

Box

Competitive Guide

Egnyte Enterprise vs. Box Enterprise Advanced

THE BOX PRODUCT AND COMPANY NAMES MENTIONED IN THIS DOCUMENT ARE TRADEMARKS™ OR REGISTERED® TRADEMARKS OF BOX. USE OF THE NAME DOES NOT IMPLY ANY AFFILIATION WITH OR ENDORSEMENT BY THEIR OWNERS. THE OPINIONS EXPRESSED ABOVE ARE SOLELY THOSE OF EGNYTE, INC. AS OF April 2025, AND EGNYTE, INC. MAKES NO COMMITMENT TO UPDATE THESE OPINIONS AFTER SUCH DATE.

Table of Contents



Quick Look



Why We Win



Positioning

Quick look



Our strengths

- Desktop app with drive letter support
- Granular subfolder permissions
- Central shared link management portal
- Appliance-based hybrid caching
- Full administrative control over external users
- S&G covers Egnyte & 3rd party repositories
- Pre-validated GxP environment + eTMF
- Snapshot-based ransomware recovery
- Support for 3rd party storage



Their strengths

- 1 500+ pre-built integrations
- Box Hubs serves as both a multi-file Q&A (with Box AI) and an intranet-lite solution
- Event-based automation module (Box Relay)
- Proprietary notes & whiteboard apps (Box Notes & Box Canvas)
- Self-serve migration (Box Shuttle)

Why We Win

Top 3 reasons why we win

1. **No drive-letter experience on desktop:** Due to the vastly different approach in implementing their Desktop App, it doesn't connect to the OS as a drive but as a catalog under the local user account. Due to this approach, applications/files that use paths to cross-reference locations (like macros in Excel) won't work for anyone else but the user who created them.
2. **No option of governing 3rd party repositories:** Only Box is covered, so additional solutions are required if data is stored in other repositories.
3. **Lack of granular subfolder permissions:** Box uses the *waterfall* permission model, where child folders always inherit permissions from their parents. Therefore, users must create folders on a higher level than necessary to prevent unauthorized users from accessing data. This approach can easily lead to data sprawl, challenging management and user experience.

Their other main weaknesses

1. **No hybrid caching:** This is especially important in locations with low-bandwidth internet access or many users accessing the cloud simultaneously
2. **Only one shared link per file:** Due to their architecture, only one shared link can be created per file. This can cause many problems, ranging from daily inconveniences (e.g. not being able to use the same link for internal and external users) all the way to potential data leakage (e.g. in time-sensitive access scenarios)
3. **No central shared link management dashboard:** Admins can't easily manage shared link security; In Box, admins must generate multiple .csv reports and review each link individually.
4. **Limited control over external users:** External users can be granted the same collaborator access and sharing rights as managed users, but your control over the content they own and their security settings are limited.
5. **Limited ransomware self-recovery capabilities:** Box doesn't have the capability to rewind the state of a repository to a certain date, which is especially useful after being struck with ransomware. While Box's support can help recover files, it may take them weeks to do so unless customers pay more. Importantly, Box doesn't have a comparable solution to our snapshot-based recovery.
6. **No support for 3rd party storage:** Box Zones is designed to meet customers' data residency requirements. However, it does not support integrating with third-party storage providers, such as Amazon S3. This may create problems for businesses already under contract with another storage vendor.

Limited data governance capabilities	Hampered productivity	Challenging management: External collaborators & data	Limiting architecture
Issue 1: No option to govern data stored on-prem nor in 3rd party cloud systems Issue 2: Box themselves encourage more demanding customers to use third-party CASBs to govern their data Box: For large organizations that often use multiple cloud EFSS platforms, the option to govern these sources with one solution is important to improve visibility and assure the same high level of security. Box recognizes this, but instead of extending its coverage, it promotes the use of third-party solutions to govern its data, which can significantly increase company operational costs. Their solution also offers fewer PII detection patterns than Egnyte. Egnyte: Egnyte enables organizations to execute comprehensive data management strategies that include a flexible collaboration platform, a full set of data governance controls, reporting, ransomware recovery, alerting, AI features, and more. Thanks to this, customers get the most out of their data while driving down risks and management-related costs. Moreover, in addition to PII, Egnyte can also detect the type of documents and prevent them from being shared outside of the company without control.	Issue 1: No automatic global file locking Issue 2: No drive letter on desktop Issue 3: No local folder backup Issue 4: No shared link management portal Issue 5: Only one shared link per file Box: The lack of a drive letter and automatic file locking negatively impacts day-to-day productivity, leading to conflicting versions and incompatible cross-references. This is further exacerbated by the lack of a shared link management portal, which hinders visibility into shared resources’ consumption. Additionally, in case of a device failure, the lack of the option to back up local folders can lead to situations where crucial data might be lost. Importantly, users can only create one shared link to files residing in Box (!) Egnyte: Egnyte offers all of the aforementioned options, immensely improving the day-to-day user experience by smoothing the way they work and securing information that otherwise usually wouldn’t be backed up, such as important programs’ config files.	Issue 1: External users use individual Box accounts Issue 2: SAR is not a native capability Issue 3: No full retention capabilities – no archiving Box: Box requires third-party apps for automated data privacy/SAR report delivery, which increases the cost of their overall offering. The lack of archiving increases the available attack/leakage surface, especially since external collaborators’ accounts are standalone Box accounts, preventing admins from controlling them to the same extent as company accounts. Egnyte: Egnyte’s Standard User role allows companies to enable external collaboration while preserving all control options over these accounts, as they are entirely contained within their Egnyte domain. Archiving saves space, reduces the attack/leakage surface, and helps companies comply with local regulations. This is accompanied by the native option to process Subject Access Request events, allowing companies to remain fully compliant with the highest data protection standards, such as GDPR or CCPA.	Issue 1: No snapshot-based recovery Issue 2: Very limited number of supported data storage regions Issue 3: No support for 3rd party object storage Issue 4: No hybrid solution Box: Having the option to recover from a ransomware attack seamlessly is crucial. The same applies to compliance with data sovereignty regulations. Box’s customers can have issues with both of these things as Box Zones introduces additional costs, doesn’t support linking 3rd party object storage, and doesn’t have the option to revert the state of the repository without engaging the support team. Egnyte: Egnyte offers snapshot-based recovery, enabling repository restoration to specific dates without requiring support team engagement. Thus, it frees CIOs from ransomware remediation worries. Moreover, because Egnyte natively supports a wide range of data storage locations, connections to third-party object storage, and an appliance-based local caching solution, companies have greater flexibility in configuring their environments.