EFSS with Secrata: Secure and Accessible Information Sharing for Ports and Transportation Infrastructure

challenge

Port Authorities must comply with broad and restrictive security regulations when accessing, transferring, and sharing sensitive information. Airports, ports, and railway transfer terminals face daunting security requirements; at the same time, they must be able to securely share vast and diverse information across federal, state, and local government agencies and between commercial organizations.

Securing the nation's transportation and shipping infrastructure against disasters, terrorism, and other security threats requires that organizations and individuals be able to securely and efficiently share sensitive information and files in in scheduled, *ad hoc*, and emergency or emergency situations. Using FTP, email attachments, and even many secure file sharing applications does not ensure proper security or support accessibility requirements.

Airport, port, and transport facilities operate in a cross-agency environment where security requirements differ and potential data sources and recipients change quickly. Information and data formats change, and in some cases, individual identities and privacy must be ensured. File sharing situations develop quickly, and the need to allow authenticated individuals access to sensitive information must not compromise that information's security. As well, the information must not be accessible to unauthorized users and cannot be vulnerable to security threats while being stored, accessed, or transferred.

Ensuring both security and accessibility under these conditions means that information must be both available and reliable, and it must be accessible on different devices and from multiple sources. All data and files must be protected beyond the individual enterprise—that is, a TSA official who needs access to security footage from an airport CCTV feed may need to access information from his office, a mobile command center, or in emergency situations, from his smartphone or laptop. Current secure file sharing applications and cloud services do not meet security regulations under these conditions. These same applications and services cannot ensure the accessibility of that information to the necessary array of individuals and organizations, across devices and from diverse sources.

EFSS with **Secrata**

Enterprise File Sync and Share (EFSS) with Secrata is a secure file sync and share service that meets the tight security requirements of the different federal and state regulatory agencies governing the nation's transportation and shipping infrastructure. EFSS allows individuals and organizations to share information securely across agencies and enterprises, from different devices, and stored in different locations.

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.

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's servers. This means that individual privacy is ensured: sensitive information cannot be hacked or accessed by unauthorized users.

When a airport, port, and transportation infrastructure officials must access and share data, EFSS with Secrata's multi-tier security architecture provides the security required by federal regulations and the accessibility that is essential in both scheduled and emergency situations.

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

Control of Your Own Cloud: EFSS allows all file content to be registered where it resides--on network storage behind an enterprise firewall, on mobile devices, and from other cloud services

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 files

EFSS at SeaTac International Airport

When a TSA official separates an individual during a pre-boarding airport security operation at SeaTac, CCTV footage of that individual often must be reviewed by different government agencies, including Customs and Border Patrol and DHS. In order to securely share that footage while preserving the individual's right to privacy, SeaTac uses EFSS to create a secure shared workspace where invited individuals may access and view the file footage.

EFSS efficiently supports the sequential security procedure required by TSA and DHS with a logical workflow. Within minutes of the event being captured on CCTV, a EFSS workspace is created containing the relevant footage and images, TSA attorneys are first invited to and authenticated by EFSS's multi-tier security system. Only after they authorize other users, including DHS or CBP officers and agents, can the footage be accessed and viewed. This ensures that airport and TSA procedures are followed, the individual's privacy is protected, and the necessary agencies can access the information they need to ensure the airport's security and safety.