Kiteworks Doubles Down on Its Data Control Plane Commitment with Launch of Agent and Human Error Prevention

Data Policy Engine governing email, file sharing, and AI agents now covers emails sent to the wrong recipient: the breach type DLP tools are built to miss.

SAN MATEO, CA, UNITED STATES, August 13, 2026 /EINPresswire.com/ -- Kiteworks, which empowers organizations to ensure regulatory compliance and effectively manage risk in every send, share, receive, and use of sensitive data, today announced the general availability of Agent and Human Error Prevention (AHEP). AHEP extends the governance, enforcement, and audit infrastructure of Kiteworks' control plane for secure data exchange to outbound email, warning users before a misdirected send occurs rather than scanning for it after the fact. The launch signifies a doubling down on the commitment at the center of its platform: one control plane governing every channel, every human workflow, and every agent workflow, without exception.

> Misdirected email has sat outside [traditional] governance for years because it isn't a data-pattern problem, it's an intent problem."
>
> *Tim Freestone, Chief Strategy and Marketing Officer at Kiteworks*

Misdirected email is the single largest data security incident category reported to the UK Information Commissioner's Office, accounting for 21% of all reported breaches,[1] and Verizon found the human element – including misdirected and misdelivered communications – present in 62% of confirmed breaches, rising to 69% in the public sector, where high-volume correspondence drives misdelivery errors.[2] Traditional DLP tools scan for forbidden data patterns, not wrong recipients, so they miss the scenarios that actually cause harm: a reply-all to 40 clients, a contract sent to a personal Gmail account, a one-character typo in a domain name. Rules cannot anticipate intent.

"The control plane for secure data exchange has always been about governing every send, share, receive, and use of sensitive data, for humans and agents alike," said Tim Freestone, Chief Strategy Officer at Kiteworks. "Misdirected email has sat outside that governance for years because it isn't a data-pattern problem, it's an intent problem. And intent is exactly what a policy engine that already knows the sender, the recipient, and the context is positioned to catch. AHEP isn't a new tool bolted onto the inbox. It's a new module of the same Data Policy Engine we use

to govern file sharing, MFT, APIs, and agent access, extended to the channel with the least room for a scanning-after-the-fact approach. That's what doubling down on the control plane looks like in practice."

What AHEP Does

AHEP analyzes multiple signals simultaneously as a message is composed: recipient type, recipient volume, identity match, attachment presence, and domain validity. It surfaces a warning only when those signals align, keeping false positives low. It ships with three pre-built policies that require no custom development:

- BCC/reply-all protection flags exposure when a message goes to a configurable number of external "To" or "CC" recipients and moves them to BCC in one click.
- Send-to-self detection fires only when a personal-domain recipient (Gmail, Yahoo, iCloud, etc.), a close identity match to the sender across four independent dimensions, and an attachment all align, targeting the specific pattern behind insider data exfiltration.
- Domain typo detection flags domains that are a single character off from a known-good address and offers a corrected recipient and separately flags addresses with no valid mail server record.

Each policy can be set to off, on, or report-only, with suggest or warn behavior, and every shown, dismissed, resolved, or bypassed event is logged with policy identity, timestamp, and the user's decision. These decisions and activities are logged in the same audit trail Kiteworks already maintains across email, file sharing, SFTP, MFT, and forms.

A Platform Capability, Not a Point Product

AHEP runs entirely within the customer's Kiteworks environment; no email metadata leaves the platform. This design answers a hard constraint in ITAR, CMMC, and FedRAMP environments and other sovereign-cloud mandates: sensitive data, metadata included, cannot transit third-party infrastructure. AHEP extends the Data Policy Engine and control plane that already govern access, encryption, and compliance reporting for Kiteworks customers, rather than shipping as a standalone email security product layered on top of the environment.

"AHEP ships as a capability inside the platform our customers already run, not a new console to log into," said Yaron Galant, Chief Product Officer at Kiteworks. "The first phase covers the three mistakes we see most often in outbound email: reply-all exposure, send-to-self, and misspelled domains. None of them need a model, just the right signals evaluated at the moment someone hits send. We built the architecture to extend the same way the rest of the Data Policy Engine does by adding phases without asking a customer to stand up new infrastructure."

AHEP is available now, supporting the Kiteworks Web App and Outlook Classic (Outlook 2016 and later) at launch, with future phases planned to add machine-learning-based behavioral analysis. Read the solution brief for more detail.

Endnotes

1. UK Information Commissioner's Office, "Data Security Incident Trends," updated February 27, 2025, https://ico.org.uk/action-weve-taken/complaints-and-concerns-data-sets/data-security-incident-trends/.
2. Verizon, 2026 Data Breach Investigations Report, https://www.verizon.com/business/resources/reports/dbir/.

About Kiteworks

Kiteworks' mission is to empower organizations to ensure regulatory compliance and effectively manage risk in every send, share, receive, and use of sensitive data. The Kiteworks platform delivers secure and compliant data exchange across email, file sharing, APIs, and AI agents, controlling, monitoring, and protecting every data interaction between people, machines, and systems in a unified control plane. Kiteworks unifies, tracks, controls, and secures sensitive data moving within, into, and out of the organization, significantly improving risk management and ensuring regulatory compliance across every data exchange. Headquartered in Silicon Valley, Kiteworks protects over 100 million end users and thousands of global enterprises and government agencies.

David Schutzman
Kiteworks
+1 203-550-8551
email us here
Visit us on social media:
LinkedIn
Facebook
YouTube
TikTok
X
