EFSS with Secrata:

Secure File Sync & Share for the Enterprise

challenge

Secure information access and sharing is a fundamental requirement for the legal profession. Shared case information is proprietary, privileged, and sensitive. As such, using FTP, email attachments, and even many secure file sharing applications does not ensure proper security or support the differing access needs of today's legal environment. BYOD (Bring Your Own Device) initiatives create additional challenges for IT and InfoSec professionals at firms and agencies, as individuals both access and store information using "unsecured" devices.

Legal professionals must be able to access information on demand, from diverse sources and different devices; often, the files they must access represent a small subset of a vast collection or archive. These files may be stored behind the firm's firewall, on a mobile device or laptop, or in an online storage service. Currently, to access these files, lawyers or their staff must search multiple sources, using different interfaces, and often, they must know the specific files or documents they need. These requirements limit the utility and the accessibility of the information as well as costing the firm billable time.

Data security and integrity are also issues facing the legal community. Not only must firms be able to securely share files and data with individuals outside the firm, they must be able to track precisely who has accessed what files and when. Firms are often faced with the dilemma of whether to sacrifice file-sharing security for information accessibility.

EFSS with **Secrata**

EFSS is a secure file sync and share solution that meets the tight security requirements and rigorous access and availability needs of the legal community. EFSS allows individuals and organizations to share information securely across firms, departments, and enterprises, from different devices, and stored in different locations. With the EFSS Insight Engine, security metadata describing all file sharing, access, and storage events are tracked and aggregated in a central data-mining engine used to meet regulatory requirements and prevent security breaches.

Using EFSS, information and files are accessed in invitation-only workspaces, and data is protected when accessed, managed, transferred, and stored. EFSS is a trusted cross-enterprise solution that leverages on-site file repositories, cloud file storage services, and hybrid solutions and services securely and reliably. Firms can decide where to store specific information based on security requirements or availability needs, and authorized individuals can access and manage that information using a single interface from any registered device. Importantly, using the same interface, authorized users can efficiently browse, search, share, transfer, and otherwise manage all cataloged files on all registered devices—file repositories, cloud services, storage devices, mobile devices—without sacrificing security.

Unlike cloud services and file repositories, EFSS never stores or moves information in the clear—all files are shredded into chunks, and each chunk is encrypted individually before those chunks are stored or moved. As well, the passwords and keys to re-assemble files are never stored on EFSS servers. This means that individual privacy is ensured: sensitive information cannot be hacked or accessed by unauthorized users.

EFSS supplies legal IT and InfoSec admins with full audit log information for data shared using mobile devices, file transfer technologies, and cloud data services at the file and event level. The EFSS Insight Engine audits and reports each event, for each user, on each device or service used. This information can be sent to existing enterprise security management solutions in real-time, which both accelerates awareness of potential data security incidents and allows administrators to predict and prevent future security lapses using data mining techniques.

Unmatched Security: File shredding and multi-layer encryption, over the wire and at rest, files are "chunked" and individually encryped and can only be reassembled by an authorized recipient with specific encryption keys.

Highly Granular Auditing for Threat Detection and Event Management: 's Insight Engine mines and aggregates file access, sharing, and storage data to detect and prevent costly security breaches.

Searchable, Cataloged Content: By creating a catalog of all files, EFSS enables secure file browsing, search, management, sharing, and access through a single interface.

Authentication: All individuals must be invited and authenticated before accessing any file, and all access events from any device are tracked and fully reportable on a per user, per file basis.

Unlike cloud services and file repositories, EFSS never stores or moves information in the clear—all files are shredded into chunks, and each chunk is encrypted individually before those chunks are stored or moved. As well, the passwords and keys to re-assemble files are never stored on EFSS servers.