BSafes Solution

Secure Note-taking Web App with
End-to-End Encryption for Teams & Individuals

TABLE OF CONTENTS

INTRODUCTION AND BACKGROUND

The emergence and growth of mobile devices, as well as their portability nature, offers favorable conditions for use in taking notes. With this regard, vendors have developed a large range of note-taking apps for end-users. Note-taking apps offer real benefits to diverse users, such as engineers, secretaries, and innovators who wish to document aspects of their lives and work for future reference.

In some cases, mobile devices come bundled with note-taking software. However, such default programs have limited to basic features, such as typed-in text. As a result, other innovators have captured this opportunity to create feature-packed note apps to meet advanced user needs, such as handwriting and sketching input as well as adding media files, such as audio, images, and videos. Users can synchronize the note-taking apps between all their devices. In some cases, the apps enable collaboration and working with teams.

Regardless, the same note-taking apps that offer convenience also introduces security issues. Users are now concerned about the steps the apps developers take to ensure that hackers are not infiltrating on their interactions with the apps or unauthorized people are not accessing their notes.

THE SITUATION: IS YOUR NOTE-TAKING APP MEETING SECURITY AND PRIVACY NEEDS?

As already stated, many players develop and offer note-taking apps to fill the void of basic feature software. They develop advanced applications with awesome features to meet the needs of end-users.

Individuals and teams have stored sensitive information in the apps. A study by DuckDuckGo found that 45.3% of users have saved one or more of the following in a note-taking app:

- Username
- Password
- Social security number
- Credit card information
- Security or PIN codes

Unfortunately, 58.2% of users were not aware that their note-taking apps do not encrypt their data by default.[1]

This fact is alarming, considering that most note-taking app developers do not encrypt their application operations by default.

Some of the issues with the apps include:

[1] https://spreadprivacy.com/privacy-risks-note-apps/

INCREASED CYBERATTACKS ON NOTE-TAKING APPS

Deplorably, a good number of note-taking apps are affected by all sorts of bugs and design caveats that present potential openings for cybercriminals and unauthorized access.

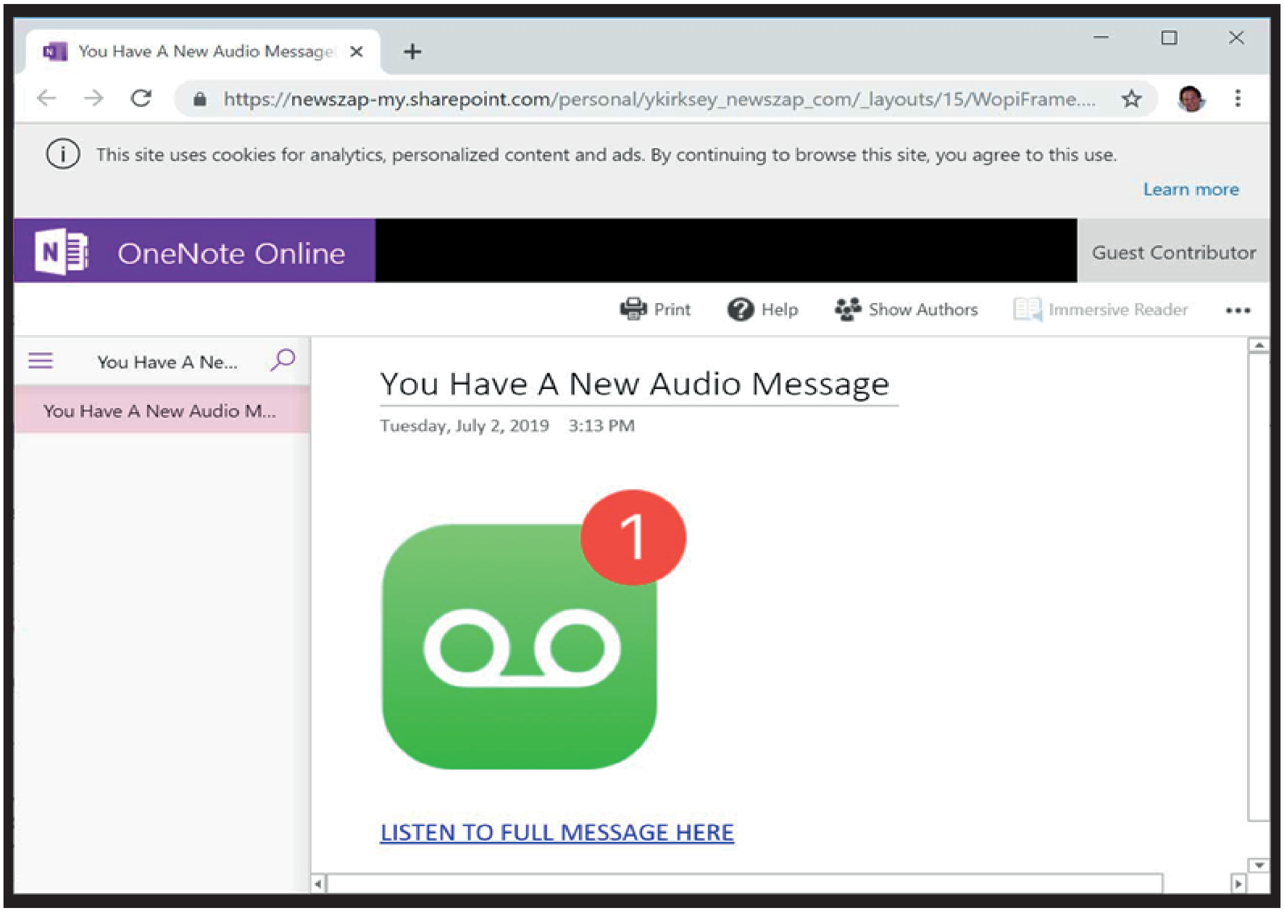
REPORTED INCIDENTS WITH NOTE-TAKING APPS

Windows allegedly discontinued its note-taking application, the Windows Journal that allowed users to create and organize handwritten notes and drawings. In a release published on their website on September 13, 2016, Windows revealed that the "file format that is used by Windows Journal (Journal Note File, or JNT) has been demonstrated to be susceptible to many security exploits.[2] As a result, the vendor removed the application from all versions of its products.

Wryly, Windows recommended users to download OneNote as a substitute for their obsolete app. In July 2019, Bleeping Computer uncovered a fake OneNote audio note phishing attack. In this incident, scammers devised innovative methods to convince victims to reveal their login credentials. They send emails with the subject "New Audio Note Received" and they indicate that the email originates from a contact in the target's address book.[3] Once the unsuspecting victim clicks on the link to listen to the audio message, they are redirected to a fake OneNote online page hosted on Sharepoint.com

[2] https://support.microsoft.com/en-us/help/3161102/update-for-windows-journal-component-removal

[3] https://www.bleepingcomputer.com/news/security/beware-of-fake-microsoft-onenote-audio-note-phishing-emails/


You Have A New Audio Message
https://newszap-my.sharepoint.com/personal/ykirksey_newszap_com/_layouts/15/WopiFrame....

This site uses cookies for analytics, personalized content and ads. By continuing to browse this site, you agree to this use.

Learn more
OneNote Online

[redacted]

Guest Contributor
Print
Help
Show Authors
Immersive Reader
You Have A Ne...
You Have A New Audio M...

You Have A New Audio Message

Tuesday, July 2, 2019 3:13 PM

LISTEN TO FULL MESSAGE HERE

Figure 1: Fake OneNote online page used for phishing attacks

Scammers hoodwink users to provide their Microsoft login credentials in a fake page that appears like the ones for Microsoft services, such as OneNote, Outlook, and Office 365.

In a different incident, a cross-site scripting vulnerability in Evernote's Web Clipper Chrome extension allowed hackers to infringe active sessions of other websites in the same browser.[4] The June 2019 note-taking app's flaw created an opportunity for criminals to execute code that allowed them to perform actions without the user's knowledge. Consequently, hackers gained unauthorized access to sensitive user information on affected third-party services and websites for more than 4 million users.[5] This information includes confidential information, such as financial details, user credentials, personal emails, and social media conversations. Evernote responded with a patch four days after learning about the vulnerability.

[4] https://arcticwolf.com/resources/blog/a-chrome-extension-vulnerability-exposed-4-6-million-evernote-users-to-potential-cyberattacks

[5] https://spreadprivacy.com/privacy-risks-note-apps/

DATA PRIVACY CONCERNS

One question that lingers on a user's mind is, can note-taking app vendors access my notes and other data in their software? The answer is yes, for the following obvious reasons:

1. Lack of End-to-End Data Encryption

A common issue in most note-taking apps is no protection at all. Most of the programs store notes in plaintext, despite the fact that users sync them between their devices. On the other hand, some tools allow only partial encryption, and limited use cases.

Encryption keys stored on the vendor's server, making the architecture weak and susceptible to attacks.

2. Encryption at Rest – Weaknesses

Most cloud-based note-taking apps offer encryption at rest as a way of securing users' information. Sad to say, this form of securing data that occurs at the service provider's data center could potentially allow the developer to view and analyze user information for their business needs in roles such as engineering, marketing, government order, and so forth.

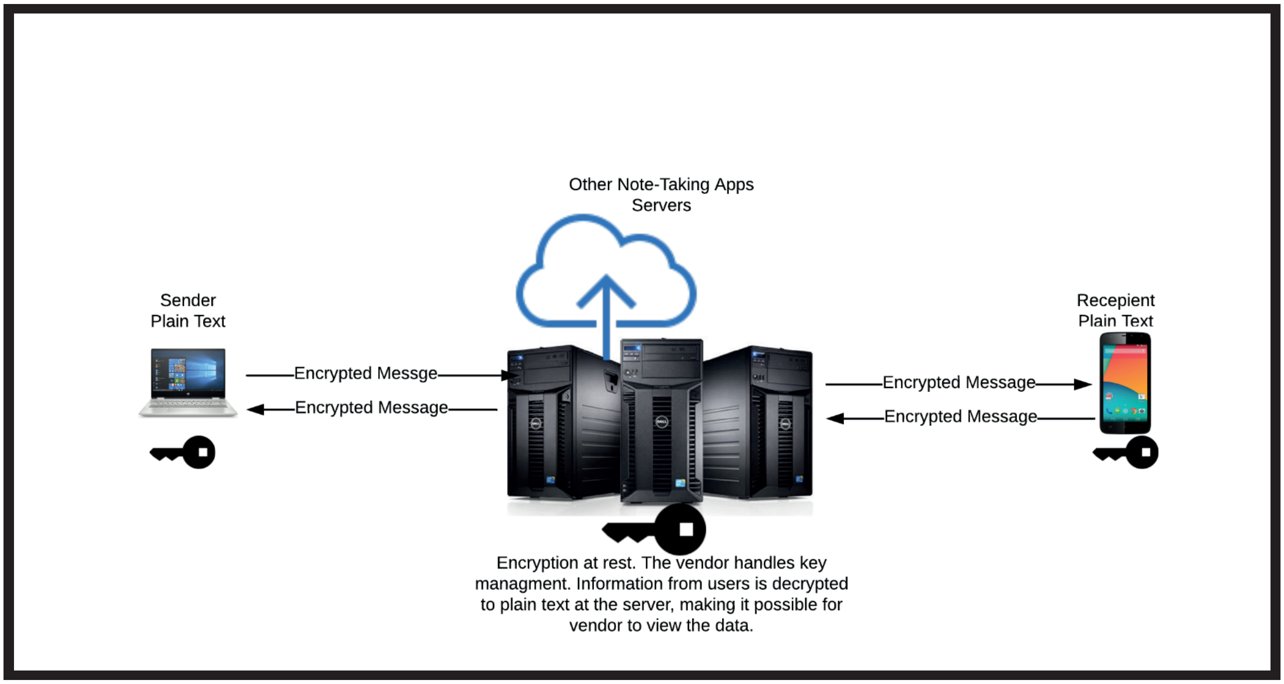

Other Note-Taking Apps Servers
Sender Plain Text
Encrypted Messge
Encrypted Message
Recepient Plain Text
Encrypted Message
Encrypted Message
Encryption at rest. The vendor handles key managment. Information from users is decrypted to plain text at the server, making it possible for vendor to view the data.

Figure 2: Encryption at rest – Vendor handles key management, can as well view user information in plain/original text

COMPLIANCE REQUIREMENTS

Governments and privacy advocates around the world are pushing for laws and regulations to protect users' data. Good examples include the European General

(GDPR), California Consumer Privacy Act of 2018, and the Asia Pacific Data Protection and Cybersecurity Guidelines.

These regulations require businesses to secure users' data with the strongest protection measures possible.

COSTS

Going premium with existing note-taking apps that have invested in appropriate security and data privacy measures costs an arm and a leg for users in the long run. On the contrary, free versions of the tools feel like trial versions with limited features such as limited device synchronization, a small upload limit, lack of email forwarding, and no access to notes while browsing offline.

LACK OF ESSENTIAL FEATURES

Some note-taking apps lack crucial features for teams and collaboration capabilities.

BSafes: THE SECURE NOTE-TAKING APP FOR TEAMS AND INDIVIDUALS

For all note-taking apps users concerned about their data privacy and security, they may need to rethink their use of the programs. From the analysis above, a bunch of the existing apps have a tainted reputation with privacy and data security. Individuals and teams, in view of this, should recourse to an encrypted note-taking app for their needs.

We introduce BSafes, the secure note-taking app for teams and individuals, with end-to-end encryption. The BSafes App is designed from the ground up, open-source client-side using no additional proprietary software, to help seal the holes along the information highway where crucial user data travels. In this case, the solution protects information from slipping through cracks or getting exposed to unauthorized users.

BSafes Note-taking App provides an information-sharing service that restricts access through industry-standardized hard to crack methods and is compatible with devices running on diverse technologies and environments. With BSafes, teams can work together while enjoying maximum data protection provided by end-to-end encryption from the sender to the recipient.

What benefits does BSafes offer its users?

End-to-End Encryption with AES 256 Bits

Existing note-taking apps do not offer end-to-end encryption. For this reason, the apps are only suitable for general note-taking activities that would not cause harm to a business or individual in case of a data breach.

However, in case a user needs to take notes on confidential information, such as trade secrets, and sensitive data (usernames, passwords, financial details), they require an extra layer of protection. Individuals and teams can achieve this requirement through automatic encryption of all data before the app transfers it to the cloud. In effect, no other unauthorized users can retrieve or modify such information.

With BSafes, users achieve increased security levels through end-to-end encryption applied to all contents in a note, unlike in other apps that only allow you to encrypt only private information, such as personal details and account credentials.

In this case, BSafes App deploys an open-source encryption standard audited by security specialists to scramble plaintext data in notes and render it unreadable to anyone, including cybercriminals and the vendor, who does not have the decryption key that is usually a password or a passphrase. In this case, even the third-parties, such as system developers, administrators, and cloud service providers, cannot access or modify the encrypted data. This restriction also includes people at BSafes.

WhatsApp messaging service also uses end-to-end encryption to protect data sent in text messages from user to user. As a result, unintended recipients cannot see the message before it arrives at the destination. However, WhatsApp does not offer the range of note-taking services that BSafes provides.

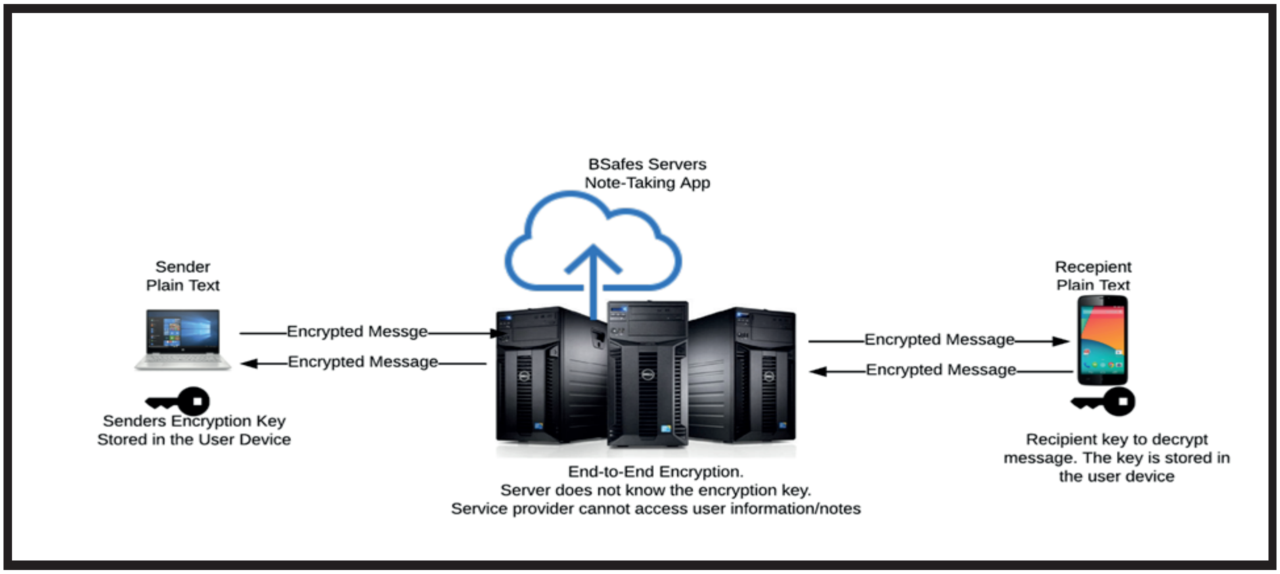


Figure 3: BSafes End-to-End Encryption

ENCRYPTION KEYS STORED ON USER SIDE

Of course, BSafes responsibly secures user data and notes in various ways, with the main one being storing everything encrypted. However, in case hackers get their hands on the encryption keys, they can effectually decrypt the ciphertext back to the original plain text.

On this ground, the BSafes app design allows the storage of encryption keys on the user's side. Anyone sitting between the user and the cloud cannot access the encrypted data.

During the sign-up process, users create their key that BSafes uses to encrypt data. To maximize data protection, BSafes allows users to own the key, instead of sending it to the server. You can also keep recreating your key. If you lose your key, you cannot see your data, and BSafes cannot recover it. Hackers also will find it impossible to get hold of the key.

OTHER BSafes FEATURES

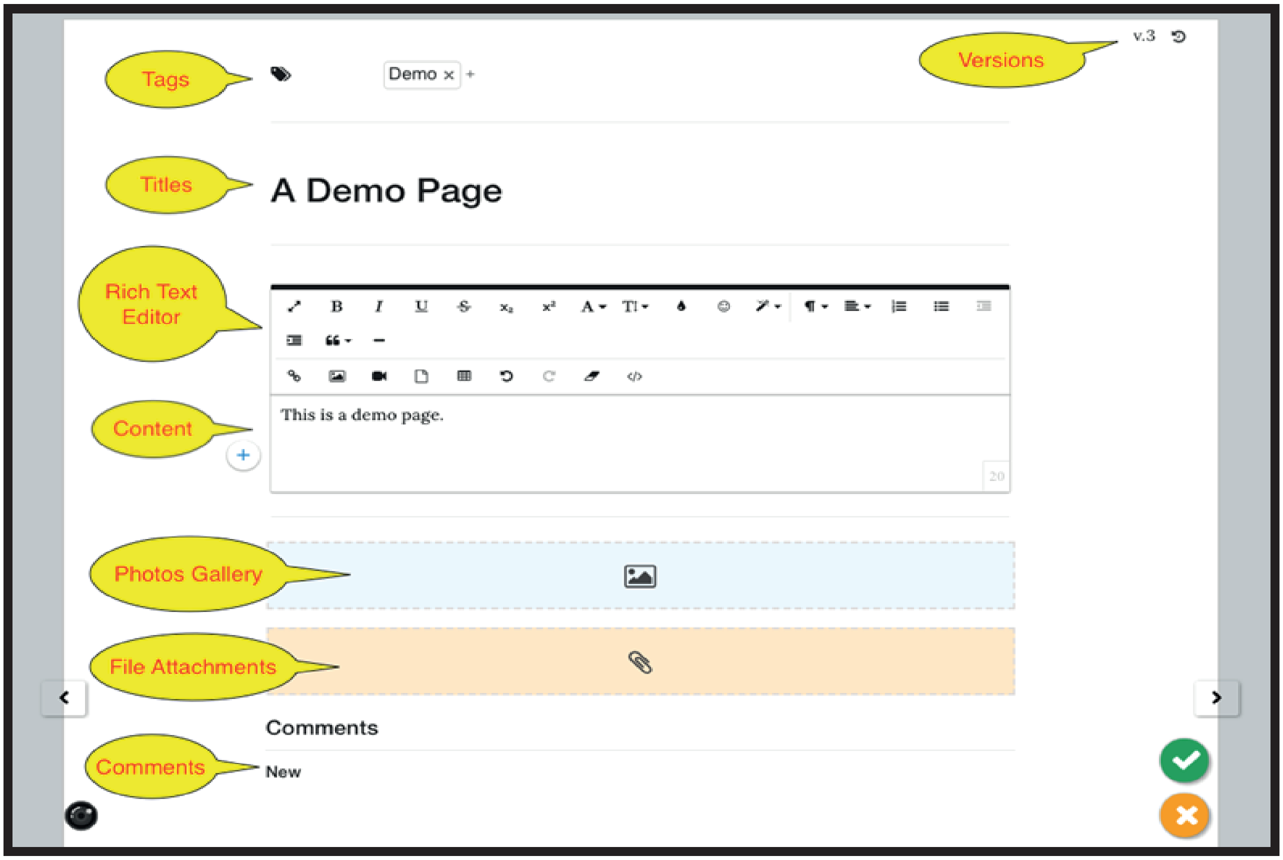
1. Enhanced Collaboration Capabilities

BSafes is designed for teams from the ground up. The app enables team collaboration in a dedicated workspace. Only team members could read and write notes in a team workspace. In one BSafes' account, a business user can have as many members and teams as you need.

An account owner can add as many members as needed using BSafes. Each member has his or her workspace, and own key to encrypt and decrypt data. Any member could invite other members to a team. Team members collaborate on a dedicated workspace where they could read and write shared notes.

Other members of the same team, however, cannot view the contents of a personal workspace. Simply stated, no other member could read your pages without the encryption key.

By establishing the team and member structure with known individuals within a network, and relying on the end-to-end encryption model, team members can administer the data accordingly in the same way they would walk right up to a person and pass a note to them palm-to-palm in a handshake gesture. The information transfer remains unseen, unknown, and hidden to everyone apart from the participants. The one stop made between the message source and the intended destination is the air between the shaking hands. In the BSafes scenario, this happens to be the server space. It is where most companies have fallen into spotty blunders in terms of data privacy and security.



v.3

Demo

A Demo Page

This is a demo page.

Comments

New

Figure 4: A Sample BSafes Note Page

2. Powerful Search and Sort Capability

Users could search pages using titles or tags. Interestingly enough, BSafes also encrypts page tags and titles, so no one could suspect the content in pages based on the title and tags used to reference it.

BSafes breaks down every item's title into words and encrypts them into searchable tokens. Users can type the titles to search for an item.

Another fascinating feature is the diary. BSafes orders pages in a diary by dates. In effect, users can view the contents of the diary sorted by dates. You can jump to a specific day by selecting the date.

3. Media-Rich Content on BSafes Notes

Users could add title, media-rich content, photo gallery, audio, video, and other file attachments on a page. BSafes Note-taking software generates notes that can have media-rich content such as audio and video files, interactive photo galleries, and other miscellaneous file attachments, such as compiled executables for programming activities.

You can also add comments on a page regarding work orders, tasks, roles, or timetables to provide updates on the team member who worked on each page last, as well as the tags.

The app allows users to attach up to 100 files with a size of 500 MB on a page.

With all this, BSafes offers the WYSIWYG standard, which is a rich text editor for in-line editing of complex notes. The standard allows users to create bullet lists, tables, and writing with diverse formatting options for improved readability.

4. Easy Navigation

For every item, on the upper left corner, you can see the path that leads to the current item. The tool offers features that help users t navigate within the same container and to next or previous pages of a notebook.

5. Compatibility

BSafes is compatible with all modern HTML 5 browsers on Windows, Mac, Linux, iOS, and Android. Besides, it works on all devices and computers with modern browsers.

Unlike other note-taking solutions that work as independent tools, BSafes features incorporation with different software like inside interchanges programs and calendars, and other outside applications, such as Invision and Sketch.

6. Organization

Similar to a physical workspace, BSafes offers boxes, folders, notebooks, and diaries for users to organize their pages. Besides, members have their workspace, while a team has a dedicated team workspace.

Unlike a folder that contains only pages, a box could contain all items, such as pages, notebook, diary, folder, or even another box. Users can view contents in the box to identify all the items stored.

7. Offsite Backup

BSafes provides a desktop app that allows users to download personal and team notes to a local computer for offline backup and offline reading.

8. Themes, Actions, and Editors

Users also get access to additional adjustable themes for tweaking the appearance based on their tastes. Besides, BSafes offers powerful and custom editors for working with Code, Markdown, and different features like custom textual styles, colors, alignment, tables, and so forth for making rich documents.

BSafes USE CASES

There are many applications for BSafes Note-taking software. Since the app is optimized for data security, scalability, and affordability, it is ideal for major high-fidelity media projects, remote-operation filming, and video production.
The freedom of file type inclusion means any industry or profession can make use of the service so long as they have a need to share ideas or work among teams of people across the Internet.

BSafes COSTS

BSafes is highly affordable. The product costs only $2.99 per month per account for unlimited members and teams. Unlike in other products, BSafes charges fees based on account usages, and not by the number of teams or members.

For $2.99 a month, users get the following features and benefits:

- Unlimited members
- Unlimited teams
- Unlimited upload bandwidth
- 10 GB storage
- 5 GB download bandwidth
- 5,000-page versions

Users could also buy extra quotas for $0.99, which includes an additional 10 GB storage, or 5 GB download bandwidth, or 5,000-page versions for the month.

GET STARTED

Users can simply access BSafes at **www.bsafes.com** and register using their email, google, or facebook account. The system requires you to create a key that BSafes will use to encrypt all your data.