Kiteworks

FEATURE BRIEF

Transform Third-party Collaboration Risk Management

SafeEDIT Next-gen DRM Maximizes Productivity *and* Security

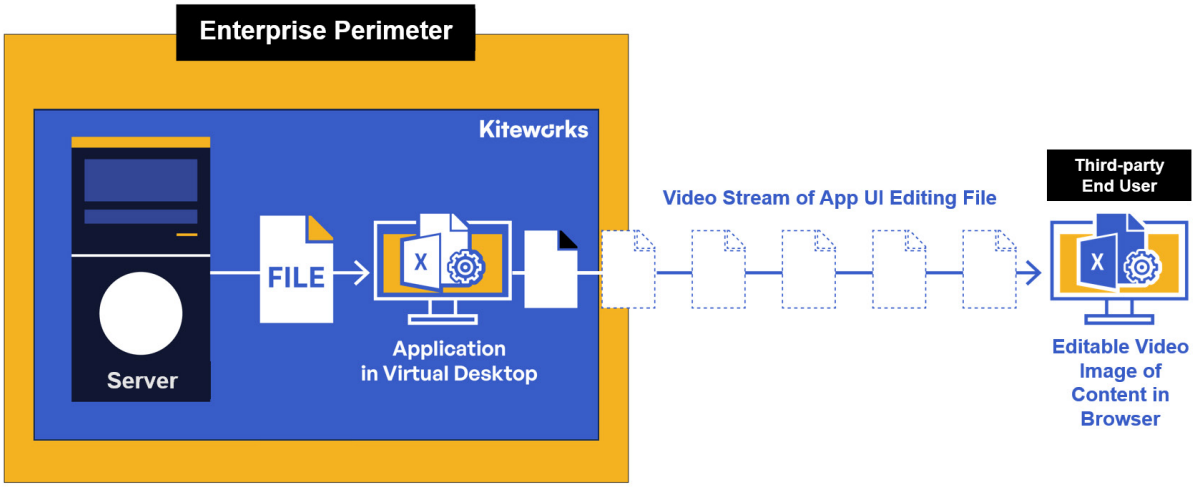
The Collaboration Risk/Trust Contradiction

Many important business processes require collaborating with untrusted individuals, especially third parties, using sensitive content. For example, a mergers and acquisitions team needs outside investors, sellers, buyers, bankers, and attorneys to view, annotate, and alter due diligence documents, financial spreadsheets, and contracts. Manufacturers need suppliers to navigate and alter CAD drawings, which often contain sensitive intellectual property. These requirements create a risk/trust contradiction: The organization must manage security and compliance risk, yet give untrusted parties access to their most sensitive content.

Until now, legacy DRM vendors tried to address this contradiction with compromises, providing their customers with a risky, agent-heavy editing infrastructure and a static read-only viewer. Agent-based adoption has been poor because the legacy approach still puts the sensitive content in untrusted hands, the collaboration experience is restrictive and complex, it supports only a narrow set of content formats, and the deployment is unwieldy and inappropriate for working with external parties. The static viewer approach, too, has limited usage because it removes interactivity and navigation in the content, and doesn't allow collaboration at all.

The Ultimate Risk Reduction With Kiteworks' Next-gen DRM: SafeEDIT

Kiteworks defuses the collaboration risk/trust contradiction at the content layer without compromising security or productivity: An authorized external party can edit any kind of file naturally in their standard browser without plugins, but the content itself never leaves the Kiteworks secure enclave.



Data never leaves the enterprise perimeter for the highest level of security, control, and tracking, while enabling use of content by the recipient.

Instead, the Kiteworks server streams an editable, zero-latency video rendition of the application user interface securely to the authorized user, and then applies the user's clicks back to the application. Thus, the video stream provides a native application experience for reading, navigating, and editing files. The Kiteworks server automatically manages the access controls, the virtual desktops, and the file versions.

Key Benefits

- **Natively Edit Any File Type:** Unlike legacy DRM, where the vendor must write specific code for each version level of each file type, SafeEDIT works natively with literally any file type with an application that has a user interface. Legacy DRM products typically support only Microsoft Office files, PDFs, text files, and standard images, and in some cases, specific releases of certain CAD products. In many cases, legacy DRM Office support is via non-native applications, such as OnlyOffice or LibreOffice.
- **Keep Files in the Kiteworks Secure Enclave:** Unlike legacy DRM encryption-wrapping approaches, which typically distribute the file to the end-user and decrypt it on their desktop for editing, Kiteworks SafeEDIT eliminates the leakage risk by only exposing a video stream of the application UI.
- **Support Editing on the User's Desktop Without Plugins, Agents, or Apps:** Unlike legacy encryption-wrapping DRM, which requires an agent or plugin on the user's client to decrypt the file and manage the viewing and editing, SafeEDIT only uses a standard browser and internet connection—there is never anything to install. This ensures a seamless experience for third-party recipients, since they use systems outside of the organization's control and may not be able to access and install any agents.
- **Manage Versions Automatically:** Unlike encryption-wrapping DRM, which sends multiple copies of a file to multiple users who then make uncoordinated edits, SafeEDIT manages the document versions centrally in the Kiteworks repository to ensure a single version of the truth.
- **Secure Copy/Paste:** Unlike most legacy DRM systems, SafeEDIT policies can enable copy/paste within an application separately from copy/paste from the application to the user's desktop operating system. This improves editing productivity, since copy/paste is still available in the editing process within the document, and security, since content cannot escape the document.
- **Centralized Authorization:** Unlike legacy DRM systems that associate file encryption keys with the user rather than the enterprise, the organization maintains access to and control of Kiteworks SafeEDIT documents even when employees leave.
- **Comprehensive Audit Log:** All user activity between a file and its application is comprehensively logged to track who had access for business operations and compliance logging.

Kiteworks

Copyright © 2024 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, into, and out of their organization, significantly improving risk management and ensuring regulatory compliance on all sensitive content communications.