Email ENCRYPTION scenarios

1. Standard email from an Office 365 user to a Gmail user

   - User at company A clicks "send" on an email message via Office 365.
   - Message passes to the corporate firewall where it is sent via an SSL or TLS encrypted channel to Office 365.
   - Office 365 decrypts, processes, and forwards the message via an SSL or TLS encrypted channel to Gmail.
   - Gmail decrypts and processes the message.
   - Gmail sends the message via an SSL or TLS encrypted channel to company B’s corporate firewall, which forwards it to the intended recipient.

2. End-to-end enterprise email encryption

   - User at company A clicks "send" on an email message.
   - The message is encrypted.
   - The message passes through the sender’s corporate firewall.
   - The path of the message takes multiple hops around the Internet with only the metadata showing.
   - The message passes through the recipient’s corporate firewall.
   - The message is decrypted and forwarded to the recipient.

3. Cloud-based end-to-end encryption

   - User at company A sends a message, which is encrypted on client device.
   - The message is sent to a cloud-based email encryption provider.
   - The encrypted message is sent to the recipient’s account with the same provider.
   - The message passes through company A’s corporate firewall.
   - The encrypted message is sent to the cloud vendor.
   - The message is decrypted by a vendor such as Docusign.
   - The recipient at company B reads the decrypted message on a secure website.

4. End-to-end encryption with delivery to the public

   - User at company A sends a message, which is encrypted on client device.
   - The message passes through company A’s corporate firewall.
   - The encrypted message is sent to the cloud vendor.
   - The recipient at company B receives the encrypted message on a secure website.
   - The recipient at company B reads the decrypted message on a secure website.