

# DATA SHEET

## Client Agent and Mobile app

### Part number: KAPPIV203

#### DESCRIPTION:

Client agent for Windows and macOS operating systems and mobile app on iOS and Android. Data discovery and classification on Windows/macOS. Encrypts unstructured data on public cloud storage, desktops, laptops, smartphones, tablets, VDI and enterprise file servers. Performs end-to-end encrypted file sharing.

#### **Supported operating systems**

Windows 7 or higher  
macOS Yosemite or higher  
iOS 8 or higher  
Android 4.1 or higher

#### **Minimum Storage Required**

120MB on Windows and Mac computers  
17MB on iOS and Android devices

#### **Minimum Processor Required**

Intel Xeon or i5 and higher processor on  
Windows and Mac

#### **Minimum Memory (RAM) Required**

2GB on Windows and Mac computers

#### **Availability**

On Apple App store for iOS devices  
On Google Play Store for Android device  
Downloadable .DMG and .EXE files from  
Kapalya's website.

#### **Public Cloud Supported**

Amazon S3 object stores  
Box cloud storage

#### **File servers supported**

Windows Server 2003 or higher  
Red Hat Linux, Ubuntu, CentOS, SuSe Linux

#### **Private Cloud supported**

VMWare ESXi 5.5 or higher  
Hyper-V

#### **Virtual Desktop Infrastructure supported**

Any VDI that servers Windows 7 or higher desktops

#### **Crypto**

Advanced Encryption Standard (AES)

#### **Keys**

256 bit symmetric keys in GCM mode

For further information visit [kapalya.com](http://kapalya.com)

## Key Features

- Full-data encryption (client-side encryption) and **seamless file sharing** on any device, corporate server and public cloud while at-rest or in-transit.
- **Data classification engine** auto-detects 250 + file types for sensitive data (plus options to customize).
- Zero-knowledge encryption **masks cloud admin** visibility into your data and encryption keys.
- A unique key for each file provides ultimate data security, eliminates the need to manage key rotation and enables full end-to-end cloud agnostic encrypted file sharing.
- Full management of your own keys – Kapalya, cloud admins and your internal admins will never have access to your keys.
- Provides **real-time encryption key management** based on patent-pending algorithms.
- Keys cannot be compromised because encryption keys are never stored on endpoints or cloud servers.
- **Frictionless SSO to application**, cloud servers and seamless VPN from mobile endpoints.
- Easy-to-use file system provides a user experience similar to Mac Finder or Windows Explorer.

### Compliance:

HIPAA, PCI, PII, FTI, SOX, FIPS140-2, NIST 800 -53, IRS 1075, PHI, SOC 1 and 2

## About Kapalya

Kapalya delivers a unique approach to enterprise-wide encryption key management by serving keys in real-time to 1000s of users across multiple platforms like endpoints, mobile, cloud storage and file-servers, and destroying them after the encrypt and decrypt functions are completed. Kapalya's goal is to support organizations around the globe in protecting their unstructured data wherever it resides, and meeting compliance requirements.

For further information visit [kapalya.com](https://www.kapalya.com)