Kiteworks

CAPABILITY BRIEF

Top 6 Reasons to Add Email Protection Gateway (EPG) to Your Kiteworks Deployment

Kiteworks integrated its acquisition of totemomail, the leading email encryption gateway used by a long list of multinational organizations, into the Kiteworks hardened virtual appliance. Rebranded as the Email Protection Gateway (EPG), this proven technology automates coverage of all sensitive digital content sent and received via email in the Kiteworks platform.

1. Extend the Reach of Logging and Audit

See what you've been missing. Normalize and leverage syslogs and metadata across all sensitive email to track malicious exposure of private information.

2. Automate Protection

Avoid mistakes and remove the guesswork. Give the encrypt-or-not decision for each email to automated policies, not users or plugins, and free up IT resources with automatic certificate and key management.

3. Ease the Experience for Recipients

Onboard recipients effortlessly. Recipients use their normal email address and their normal client with no plugins, while the keys are exchanged automatically for S/MIME, OpenPGP, and TLS standards.

4. Centralize Content Communications Administration

Unify management of sensitive content communications, including email encryption. Manage a single set of controls, policies, user roles, and indicators across all sensitive email, file sharing, web forms, SFTP, and MFT.

5. Extend the Reach of Email Privacy Protection

Full coverage of email. Extend end-to-end protection to every email containing sensitive content that moves in and out of the organization natively in standard email clients without plugins.

6. Protect Bidirectional Email Privacy

Manage email risk. Extend threat scanning, malware security, and policy enforcement to all incoming email.