SENSITIVE CONTENT MANAGER

THE CHALLENGE

Sensitive content management across a broad community of users – available on and off network – has long proven a challenge for many organizations. The move to cloud-based document centric tools has given us data sharing capabilities, but don't have enterprise access controls in mind. Email is no longer the answer due to heightened security concerns, and platforms such as SharePoint and other content management services generally require a live connection – something that is not always available to users.

In many cases, full editing and other manipulation of content is not required or even warranted for collaboration teams. These tools have primarily proven necessary for tasks such as annotating, collecting signatures, or for other general activities such as polling and voting. Collaboration has now become less of a need for basic editing in favor of secure content distribution purposes, especially when 3rd party vendors are involved.

With the heightened risk landscape, data now needs to be 100% secure and protected in case of device loss, and content must be managed by access permission policies including who sees what, when, where, and how many times. Full Digital Rights Management capabilities need to be auditable, repudiable, and fully manageable by enterprise toolsets.

THE SOLUTION

Data443's Sensitive Content Manager Solution is a security-centric collaboration service designed to give organizations the tools needed for successful content sharing, collaboration and safe distribution with full enterprise management in mind. With a continuous sync feature, encrypted data is automatically downloaded and updated in real time –no matter where they are – ensuring that users have the most accurate data available.

This custom branded and configured native application for Apple, Android and Windows devices reduces operational risk by ensuring that content saved has correct access controls, so only the correct users can view what is stored. By limiting to a specific number of views, sharing restrictions, printing and other controls, Sensitive Content Manager is built for all teams, workgroups, and committees in mind, including audit committees, professional football teams and bank boards.

ONBOARDING

- Onboarding workshop to finalize any branding requirements, user onboarding, and structure setup 2-4 hour. Less than 2 hours to full deployment and solution value
- Custom Branded application – 2 business days. Immediate reporting as data comes in
- Custom URLs & Certificates 1-2 Business Days. Dynamic Compute Scaling automatically
- RBAC Design (Optional)
- Authentication &SSO integration (Optional)

KEY FEATURES

- Easy integration with user directory services such as AAD and LDAP for centralized enterprise user administration and single sign-on (SSO) password management.
- Total access control with permission capabilities. Perform Global Search and Discovery across all unstructured and structured datasets
- Complete RBAC model within the application platform – meeting your needs for complex content associations
- DRM controls are integrated within the RBAC model and explicitly – manageable by content level as well and self-manageable by publisher
- Fully brandable application interface – online
- Available for desktop and mobile devices – private branded applications available
- Unlimited storage & transfer services

HOW IT WORKS

Hosted in either the Microsoft Azure cloud, your private cloud, or on premises data storage repository, Sensitive Content Manager can support the storage of content on private or public servers controlled by the user. With a rapid workshop-driven deployment, the system is up and running for your userbase within hours, and content is immediately available with notifications

(SMS/Push) and full encryption capabilities. In as little as 2 days, your fully branded mobile applications are rendered, which can be deployed via Mobile Device Management (MDM) or other techniques. Using our Data Identification Manager, you can automatically classify sensitive information and using policy protect it with Sensitive Content Manager.

Protected by AES-256 encryption, all content (rich media, documents, spreadsheets) is encrypted immediately prior to being affixed to a user. Full Digital Rights Management (DRM) controls are associated within the Role-based Access Control (RBAC) system and assigned and managed from the permissions console. These continue to be editable throughout the lifecycle of the dataset – including remote destruction of the data at any time. Data stored on end user devices require matching certificate pairs, rendering local storage useless in the event of device loss or theft.

Sensitive Content Manager is designed with productivity timelines in mind. Zero training is necessary, and IT Teams may deploy the endpoint application to a user base quickly, without impediments. Whether for board meeting minutes, sports play updates, training videos, or sensitive manuals for remote maintenance of industrial control systems, content will continuously and automatically be up to date.

BENEFITS

- **Create and publish documentation in real-time.** Works with PDFs, Office Documents, HTML5, and other rich media. Select your content to be protected, optionally convert it to universal formats, encrypt the files, upload the content to the appropriate storage location, and make the content available to authorized end-users.
- **Full distribution and user management capabilities.** Register, manage and monitor protected content based on internal system policies on a global or individual level. With digital rights management (DRM) functions, content can be distributed securely with various controls.
- **Audit-friendly reporting and analytics functionality.** Leverage a comprehensive suite of reports and data interfaces for auditing users, content, and activities. Reporting is implemented using industry-standard interfaces, allowing for data and presentation customizations. Sensitive Content Manager can even be integrated into your own reporting systems or executive dashboards using provided data views.

ABOUT DATA443

Data443 Risk Mitigation is a leader in data security and privacy management – a critical element of IT security protecting access to All Things Data Security™ across the enterprise and in the cloud. Data443 provides the necessary visibility and control needed to protect at-scale, obtain compliance objectives, and enhance operational efficiencies.