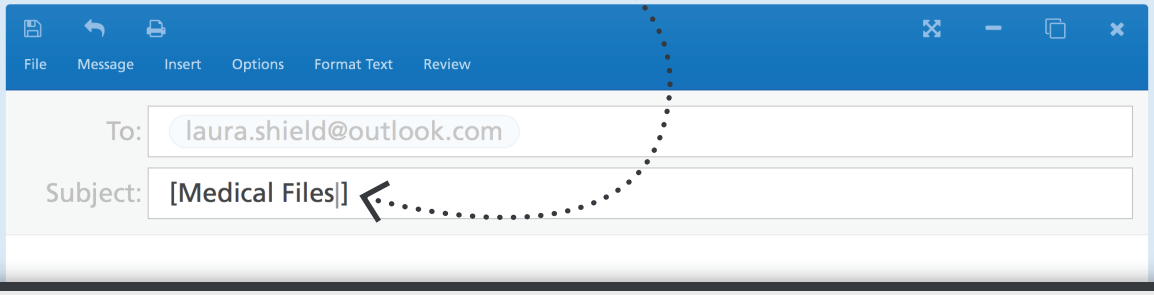
Bracket® Encrypted Email

Bracket is painless email encryption

Email encryption has a reputation for being a pain to use. You have to create an account, download and install an app or plugin, open the app, sign in, and finally create and send thier message. Then the recipient on the other end has to repeat all the same steps just to read the message. Bracket is so much easier to use. **To securely send an encrypted email from any email client on any device just wrap the [subject] in brackets.**



The best of both worlds!

Maximum Security

- ✓ *Multi-layer AES-256 encryption*
- ✓ *Compliant with HIPAA, FINRA etc.*
- ✓ *Two-factor authentication*
- ✓ *Distributed encryption keys*
- ✓ *Geolocated sign-in requests*
- ✓ *Message expiration and recall*
- ✓ *SMTP TLS import/export gateway*

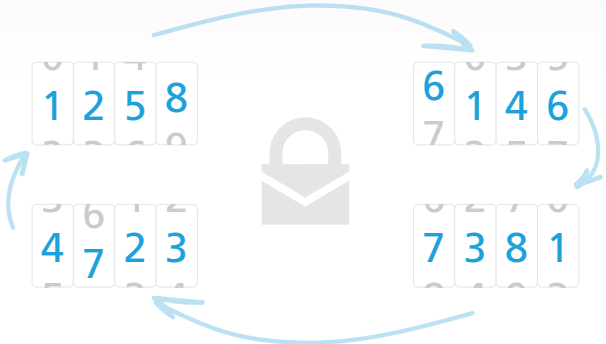
AND

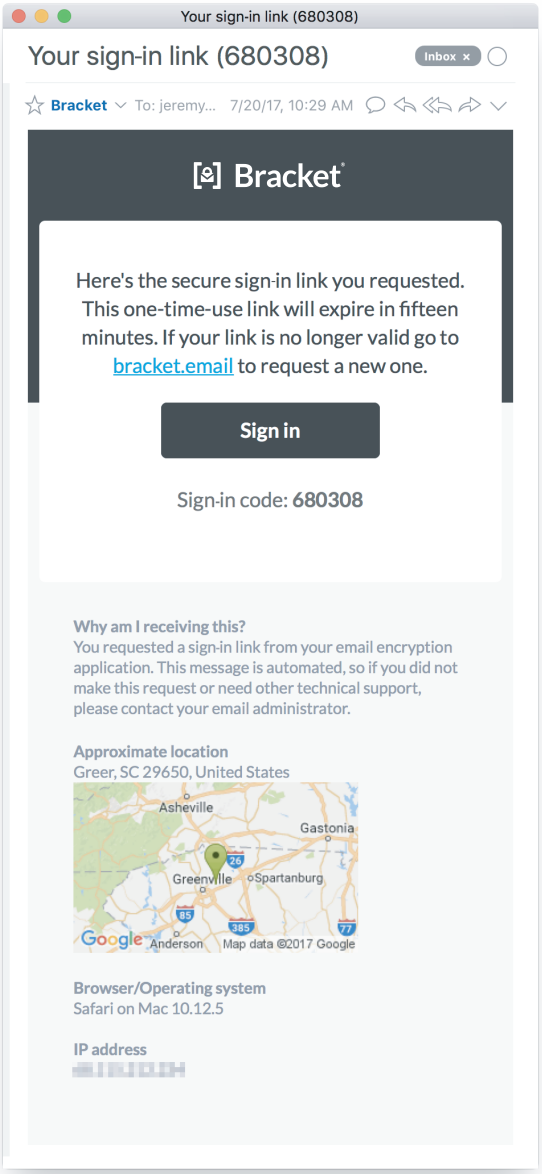
Ease of Use

- ✓ *Nothing to install*
- ✓ *Password-free sign-in*
- ✓ *No recipient account creation*
- ✓ *Send from any email client*
- ✓ *Personalized notifications*
- ✓ *Large attachment sending*
- ✓ *Built for mobile and desktop*

Exceeds compliance standards

Don't let Bracket's ease of use fool you. The encryption methods used by Bracket **satisfy even the most stringent compliance standards such as HIPAA and FINRA**. Bracket is built on a distributed, multi-layer AES-256 encryption design with automatic key rotation... the same kind used by the NSA (National Security Agency).





Inbox authentication

Lightning fast sign in without sacrificing security

Securely sign in without a password

Simply request to sign in using your email address, then click the secure link from your inbox (the same way password resets are handled most of the time). Bracket bakes in extra security so it's actually more secure than password logins.

Expiring, one-time-use links

Bracket sign-in links expire 15 minutes after being delivered. In addition, each sign-in link only works once, so you never have to worry about someone rummaging through your inbox and opening old links.

Geolocation of sign-in requests

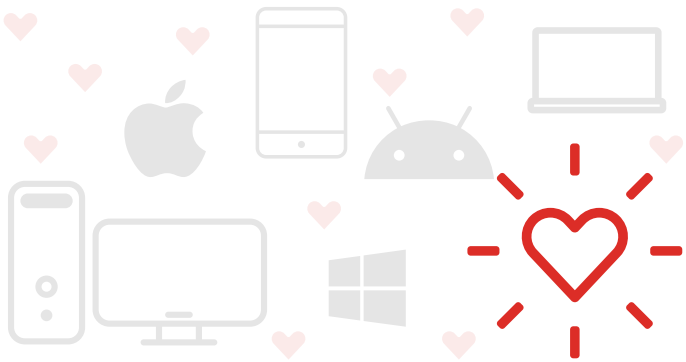
As an addional layer of security, sign-in request notifications also include the requesting device IP and approximate location.

Advanced device fingerprinting

Sign-in links will only work from the device that originally requested access. If a different device attempts to sign in, the link is invalidated and the session is blocked.

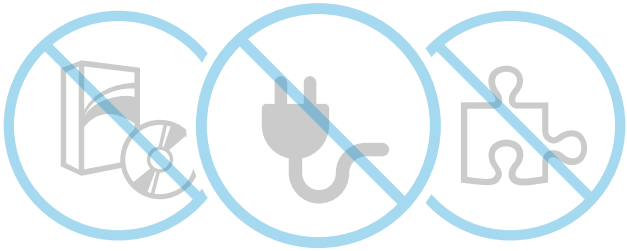
Send from any email client

Email encryption is usually constrained to a specific operating system or mail client, but Bracket frees you up to send encrypted email from literally any email client. So whether your users prefer iPhone, Android, Windows, Linux, or PC (or maybe they just can't let go of their Blackberry)... it simply doesn't matter with Bracket.



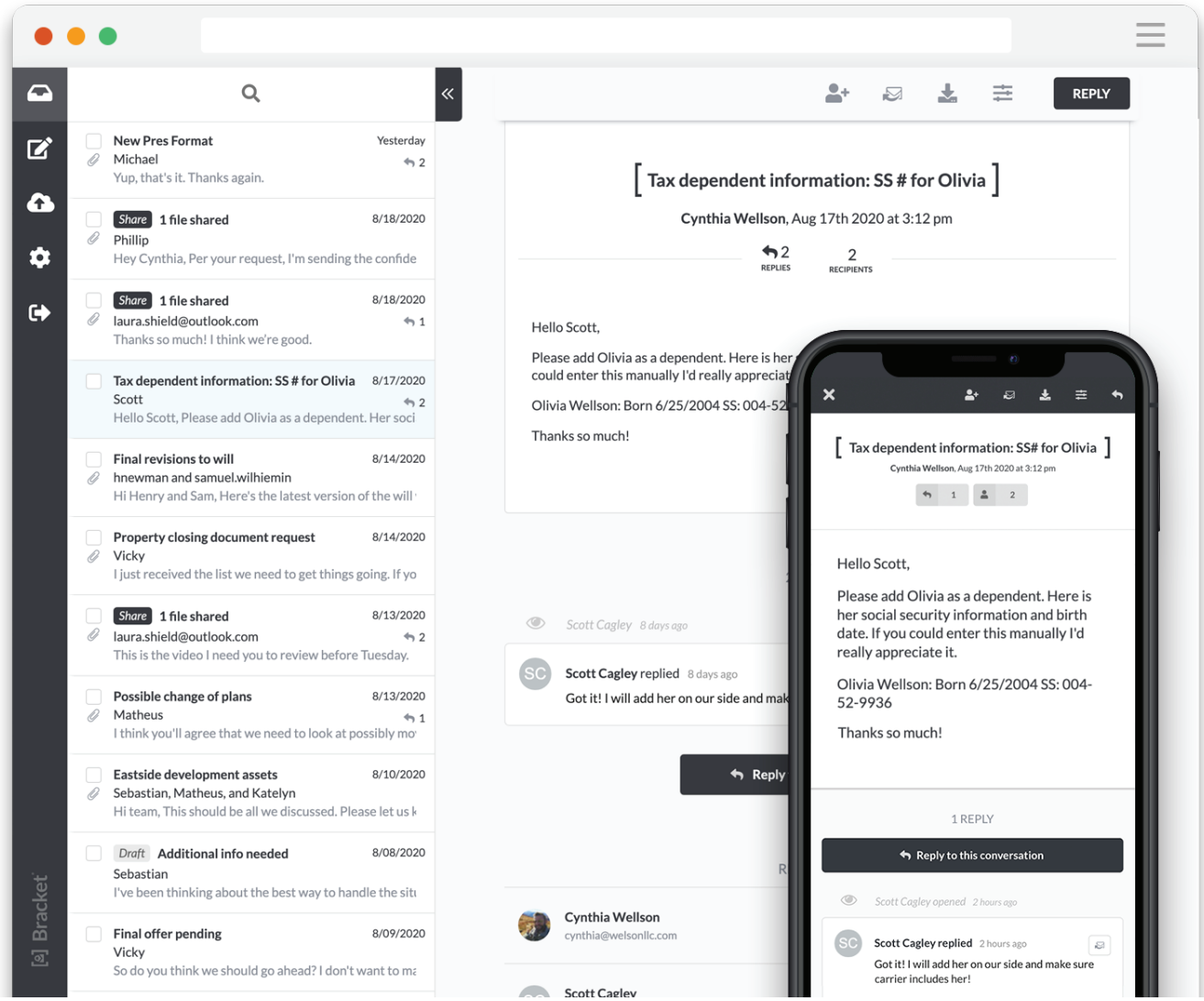
No apps or plugins to install

Most encryption solutions rely on downloading and installing numerous apps and plugins depending on where you're sending from, but Bracket takes a different approach. To send an encrypted email with Bracket, just wrap the subject in brackets and send it on its way. It's really that simple.



View and create messages in the intiutive UI

The Bracket user interface cuts out the clutter for an enjoyable user experience.

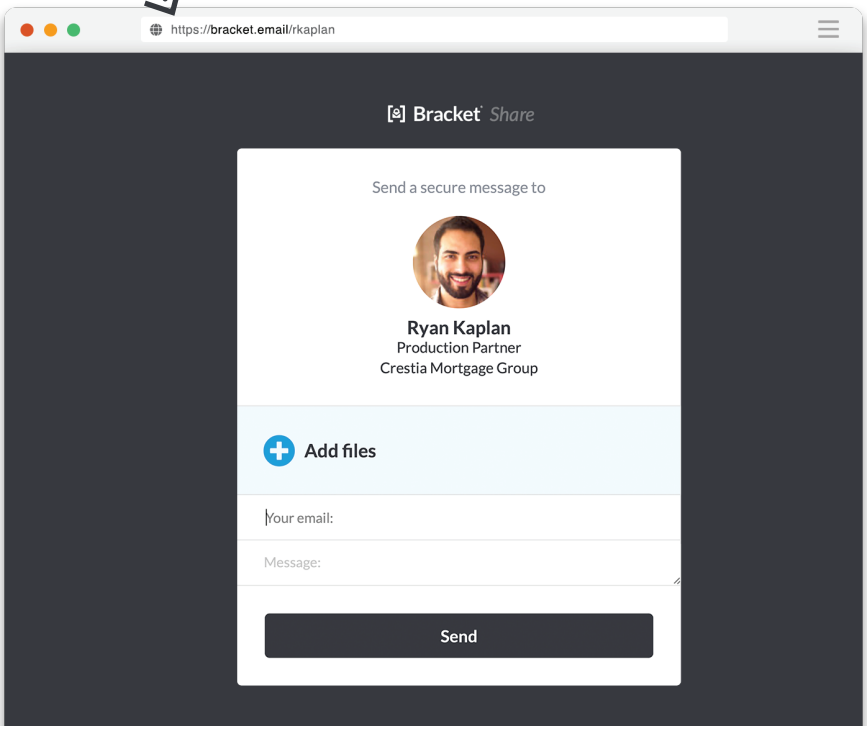


Includes an encrypted file transfer page for every user

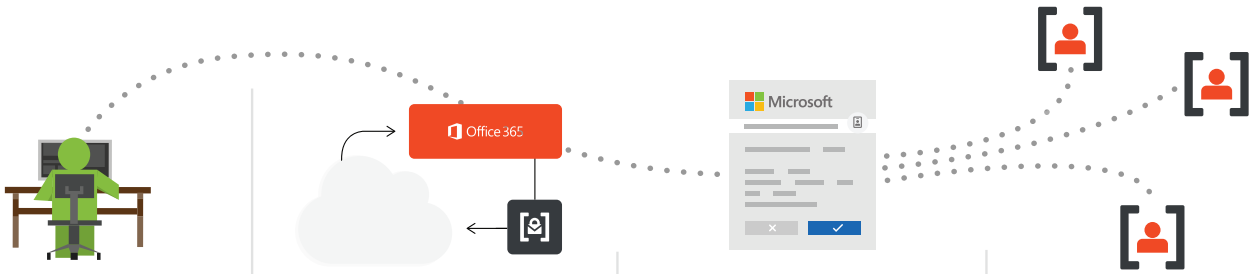
Just give your personalized share link to anyone you trust

Included with Bracket is our encrypted file transfer service, Bracket Share. This gives users their own personalized file transfer page with a simple URL they can give to anyone. When files and messages are shared through a share page, the recipient is notified and the message is added to their Bracket inbox with the files attached... just like a regular Bracket message.

- **Easy, customizeable share link**
  Make a share link that fits you, so it's easy for contacts to recognize and remember.
- **Personalized with your profile**
  Your profile builds visual trust so your contacts know where their files are going.
- **Up to 25 1GB files per share**
  Share as many as 25 huge files at once without worrying about storage limits.
- **Built-in abuse prevention**
  Shares are validated with Bracket's inbox authentication to block unwanted senders.



Instantly add to Office 365 with no MX changes



1
Add a new domain in the management console.

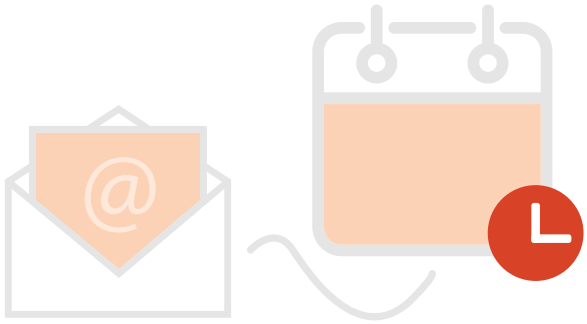
2
Choose the Office 365 option with no MX.

3
Authenticate using secure Microsoft verification.

4
Watch as Bracket automatically deploys to O365 users.

Ephemeral message storage

Sensitive data shouldn't default to being kept forever. With Bracket, all data is temporary and there are no mailbox quotas to keep track of. Just send and receive secure messages and go on with your day. By default, messages expire in 1 year, but you can set any message to expire sooner if you wish.



We've also made it easy to securely get your data out of Bracket and back in to the other email systems you use that are designed for retention, discovery, and reporting. Seamless archive integration allows you to automatically have your data securely journaled to an archive. The optional 'Export to Inbox' feature even allows users to instantly and securely transfer the message to their normal email inbox.

Personal data key

A personal data key gives you ultimate control of your encrypted message data. When you enable this feature, all of your messages are encrypted in a way which requires the personal data key in order to decrypt the data. And since this key is never stored in Bracket, only you hold the key to reading your messages. You control the key, you control your data.

Need encryption? Just Bracket.

- ✓ *Satisfies regulatory compliance*
- ✓ *Surprisingly affordable*
- ✓ *Works on any platform/device*
- ✓ *Nothing to install or maintain*
- ✓ *Scaleable deployment*
- ✓ *Handles files up to 1GB*

Bracket® Encrypted Email
CloudFilter™ Total Email Security
SafeSend™ Enhanced Outbound
XtraMail™ Email Continuity
SecureStore™ Archiving
CloudMail™ Secure Hosted Email