Kiteworks

SOLUTION BRIEF

FOR SECURITY AND COMPLIANCE TEAMS

STOP AGENT AND HUMAN EMAIL ERRORS COLD

Kiteworks Agent and Human Error Prevention: Intelligent Email Protection for Regulated Industries.

CMMC 2.0 | FedRAMP | HIPAA | ITAR | GDPR | BSI C5 | FIPS 140-3 | NIS 2 | PCI DSS

The Breach Most Security Tools Miss

Misdirected email is the #1 data security incident reported to the UK Information Commissioner's Office, accounting for 21% of all reported breaches.[1] Ninety-six percent of organizations experienced data loss from misdirected email in the past year.[2] Yet traditional DLP tools cannot stop it: they scan for forbidden data patterns, not the wrong recipient. When an employee CCs 40 clients on a confidential message, sends a contract to a personal Gmail before leaving the company, or mistypes a domain by one character, DLP sees nothing unusual. The data is authorized. The recipient is wrong. Rules cannot anticipate intent.

Detection at the Moment That Matters

Kiteworks Agent and Human Error Prevention (AHEP) analyzes multiple signals simultaneously during composition: recipient type, volume, identity match, attachment presence, and domain validity. Only when signals align does a targeted warning appear, keeping false-positive rates low. Three pre-built policies are included, each configurable without custom development. Unlike standalone email security tools layered on top of your environment, AHEP is built into the same platform where regulated data already lives, governed by the same control plane that enforces access, encryption, and compliance policy across every channel.

The Scale Of The Problem

21%

Of All UK ICO-Reported Data Breaches Involve Misdirected Email[1]

96%

Of Organizations Experienced Misdirected Email Data Loss in the Past Year[2]

3

Pre-Built Policies Included: Zero Custom Development Required

Benefits By Role

CISO / Head of DLP

Reduce breach exposure from agent and human error without writing custom rules; all three policies are pre-configured and ready at deployment. AHEP addresses the risk category that traditional DLP tools miss entirely: authorized data sent to the wrong recipient.

Chief Compliance Officer

Reduce GDPR and HIPAA mandatory notification obligations directly. Every warning event and user decision is recorded in the Kiteworks audit log, giving regulators and auditors a specific, timestamped, defensible record that safeguards were in place at the moment of risk.

CIO / IT Leadership

No new tool to deploy, no new vendor to onboard, no new integration to maintain. AHEP is part of the Kiteworks platform, works with Outlook Classic and the Kiteworks Web App, and is included in the platform. Not an add-on purchase.

Three Pre-Built Policies: Start Observing, Enforce When Ready

Each policy ships fully configured with a detection trigger and one-click resolve actions. Administrators set a status for each policy — Off, On, or Report Only — and can start every policy in Report Only to see how often it fires before any alert reaches a user, then switch to On when ready to enforce.

1 POLICY 1

BCC Warning

When a user sends to a configurable number of external recipients in TO or CC, Kiteworks flags the exposure before the message leaves and moves all recipients to BCC in a single click, eliminating reply-all risk across client lists, candidate pools, M&A communications, and multi-party matters.

2 POLICY 2

Send-to-Self Detection

Fires when three conditions align simultaneously: recipient on a known personal domain (Gmail, Yahoo, iCloud, and similar); recipient's display name or email address closely matches the sender's own across four independent dimensions; attachment present. All three must be true, keeping false-positive rates low. Directly targets the most common insider data exfiltration pattern: employees copying files to personal email before leaving.

3 POLICY 3

Domain Typo Detection

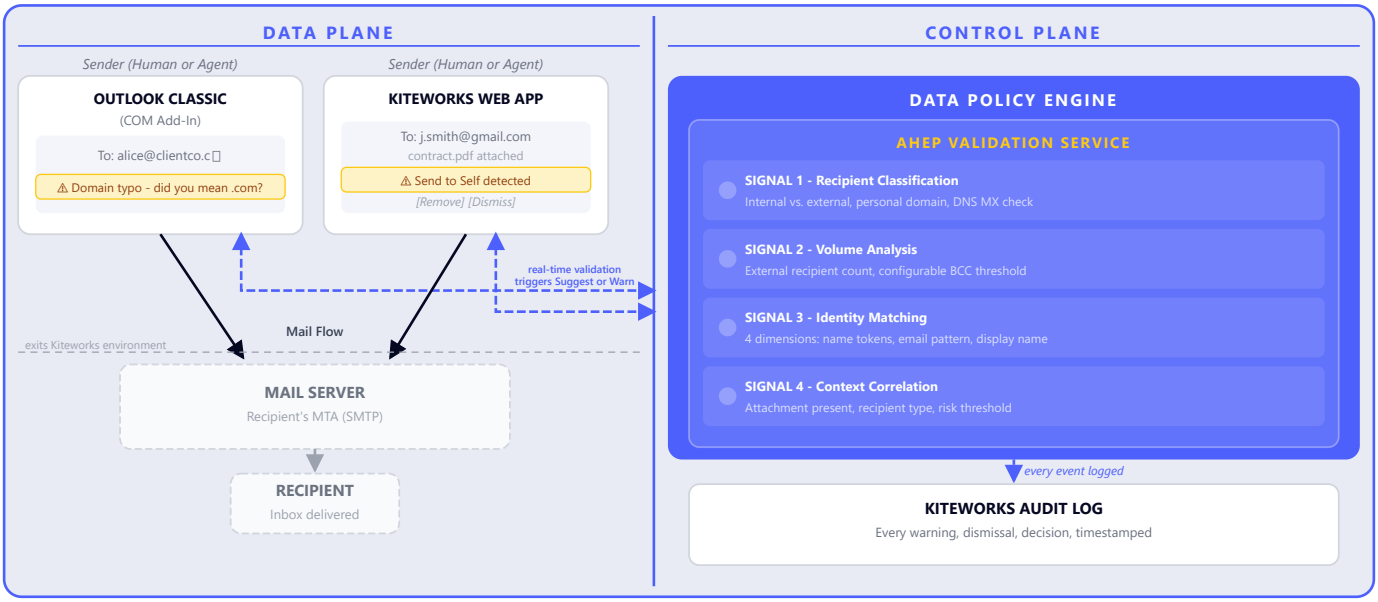
Kiteworks checks every recipient domain before send. Addresses one character away from a known consumer domain are flagged and a corrected address is offered in one click. Addresses with no valid MX record are flagged as undeliverable. Applies to TO, CC, and BCC.

A Platform Capability, Not A Point Product

One Control Plane. One Audit Log.

Standalone email error-prevention tools are layered on top of your existing environment, adding another vendor, another data dependency, and another integration to maintain. Kiteworks AHEP is built into the Data Policy Engine that already governs access control, encryption, compliance reporting, and policy enforcement across email, file sharing, SFTP, MFT, and Forms. One vendor. One control plane. One audit log across every channel. Critically, AHEP runs entirely within the customer's environment. No email metadata leaves your infrastructure. For organizations operating under ITAR, CMMC Level 2, FedRAMP, or sovereign cloud mandates, an architectural dependency on a third-party SaaS service is often a disqualifying factor. Kiteworks processes everything in-environment.

Agent and Human Error Prevention (AHEP) Architecture

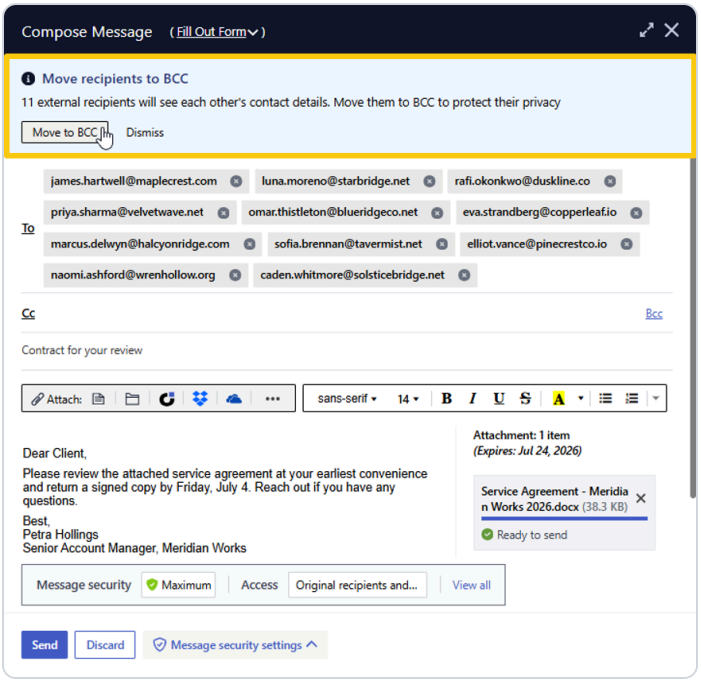


Data Plane: email routes directly from client to mail server. Control Plane: the AHEP Validation Service evaluates each message as it's composed, surfacing a Suggest or Warn alert if a policy fires. The two client windows show examples of policy-violation messages: a domain-typo warning in Outlook Classic and a send-to-self detection warning in the Kiteworks Web App.

From Compose Window To Audit Log

Real-Time Alerts With Full Traceability

Every change in the compose window (adding a recipient, removing one, attaching a file) triggers a real-time validation pass. All enabled policies are evaluated simultaneously; results are cached when nothing has changed, keeping the experience non-disruptive. Alerts appear inline in the compose window, color-coded by severity, with a title, description, and one-click action buttons. Each policy carries a configurable directive: Suggest (informational, user can send without acting), Warn (user must consciously acknowledge before proceeding), or Report Only (fully evaluated and logged, but no alert shown; recommended as a starting point to measure impact before enforcement). When multiple policies fire simultaneously, the most severe directive governs. Every alert event (shown, dismissed, or resolved) is recorded in the Kiteworks audit log with the policy identity, directive level, timestamp, and user decision. When a user dismisses a Warn and sends anyway, that choice is documented. The organization's control posture remains defensible.



BCC Warning alert in the Kiteworks compose window: 11 external recipients flagged, with one-click Move to BCC action.

Platform Capabilities

In-Environment Processing

All AHEP validation runs within the customer's infrastructure. No email metadata leaves the environment, a hard requirement for organizations under ITAR, CMMC, FedRAMP, or sovereign cloud mandates that prohibit external metadata dependencies.

Configurable Policy Controls

Each policy operates in one of three states (Off, On, or Report Only), and when active, carries either a Suggest or Warn directive that controls how its alert appears to users. Administrators configure and tune all three policies through the platform dashboard. No custom development or professional services engagement required.

Complete Audit Trail

Every alert event (shown, dismissed, resolved, or bypassed) is recorded with policy identity, directive level, timestamp, and user decision. When a user sends despite a warning, that choice is documented, keeping the organization's control posture defensible before regulators and auditors.

Real-Time, Multi-Signal Validation

Every recipient change triggers simultaneous evaluation across all enabled policies. The system cross-references recipient type, volume thresholds, identity matching dimensions, attachment presence, and domain validity in parallel.

Compliance-Ready Controls

AHEP maps directly to GDPR Article 32, HIPAA Security Rule, CMMC 2.0, and ITAR requirements for documented safeguards against accidental disclosure, providing a specific, logged, auditable answer when regulators or auditors ask what prevents accidental data exposure.

One Control Plane Across Every Channel

AHEP is governed by the same Data Policy Engine that controls access, enforces encryption, and generates compliance reports across email, file sharing, SFTP, MFT, and Forms. Extending data governance to agent and human-error scenarios requires no additional point products or integrations.

Built For Regulated Industries

Where Misdirected Email Represents the Leading Breach Type[3]

Healthcare
PHI sent to the wrong recipient triggers mandatory breach notification under HIPAA. AHEP provides an auditable control that documents every warning and every user decision, giving compliance officers defensible evidence that safeguards were in place.

Financial Services
M&A communications, client lists, and trade confirmations carry significant breach liability when CC'd to unintended parties. BCC enforcement and identity-matching protect the most time-sensitive and confidential transactions.

Legal and Professional Services
Privilege waiver risk and multi-party matter confidentiality make recipient accuracy critical. Domain typo detection and BCC enforcement apply across all external communications, with no configuration overhead per matter.

Defense and Government
CUI and ITAR-controlled data require in-environment processing with no external metadata dependencies. AHEP satisfies CMMC 2.0 and ITAR accidental-disclosure controls while keeping all validation on-premises or in your private cloud.

Availability

AHEP alerts are currently supported on Kiteworks Web App and Outlook Classic (COM add-in, Outlook 2016 and later). Future phases plan to add ML and AI-based behavioral analysis, building an increasingly sophisticated detection foundation over time. Product plans are subject to change.

Sources

[1] UK Information Commissioner's Office (ICO), Q4 2024 Data Security Incident Trends; Osterman Research, 2025. [2] Abnormal Security, Email Security Insights Report, 2025. [3] Verizon Data Breach Investigations Report (DBIR), 2025.

See Agent and Human Error Prevention in action.

www.kiteworks.com info@kiteworks.com

Kiteworks

Kiteworks' mission is to empower organizations to effectively manage risk in every send, share, receive, and save of sensitive content. The Kiteworks platform provides customers with a Private Content Network that delivers content governance, compliance, and protection. The platform unifies, tracks, controls, and secures sensitive content moving within, through, and out of the organization; significantly improving risk management and ensuring regulatory compliance on all sensitive content communications.