

Egress Switch Secure Workspace

Offering internal users and external third parties access to documents and information, collaboration tools enable content to be shared easily and collectively worked on – delivering efficiency gains and cost-saving potential.

However, if inadequate encryption and access control mechanisms are put in place to safeguard the data, the risks can also be significant, resulting in costly fines and damaged reputation. Without audit functionality and end-to-end control over shared information, organizations have little or no visibility over precisely what has left their corporate network.



The benefits

- Enterprise file sync and share - secure shared data regardless of file size
- Real-time document creation and online editing
- Detailed audits and reports so you can track who is accessing your data
- Free for your third parties to use
- Real-time control over what a recipient can do with shared content, including date and time restrictions
- Flexible secure access across desktop and mobile devices
- Take decision-making away from end-users by enforcing centralized data protection policies including content control and sharing rules
- No infrastructure required to implement
- Brand in line with corporate guidelines
- Enhanced efficiency and cost saving by reducing the time taken to share data
- Role-based security policies
- Secure online document view provides restricted view-only access
- Bulk import secure content from .zip archives

Secure collaboration and online editing made easy

Switch Secure Workspace provides end-to-end data protection without compromising collaboration functionality. The service can be used to create open or closed communities of users able to securely share files and work together on joint projects, protected by sophisticated encryption and user permission controls. As well as offering online editing of documents, version control and messaging functionality, Switch Secure Workspace can be accessed from any internet-enabled device, supporting flexible collaboration from multiple locations.

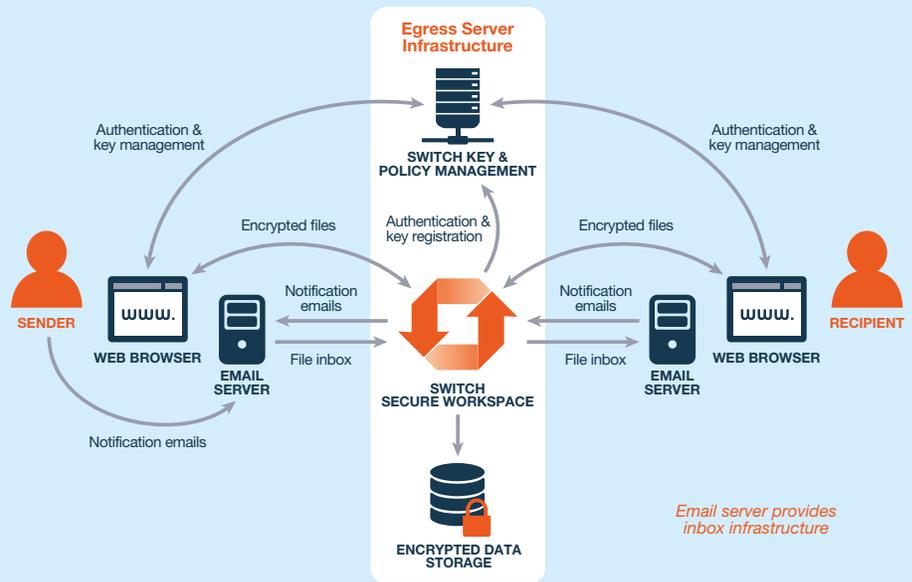
Sophisticated control over shared information

Switch Secure Workspace offers highly flexible granular permissions for individual users, as well as read-only and rights management control, ensuring only the intended recipients can access and edit shared information. This not only simplifies project management, but also means documents and data never leave your control, regardless of collaboration requirements.

Users can be added or removed from a secure workspace at any point throughout the collaborative process. Files can also be shared from within a workspace using a secure link that offers real-time control, including the ability to revoke a user's access. In addition, control over the file types that can be uploaded to a workspace extends the internal management and assurance over the information being shared from within an organization's network. The customizable user interface and branding options also ensure that every workspace reflects both an individual project's data sharing requirement and corporate guidelines.

Internal management and control

Each individual secure workspace offers detailed auditing and reporting functionality, including the date and times that users access, download, upload and edit files. This information can be exported to meet compliance and regulatory rules. Role-based security, meanwhile, means system administrators can remain in control of their users and their content at all times. These individual user permissions can be altered throughout the lifecycle of shared information as projects develop, and extend to online editing functionality to maintain security over ongoing projects.



Flexible system integration

Switch Secure Workspace integrates seamlessly with DMS and CMS systems, and email clients such as MS Outlook and Lotus Notes. In addition, the unique email address provided to each secure workspace enables content to be sent to the Secure File Inbox, from where it can be manually or automatically processed. In addition, Switch Secure Workspace supports single sign-on via Microsoft Active Directory using ADFS (Active Directory Federation Services) for internal users and for external third parties to provide unified identity management and streamlined access to secure collaboration functionality. This flexibility means users and groups can centralize all project files, resulting in a more efficient, more organized workflow.

Security overview

- Secures data at rest and in transit using AES-256 bit encryption
- Utilizes FIPS 140-2 certified libraries
- Secure authentication and user enrolment
- ISO 27001:2013 certified
- Skyhigh Cloud Trust™ rating of Enterprise-Ready
- Uses data centers accredited to ISO 27001/27018/9001
- Listed under Cyber Security Supplier to Government Scheme
- Patent protected (GB 0806429.7 | US12/353,390 | GB 0907665.4)

About Egress Software Technologies Inc

Egress Software Technologies is the leading provider of information security services designed to secure shared data from start to finish and delivered to customers in the Public and Private Sectors using a single platform: Egress Switch.

Taking a holistic approach to information security, the Switch platform is made up of highly integrated and flexible service lines that enable users to securely share and collaborate on sensitive data. These award-winning services include email and document classification, the only email and file encryption product to be CPA certified by CESSG, secure managed file transfer, and secure online collaboration.

Using patented key management, the platform utilizes a unique community-based licensing model that consists of paying and free Switch subscribers, who are able share information securely with one another using a single global identity.

