

Security Overview



Syncplicity Business Edition delivers a highly secure and dependable file management platform built to meet the requirements of businesses. Ensuring customer data is safe and available are of the utmost importance. In order to achieve the goal of security, Syncplicity's service is built upon many years of experience and uses multiple levels of defense-in-depth to ensure end-to-end confidentiality of customer data.

Hosting Certifications

All of Syncplicity's servers are housed in data centers that have successfully completed a SAS70 Type II audit and testing from independent auditors. SAS70 certifies that each data center has met rigorous requirements around physical security, physical access, and internal controls.

Network and Storage Security

All data being transported or stored within Syncplicity is encrypted with the highest levels of encryption available for each phase of its lifecycle to protect files the moment they leave a client's computer. Data in flight and at rest are encrypted using military grade AES encryption set to its highest 256-bit level.

AES-256 SSL encryption is used for all authenticated website access, as well as client interactions with the service backend. No data is ever transmitted unencrypted over the internet.

To ensure client security, the client never opens any externally accessible port, communicates with any non-authenticated source, and stores cached credential information in an encrypted format to close three of the most common client attack vectors.

All files within Syncplicity are stored with AES-256 encryption using a strongly generated key that is unique to each file revision. In the unlikely case of a brute-force compromise of a

- AES-256 encryption of data during transmission and at rest in our data centers and on user mobile devices
- Data stored in four geographically dispersed SAS70 Type II data centers using high redundancy storage
- 99.999999999% data durability
- Encryption keys and data stored in separate data centers
- Internal controls protect user privacy
- Customer IT Controls and transparency protect user data

given key or a weakness found within the AES encryption algorithm itself, the combination of using the highest level of AES and a unique key per file revision substantially increase security by increasing the level of work required for a compromise and by limiting the potential scope of vulnerability to a single file revision.

All files are stored in quadruplicate across three data centers to provide 99.9999999999% durability for files and provide availability in the face of

the loss of two data centers. If a file is deleted, the encrypted file itself will be removed from storage and the related encryption key for each of its associated file revisions will be destroyed. When storage is decommissioned, all current providers use the techniques detailed in DoD 5220.22-M (“National Industrial Security Program Operating Manual”) or NIST 800-88 (“Guidelines for Media Sanitation”) to destroy the encrypted customer files as part of the decommissioning process.

Internal networks are kept clearly divided from external networks and are protected by industry standard firewall and proxy configurations to prevent unauthorized direct access.

Best-in-Class Mobile App Security

Syncplicity protects user data on mobile devices by using AES 256-bit encryption for data during transmission *and while stored on the mobile device*. Syncplicity Mobile Apps allow users to set 4-digit PINs in addition to their normal device password as an extra layer of security. Failure to properly enter the 4-digit PIN will automatically delete user data.

Syncplicity Mobile Apps can also be remote-wiped by users or Admins if a device is lost or stolen.

Two Data Center Policy

For an additional layer of security, Syncplicity maintains all servers responsible for authentication and encryption key management in a separate data center from the data centers housing the encrypted file

data. The encrypted file data and proper file version encryption key are brought together only on an as-needed basis and in a tracked manner. By keeping the encryption key completely separate from the file vault, Syncplicity provides a higher level of security by not having a single point of compromise.

Internal Syncplicity Controls

To ensure proper internal controls on access to customer files, employee access to the Syncplicity infrastructure is controlled and managed. Systems are monitored for security issues and software updates.

Syncplicity only provides data center access to employees who have a legitimate business need. When an employee no longer has a business need, access is immediately revoked. Additionally, no employee besides our VP of Engineering and our CTO have access to both authentication and key management data centers and encrypted file storage data centers to prevent any potential unauthorized disclosure of customer data.

Customer-controlled Policies

Syncplicity offers business several ways to protect data from loss at the user-level. The Syncplicity Security and Compliance Center in our Business Edition gives companies and their IT Administrators:

- Centralized control over which devices -- either computers or mobile -- inside or outside the company may be used to access,

sync and share files and folders, along with tracking of the sync and sharing of corporate data for compliance purposes.

- Easy enforcement of data retention policies, enabling shared files and folders to be automatically and permanently deleted from user devices when that information is un-shared with a user, whether they are an employee, contractor or anyone outside of the company.
- The ability to remote wipe any user’s account, their individual computers or mobile devices of all corporate data managed under Syncplicity associated with a user or particular device, in the event a device is lost, an employee is terminated, a contractor is finished with their assignment, or for any other information compliance reason.
- Native support for single sign-on (SSO) against any SAML or OpenID based federated identity provider to enable use of existing credentials such as Active Directory/LDAP, Google Apps, and OneLogin, including optional 2-factor authentication.