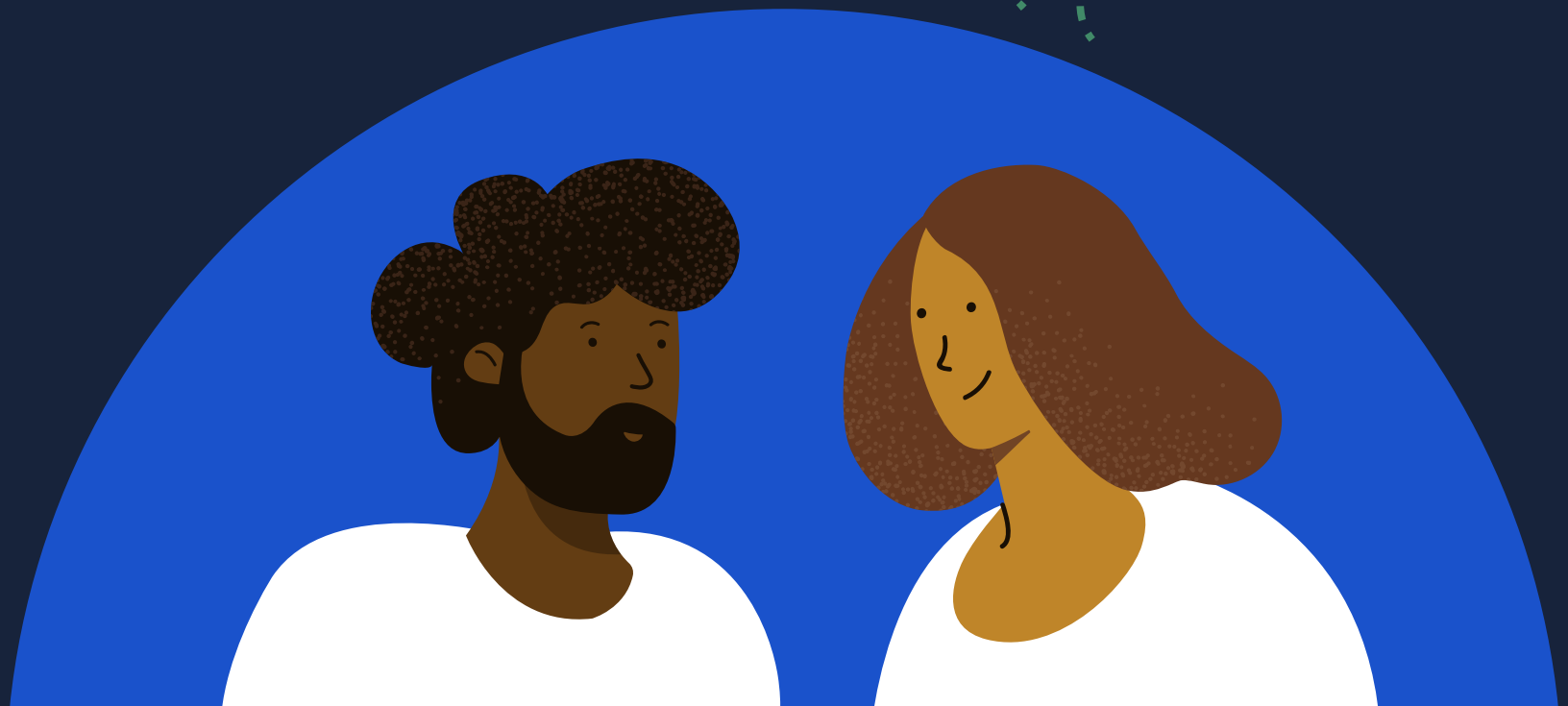
Mattermost

Out-of-Band Communication

Maintaining business continuity



Improve your collaboration strategy with out-of-band communication

These days, most organizations rely on several different secure communication mediums — like email, real-time chat, video calls, and SMS — to transmit information, collaborate, and keep teams aligned.

While modern communication tools help teams stay connected, the digital landscape is not without its challenges. For most organizations, it's only a matter of time before network disruptions, security breaches, and system failures impact main lines of communication.

To avoid communication problems, organizations in complex, mission-critical environments should use an out-of-band (OOB) communication solution alongside their regular business collaboration system. This will ensure they can still communicate even if their main line is compromised.

What is out-of-band communication?

Out-of-band communication is a method of communication that occurs outside of an organization's primary network, enabling team members to collaborate securely when main communication channels are unavailable or compromised.

Since out-of-band communication networks are not connected to everyday tools — they must exist entirely on their own — teams can use them for business continuity planning, incident response, and classified discussions.

Some of the more common out-of-band communications methods include:

- Private and public messaging channels, including audio, video, and screenshare;
- Non-company email accounts;

- File-sharing tools; and
- One-way alerting and messaging to all team members.

To bolster security, many out-of-band communication solutions — also known as backup communications systems or segmented communication channels — incorporate advanced features, like multi-factor authentication (MFA), encryption, and single sign-on (SSO), all of which must also exist outside of the organization's primary network.

While out-of-band communication is primarily considered a failover solution, some highly sensitive and classified communications may only exist across out-of-band channels.

Benefits of out-of-band communication

Organizations with strict security requirements — including technology enterprises, utility providers, financial services companies, and even military units — rely on out-of-band communication to support mission-critical work when the stakes are highest.

With that in mind, let's examine some of the primary benefits organizations experience by deploying an out-of-band communication solution.

Increase organizational resilience

By providing an independent communication channel that's separate from their primary network, organizations increase resiliency, ensuring they're able to collaborate effectively in the event they experience network congestion, outages, data breaches, or failures. This extra layer of redundancy enables organizations to stay connected and aligned during the most challenging of circumstances.

Ensure data and systems security

Out-of-band communication enhances security by creating a separate communication channel that's less vulnerable to common network threats and attacks. For example, sending security alerts and management commands via out-of-band channels are less likely to be intercepted or tampered with by malicious actors. Stakeholders could also relay sensitive business information via OOB systems, which can employ end-to-end encryption (E2EE) or self-destruction.

Improve team focus

When primary modes of communication are inaccessible or compromised, every second counts. In fact, research suggests downtime can set the average enterprise back $5 million per hour — not counting fines or other penalties. By establishing an out-of-band communications network before disaster strikes, teams can enhance their focus during crises with a dedicated channel where they can send and receive information when time matters most.

What's more, such channels can also be configured to prioritize critical messages, making it easier for teams to identify and focus on the most urgent information while minimizing distractions (e.g., non-essential messages).

Out-of-band communication: Challenges & key considerations

While the benefits of out-of-band communications speak for themselves, deploying a reliable, secure solution is not without its challenges. In this section, we examine three key considerations to keep in mind as you begin thinking about deploying an out-of-band communication channel.

1. Security and access control

If a bad actor is able to infiltrate your out-of-band communication network, it defeats the point of having one in the first place. For this reason, it's critical to ensure your out-of-band channels are secured against unauthorized access. Otherwise, they can become a point of vulnerability and compromise your entire operation.

By deploying an out-of-band solution that includes strong authentication mechanisms and robust access controls, you can prevent unauthorized individuals from eavesdropping on mission-critical communications.

2. Scalability and redundancy

Since your out-of-band channel is designed to help you navigate emergencies or share the most sensitive information, it needs to be entirely reliable and capable of handling increased demand and future growth. This is why it's so important to choose a solution that has built-in redundancy and failover mechanisms to ensure high availability, which is essential for ensuring continuity during system failures.

3. Adaptability

No two organizations are the same. As such, your out-of-band communication solution should be highly adaptable and capable of supporting unique workflows. For this reason, it's worth looking into open source solutions, which are battle-tested by an army of community researchers and are entirely customizable. Since open source platforms offer full access to source code, you'll be able to customize your system to meet your organization's compliance, security, and workflow requirements.

Out-of-band communication: Use cases

At this point, you understand the benefits and challenges of out-of-band communications. Now, let's take a look at some of the real-world ways organizations might use out-of-band channels to navigate emergencies.

1. Business continuity

Recently a global media company experienced a catastrophic outage that knocked out their engineering division's infrastructure and primary communications channels. Due to massive scale, the company was losing $100,000 of revenue every minute their systems were down.

Luckily, the organization had deployed an OOB solution. As a result, engineers were able to stay in touch with colleagues around the world, working quickly to remediate the outage and bring their network back online. With a backup communications system in place, the team could communicate at scale while ensuring sensitive data was protected, working together to rapidly respond to the incident and resolve it.

2. Incident response

Cybersecurity incidents — like data breaches and network compromises — require rapid response to mitigate damage and prevent hefty financial losses. In fact, according to IBM, the average organization is on the hook for $4.45 million for each breach.

When breaches occur, time is of the essence. Having an out-of-band communications solution provides an extra layer of security and reliability that incident response teams can use in the event a cyberattack takes down their main lines of communication. As a result, they can exchange critical information, coordinate actions, and make decisions uninterrupted.

Out-of-band channels are particularly valuable when it comes to confirming incident alerts, sharing real-time threat intelligence, and executing response plans during emergencies. Whether the primary network is under attack or the incident response team simply needs a highly secure, isolated channel to remediate critical issues, an OOB channel is a lifesaver when every second counts.

3. Sensitive or classified discussion

Within global security-focused organizations, various teams — including high-ranking officers, intelligence units, and strategic planners — need to collaborate and discuss sensitive or classified information. Of course, maintaining the confidentiality and security of these discussions is paramount to safety and mission success.

In military settings, classified discussions involve sensitive information that, if compromised, could have severe consequences on national security. In enterprise settings, such discussions involve trade secrets and intellectual property that need to be kept secret to maintain competitive advantage. Since regular communication channels can be susceptible to interception or cyber threats, teams in either scenario need an out-of-band channel they can use to share the most sensitive information.

By deploying an out-of-band solution, organizations can provide a level of security that is essential for discussing sensitive and classified information, in turn safeguarding company secrets or national security. Plus, leadership can collaborate and make critical decisions in a secure environment, making success that much easier to achieve.

How to implement an out-of-band communication channel

To ensure success with your out-of-band communication investments, you need to define your purpose up front. What use cases are you anticipating needing an out-of-band channel for?

After you've determined your requirements:

- **Select out-of-band technology.** Choose the technology that best suits your needs, with dedicated networks, separate communication channels, and specialized hardware
- **Implement access controls.** Configure access control policies to ensure only authorized users and systems can access out-of-band channels. Implement strong access controls, like MFA, to keep bad actors at bay.
- **Ensure redundancy and failover.** Since your out-of-band channel is more or less worthless if it's not operational when you need it, you need to implement redundancy and failover mechanisms to ensure it's always accessible — even in the event of hardware failures and network issues.
- **Test the solution.** After you've configured the solution, test it according to your defined requirements, including network settings, protocols, and security parameters. Try to mimic a real-world scenario you might encounter and make sure the solution functions as expected.
- **Document your processes and train your team.** Once you're happy with the setup, document out-of-band processes, including channel configurations, so that relevant stakeholders can reference them as needed. While you're at it, provide training to staff responsible for using and managing the out-of-band channel. Incorporating your OOB channel into regular incident response and security exercises ensures that your team is familiar with the technology and how to use it before it's needed.

Getting started with out-of-band communication with Mattermost

Mattermost helps organizations accelerate mission-critical work, even in the most complex environments, by allowing them to collaborate effectively and securely.

A familiar interface for focused collaboration

Mattermost's fast, familiar interface, collaborative playbooks, and customizable integrations give your team a shared workspace to stay focused when minutes count, whether they use Mattermost for daily collaboration or emergency communication.

Adapts to any workflow

Out-of-band communications may still rely on data from other tools in your workflow. Connect with in-house and SaaS-based tools with webhooks, plugins, API access, and source code access to customize Mattermost to fit your team's needs precisely.

Security-first deployment options

Maintain data control with a resilient collaboration hub that offers the ability to deploy to any public or private cloud, including air-gapped networks. Conform to your organization's compliance and security standards without sacrificing usability.

Download Mattermost to get started now.

About Mattermost

Mattermost is a leader in secure collaboration for mission-critical work in complex environments. The Mattermost platform enables enterprise, defense, and governmental organizations to increase speed, efficiency, and resilience in vital operations while meeting nation-state-level security and compliance requirements. The company offers self-sovereign open source and enterprise products, as well as managed cloud services. For more information visit mattermost.com.