WITWAY CORPORATION

AI changed everything. A new approach is required to fight email phishing, impersonation, thread hijacking, and deepfake attacks.

Our solution provides robust sender identity assurance to protect organizations from phishing, thread hijacking, email impersonation, and AI-generated deepfake attacks in virtual meetings, ensuring secure communication without disruption.

Key offerings include **Verify Sender, Verified Meeting** for Microsoft Teams, **ReplyGuard**, and **Conditional Sharing Mode**.

1. What is **Verify Sender**?

Answer:

Verify Sender is a security feature that ensures the legitimacy of email and meeting invite senders. It utilizes advanced authentication methods, such as passkeys and digital signatures, to verify the identity of the sender before the message reaches your inbox. This verification process helps protect you from phishing attacks, email spoofing, and impersonation attempts by malicious actors.

Problem it Solves:

- **Phishing and Spoofing Prevention**: By confirming the sender's identity, it reduces the risk of falling victim to deceptive emails designed to steal sensitive information or spread malware.
- **Impersonation Protection**: Ensures that the communication you receive is genuinely from the claimed sender, maintaining trust and security in your digital correspondence.

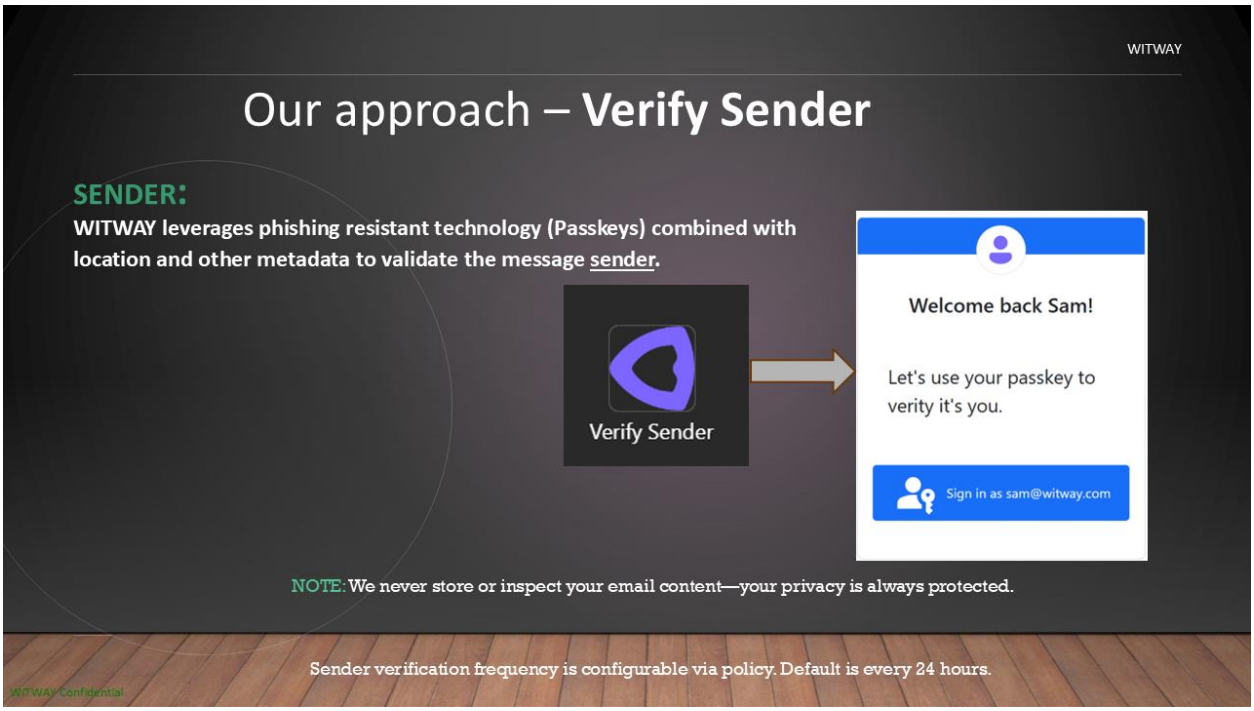

Figure 1: Verify Sender: Email sender experience. Sender verification frequency is 24 hours by default and is configurable.

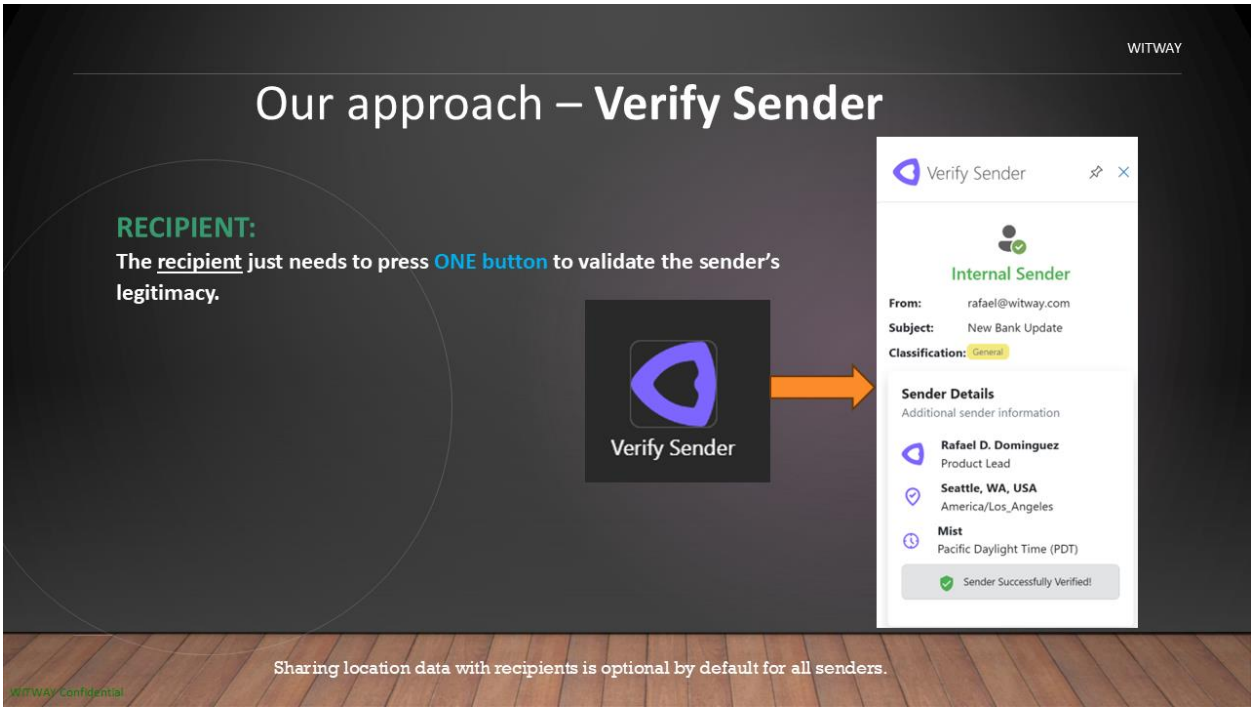

Figure 2: Verify Sender: Email recipient experience. Only the sender is verified.

2. What is **Verified Meeting** for Microsoft Teams?

Answer:

Verified Meeting for Microsoft Teams is a feature that enhances the security of your virtual meetings by verifying the identities of all participants. It employs robust authentication techniques to confirm that attendees are who they claim to be, effectively preventing unauthorized access and safeguarding against impersonation through deepfake technology.

Problem it Solves:

- **Deepfake Attack Prevention**: By verifying participant identities, it blocks malicious actors from using deepfake audio or video to impersonate others during meetings.
- **Unauthorized Access Control**: Ensures that only authenticated individuals can join the meeting, protecting sensitive discussions from eavesdropping or disruption.

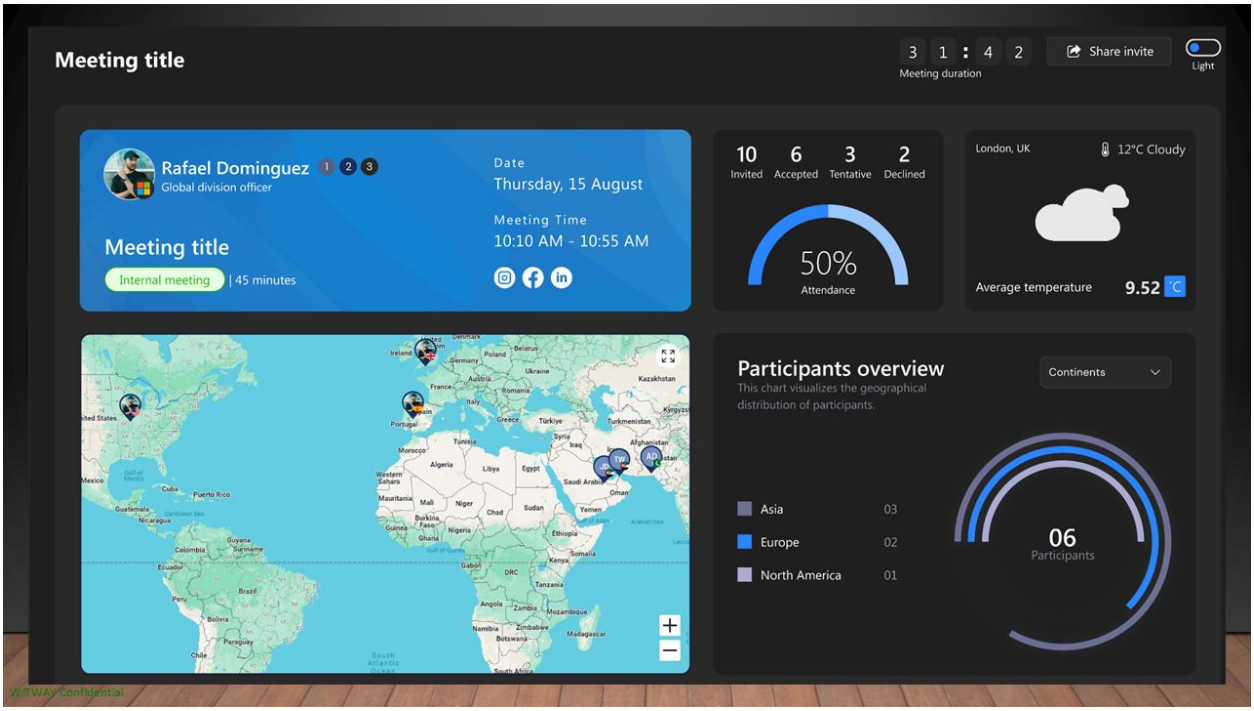

Figure 3: Verified Meeting for Microsoft Teams: Prompts each participant to share their location when they join. Can require an organizer to use Passkeys to verify their identity when they join. Participants can see host verification status.

3. What is **ReplyGuard**?

Answer:

ReplyGuard is a feature designed to prevent thread hijacking in email communications. It monitors ongoing email threads for any unusual activity or unauthorized attempts to insert malicious content. By validating each participant in the conversation, ReplyGuard maintains the integrity of your email threads and protects against potential security breaches.

Problem it Solves:

- **Thread Hijacking Prevention**: Stops attackers from infiltrating email conversations to send fraudulent messages or phishing links under the guise of a trusted participant.

- **Communication Integrity**: Keeps your email exchanges secure by ensuring that all replies are from verified sources, reducing the risk of information leakage or malware infection.

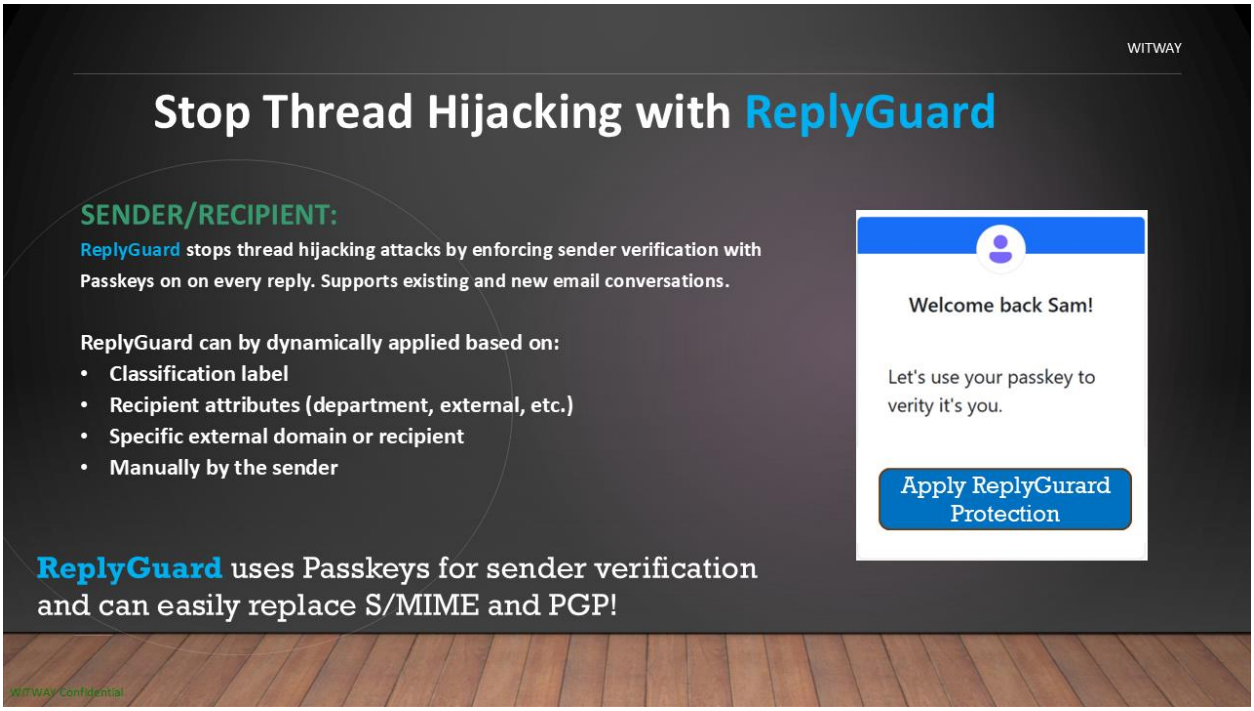

Figure 4: ReplyGuard: Applies to any sender based on policy (sender or recipient department, domain, email, classification label, etc.)

4. What is Conditional Sharing Mode?

Answer:

Conditional Sharing Mode is a security feature specifically designed for content sharing during online meetings in Microsoft Teams. It ensures that any content you share—such as presentations or documents — is visible only to authorized or verified participants in the meeting. By implementing strict access controls, it prevents unauthorized individuals from viewing sensitive information, even if they somehow gain access to the meeting link.

Problem it Solves:

- **Unauthorized Access Prevention:** Protects shared content from being accessed or viewed by unverified or unauthorized participants during online meetings.
- **Data Leakage Reduction:** Minimizes the risk of confidential information being exposed to unintended audiences during virtual presentations or collaborations.
- **Enhanced Meeting Security:** Adds an extra layer of security to your Microsoft Teams meetings by ensuring that only intended participants can view shared content.

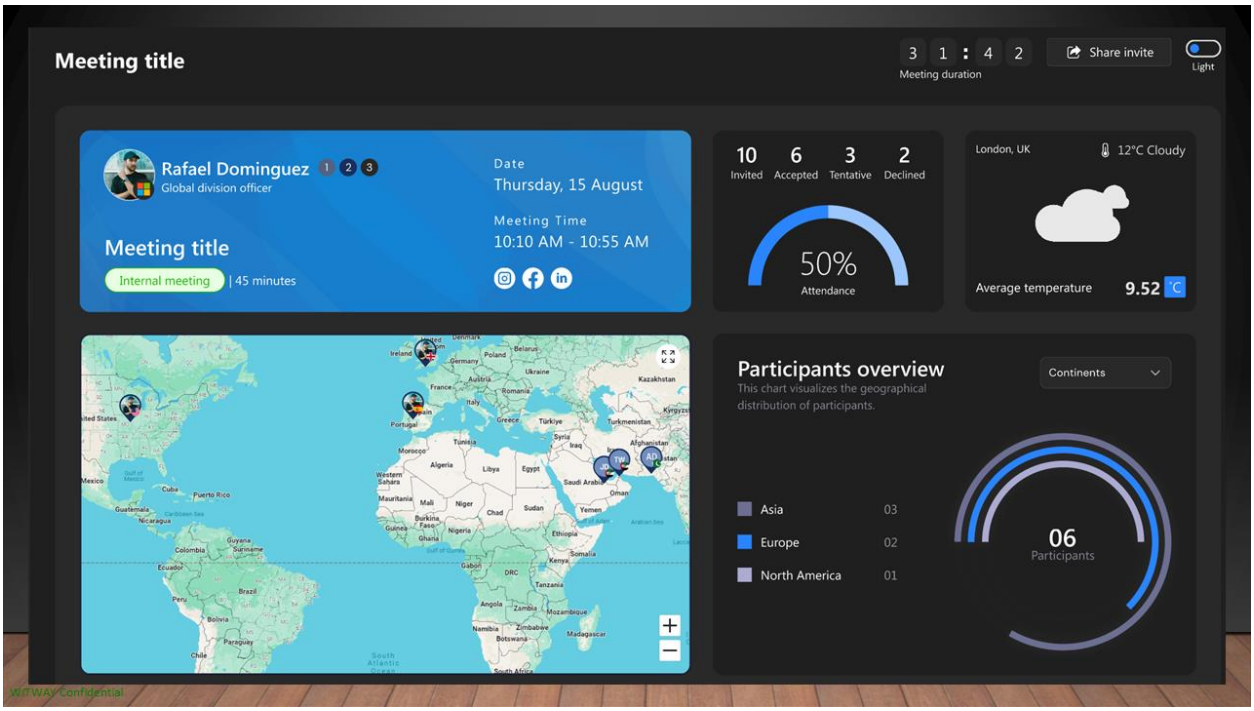

Figure 5: Verified Meeting: Only content shared through this application can be restricted from view by non-authorized participants.

WITWAY CORPORATION

7901 4th St N STE 300

St Petersburg, FL 33702

support@witway.com