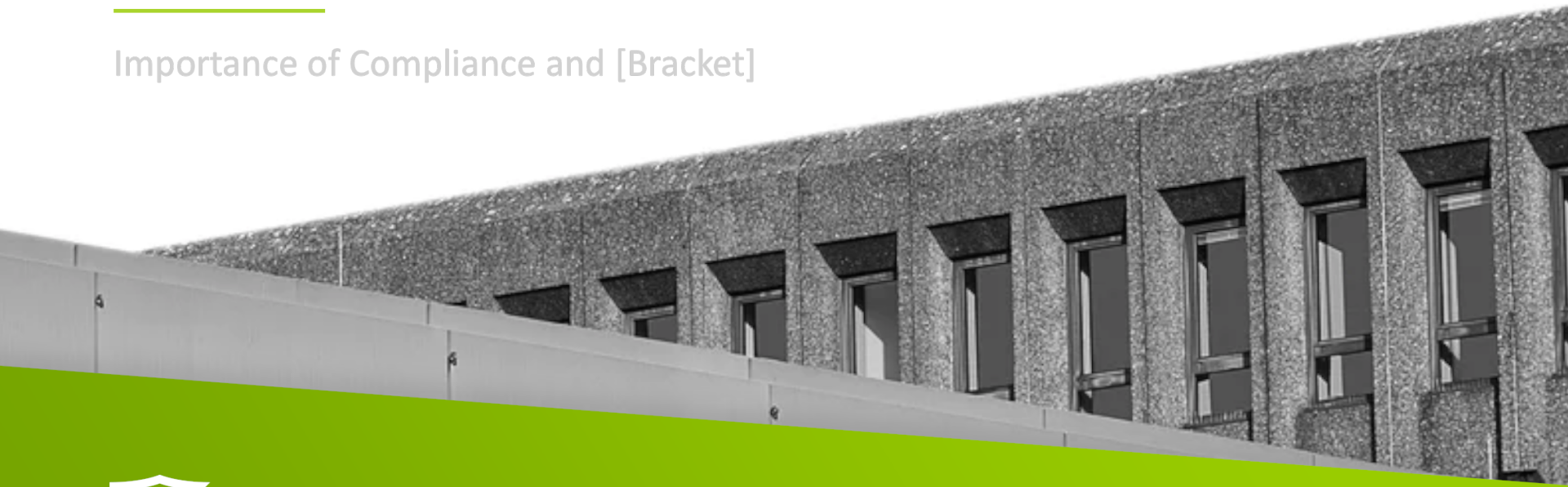
Email Encryption

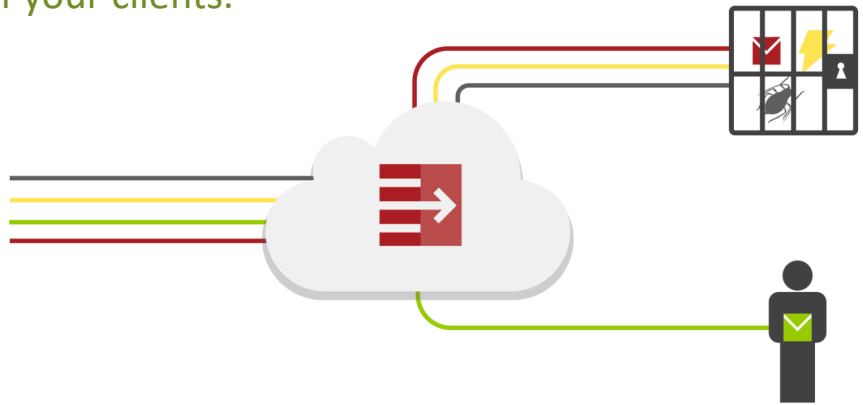
Importance of Compliance and [Bracket]



mailprotector®

Why should you use email encryption?

Email is a vital form of communication. Many organizations rely on email to send sensitive, confidential information within and outside the organization. To ensure your customers are protected, email encryption services do just that by following various compliance regulations, promoting safe email practices in your email environment and protecting the privacy of your clients.



Compliance and why is it important?

- The definition of compliance is “the action of complying with a command,” or “the state of meeting rules or standards.”
- Depending upon what rules, standards or regulations your organization is subject to, you need to identify data deemed confidential (HIPPA, S-OX, GLBA, PCI, etc.)
- After confirming confidential data, your organization will want to determine who should have access to send and receive such information
- Lastly, you team would look to set policies that can be enforced by technologies to encrypt, archive, or even block transmission of email content based on users from any type of platform such as **web or mobile** -- 81% of people use a smartphone to check their email

Determining the type of compliance needed or required

Employee to Employee

Encryption within your company

Company to Company

B2B Encryption

Legal to Company

HIPAA, S-OX, GLBA, PCI

Company to Government

State and Federal Law Encryption

i.e. Department of Revenue, Department of Defense

Bracket™

People hate email encryption, so we decided to make it better. Bracket allows your company to stay within compliance while using your favorite email app on your phone, tablet, or desktop computer. You can send an encrypted email from any client configured to accept and send mail for your specific email account – Just wrap the subject in brackets **[like this]**.

Bracket™

- No password needed – Whether you're requesting a sign-in link or viewing a message from a notification, the email you receive contains a one-time-use button that securely signs you in and takes you directly to the message.
- No agents to install or maintain, just add brackets to the subject line of the email
- Easily send messages with attachments as large as 250MB in size!
- Device fingerprinting which means to sign into Bracket, you must use the same device to sign in the bracket that was used when requesting the sign-in link.
- Ability to track geolocation signature of sign in requests which shows the approximate location from which the sign-in request originated
- Permissions to enable expiring one-time links as needed
- Automatically uses SafeSend to monitor employee use of adoption or encryption

Bracket™

- Anyone and any device can receive a Bracket email
- Easy access to encrypted email for all recipients
- SafeSend allows you to customize filtering of inbound/outbound messages and set own permissions by users or user groups
- Satisfies most regulatory compliance specs
- Automation available

Office365

- Most expensive version of O365 required for safe email encryption
- Both users require O365 to read encrypted email
- Passcode required for users to read email that do not have O365 which often cause warning messages that can lead to ignore emails
- Messages will take longer to load
- No SafeSend = unable to set own rules and permissions
- No automation

"Mailprotector has changed the entire security dynamic with Bracket. My customers prefer the interface to regular email, which makes email privacy a comprehensive experience. That is a game changer that is making me a lot of money.

Patrick | Results Technology