Kiteworks

Take the Risk Out of Mobilizing Your Executives

5 Best Practices for Executive and Board Sensitive Content Communications

Executive Summary

Enterprise CEOs and top executives send and receive corporate secrets every day in the riskiest locations, using the riskiest equipment: their mobile phones and tablets. They depend on these devices to stay productive in spite of a demanding travel schedule as they visit customers, investors, and branch offices.

After all, they can't pause operations while they travel, or even while stuck in a series of meetings. Each day, staff members send briefing documents, slide decks, purchase approval requests, and project status reports. Executives need to work with the board and attorneys, or review the latest version of a contract—all in scraps of free time in airports, hotels, and office hallways.

But this productivity boost comes with the risk of unintentionally exposing confidential information—preliminary financial results, M&A, negotiations, lawsuits, or trade secrets—with potentially company-changing consequences. Mitigate this risk by following five best practices that maximize your executives' and board members' mobile productivity while locking down your corporate secrets.

Best Practice #1:

01 Safeguard Executive Productivity and Security on the Road

Provide Simple, Secure Mobile Email

CEOs use their mobile email throughout the day for sharing financial plans with board members, getting sensitive legal advice from their attorneys, or other confidential communications. But if they send email and attachments using standard apps, they are vulnerable to scanning by mobile vendors, governments, and bad actors. And when things go wrong, they have no audit trail to prove who had access to which files. Finally, their important inbound communications are buried in spam, slowing their responses.

Prevent this scenario by layering a secure end-to-end email system for your executives on top of your corporate email. Encourage adoption by delivering consumer-grade ease of use, and by providing secure access to essential headquarters file stores. Encrypt all files and messages in transit, as well as offline files stored on the device. Cut out spam by filtering out unknown senders. And make sure executives never miss an opportunity: Give them an immediate notification when their recipient downloads a document or sends a reply.

Complete the solution by securing the content at the recipient's end, no matter how insecure their own organization's email system. Provide a secure, simple way for these external parties to view messages and download attachments, and automatically encrypt their replies, without installing software.

Best Practice #2:

02 Help Staff Prep and Support Traveling Executives

Push Content Securely to Mobile Devices

Internal-facing communications are just as important as the external-facing interactions. As an executive travels to a string of meetings, her staff members need to prepare her with agendas, briefing documents, and slide decks. They must push them into her topic folders automatically, so they are already in her device when she finally has a moment to review them and reply. Enable her to open them offline, since an international flight might be an executive’s only clear time to review and annotate a complex proposal or contract PDF.

Internal-facing communications are just as important as the external-facing interactions.

Best Practice #3:

03 Digitize and Govern Board and Committee Communications

Provide Secure Collaboration Folders

Your biggest information-sharing risks often occur with external parties like your board members, attorneys and bankers, private equity firms, and M&A advisors. Nearly everything you share with them can tip off competitors or run afoul of financial disclosure laws if leaked. And many of these external parties, like your executives, consume information on the run using mobile phones and tablets.

Keep this constantly changing information rigorously organized using shared folders. Set each folder's permissions so only parties with a need to know can see it, and only those with a need to input can change it. And with such sensitive information, be sure to implement an immutable audit trail and automatic expiration policies.

Add collaboration support for external committees that work together on projects, such as contracts, acquisitions, or financial transactions. Provide easy, seamless editing in Microsoft Word, Excel, and PowerPoint apps, or annotation and signoff of PDFs, automatically saving changes back to the secure collaboration folder. Whether the external recipient uses a browser or mobile app, provide notifications, track all file versions, and maintain the audit trail.

Best Practice #4:

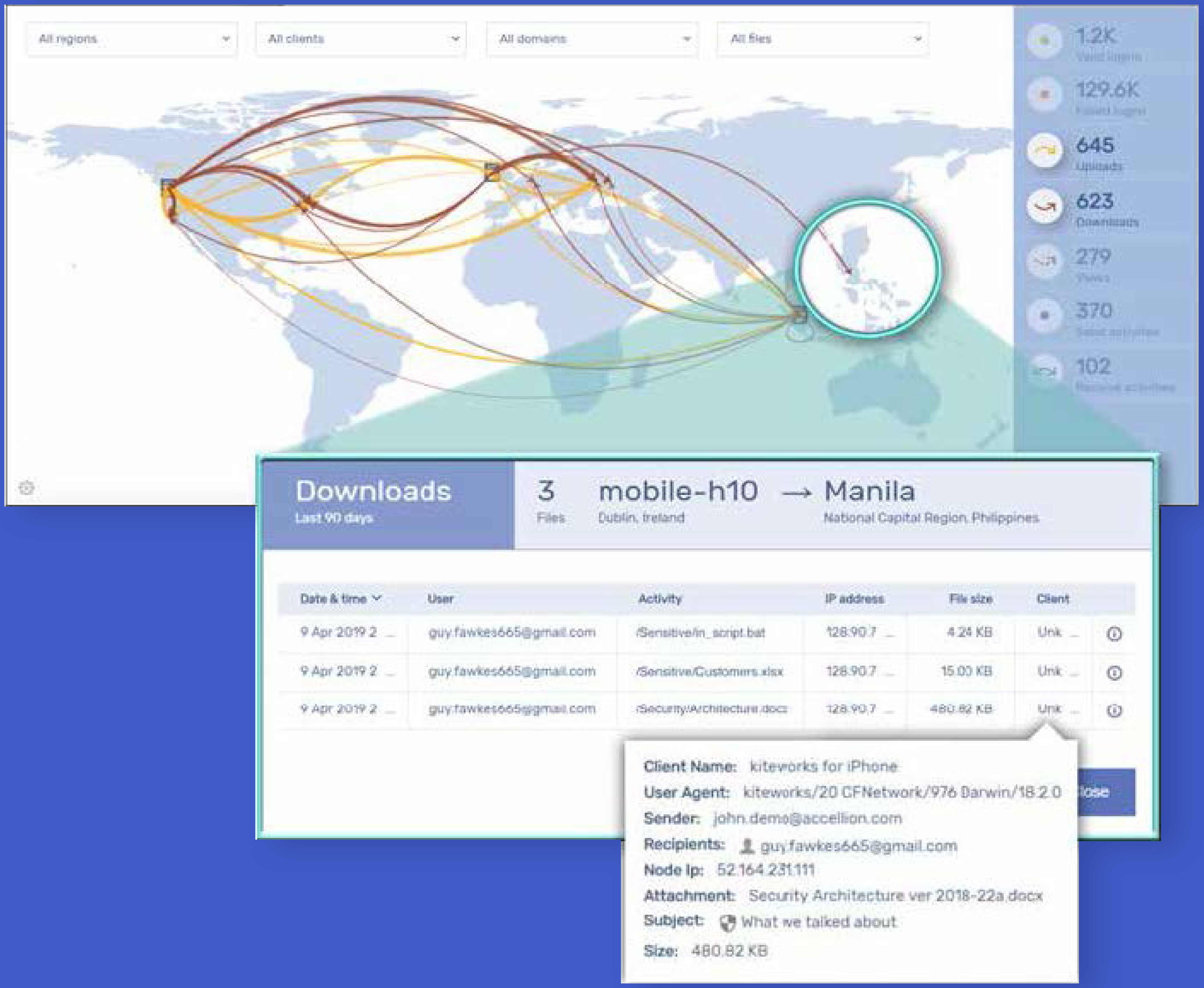
04 Secure Your Mobile Content

Protect Files End-to-End on Any Mobile Device

Today, your executives may use commodity cloud file shares and email in the clear to stay in touch with staff and outside parties. But public cloud vendors for these tools have the ability to scan the metadata of your data transfers, increasing your risks. And when served a subpoena, they have the ability and the obligation to turn over your confidential data without a warrant.

Mitigate the risks of mobile email and shared folders with a best-of-breed security and governance foundation. Implement the service on a hardened, scalable server cluster, encrypting information with IT-controlled keys when in transit and when stored in the device or server. Control who has access to your data by deploying this service using on-premises, FedRAMP, or private cloud infrastructure. Since external users are out of your control, harden the app to run securely on their personal devices.

Empower the administrator with role-based policy controls, management of mobile device users, whitelisting of helper apps such as Microsoft Word, and security integrations such as LDAP/AD and MDM. Finally, eliminate the risk posed by enterprise data on an off-board or stolen device by remotely wiping it, without affecting the user’s personal content.



Downloads
Last 90 days

3 Files — mobile-h10 (Dublin, Ireland) → Manila (National Capital Region, Philippines)

Date & time	User	Activity	IP address	File size	Client
9 Apr 2019 2 ...	guy.fawkes665@gmail.com	/Sensitive/in_script.bat	128.90.7 ...	4.24 KB	Unk ...
9 Apr 2019 2 ...	guy.fawkes665@gmail.com	/Sensitive/Customers.xlsx	128.90.7 ...	15.00 KB	Unk ...
9 Apr 2019 2 ...	guy.fawkes665@gmail.com	/Security/Architecture.docx	128.90.7 ...	480.82 KB	Unk ...

Client Name: kiteworks for iPhone
User Agent: kiteworks/20 CFNetwork/976 Darwin/18.2.0
Sender: john.demo@accellion.com
Recipients: guy.fawkes665@gmail.com
Node Ip: 52.164.231.111
Attachment: Security Architecture ver 2018-22a.docx
Subject: What we talked about
Size: 480.82 KB

Best Practice #5:

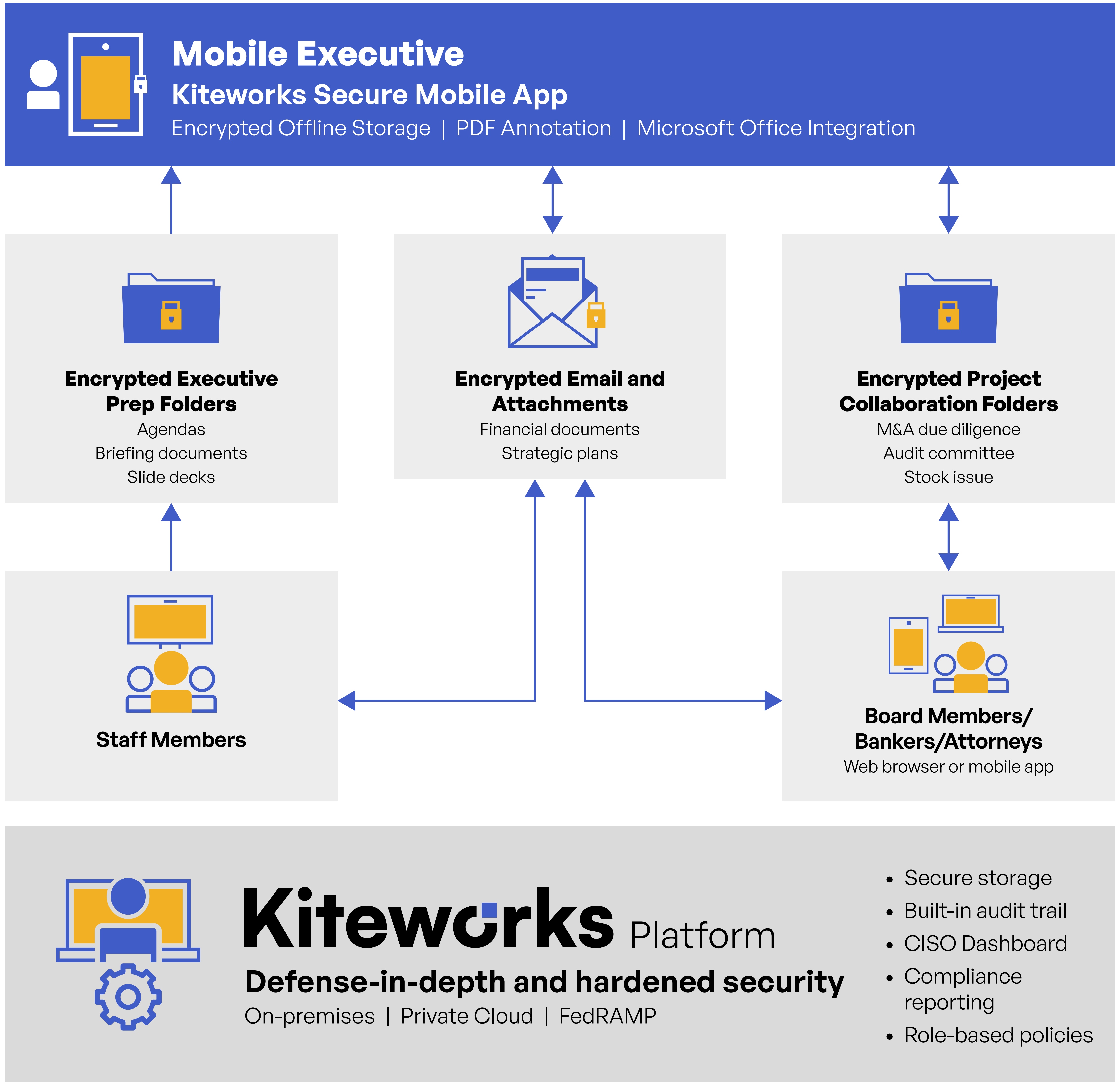
05 Prevent Breaches

Provide Visibility Into Every Mobile File Transfer

To defend against the insider and outsider threats of your communications with mobile executives and board members, you must have visibility of every file entering and leaving your organization via mobile devices. Begin by implementing a consolidated audit trail of all mobile transfers between your organization and these traveling or external parties. Once you have this metadata, create clear and complete real-time visualizations that answer the most important security questions about the information entering and leaving the firm. Where is it coming from? Where is it going to? Who is sending it? Who is receiving it? Is it sensitive? Is the transaction normal, or is it a threat?

Kiteworks-enabled Private Content Network

Prevent Mobile Executive Breaches and Compliance Violations



Mobile Executive

Kiteworks Secure Mobile App

Encrypted Offline Storage | PDF Annotation | Microsoft Office Integration

Encrypted Executive Prep Folders

Agendas
Briefing documents
Slide decks

Encrypted Email and Attachments

Financial documents
Strategic plans

Encrypted Project Collaboration Folders

M&A due diligence
Audit committee
Stock issue

Staff Members

Board Members/ Bankers/Attorneys

Web browser or mobile app

Kiteworks Platform

Defense-in-depth and hardened security

On-premises | Private Cloud | FedRAMP

- Secure storage
- Built-in audit trail
- CISO Dashboard
- Compliance reporting
- Role-based policies

Kiteworks

www.kiteworks.com

July 2022

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, into, and out of their organization, significantly improving risk management and ensuring regulatory compliance on all sensitive content communications.