Kiteworks

FEATURE BRIEF

Enhance Kiteworks Secure Email With the Email Protection Gateway (EPG)

Feature Selection Decision Guide

Solve your organization's unique email risk management and productivity needs with Kiteworks Enterprise email, or level-up with the additional protection, privacy, and compliance of EPG.

Level 1: Ensure Email Privacy and Compliance With Kiteworks Enterprise

Kiteworks Enterprise provides powerful email protection and policy control capabilities as standard:

Double Encryption for the Strongest Protection: Encrypt sensitive emails with AES-256 ciphers in transit and at rest, and control content with policies for expiration, forwarding, viewing, download access, and domains.

Complete Control and Tracking for Streamlined Compliance: Track every secure email in the normalized Kiteworks audit log. It consolidates reporting into a centralized console along with your other Kiteworks communication channels. No more patching information together.

Reduce Workarounds Caused by File Size Limitations: File size limits can frustrate senders of terabyte files such as legal evidence and analytic datasets, incenting them to try unsanctioned, noncompliant workarounds. Kiteworks Enterprise email removes that risk and frustration by making compliant file transfers up to 16 TB simple and reliable.

Level 2: Amplified Email Risk Reduction With the Email Protection Gateway (EPG)

Take a giant leap forward in email protection and compliance with these additional capabilities:

Enforce Policies Centrally and Apply Broadly: The policy-driven Email Protection Gateway (EPG) automates encryption, providing seamless compliance and reducing user mistakes and workarounds. And because it sees all the outbound and inbound emails, not just the sensitive sent messages, it increases the power of audits and analytics.

Further Reduce Unsanctioned and Risky Workarounds: Kiteworks EPG makes email encryption invisible to users, removing another set of frustrations that may lead them to try unsafe workarounds. They work as usual, with their standard clients and without plugins, as the system applies your policies behind the scenes.

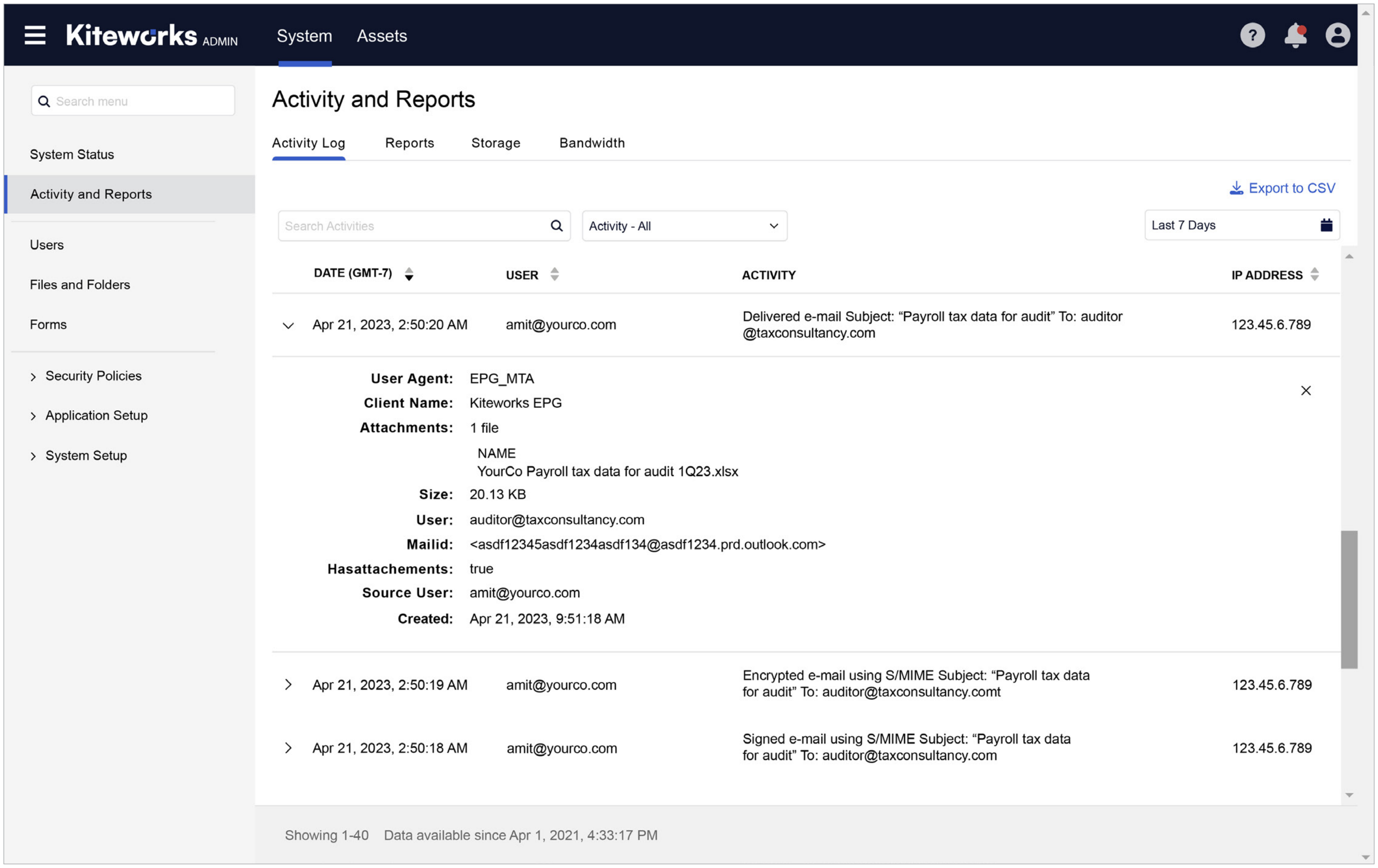
Universal Encryption Compatibility for Seamless Sensitive Data Exchange: Communicate with partners, customers, and regulators who require encryption protocols such as S/MIME, OpenPGP, and TLS. And because it's Kiteworks, it automatically makes those protocols' key housekeeping hassles invisible to your users, further reducing the incentive to try workarounds.

Detailed Feature Comparison

Feature	Kiteworks Enterprise	Kiteworks Enterprise + EPG
Decision of which emails to protect		
Manual by end-user	✓	✓
Applies Microsoft AIP sensitivity labels in policies	✓	✓
Outlook plugin encryption automation based on 3 conditions	✓	
Centrally automated policies for encryption and over 60 other actions based on over 50 different conditions		✓
Logging and audit coverage		
Protected outbound email	✓	✓
All outbound and inbound email		✓
End-user deployability		
Web client/portal and mobile app	✓	✓
Outlook plugin for large files up to 16 TB	✓	✓
Automated key management		✓
Any standard email client (no plugins needed)		✓
Use cases		
Outbound email protection	✓	✓
Large attachments up to 16 TB (via web and Outlook Plugin)	✓	✓
Scan files with DLP, antivirus (AV), and advanced threat prevention (ATP)	✓	✓
S/MIME encryption standard support		✓
OpenPGP encryption standard support		✓
Inbound email protection		✓
End-to-end encryption (strict)		✓
End-to-end encryption (w/scans such as AV, DLP, ATP)		✓
Encrypt emails stored in external cloud email services		✓
Microsoft RMS support with external email auto-conversion		✓

Track Every Send and Receive With the Centralized Kiteworks Audit Log

No matter which feature you use to protect your email, you can count on the same unified visibility across third-party communication channels, and the same centralized view of all sensitive information shared outside the enterprise. With total visibility into where data is going, who is accessing it, and how it is shared, the Kiteworks Private Content Network enables tight governance, strict compliance, preemptive threat detection, and fast incident response.



DATE (GMT-7)	USER	ACTIVITY	IP ADDRESS
Apr 21, 2023, 2:50:20 AM	amit@yourco.com	Delivered e-mail Subject: "Payroll tax data for audit" To: auditor @taxconsultancy.com	123.45.6.789
Apr 21, 2023, 2:50:19 AM	amit@yourco.com	Encrypted e-mail using S/MIME Subject: "Payroll tax data for audit" To: auditor@taxconsultancy.comt	123.45.6.789
Apr 21, 2023, 2:50:18 AM	amit@yourco.com	Signed e-mail using S/MIME Subject: "Payroll tax data for audit" To: auditor@taxconsultancy.com	123.45.6.789

User Agent: EPG_MTA
Client Name: Kiteworks EPG
Attachments: 1 file
NAME
YourCo Payroll tax data for audit 1Q23.xlsx
Size: 20.13 KB
User: auditor@taxconsultancy.com
Mailid: <asdf12345asdf1234asdf134@asdf1234.prd.outlook.com>
Hasattachements: true
Source User: amit@yourco.com
Created: Apr 21, 2023, 9:51:18 AM

Showing 1-40 Data available since Apr 1, 2021, 4:33:17 PM

The comprehensive Kiteworks audit log helps employees in a variety of roles reduce risk and support operations. Compliance and privacy teams use it to demonstrate compliance with regulations and internal policies. SecOps uses its real-time syslog and SIEM feed for threat detection, alerting, and forensics. Admins use it in troubleshooting and monitoring.

Kiteworks enables these users with a variety of interfaces, such as the filterable and searchable Activity Log, scheduled and ad hoc reports, CSV exports, syslog feeds, APIs, and the Splunk Forwarder. Even end-users can track certain activities, such as downloads of large files they've sent.

Kiteworks

May 2023

www.kiteworks.com