SSH

Bolting a critical security layer onto Microsoft 365 for sensitive communications

White paper

Index

Introduction: Beyond everyday tools for sensitive business communication

Layered security has been a common practice in IT for some time already. It simply means that the more critical the data or a target to access is, the more robust the security controls need to be.

This hasn't been the case in business communications. Organizations are still sharing sensitive data or discussing business-critical topics using everyday business tools. Examples of such information include:

- Trade secrets
- Medical records
- Pharmeceutical data
- IPR
- Acquisition projects

But things are changing. For example, US authorities have woken up to this oversight. Wall Street companies have been fined for over 1,8B dollars for using unauthorized, off-channel communications (like WhatsApp) when discussing trade secrets.

The message from the authorities is clear: everyday business tools are not acceptable forms of communication when sensitive data or topics are being discussed or shared.

Companies can do a lot by configuring their existing tools, like Outlook, to work with the added security features of Microsoft Purview that helps companies govern and secure data across their entire data estate.

Even though the Microsoft toolset provides a lot of value, there are some areas where it could use a serious security boost.

In this white paper, we'll discuss how to secure your sensitive business communications: 1) by keeping your Microsoft 365 setup and adding an extra layer of security as a bolt-on and 2) isolating your business communications from Microsoft 365 for complete data sovereignty.

We will compare features available from Microsoft Purview with those available in our solution: SSH Secure Collaboration 2024. The solution is a collection of applications that enables secure sharing, instant messaging, video conferencing, signing and storing of sensitive data with internal and external stakeholders.

What is Microsoft 365 security great for?

Microsoft 365 refers to an entire suite of applications and services, including communication services like Microsoft Teams and Outlook.

All the applications and services utilize Microsoft Purview as a centralized, overarching solution aimed at maintaining security compliance and mitigating risk factors. For Office 365 users specifically, Microsoft Purview encrypts email exchanges and identifies confidential information through Azure Information Protection (AIP).

What do both Microsoft 365 and Secure Collaboration do well?

Encryption: This makes your messages unreadable to anyone except the intended recipient. If someone were to intercept the message, they still can't read it.

Verifying identity: Both solutions can verify the identity of the recipient before opening the email, adding an extra layer of security much needed for sensitive communications.

Action restrictions: Prevent recipients from forwarding, copying, or printing your emails, granting you extended control over sensitive information even after it has left from your inbox.

Multi-platform support: Send secure emails using platforms like Yahoo!, Gmail, and other email services. Recipients of these encrypted emails, irrespective of their email client, can view these messages without any additional steps, providing a seamless user experience.

There's a reason why both Microsoft 365 and Secure Collaboration are widely used: they user-friendly, offers a familiar interface, and utilizes an integrative cloud environment that facilitates easy data retrieval, editing, and sharing.

But Secure Collaboration takes takes sending and receiving confidential, restricted and secret communications to another level. Let's dive in.

Why is Secure Collaboration 2024 a vital Microsoft 365 bolt-on for sensitive communications?

Microsoft 365 is a great and established solution for everyday business communication. It easliy covers up to 199/200 of use cases inside an organization.

Secure Collaboration is the solution your ogranization needs for high-impact cases: when sensitive information that simply can't leak is shared and needs to be tracked, identified and audited for full compliance. The solution purpose-built for sharing confidential, restricted and secret information. All the robust security features you need to separately configure for Microsoft Outlook users are on by default in Secure Collaboration - and then some.

The idea of having an isolated, secure and authorized channel for sensitive or business-critical communications is built-in into Secure Collaboration. With the solution, your organization gets an authorized, official channel to discuss, share and collaborate on sensitive and business critical topics. With it, you move from off-channel communications to authorized ones and pass audits and any other internal or external scrutiny with flying colors.

Benefits

Inbound emails with strong authentication

Allow verified-only external stakeholders to send a confidential email to you directly from a web browser without them having to configure anything for sending.

Handle gigabytes of data in sensitive communications

Regular email services allow sending attachment with up to 30Mb of data. With our solution, the limit is measured in gigabytes. Serious business needs serious bandwith.

Control your data for full data sovereignty

Secure Collaboration 2024 comes with flexible deployment options, including cloud, SaaS and on-premises. The on-premises option gives you the full control over you data, since you can host the service in your own isolated environment that doesn't leave any trail of activity on third-party servers.

Take control over your encryption keys

When building secure channels using the Microsoft ecosystem, they control the encryption keys. Secure Collaboration gives you the power to control even your own encryption keys.

Multiple ways to authenticate

Give your internal and external stakeholder the flexibility to choose from various autentication methods, that include MFA, PIN, SSO, and bank IDs. Some authorities are prohibited by law from sending regular emails.

Strong encryption AES 256 and an audit trail of activities

In Secure Collaboration 2024, the default setting is to awlays have the strongest encryption available on. With the solution, you get a solid audit trail of activites and evidence of sending and receiving communications.

Outbound emails for multiple platforms

Secure Collaboration is also great for sending encrypted emails to any recipient or any email provider, regardless of the platform without the recipient having to have set up their own solution.

Great professional support

24/7 support is available if your team needs help.

Trusted by authorities for sensitive communications

A host of authorities have chosen Secure Collaboration 2024 to fulfill their security, compliance and regulatory needs. It is built by a security-first company that designs their services with regulations like, NIS2, DORA, PCI-DCC in mind.

Restrictions as per confidentiality level

Protecting sensitive information within your organization is possible with flexible classification options within Secure Collaboration 2024 policies to limit excessive data sharing and access. Micro-segmentation capabilities are available to verify users at every security zone.

Securing business communica-tions with Microsoft 365

Use case: Registration and configuration free method for customers to receive sensitive information securely

A B2C organization, such as a bank, is helping a customer set up an account. They send over a confirmation email, but the customer is unable to view it without registering for a Microsoft account. The customer doesn't want to register for a Microsoft account and contacts the organization for alternative ways to complete the process. The abandoned email is not encrypted, providing an open door into this exchange.

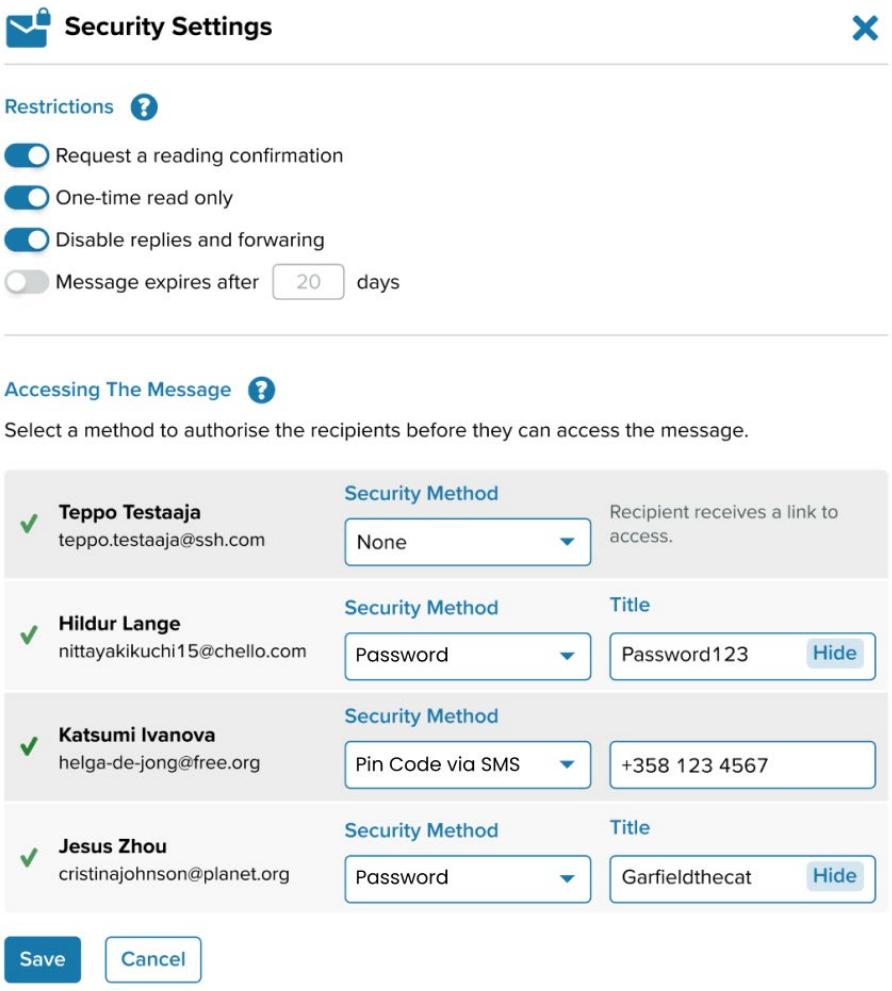
Solution

A lack of interoperability and navigational ease leads to delays in the process, reduced efficiency, and poor customer satisfaction. With Secure Mail, businesses using Microsoft 365 can safely send encrypted and readable emails to external recipients, and vice versa, without parties

SSH

needing to install any software. Upon receiving an email, multi-factor authentication (MFA) and pin codes can be deployed to confirm the recipient's identity. A highly adaptable tool, Secure Mail seamlessly integrates into existing email applications for painless onboarding.

An example security setup of Secure Mail and various authentication methods, like password or PIN code.



Securing business communications without Microsoft 365

Use case: Secure email accounts without using the Microsoft ecosystem

A healthcare organization is sending emails to their external stakeholders without linking their services to Microsoft at all. They have a web portal through which the email is sent to the recipient in a straightforward fashion without hosting any data on services in public cloud.

Solution

With Secure Collaboration 2024, you can build an independent and super secure transmission channel that is protected from large-scale attacks which are typically targeted at cloud servers and services. Your organization is in complete control over your data, since the service is hosted by you on servers that you own and maintain.

An additional benefit is that Secure Collaboration 2024 is extremely hard to breach since it is not available in a publicly hosted service but in a secure environment that is controlled by the organization.

Use case: Tailored security controls and infrastructure under control

A government branch needs to send and receive diplomatic correspondence regularly and need to customize the security policies more than available in the Microsoft ecosystem. Moreover, they are not keen on the idea of sending secret correspondence over public infrastructure and want to move to a security-first model.

Solution

With Secure Collaboration 2024, the organization can build an infrastructure that complies with their internal requirements without them being dependent on an external service. They can still use expert help from SSH Communications Security to tweak their environment to fit their needs.

The organization can also ensure compliance and demonstrate how the correspondence travels sender-to-recipient and have a solid audit trail of all activities. They also have complete control over their data in a highly restricted environment that they control for full data sovereignty.

A closer look: Secure Collaboration 2024 by SSH Communications Security

Sending and receiving unprotected emails is akin to leaving your mailbox wide open for neighbors to rifle through. Don't let your valuable and confidential emails slip into the wrong hands. Secure Collaboration 2024 keeps all shared data safe, giving you the tools that you need to comprehensively manage and monitor all email correspondence, while saving you time and money.

Applications for Secure Collaboration 2024

All organizations can benefit from supplementing their Microsoft 365 email solution with Secure Collaboration 2024 or completely replacing their Microsoft 365 setup in sensitive communications for full data sovereignty. But what does this look like in practice, and across different industries?

Here are several common use cases:

- All heavily regulated institutions can avoid hefty fines from authorities by building authorized channels for customer-facing and internal sensitive communications.
- Financial institutions can relay internal business information and private customer data without the risk of unwanted intruders exploiting sensitive documents.
- Legal offices can quickly and safely send time-sensitive documentation to all respective parties without violating confidentiality.
- Public sector and governmental offices can securely share highly confidential and restricted information via email without the risk of falling victim of an email-based cyberattack.
- Customers can easily contact and exchange private information with businesses they trust with the email resources they already have.
- Large file attachments can be relayed to intended recipients without formatting or downloading errors that disrupt communication.
- Marketing agencies, technology companies, and creative entities can keep classified project information and details secret as they exchange ideas and progress throughout their lifecycle.

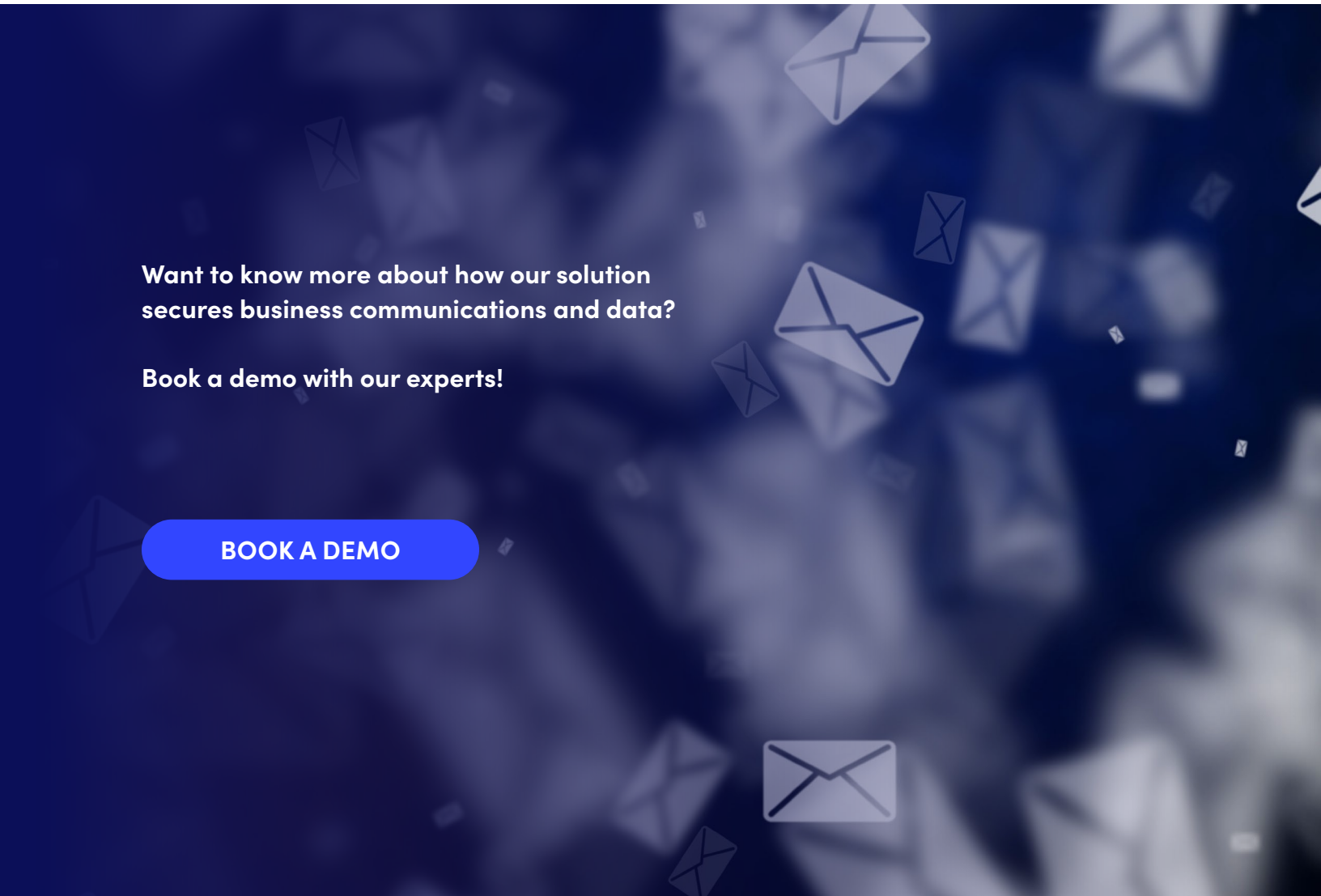
With Secure Email, data sharing has never been safer or easier!

Address all email security pain points with SSH

Microsoft 365 and Microsoft Purview are great tools for businesses wanting a secure way to exchange data while remaining productive, but they have limitations. With business communications tools being a popular medium for hackers and authorities putting more emphasis on compliance it's crucial that you sufficiently protect this communication channel.

Secure Collaboration 2024 upgrades your cybersecurity arsenal while enhancing the user experience for better integration, better efficiency, and better protection.

Learn more about Secure Collaboration 2024 >>>



Want to know more about how our solution secures business communications and data?

Book a demo with our experts!

BOOK A DEMO

We'd love to hear from you!

Get in touch with our experts around the world.

GLOBAL HEADQUARTERS

Helsinki

SSH COMMUNICATIONS
SECURITY CORPORATION
Karvaamokuja 2b, Suite 600
FI-00380 Helsinki
Finland
+358 20 500 7000
info.fi@ssh.com

US HEADQUARTERS

New York City

SSH COMMUNICATIONS
SECURITY, INC.
434 W 33rd Street, Suite 842
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

SSH