Kiteworks

SOLUTION BRIEF

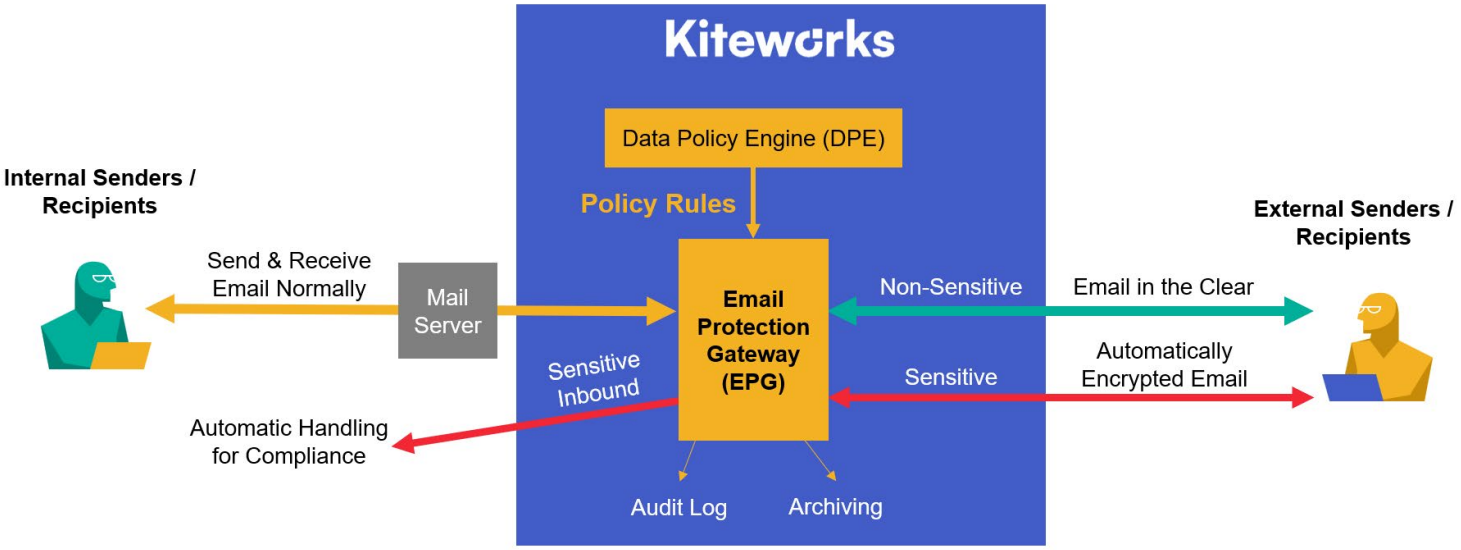
Close the Email Compliance Gap With Automated Policy Controls

Kiteworks Email Protection Gateway (EPG)

Email carries an organization's most sensitive data, such as contracts, patient records, financial information, and controlled unclassified information (CUI), yet most organizations leave email data protection to individual users. A single misdirected message or unencrypted attachment can trigger a data breach, regulatory sanction, or reputational crisis. Frameworks including HIPAA, GDPR, CMMC 2.0, ITAR, and SOX impose explicit requirements on how sensitive data must be handled in transit, and enforcement actions tied to inadequate email security are rising. Ad-hoc encryption tools cannot reliably meet this bar, because they depend on users making the right decision every time.

The Kiteworks Email Protection Gateway (EPG)

Kiteworks EPG puts your IT and compliance teams in control of every email entering and leaving your organization, automatically and without burdening end-users. It enforces your organization's policies on every message: encrypting, routing, rejecting, or blocking emails based on the data and user attributes, with no action required from staff. Security and compliance teams gain complete, centralized visibility across email and all other sensitive data exchange channels like file sharing, managed file transfer (MFT), SFTP, and data forms, through a single dashboard, dramatically simplifying audit preparation, incident response, and regulatory reporting.



Kiteworks EPG Applies Your Data Policies Automatically in the Mail Stream

Kiteworks email data protection automatically enforces the appropriate policy, encryption, and compliance on every email — inbound and outbound — removing the risk of human error and giving security and compliance teams complete audit visibility across all email traffic.

Kiteworks EPG: The Control Plane for Email Traffic

Protect ALL email traffic with automatic policies. Your policies automatically govern every message by sender, recipient, data, data classification label, and message attributes — with no user involvement required. The Data Policy Engine (DPE) enforces the full spectrum of protective actions, from encryption to quarantine and rejection.

Prevent human errors when sending emails. Since EPG invisibly applies your policies directly in the email stream, users do not need to make potentially erroneous decisions about which emails to encrypt, and which recipients should not receive the data.

Prove compliance with logging of ALL email events. EPG logs every inbound and outbound message with normalized, immutable records in the unified Kiteworks audit log, capturing the full policy decision context, including the rule matched, the action taken, and the delivery outcomes, even for non-sensitive emails it passed through. Audit data is unified and normalized with all other Kiteworks platform activity and feeds directly into your SIEM so you can prove compliance of all data exchanges.

Leverage your data classifications with MIP sensitivity label integration. EPG reads Microsoft Purview (MIP) sensitivity labels in attachments and messages and applies the correct policies to each class of data automatically.

Automate compliant handling of sensitive incoming emails. Policies can identify likely sensitive data, such as controlled unclassified information (CUI) from a defense contractor or protected health information (PHI) from a hospital, and route it to a compliant path so your employees cannot mishandle it.

Provide encryption for external recipients that just works. EPG seamlessly onboards the encrypted email recipients and provides each one with the type of encryption they need in their environment, whether webmail/TLS, S/MIME, or OpenPGP. Kiteworks provides optional FIPS 140-3 Validated encryption.

Meet email archiving requirements automatically. EPG's built-in archiving of messages and attachments automatically handles departmental retention schedules and eDiscovery readiness. Emails also feed into external, industry-standard journaling products.

Exchange files of unlimited size to avoid workarounds. Attachments up to 16 TB are staged on Kiteworks platform servers and delivered via an authenticated web portal, bypassing the file size limitations of standard email infrastructure with no change to the sender's workflow.

Show end-users the status of email receipts so they can take action. By subscribing to notifications or clicking on simple tracking reports, senders always know, and can prove, whether recipients have opened emails and downloaded attachments.

Control recipient actions to maintain compliance. Automatically apply built-in digital rights management (DRM) policies to recipients with view-only access controls, access expiration, and forwarding controls. Replies to encrypted emails are automatically encrypted to continue the chain of compliance.