collabspace

Collabspace Content Security, Data Protection & Backup

Collabspace Network Security

Collabspace is a a multi-tenant SaaS solution built on top of Microsoft Azure with all data stored within Microsoft Azure data centers. All content sent to and from Collabspace is encrypted in transit using HTTPS with any modern browsers that support AES-128 or higher, such as Chrome, IE 11, Edge, and FireFox.

All external interfaces require authentication, either via Azure Active Directory or mutual authorization-code or token-based authentication. Any non-secure or non-essential ports are disabled. All communication occurs via HTTPS.

- **Data Segregation:** while all tenant-specific content is isolated on a tenant-by-tenant basis, tenants share the computing power of the service for purposes of activities such as content indexing and processing.
- **Content Connectors:** content is sourced from on-premises or cloud-hosted content repositories using an agnostic and extensible Collabspace Content Connector Framework.
- **Data Storage:** Content can be sourced through periodic crawling, real-time events, or a combination of both to ensure all content and version changes are captured in the secure Collabspace Content Storage System.

Azure Security Foundation + Additional Layers

While Azure comes with built-in controls and services, Collabware fortifies your content with additional protection measures, including:

- **User Permissions:** While Collabspace fully integrates with Azure Active Directory for authentication and authorization controls, Collabspace enables role-based access permissions for certain content.
- **Security Trimming**: Collabspace automatically trims search results to only the content the user has access to. Users will not see results or match counts for content that they do not have access to.
- **Content & Archive Security:** Collabspace utilizes a tenant-isolated encryption service to transparently provide encryption keys on a rotating basis, which are then used to individually encrypt BLOBs.
- **File Plan Security**: Each individual record category node within a file plan can be individually secured for both administrative and end-user purposes.
- **Versioning:** Each version of a file is stored as a separate Binary Large Object (BLOB) and individually encrypted to ensure maximum content recoverability and protection.

Prevent and Recover from Data Breach or Ransomware Attack

Create a secure backup of all content for your business continuity plan.

- **Immutable Storage:** content cannot be tampered with in Collabspace WORM Storage (Write Once Read Many).
- **Redundancy:** Collabspace automatically stores a geo-replicated copy of all content to ensure recoverability in the event of a Microsoft Azure data center outage.
- **Restore Data:** In the event of a ransomware attack or data breach of local storage, administrators can search and export the backup files from Collabspace.
- **Data Continuity:** Maintain productivity with little to no downtime and avoid costly measures for system repair.

Other Collabspace Security Features

Cloud-Based SIEM

A cloud-based SIEM is used to collect, store, monitor and analyze platform logging to prevent and audit security threats.

Data Encryption in Transit

All data is transmitted via HTTPS protocol. Internal components leverage mutual authentication when communicating.

Data Encryption at Rest

Tenant-isolated encryption service provides keys on a rotating basis and individually encrypts BLOBs at the client level.

Content Audit

All activities performed against content stored in the archive are audit tracked and the audit entries can be viewed for each individual content item.

File Plan Compliance Policies

Create & enforce one or more compliance policies within each record category using auto-categorization rules and enforce workflows.

Discovery Administrator

Admins can be designated so they can toggle between searching content only they have been given permissions for (default) or all organizational content.

Information Security at Collabware

Collabware staff have no access to any customer data, unless expressly granted by customer administrators. Internal policies are followed by Collabware's staff and Product Operations team, as documented as part of the SOC2 Compliance & Security Audit.

- Incident Management including staff education sessions on incident response activities, roles & responsibilities.
- Breach Management including staff education sessions on proper identification and reporting of potential or actual data breaches & response activities.
- Code of Conduct where staff are required to comply with IT acceptable usage policies & are made aware of potential sanctions for employee misconduct.
- Vulnerability Management including third party penetration testing to ensure system security & integrity.
- System Monitoring including event logging and notification of any component configuration changes, user login & system performance.
- Network & Operating System Security including how Collabspace requires Azure AD authorization for access.

Audit with Immutable Event Logs

All activities performed against content stored in the archive are audit tracked and audit entries can be viewed for each individual content item. Event logging within Collabspace cannot be turned off and tracks numerous activities, including:

- Authentication (success or fail)
- Component Startup/Shutdown
- Component configuration changes

Each log message for each component contains:

- Event date & time
- Event description
- Account ID
- End Result (success/fail)
- Error ID (if available)

Contact Us

See how Collabspace and other Collabware products can enhance your organization's productivity while ensuring compliance and content security. Please contact us for more information about our security measures.

collabware

www.collabware.com

contact@collabware.com

1-855-268-0442