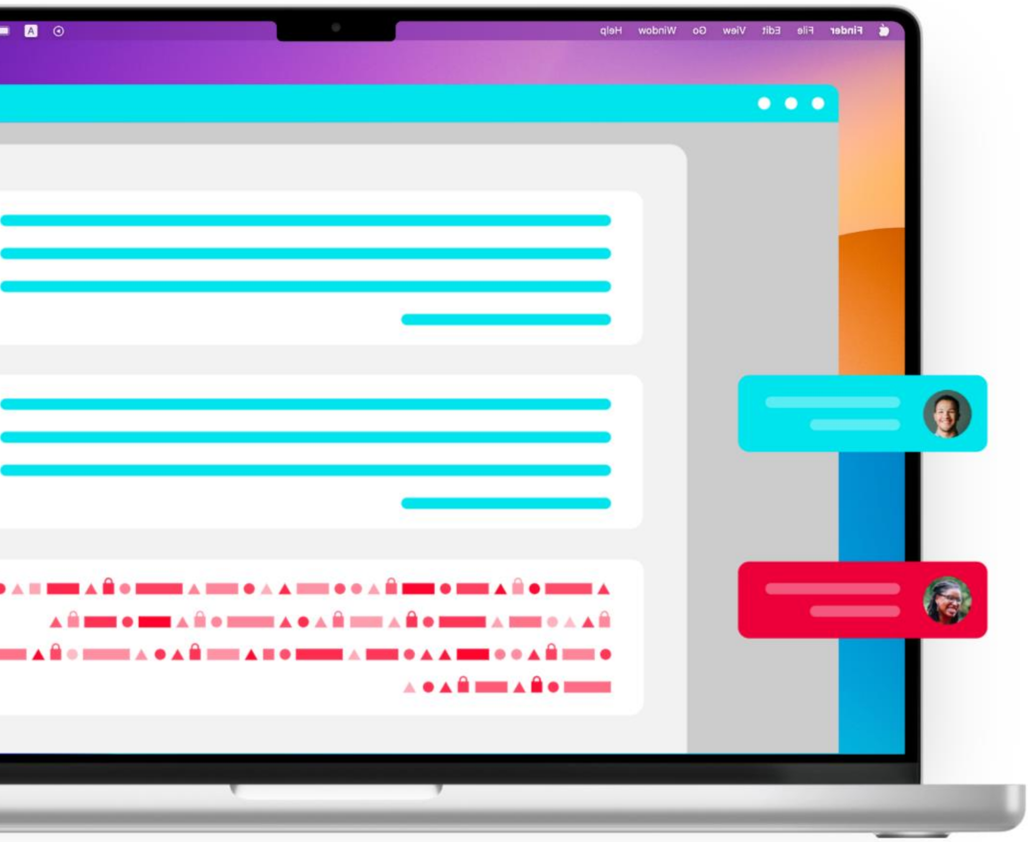
klarytee

Data centric security for the future of work



Klarytee is a platform that helps enterprises achieve granular control of their data by building encryption and access control into the data itself, so it stays protected wherever it goes

Documents **Emails** **Databases** **CRMs** **Webpages**

Security built into data itself for visibility and control beyond the enterprise boundary

- ✓ Reduce accidental and malicious **data loss**
- ✓ Enable secure and compliant use of **Cloud and SaaS**
- ✓ Enforce consistent security across **supply chain**
- ✓ Gain complete **visibility** of where the **organisation's data** is and who is accessing it

A new way to think about security

Built-in security

Security integrated with products you already use daily that lasts forever, independent of IT infrastructure, device, storage, transmission or format.

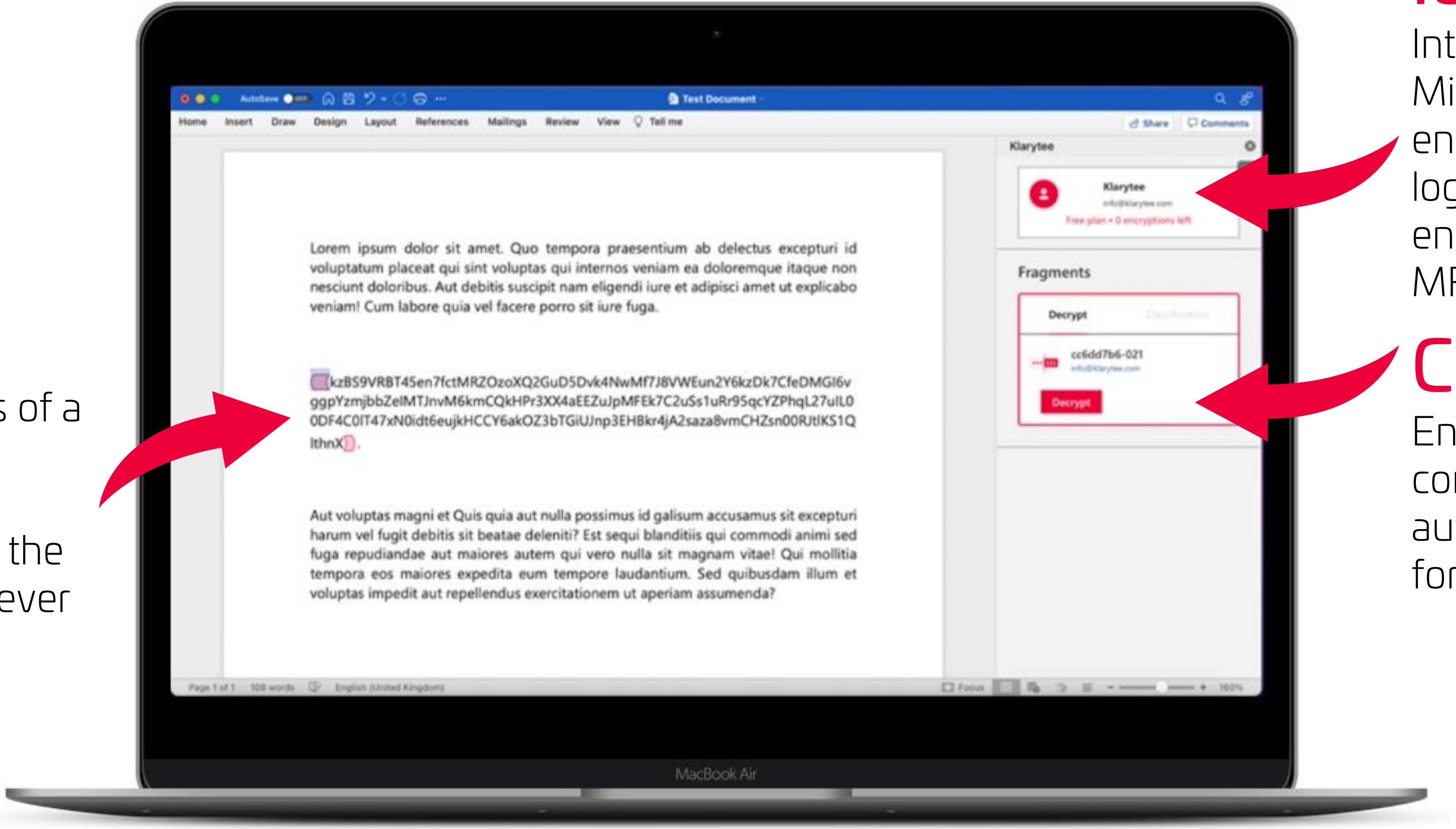
Granular protection

Enforce authentication, that can be applied to individual fragments ranging from a single character to an entire document.

Visibility & control

Complete visibility into who’s accessing your data wherever it goes, even on customer and supplier infrastructure, and revoke access in real-time.

Integrated into your existing workflows



Lorem ipsum dolor sit amet. Quo tempora praesentium ab delectus excepturi id voluptatum placeat qui sint voluptas qui internos veniam ea doloremque itaque non nesciunt doloribus. Aut debitis suscipit nam eligendi iure et adipisci amet ut explicabo veniam! Cum labore quia vel facere porro sit iure fuga.

kzBS9VRBT45en7fctMRZOzoXQ2GuD5Dvk4NwMf7J8VWEun2Y6kzDk7CfeDMGI6vggpYzmjbbZeIMTJnvM6kmCQkHPr3XX4aEEZuJpMFEk7C2uSs1uRr95qcYZPhqL27uIL00DF4C0IT47xN0idt6eujkHCCY6akOZ3bTGiUJnp3EHBkr4jA2saza8vmCHZsn00RJtlKS1QIthnX.

Aut voluptas magni et Quis quia aut nulla possimus id galisum accusamus sit excepturi harum vel fugit debitis sit beatae deleniti? Est sequi blanditiis qui commodi animi sed fuga repudiandae aut maiores autem qui vero nulla sit magnam vitae! Qui mollitia tempora eos maiores expedita eum tempore laudantium. Sed quibusdam illum et voluptas impedit aut repellendus exercitationem ut aperiam assumenda?

Encrypt

Encrypt portions of a document with layered access control built into the document wherever it goes

Identify

Integrated with Microsoft ID to enable O365 logins and enforcement of MFA policies

Control

Enforce access controls and authenticate users for each fragment

Get it from Microsoft

Key features

Prevent data loss

Revoke access at any time even if you no longer have access to the document.

Non-repudiation

Cryptographically bind blocks of content to its owner.

Zero-knowledge

We don’t store any content to minimise the risk of data loss.

Real-time audit

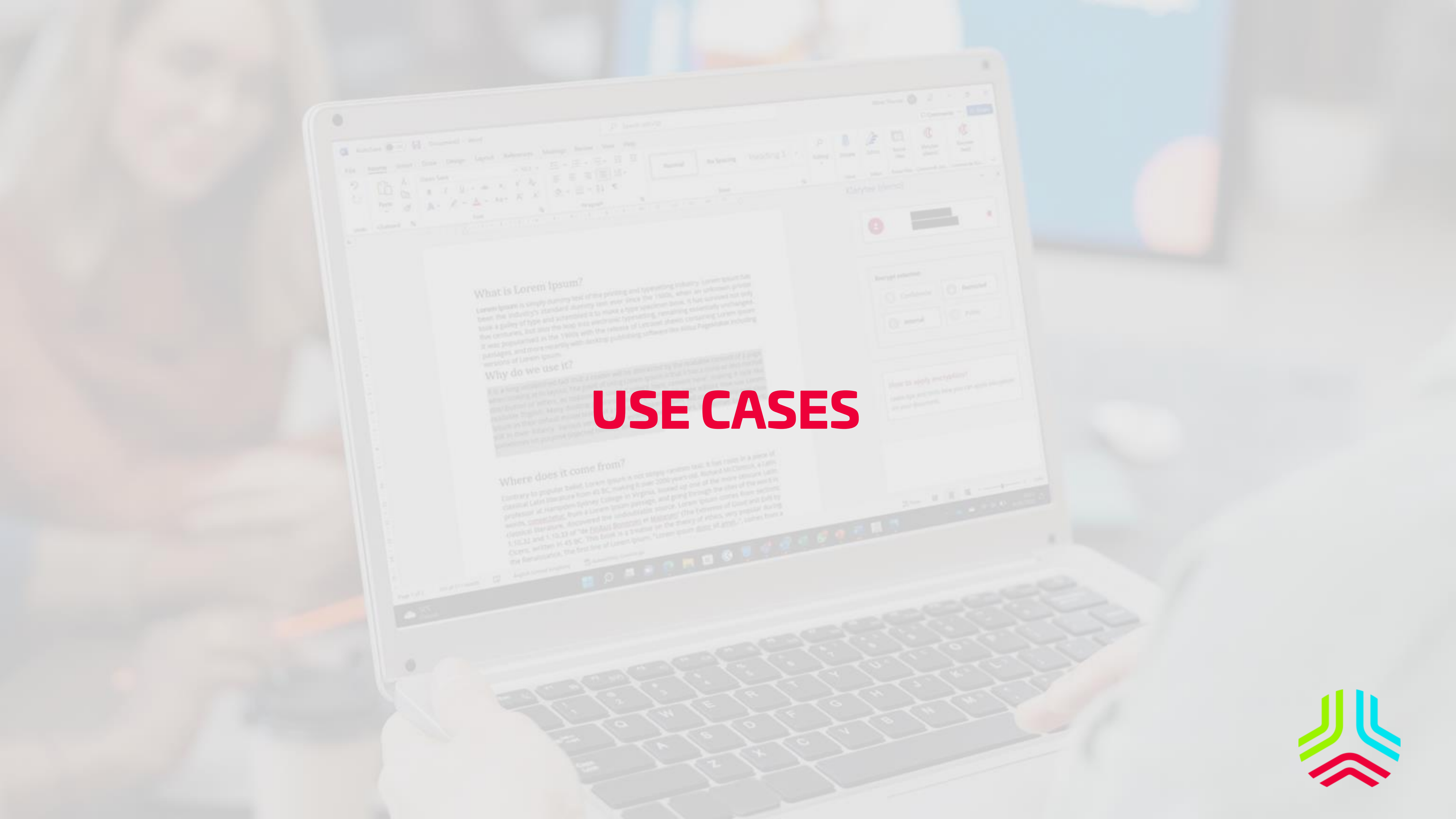
Track and manage document interactions and build up an audit trail.

Integrated workflows

Secure data instantly at its source, the moment it’s created.

Granular access control

Encrypt all or parts of a document and enforce layered access controls.



USE CASES

Use Case: Secure External Collaboration

Challenge:

Current document controls don’t apply to documents attached to outbound communications when they leave the enterprise boundary – e.g. customer and supply chain comms. Leaves organisation vulnerable to compliance and regulatory risk.

Requirements:

- Want to share documents with clients (over email, chat) without requiring a waiver
- Needs to fully integrate with enterprise identity provider

Solution:

Encrypt documents using Klarytee to protect the contents beyond the enterprise boundary and restrict access to a user even before there are onboarded

Use Case: Improved Internal Collaboration

Challenge:
Collaborating on documents that contain sensitive data is difficult because controls are applied on document level. Makes real-time collaboration friction-filled & slower, and employees use work-arounds

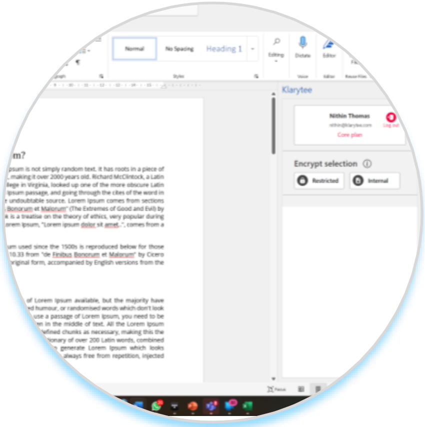
Requirements:

- Improved collaboration between Customer Identifiable Data (CID)-exposed and CID-non-exposed teams
- Storing of data anywhere
- Full integration with enterprise identity provider
- Conditional Access depending on employee location or device used

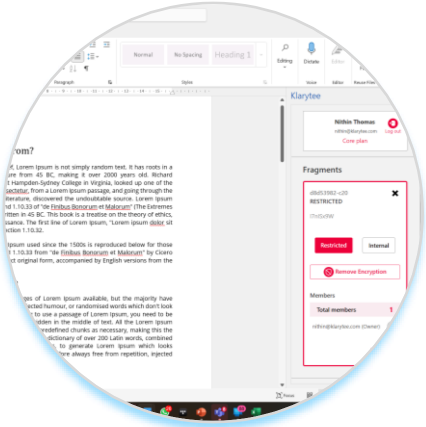
Solution:

- Encrypt documents using Klarytee to protect CID and other sensitive data to ensure robust access control without the need for multiple document versions and enable efficient and secure collaboration

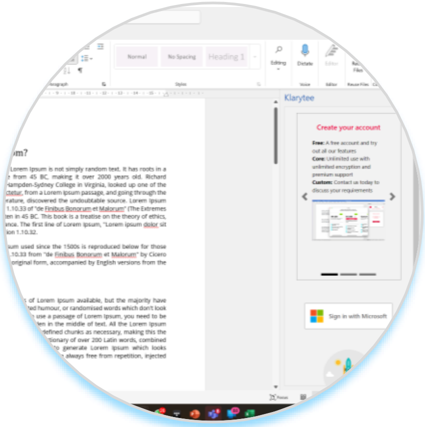
Workflow: Secure Internal & External Collaboration



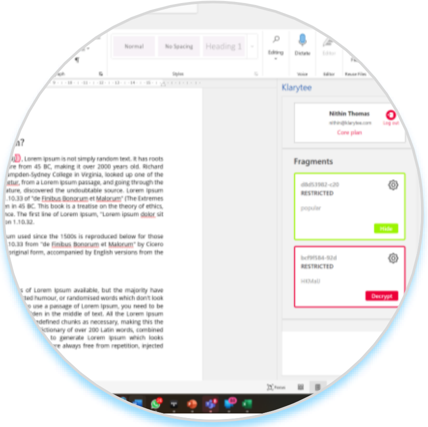
Document or email encrypted with Klarytee add-in



Document shared with an internal/external user with their unique digital ID



Employee, customer or supplier verifies their identity through the add-in



Employee, customer or supplier decrypts the document

Value:

1. Reduce customer drop-off without sacrificing security.
2. Work in real-time on one part of a document without sharing privileged information from another part.
3. Securely collaborate in with internal and external teams.
4. Control and revoke access to document throughout its lifecycle.

Use Case: Automatic remediation of exposed CID

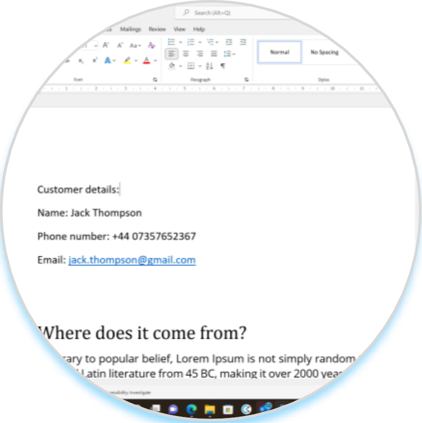
Challenge:
When using SaaS applications, there is no control on jurisdiction where data are hosted and accessed. Without a full audit trail, leaves organisation exposed to data leaks and data leaving a jurisdiction

Requirements:

- Require automatic protection of text paragraphs where scanning recognizes unprotected CID
- Require encryption-at-transit, encryption-at-rest, AND encryption-in-use
- Need full integration with internal identity provider
- Mandating expiry date, location based access controls or multi-factor authentication based on the content classification

Solution:
Encrypt documents using Klarytee to protect CID and other sensitive data by default to prevent accidental or intentional loss of CID

Workflow: Automatic remediation of exposed CID



Customer details:

Name: Jack Thompson

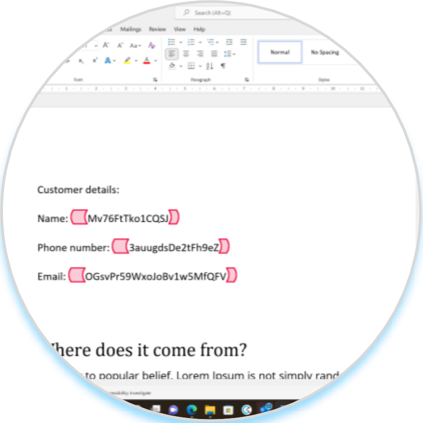
Phone number: +44 07357652367

Email: jack.thompson@gmail.com

Where does it come from?

rary to popular belief, Lorem Ipsum is not simply random
Latin literature from 45 BC, making it over 2000 year

Document or email encrypted with Klarytee add-in



Customer details:

Name: Mv76FtTko1CQSJ

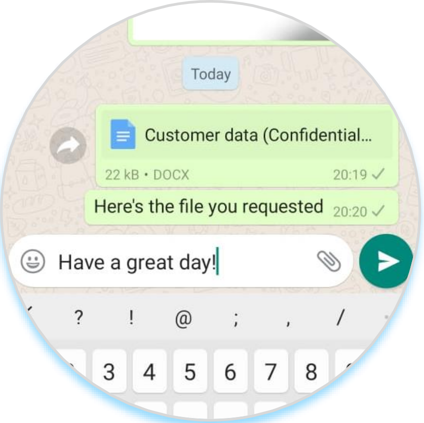
Phone number: 3auugdsDe2tFh9eZ

Email: OGsvPr59WxoJoBv1w5MfQFV

here does it come from?

to popular belief, Lorem Ipsum is not simply rand

Automatically detect and encrypt any CID with access controls based on policy

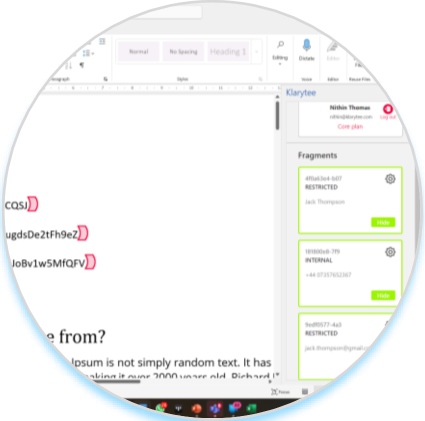


Customer data (Confidential...
22 kB • DOCX 20:19 ✓

Here's the file you requested 20:20 ✓

Have a great day!

Share document on a SaaS platform. CID remains encrypted at rest, in transit and in use.



CQSJ

ugdsDe2tFh9eZ

JoBv1w5MfQFV

e from?

Ipsum is not simply random text. It has
making it over 2000 years old. Richard

Nithin Thomas
nithin@klarytee.com
Core plan

Fragments

4f0a63e4-b07
RESTRICTED
Jack Thompson

181800e8-7f9
INTERNAL
+44 07357652367

9edf0577-4a3
RESTRICTED
jack.thompson@gmail.co

Authorised user is able to access the document following authentication

Value:

1. Employees can collaborate freely without exposing CID
2. Decrypted data is only exposed in appropriate jurisdiction
3. Maintain compliance and security on CID regardless of SaaS platform and hosting environment

klarytee

Data centric security for the future of work

www.Klarytee.com | info@klarytee.com