security features like authentication, security groups, and group policies.

#9 OAuth

OAuth is an authorization protocol that provides apps the capability for secure appointed access. In other words, OAuth doesn't share password data, but uses authorization tokens to prove an identity between users and service providers, thus serving as a security feature.

#10 Single Sign-On

Single sign-on is an authentication scheme that allows users to log in with a single ID and password to multiple software systems that are independent, but related. It mitigates risks for access to third-party sites and reduces password fatigue.

#11 ID-only push notifications

This security feature ensures that push notifications do not pass through any other services before reaching a device. Instead, the message content is fetched directly from the server, thus ensuring higher security and compliance standards.

#12 Ease of use

Although it may not seem as a security feature at all, it is crucial that the platform you provide as an all-in-one solution in your company is easy to use. If it’s not, employees will be less likely to use it, and will resort to alternatives - usually consumer messaging apps, which do not comply with enterprise security standards.

Security checklist: features your communication platform should entail

□ Open-source code

□ End-to-end encryption

□ On-premise hosting

□ Regulatory compliance

□ DLP

□ Multi-Factor Authentication

□ Safe integrations

□ LDAP/Active Directory

□ OAuth

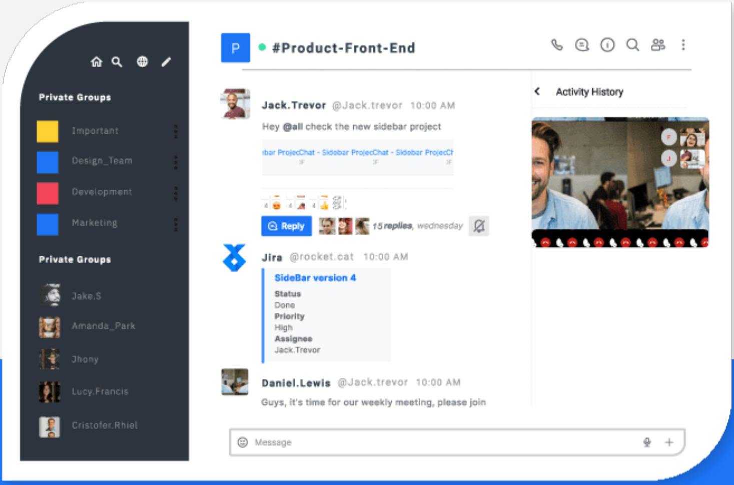
□ Single Sign-On

□ ID-only push notifications

□ Ease of use

About Rocket.Chat

Bringing data protection into every conversation rocket.chat



P #Product-Front-End

Private Groups

Important

Design_Team

Development

Marketing

Private Groups

Jake.S

Amanda_Park

Jhony

Lucy.Francis

Cristofer.Rhiel

Jack.Trevor @Jack.trevor 10:00 AM

Hey @all check the new sidebar project

Reply 15 replies, wednesday

Jira @rocket.cat 10:00 AM

SideBar version 4

Status
Done
Priority
High
Assignee
Jack.Trevor

Daniel.Lewis @Jack.trevor 10:00 AM

Guys, it's time for our weekly meeting, please join

Activity History

Message

TRUSTED BY

DB Systel GmbH · THE WORLD BANK · Continental · UNIVERSITÄT BIELEFELD

In a hybrid work environment, being able to collaborate in real-time while ensuring complete data privacy is a must!

Rocket.Chat is a communications platform that enables real-time conversations between colleagues, with other companies, and with your customers. It does everything other platforms do, **except exposing your data.**

Trusted by 12+ million users in over 150 countries, Rocket.Chat is the worlds' largest true open source communications platform fully customizable for your business.

Reduce operational costs, own your data and improve customer experience by bringing all communications under a single platform.

Schedule a demo

Sources

1 https://www.malwarebytes.com/resources/files/2020/08/malwarebytes_enduringfromhome_report_final.pdf

2 https://hitachi-systems-security.com/messaging-apps-and-privacy-how-organizations-can-avoid-and-mitigate-risks/#_ftnref2

3 https://www.businesswire.com/news/home/20190917005012/en/New-Global-Research-Shows-Poor-Data-Security

4 https://www.pewresearch.org/fact-tank/2020/04/14/half-of-americans-have-decided-not-to-use-a-product-or-service-because-of-privacy-concerns/

5 https://www.malwarebytes.com/resources/files/2020/08/malwarebytes_enduringfromhome_report_final.pdf

6 https://www.ibm.com/security/data-breach

7 https://www.tessian.com/blog/biggest-gdpr-fines-2020/

8 https://f.hubspotusercontent10.net/hubfs/8554162/The_State_of_On-Prem_Whitepaper.pdf

9 https://www.techradar.com/news/90-percent-of-data-breaches-are-caused-by-human-error