

Email Compromise Protection with Document GPS

Business Email Compromise (BEC) is one of the most financially damaging cyber threats, often resulting in leaked sensitive data, fraudulent transactions, and unauthorized access to confidential documents. Traditional email systems allow files to be downloaded, forwarded, or stolen the moment they're sent, giving attackers instant access if an inbox is compromised.

Email compromise can result in:

-  Unprotected file attachments that can be opened by anyone with inbox access
-  Phishing attacks leading to unauthorized document access
-  Loss of control once a file is sent or forwarded
-  Lack of visibility into who actually accessed sensitive attachments
-  Inability to revoke access once a document is in the wrong hands

Document GPS enhances email security by detaching sensitive data from email content and placing it in a controlled, secure document environment with full visibility and access management.

No File, No Risk

Instead of sending attachments, email secure document links with configurable view-only or edit permissions. No files are stored in the inbox.

Access Revocation Anytime

Instantly revoke or modify access to a document even after it's opened or forwarded, neutralizing the impact of a compromised email.

Real-Time Document Tracking

See exactly who accessed your document, when, and from where, even if it was forwarded or intercepted.

Anti-Forwarding Controls

Prevent recipients from forwarding or printing documents, reducing the risk of unintended exposure.

Key Benefits



Protect Confidential Documents

Prevent unauthorized access even if an email account is hacked or shared.



Control After Sending

Retain full ownership and control of your documents, regardless of where they're sent or how many times they're forwarded.



Enhance Phishing Resilience

Mitigate damage from phishing by limiting document exposure through secure access links.



Meet Compliance Requirements

Maintain control and audit trails for regulated data, supporting GDPR, HIPAA, and other standards.