Streamline the Secure Mobile Capture of Scanned Documents, Images, Video and Audio

Using mobile devices to scan business documents and capture media such as photos, video, and audio accelerates the every-day workflows that drive your business processes. Whether your staff needs digital copies of signed contracts, scanned copies of receipts, photos of whiteboards, or audio recordings of legal depositions, leveraging the convenience of mobile devices generates benefits across every business sector:

- Legal—scan documents at courthouses for remote review by collaborating attorneys.
- Insurance—upload contracts to immediately launch invoices and create photographic claims reports.
- Financial—scan loan documents and record conversations to document financial advisory services.
- Manufacturing—document defects in the production line and allow product managers and engineers to collaborate.
- Healthcare—append patient audio discussions to scanned images of lab and radiology results.
- Government—record video/audio of police interactions and collect crime scene evidence that adheres to state and federal compliance guidelines.

The Challenges of Handling Sensitive Files with Mobile Devices

When managing scanned documents and capturing images and audio as part of critical business processes, IT needs to establish policies that dictate what end users and their mobile device(s) can and cannot do. In support of the business workflows, IT also needs to enforce polices without driving users to a Shadow IT mindset.

Although smart mobile devices come equipped with hardware and apps to easily scan images and snap photos as well as record video and audio, doing so comes at a risk to the business. Files may be mishandled (for example, synced to iCloud and/or Family Share), breached by a cyber attack potentially exposing private or otherwise sensitive data to theft and misuse, or left vulnerable to an insider threat.

Before giving employees the freedom to capture business content on both bring-your-own and corporate-owned mobile devices, businesses need to overcome the following key challenges:
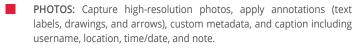
- Preventing files from going to unauthorized cloud repositories, third-party applications and other devices.
- Complying with industry regulations on how files are created, managed, stored and deleted.
- Securing data at rest on mobile devices.
- Securing data in transit (app-to-app and app-to-backend workflows).
- Establishing and enforcing business-enabling, end-user policies to promote productivity while reducing data leakage.
- Balancing business and personal considerations to avoid over-restricting employees, a key driver of Shadow IT.

Finding the right balance—allowing employees to increase productivity and accelerating business workflows, while keeping business assets and sensitive files safe—has presented major headaches to internal IT teams.

UNTIL NOW...

CAPTOR™ for MobileIron

CAPTOR™ for MobileIron is an AppConnect app for the secure capture and management of sensitive business-related content. The solution can scan documents, snap photos, record video/audio, and read QR Codes. Mobile users can then securely store and share files with coworkers or transfer to a central database. CAPTOR leverages IT policies, metadata, and watermarking to identify, track, and manage captured content.

■ **PHOTOS:** Capture high-resolution photos, apply annotations (text labels, drawings, and arrows), custom metadata, and caption including username, location, time/date, and note.

■ **DOCUMENTS:** Scan multi-page paper documents, apply annotations, and save as PDF. Supports all versions of PDF including 1.3 - 1.7 as well as PDF/A.

■ **VIDEOS:** Record video, edit, and apply "credits" identifying username, location, time/date, and note.

■ **AUDIO:** Record ambient audio, edit, save, and share as M4A or AIFF files.

As an integrated **AppConnect** solution, CAPTOR is ideal for businesses that have already deployed or are about to deploy the MobileIron mobile device management platform. CAPTOR for MobileIron encrypts all captured content in a secure container, and internal IT teams can apply policy controls to prevent data leakage and manage every aspect of how content is created and managed. IT can also wipe the CAPTOR container that stores all business files if an employee loses a mobile device or leaves the organization.

LEGAL WORKFLOW

| Capture Meeting Notes | Email Meeting Notes | Record Client Deposition | Scan Document | Annotate & Redact | Upload Case Files To Docs@Work |

CAPTOR for MobileIron: Key Features and Benefits

■ Four Capture Modes: Photo, Video, Audio, and Document Scanner — CAPTOR combines a camera, audio recorder, document scanner, and QR Code reader into one single app to capture all types of content for business.

■ Encrypted Data Container — Protects sensitive data residing on devices and in transit while also preventing access to content on lost/stolen devices.

■ Governance/Policy Controls — Allows IT to dictate each user's ability to copy/paste and print, restrict file sharing, establish a file nomenclature system, backup to a content server, and more.

■ Isolated Data Container — Stores business files in separate container from personal files; allows business files to be wiped without impacting personal files.

■ Annotations — Apply annotations to documents and photos—such as arrows, text labels, and drawings—in order to direct attention, redact text, or enhance understanding.

■ Insider Threat Alerts — CAPTOR Compliance logs events flagged as potential violations to data leakage protection (DLP) and container policies and reports them to system admins, warning of possible insider threats as they occur.

Enhanced Productivity Supported by Secure Content Capture

Whether your business captures receipts, contracts, identification cards, or photos—or your mobile users record video or conversations—CAPTOR for MobileIron provides the perfect solution: Increasing employee productivity and accelerating business workflows while protecting your vital business assets.

For more information, visit **www.inkscreen.com/mobileiron**.

About Inkscreen

Inkscreen was founded in 2012 to provide enterprise-ready mobile applications to manage and control sensitive content captured on mobile devices. Its founders have extensive backgrounds in enterprise mobility, Fortune 500 IT consulting, and ERP software. For more information, please visit: **http://www.inkscreen.com**.