SSH

Secure Business Communications Guide

White paper

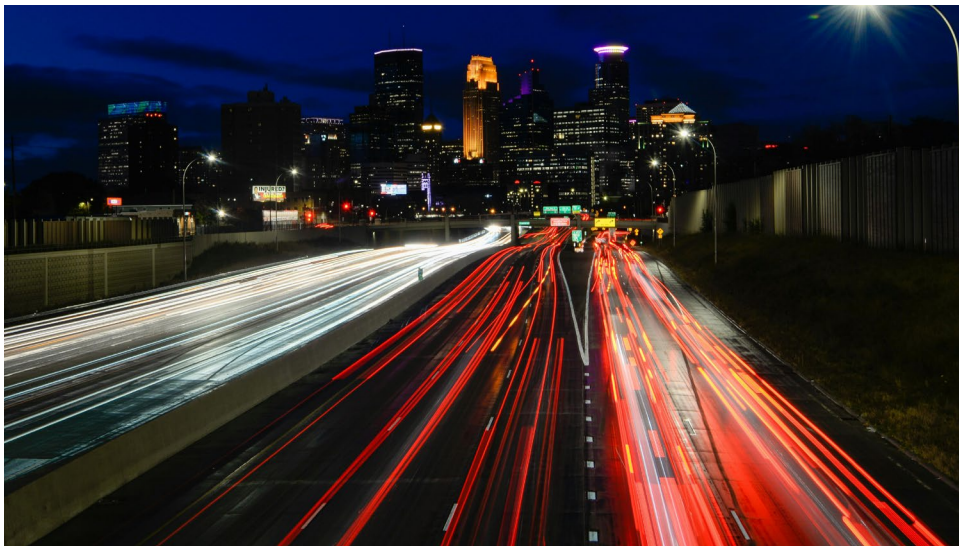
Index

SSH

Introduction – More channels are used for sensitive communications

The importance of secure business communications cannot be overestimated. The use of digital communications in business is pervasive, with the most obvious example being email. But as remote and hybrid working surges and business environments become increasingly digital, the range of enterprise digital communications tools has expanded to include chats, video conferencing, collaboration rooms, and file sharing.

Despite growing awareness of the importance of cybersecurity, awareness does not necessarily amount to the effective implementation of sensitive data protection cybersecurity measures. Not all data is created equal. Sensitive data requires more robust protection. Also, the number of individuals who can see and modify sensitive data or receive certain type of communications should be categorized appropriately in a limiting fashion.



There's more. Heavily regulated businesses have been fined by US authorities for neglecting record-keeping requirements for a tidy sum of 2 billion dollars in last year alone.

Authorities in many countries, like Sweden, are placing more emphasis on having the option to have full control over the data they handle to fulfil data sovereignty requirements. This means that they want to deploy secure communications channels in their self-hosted, often on-premises environments, at least for particularly sensitive data.

This whitepaper will address the importance of secure business communications, what is required to ensure that your business data is sufficiently protected, and why breaches continue to occur despite the many advanced cybersecurity tools available to businesses.

Examples of sensitive data

Business communications data might include, but is not limited to, the following:

- **Financial information**
- **User credentials and/or passwords**
- **Service requests**
- **Marketing strategies**
- **Pricing information**
- **HR data**
- **Confidential project files**

"Business communications data" may also refer to client data being handled or stored by the enterprise, such as credit card details and personal information.

Levels of data classification

There are three stages to effective and comprehensive data protection.

1 Determine the data's level of importance

The first stage is known as data classification. The purpose of data classification is to uphold, preserve, and reliably enforce data sensitivity and confidentiality. Effective data classification enables you to organize and understand critical enterprise data, which helps inform decisions about what level of security is appropriate for your business communications data.

Appropriate data classification will help you differentiate between non-sensitive communications and business-critical information – like contracts and financial data, or public, restricted, confidential, or secret. Data of this nature should be protected with appropriate security measures, such as end-to-end encryption, to eliminate the risk of exposure when the data is transmitted and stored.

2 Establish appropriate policies

The second stage involves selecting the appropriate tools, and devising policies, to ensure that the level of protection determined by the data classification process is being met.

For instance, while standard tools like Outlook or SharePoint may suffice for common communications, confidential communications will require more robust security measures. This might include the ability to store data in an encrypted format, rather than plain text, which ensures that the data is not readable to an intruder if unauthorized access occurs.

Your policies might require that all employees are trained in the use of these specialist tools and are using them consistently.

3 Enforce policies

It could be argued that the second stage of data protection — devising policy — is easier than enforcing it. In small and large organizations alike, ensuring complete compliance with data protection policies is a considerable challenge, particularly given that it only takes one case of human error for a breach to occur.

To reliably enforce data protection policies in your organization, you must ensure that all employees are aware of the dangers associated with poor data protection, their own personal responsibility, and what is expected of them on a day-to-day basis.

What makes a solution fit for enterprise-grade secure communications?

A security-first secure collaboration solution needs to fulfil certain requirements to meet the demands of highly regulated organizations.

1 Air-gapped communications

Air-gapped communication channels mean high security networks that are physically separated from other networks and systems. These channels are useful in highly sensitive communications, e.g. when sharing diplomatic correspondence, military or government secrets, stock exchange information, or discussing nuclear power plant controls.

For these channels to be super secure and fulfill data sovereignty requirements, they need to run on company hosted, often on-premises, servers.

2 End-to-end encryption

True end-to-end encryption means that not even the technology vendor can see the content of the communications or any trace of it. For that to happen, only the sender and receiver have access to the data. The participants need to have an easy way to exchange private encryption keys prior to initiating secure collaboration, and the data needs to be encrypted at both endpoints and all the way from server to server when in transit.

3 Securing innovations

An often-neglected part of secure communications is sharing development ideas of a company's flagship products or company IP. There are numerous cases where a product source code has leaked because of a compromise, and yet in many companies, developers and product owners still discuss IP source code or IP-related development ideas using regular business tools like Teams or Slack.

SSH

4 Securing sensitive video and voice calls

This might seem like an obvious point, but we believe it requires special emphasis. Even military secrets are being discussed using everyday video or conferencing tools, as was the case in German military. These discussions should happen via solutions that align with the company's data classification policies with security features that ensure the confidentiality of those conversations.

5 Auditing

Regulated industries and public organizations have an obligation to produce evidence of certain types of conversations, like the already mentioned discussions about stock exchange trades, patient treatment, evidence in criminal investigations, etc. A proper secure communications solution needs to enable an audit trail of discussions for the company to meet record-keeping requirements.

6 Out-of-band communications

Out-of-band communication allows teams to communicate securely when main communication channels are unavailable or compromised, e.g. due to a technical failure or a breach. These channels are separate from the organization's primary communications environment.

For these channels to maintain their availability, they need to be completely isolated from the rest of the server infrastructure.

7 Robust security out-of-the box

Bridging to other chat networks such as Teams, Slack, or Discord is an easy way to invite external users to a more secure channel. If your company or team uses multiple different chat networks, being able to consolidate everything in one place can be a significant benefit.

8 Consolidation of channels

Email and instant messaging are typically considered to be separate channels but some solutions on the market take things a step further. SalaX Secure Messaging is part of SalaX Secure Collaboration to complete your channels for sharing confidential, restricted, or secret information.

SalaX Secure Messaging – Your channel for restricted, confidential, or secret communications

SalaX Secure Messaging is a super secure application for real-time communications over end-to-end encrypted chats, and audio and video calls. Build your own authorized channels for compliance and record-keeping.

Real-time secure collaboration

Communicate within and outside your organization in real time over chat as well as audio and video calls.

Invite and connect with third-party organizations, regardless of the communication tool(s) they use. Keep your sensitive data secure even when communicating externally.

Secure by default

Protect your communications with end-to-end encryption (based on Olm and Megolm encryption protocols).

Full control over your data

SalaX Secure Messaging can be flexibly deployed in the cloud or on-premises, depending on your organization's data sovereignty needs and industry regulations.

Using a self-hosted server, you maintain full control over all messages, calls, and shared files.

Verify, audit, comply

Identify sender/recipient. Ensure maximum security with full audit trails and various reporting options. Gain control over the encryption keys used in communications.

Integrate with ticketing and project management tools

SalaX Secure Messaging integrates with tools and platforms like Jira and GitLab to keep your project management and service request management discussions always up-to-date. Tickets can be automatically sent to a secure channel for the team to discuss discuss and handle.

Connect with Other Organizations

SalaX Secure Messaging allows you to connect with other organizations seamlessly for super secure communications.

User-friendly experience

SalaX Secure Messaging looks, feels, and works like any other messaging app. No extensive training for users is needed.

We'd love to hear from you!

Get in touch with our experts around the world.

GLOBAL HEADQUARTERS

Helsinki

SSH Communications Security Oyj
Karvaamokuja 2B, Suite 600
00380 Helsinki
Finland
Tel. +358 20 500 7000
info.fi@ssh.com

US HEADQUARTERS

New York City

SSH Communications Security Inc.
66 Hudson Blvd E, Suite 2308
New York, NY, 10001
USA
Tel: +1 (212) 319 3191
info.us@ssh.com

APAC HEADQUARTERS

Singapore

SSH CommSec Pte. Ltd.
6 Raffles Boulevard, Marina Square, #03-308
Singapore 039594
Singapore
Tel. +65 6338 7160
sales.asia@ssh.com

Let’s get to know each other

Want to find out more about how we safeguard mission-critical access for leading organizations around the world?

We’d love to hear from you.

CONTACT US