

# Navigating the Skype for Business Sunset:

Your next steps

2025

2024

2023

2022

2021

2019

2018



# The clock is ticking; it's time to move away from end-of-life software!

Microsoft's decision to **sunset Skype for Business Server (SFB Server)** prompts organizations around the globe to **revisit their communication strategies**.

They **ended mainstream support for SFB Server on January 9, 2024**, which means that they **don't accept requests for new features or design changes**, nor do they honor warranty claims. Only basic fixes will be available until October 2025, and after that, **even those will stop**.

Product	Start date	Mainstream Support end date	Extended Support end date
Skype for Business Server 2015	July 30, 2015	October 13, 2020	October 14, 2025
Skype for Business Server 2019	October 22, 2018	January 9, 2024	October 14, 2025
Skype for Business Server Subscription Edit (SE)	Q3, 2025	Under Microsoft's Modern Lifecycle Policy, support can end with just 12 months' notice if no successor is offered.	

Without security updates, Skype for Business Server becomes an easy target for cyberattacks. **If you don't switch by October 2025, your business will be wide open to hackers, data breaches, and compliance risks, with no safety net.**

## What can Sfb users do about the end of life?

Microsoft recommends migrating to Teams; however, **Teams isn't suitable for organizations handling sensitive data** or bound by strict legal mandates, as it **doesn't support self-hosted deployments, raising concerns over data sovereignty**.

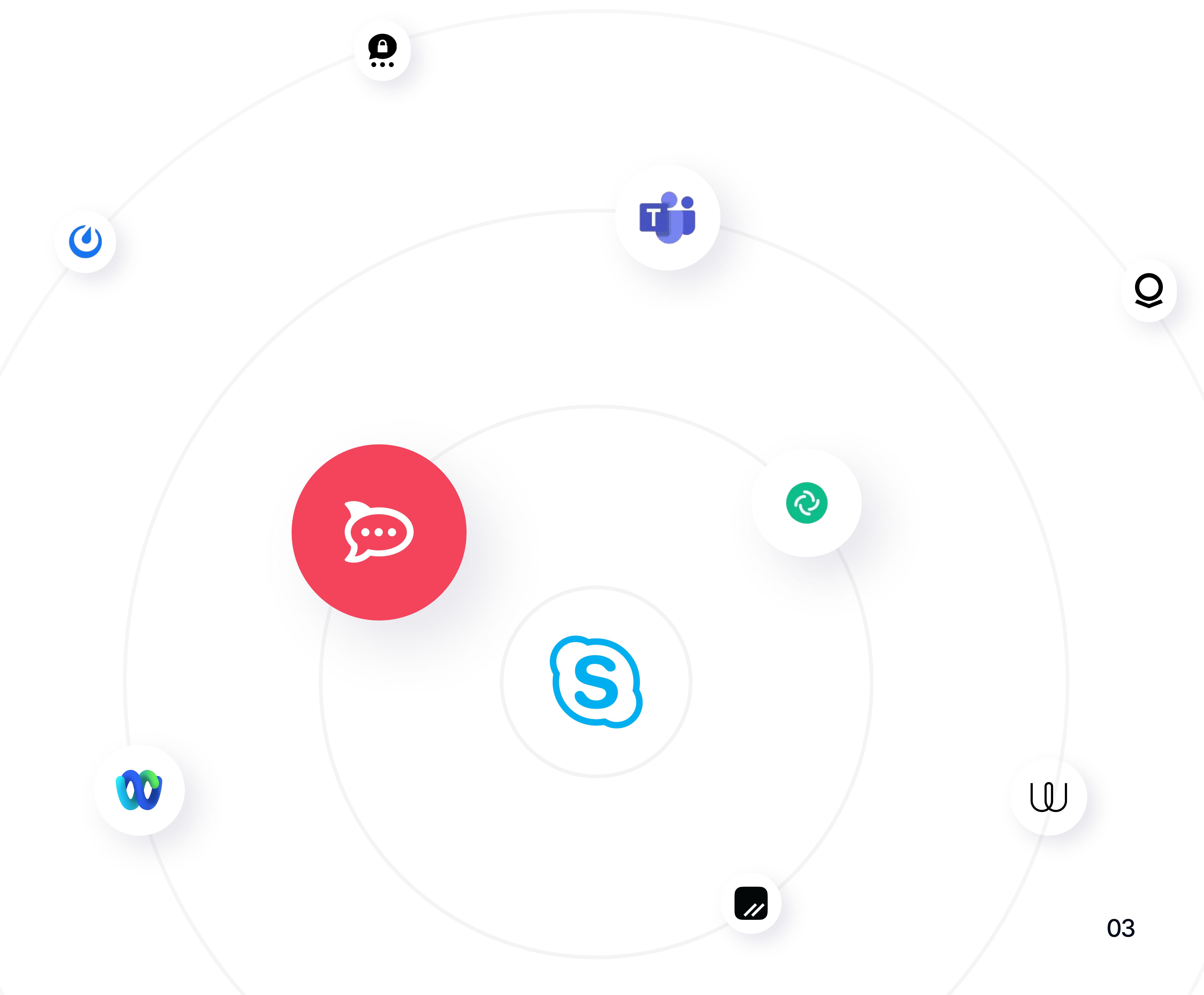
Microsoft recently announced the Subscription Edition for Skype for Business Server users, available from Q3 2025. This edition **follows Microsoft's Modern Lifecycle Policy**, which means **support could end with just 12 months' notice, or Microsoft could introduce a successor product, forcing another migration**.

With extended support ending on October 14, 2025, the **upgrade window is dangerously short, especially for large-scale organizations with complex infrastructures**.

If you need to stay on-premises to keep sensitive data out of third-party clouds and want a **secure, compliant, and reliable solution before October 2025, the time to act is now**.

# What's inside

- 01 Understanding the implications of the sunset
- 02 Time to upgrade: Seek a replacement solution
- 03 7 factors you should consider when looking for a replacement
  - Data sovereignty
  - Robust information governance
  - Advanced customization options
  - Interoperability and cross-platform messaging
  - End-to-end encryption
  - Integration with SFB ecosystem
  - Is Subscription Edition the right choice?
- 04 Comparison matrix to help you identify the ideal solution
- 05 Charting the path forward: Migration plan well suited to your business



# Implications of Skype for Business Server's **end of life**

The sunsetting of SFB Server represents a significant shift that could disrupt workplace communications if not handled effectively. It presents several challenges for organizations.

1. **Security risks:** The lack of support and updates from Microsoft leaves users exposed to security vulnerabilities, increasing the risk of data breaches and cyberattacks.

---

## 4.45M

USD that's the staggering cost of a data breach in 2023, marking a significant **15% increase since 2020**.

**Source: IBM Report**

- 
2. **Compliance challenges:** Organizations may encounter compliance gaps as regulatory requirements evolve, and unsupported software may fail to meet industry standards.

---

## 68%

of IT decision-makers in regulated industries reported **challenges in meeting compliance requirements due to outdated or unsupported software**.

**Source: Osterman Research**

- 
3. **Growth impediments:** Persisting with end-of-life software limits integration with newer technologies, and curbs growth by diverting resources to maintenance.

---

## 25%

of IT costs can be reduced if businesses transition away from legacy applications and systems.

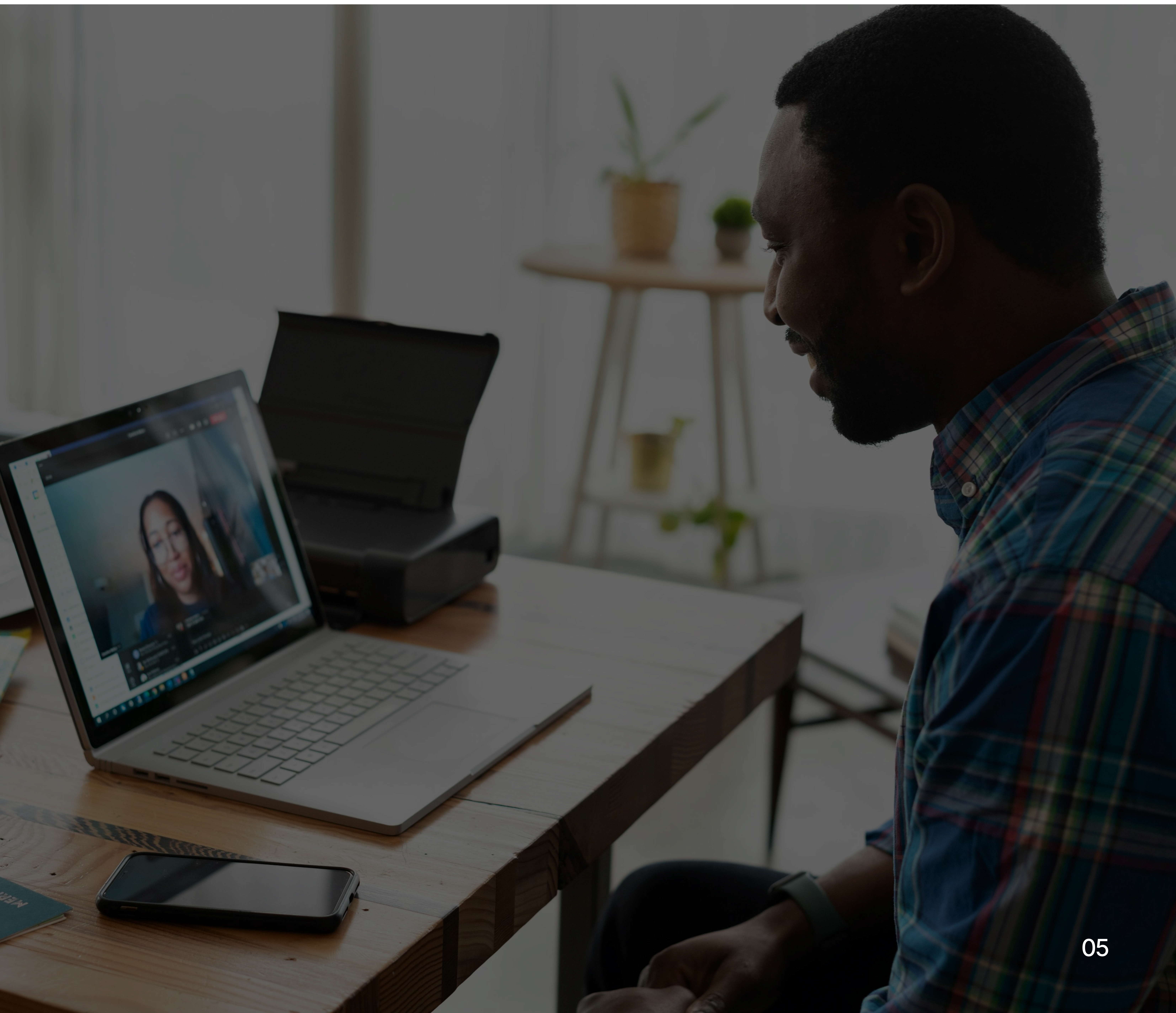
**Source: Gartner**

# Time to upgrade: Seek a replacement solution

We understand that the transition requires careful planning, but it also provides an excellent opportunity to adopt newer, more advanced tools that are in line with the demands of today's digital landscape.

When you're on the hunt for a replacement for your SFB Server, consider a communication solution that can meet legal requirements, guarantee the highest levels of data security, and boost productivity in addition to meeting the ever-evolving collaboration needs.

Take into account the following key factors that will help steer you towards an option that's best suited to your security and communication needs.



# 7 factors you should consider when seeking an **SFB Server replacement**

01

## How important are data sovereignty and the flexibility of deployment options to your business?

Data sovereignty should rank high on your list of priorities if your organization wants complete control over its data - **where it's stored, how it's sent, and who can access it**. Additionally, if your business is in a region that mandates specific data storage and handling regulations, then **data sovereignty should be a key consideration**.

The replacement solution should be flexible enough to offer **on-premise, private cloud, or air-gapped deployment**, depending on your security needs. This offers higher control of data and adapts well to **strict corporate policies**.

An air-gapped deployment acts as an extra security measure, providing isolation from unsecured networks thereby making it difficult for malicious access. This is a crucial deal-breaker if your organization requires a tight grip on their data.

But here's the catch - not all solutions make the grade. For instance, **Microsoft Teams falls short as it doesn't support on-premise deployment**. This can pose risks for organizations dealing with sensitive data or those subject to stringent data management regulations, making it not the optimal solution for every business.

So, the new SFB Server replacement should ideally offer both of these deployment choices. With this kind of flexibility, your business will be empowered to make a choice that most suitably aligns with your unique security requirements, operational needs, and regulatory compliances.



## 02

### How essential is strict information governance to your data management practices?

Highly regulated organizations, such as the government and defense, are known for dealing with highly sensitive and classified data, only a portion of which should be accessible to specific user roles. For example, high-ranking government officials will require access to economic policies or diplomatic correspondences, whereas a town clerk will need to access only local resident data on a daily basis. Similarly, in defense, a commanding officer should have access to all operational blueprints and troop data, but roles like weapons specialist or IT defense team member should remain exclusive to their respective areas.

This is where role-based access control (RBAC) comes into play. It helps by designating data access based on user roles within your organization. This ensures only the right personnel have access to specific, relevant information, which prevents unauthorized access and maintains data integrity. In case of a data breach, RBAC makes it easier to identify which roles had access to the compromised data, leading to quicker resolutions.

**Relying on a solution with predefined roles can be challenging in complex environments due to the lack of flexibility.** The roles in these sectors are often diverse and specialized, and predefined roles might not fulfill all specific tasks. This results in some assigned permissions being either too restrictive or too permissive.

Without the ability to customize user roles or permissions to fit individual needs, there may be a necessity for additional access requests or dependency on others to finish tasks — causing delays and hold-ups.

What's needed is a system that allows for **creating as many custom roles as needed** - there's simply no time for second-guessing in high-stakes environments. Enhancing such **custom roles with granular permission controls** allows specific access, enhancing both data security and role efficiency.



## 03

### Does your business require features to be tailored based on its unique needs?

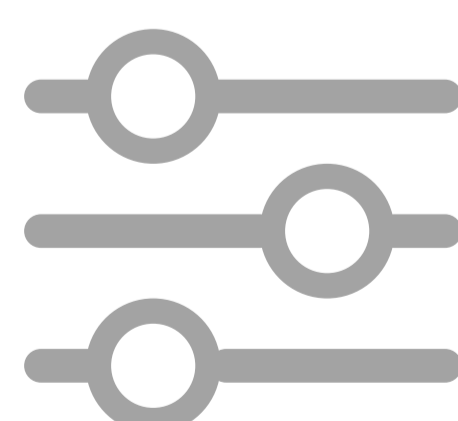
In today's challenging business landscape, a cookie-cutter approach to software solutions is no longer viable. The digital transformation, particularly in IT departments in government or defense sectors, calls for communication platforms that are **adaptive, customizable, and extendable**. Tailoring features based on unique business needs isn't just an extra perk anymore - it's an absolute necessity.

Consider the following scenario: your IT department has a critical security feature that is missing from your current communication platform. **If this platform is a proprietary solution, such as Microsoft Teams, your only option is to wait and hope that the vendor will include your requested feature in the next update(s)**. This delay can not only slow down your progress but also put your security at risk.

Conversely, if you've deployed an open-source platform, the scenario changes dramatically. In this case, your development team is empowered with ready-to-use APIs and pre-built modules, enabling them to develop and deploy the critical feature in weeks, if not days.

The essence of such platforms, particularly the ones with an MIT source license, is that they provide not just true open-source benefits but also allow autonomy over your enhancements, preventing obligatory sharing with the vendor or community.

A customizable communication platform allows your **business to evolve, expand, and adapt to new challenges or trends**, ensuring long-term sustainability. While transitioning away from SFB Server to a new solution, remember that your business is unique. It deserves an equally unique solution - a **platform that adjusts to you, not one that requires your business to adjust to it**.





# 04

## Does your organization need to partner or work with external parties such as vendors, allies, and different divisions?

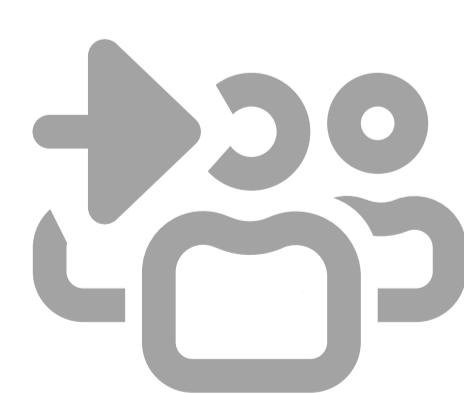
In today's ecosystem, no business operates in a vacuum; it's a web of interactions with external stakeholders – clients, partners, agencies, and so on. It's no longer just about streamlining internal communication, it's about enabling dispersed teams to **connect with collaborators and external users such as customers and citizens, without losing control over data or jeopardizing security.**

Let's imagine a defense contractor who needs to collaborate with a diverse group of parties - domestic and international military departments, private corporations, government agencies, each using different communications platforms due to their unique needs and security requirements. **The ideal tool in this scenario would be platform-agnostic**, facilitating connections with stakeholders regardless of their platform preference. This **breaks down data silos, allows for real-time information exchange, and unifies mission-critical communication.**

Or, for instance, a federal emergency management agency needing to coordinate disaster response efforts with various state/local counterparts, each operating on their own server. With Federation, the agency could **share timely, critical updates and effectively coordinate actions** while preserving the autonomy and security protocols of individual state or local agencies.

Furthermore, consider the scenario in which your organization provides a range of services to its citizens, clients, or customers. Let's say a citizen has a question about taxes. Their journey may begin with a search for answers on the government's website. If they don't find what they're looking for, they can use live chat for help. In such cases, an **omnichannel customer service platform ensures a seamless customer experience and consistent assistance at all stages.**

When looking for an SFB Server replacement, keep in mind that **you should consider not only what works best for your internal team, but also what effectively bridges the gap between you and your external collaborators and/or users.** Having a single platform for end-to-end communications not only improves efficiency, but it also reduces the cost of maintaining multiple solutions as your communication needs grow.



# 05

## How critical is end-to-end encryption (E2EE) for your classified data and sensitive conversations?

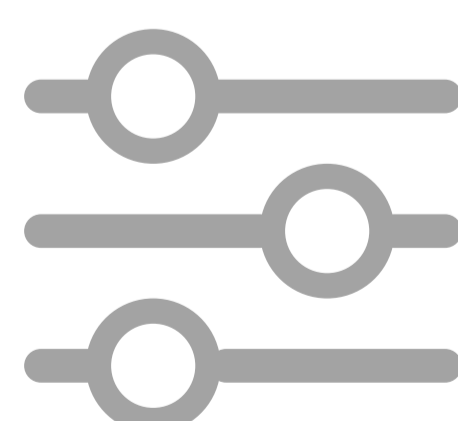
In regulated industries such as government and defense, where **classified information forms the backbone of operations**, the importance of E2EE cannot be overstated. If your business deals with sensitive data, such as national security details, military strategies, or internal policies, E2EE is not just a nice add-on; it's a necessity to **prevent unauthorized access, and data breaches**.

Without E2EE, this information can be intercepted and accessed at various points in the data transmission process, leaving it susceptible to unauthorized access and potential misuse or compromise. For instance, **if a hacker infiltrates an unencrypted communication room where strategic defense plans are discussed, the result could be a national security crisis**.

It's not just the intentional actions of attackers; sometimes, **even accidental breaches can have catastrophic implications**. A simple accidental share of confidential information in an unencrypted space can allow that information to become accessible to anyone with enough technical knowledge.

Therefore, the ability to have **fully encrypted conversations** is paramount in maintaining the confidentiality and integrity of sensitive conversations or exchanges of classified information. Also, many governments and industries have strict laws and regulations regarding the protection of data. Failure to comply with these regulations can result in severe penalties and damages to the organization's reputation.

While considering a transition from your existing communication platform, take a moment to **assess the significance of data security for your organization**. Remember, you are not just transitioning communication tools; you are transitioning the safety net for your crucial data. **Your next communication platform needs to support E2EE.**



## 06

### How well do you want to remain connected to your current SFB ecosystem?

An important factor to consider while transitioning from SFB Server is your **inclination to stay connected with your existing SFB ecosystem.**

If your business has been heavily invested in the SFB infrastructure, training, and integrations, the thought of a transition might seem daunting. It's important to take into account how much your team may be used to certain apps such as Outlook Calendar and OneDrive. Many departments would rely heavily on these apps daily. Not to mention, there's always a human factor to consider - **people grow accustomed to certain tools and change can feel overwhelming.**

However, this shouldn't preclude you from exploring other options that might offer greater advantages. Look for solutions that smoothly integrate with tools your teams use everyday. Because switching systems shouldn't mean your teams sacrifice features or apps they love and use on a daily basis.

Moving to a solution that integrates with these essential tools means everything you need is in one place. This efficient integration allows employees to **smoothly transition using their preferred tools, minimizing the learning curve, and boosting productivity.**

Many communication platforms ensure interoperability with existing systems, **providing a gradual transition rather than a jarring switch.** They can offer seamless **integration capabilities to an existing SFB ecosystem,** enabling you to leverage the new platform's benefits without completely severing ties with SFB.



# 07

## Is the Subscription Edition built to meet the future needs of my organization?

If you're in defense, government, or intelligence, you know that security, stability, and compliance are your top priorities. However, the uncertainty, high costs, and complexity that come with Subscription Edition make it a risky move. It's just not the right fit for organizations like yours that need guaranteed security, clear roadmaps, and flexibility for future needs.

The Subscription Edition operates under Microsoft's Modern Lifecycle Policy, presenting two possible scenarios: **either you'll receive a minimum of 12 months' notice before support ends, or you'll need to transition to a successor product.** Continuously adapting to new systems can strain resources and jeopardize the stability required for critical missions.

Not just that, **transitioning involves multiple steps**, including potential interim upgrades to Skype for Business Server 2019 before moving to the Subscription Edition. This process is intricate and resource-intensive, with unclear pricing and licensing terms adding to the complexity. For large-scale infrastructures, such **convoluted upgrades can lead to operational disruptions and increased costs.**

If you're working in an air-gapped environment, it's vital to maintain complete control over your infrastructure. The Subscription Edition **may introduce internet dependencies and require changes to Active Directory**, which could disrupt critical systems. These dependencies pose significant risks, **potentially exposing sensitive data to external threats and compromising mission-critical operations.**

**Our verdict:** The Skype for Business Subscription Edition may seem like a straightforward upgrade. However, for **organizations handling sensitive data, bound by strict data sovereignty mandates, or operating large-scale infrastructures that cannot accommodate frequent transitions**, this edition **may not meet your stringent requirements for security, compliance, stability, and operational continuity.**










With extended support for Sfb ending soon, **the clock is ticking.**

Waiting only increases the risks, and that's something no defense, government, or federal agency can afford. **Every decision you make now has to be strategic and secure.**

**The time to find a better alternative is NOW.**



# Choose your ideal Skype for Business Server replacement

	Skype	Teams	Cisco Webex	Element	Mattermost	Palantir	Threema	Wickr	Wire	Rocket.Chat
										
Open source license	✗	✗	✗	✓	✓	✗	✓	✓	✓	✓
Deploy on-premise or in a private cloud	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓
Air-gapped deployment	✗	✗	✓	✓	✓	✓	✗	✓	✓	✓
E2EE	✗	✗*	✓	✓	✗	✗	✓	✓	✓	✓
Custom roles and permissions	✗	✗*	✗	✗	✗	✓	✗	✗*	✗	✓
Message moderation	✗	✓	✓	✓	✗	✗	✗	✓	✓	✓
Secure guest access	✗	✗	✗	✓	✓	✗	✗	✗	✓	✓
Citizen engagement	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓
Matrix Federation	✗	✗	✓	✓	✓	✗	✗	✗	✗	✓
Cross-platform messaging with MS Teams	✗	✗	✗	✓	✗	✗	✗	✗	✗	✓
Agnostic VoIP ecosystem	✓	✓	✓	✗	✗	✗	✗	✓	✓	✓
Integration with Microsoft apps eg. Outlook, OneDrive	✓	✓	✗*	✗	✓	✗	✗	✗	✓	✓

✗\* — limited functionality; doesn't meet the required criteria.

# Goodbye Skype.

# Hello Rocket.Chat.

Rocket.Chat is a great pick to replace your Skype for Business Server. It can be deployed according to your security requirements and offers greater flexibility to adapt to your unique business needs.

## Flexible deployment options

Deploy our solutions on-premises or in a secure cloud to maintain complete control over your data. For high-stakes environments, Rocket.Chat supports air-gapped deployments, ensuring zero external network access

## Encrypted conversations

Safeguard your communications with fully encrypted private conversations. End-to-end encryption ensures that only authorized personnel can access mission-critical information, preserving confidentiality and integrity.

## Open-source advantage

Rocket.Chat is an open-source platform, granting you the highest degree of customization and control your business may need. Our pre-built Apps-Engine framework enables you to quickly and easily develop new features and apps with minimal coding to cater to your unique workflows or missions.

## Unified collaboration

Rocket.Chat partners with industry-leading platforms such as Pexip and Bluescape to provide a secure and integrated collaboration experience by bringing everything under a single roof - chats, calls, projects, people, tools, and planning boards. You can initiate a secure video call or spin up a whiteboard in real-time to unify communications.

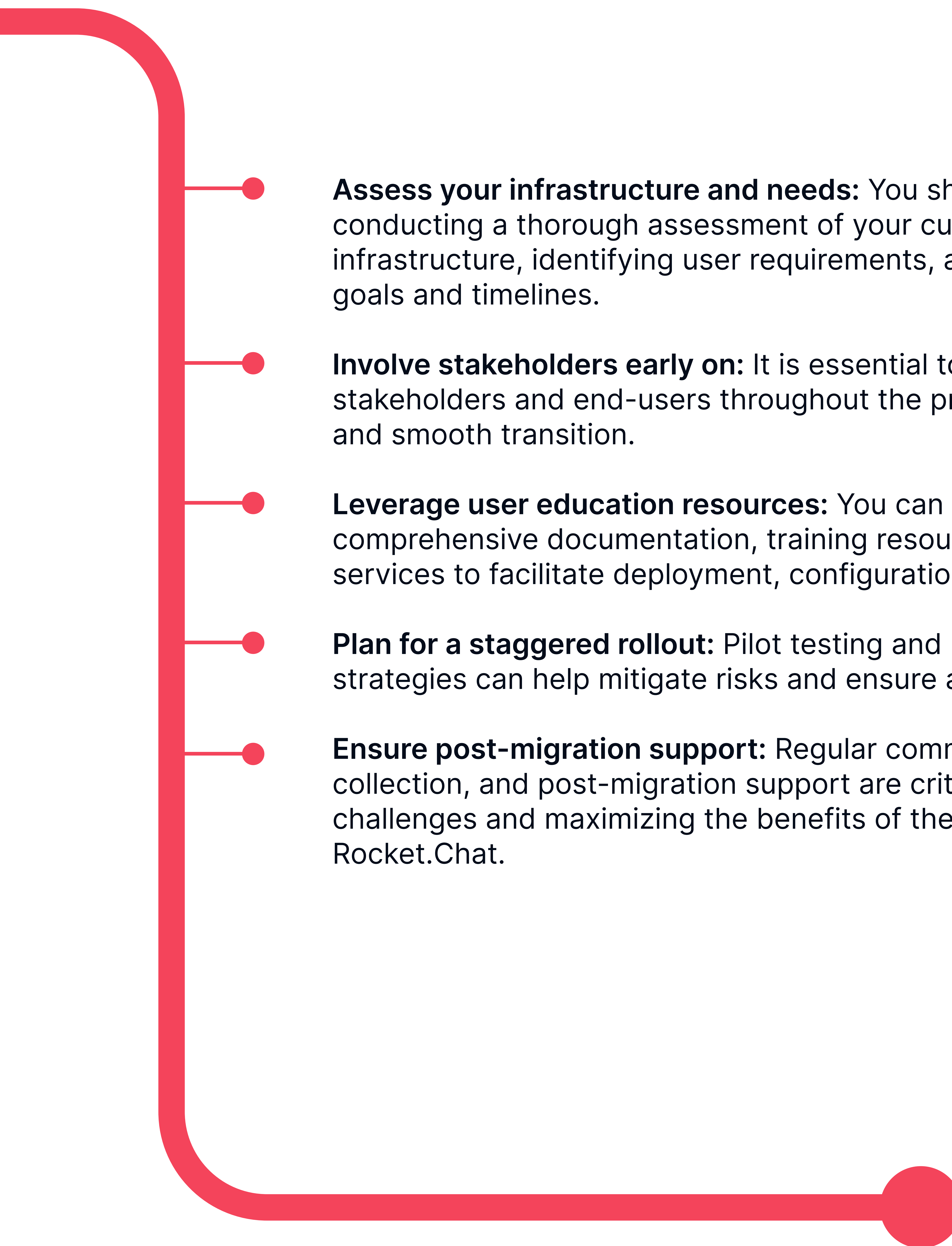
## Robust information governance

Audit every conversation and enforce data loss prevention policies to keep tabs on sensitive information shared. Restrict access to sensitive information through role-based access control, and have all conversation history available in one place to never miss important information.

## Secure cross-platform messaging

Stay connected with users on MS Teams by messaging them directly from Rocket.Chat, without having to install or juggle tools. Grant your users the flexibility to send messages from their preferred app by securely syncing users, conversations, and data across various platforms.

# We are here to help you migrate successfully and **make the most of Rocket.Chat.**



- **Assess your infrastructure and needs:** You should start by conducting a thorough assessment of your current communication infrastructure, identifying user requirements, and defining migration goals and timelines.

- **Involve stakeholders early on:** It is essential to involve key stakeholders and end-users throughout the process to ensure buy-in and smooth transition.

- **Leverage user education resources:** You can leverage Rocket.Chat's comprehensive documentation, training resources, and support services to facilitate deployment, configuration, and user onboarding.

- **Plan for a staggered rollout:** Pilot testing and phased rollout strategies can help mitigate risks and ensure a successful transition.

- **Ensure post-migration support:** Regular communication, feedback collection, and post-migration support are critical to addressing any challenges and maximizing the benefits of the migration to Rocket.Chat.

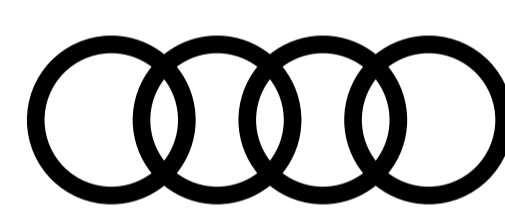
# Post-Skype era: Switch to Rocket.Chat today!

As Skype for Business Server is sunsetting, shift to Rocket.Chat for a comprehensive suite of features, unparalleled flexibility, and a commitment to security and innovation.

Empower your organization with a secure and flexible communication solution like Rocket.Chat to future-proof communication infrastructure, and drive growth and success in the digital era.

 Featured in the Secure Communications Solutions Landscape, Q3 2024 by Forrester®

Built for organizations with the **highest** security standards



Connect with our experts to discover how Rocket.Chat can streamline your transition and cater to your secure communication needs.

[Book a free consultation call](#)