SECURITY STORY

WE NEVER SEE, TOUCH NOR HOLD YOUR DATA

Gavin Ray
CTO | gavin@digi.me

another Engineering Briefing

digi.me | PRESENTATION

keeping your data secure at all times

ALL YOUR DATA IN ONE PLACE

TO SHARE WITH PEOPLE WHO YOU CHOOSE

SECURELY HELD IN YOUR OWN ONLINE STORE

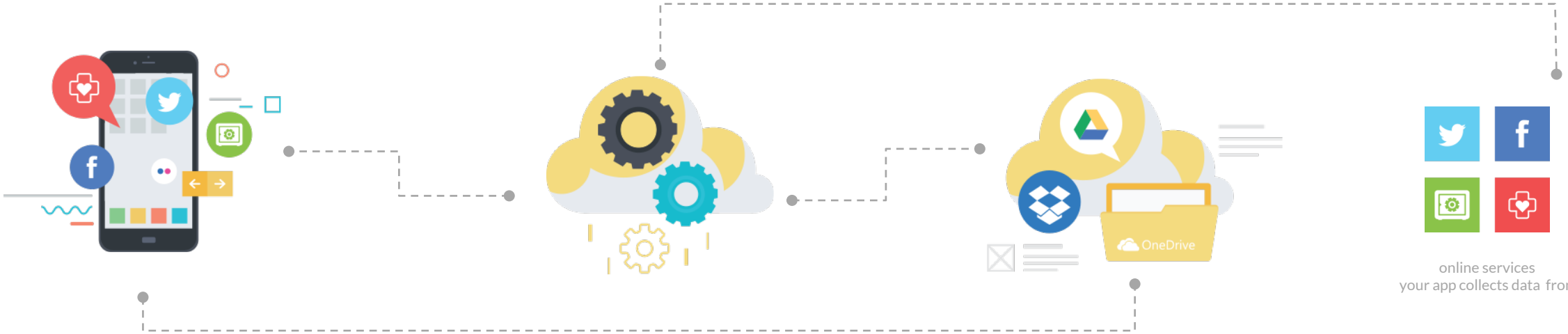
SO NO-ONE CAN RUN AWAY WITH IT

Introducing | PRESENTATION

the digi.me technology concept

Digi.me applications run on your mobile and desktop computers to let you see and use all your online data. The app has a secure connection to a Cloud service that fetches all your online data and moves it into you personal online storage.

The app does everything for you and the digi.me company never sees, touches or holds your data. We empower you to hold it and use it yourself.



APPLICATION

digi.me applications run on your device and securely asks the cloud to fetch your data from all your online services and save it in your personal online storage service

THE CLOUD

raw cloud computing power that we securely allocate just to your app when it needs to fetch all your online data for you

CLOUD STORAGE

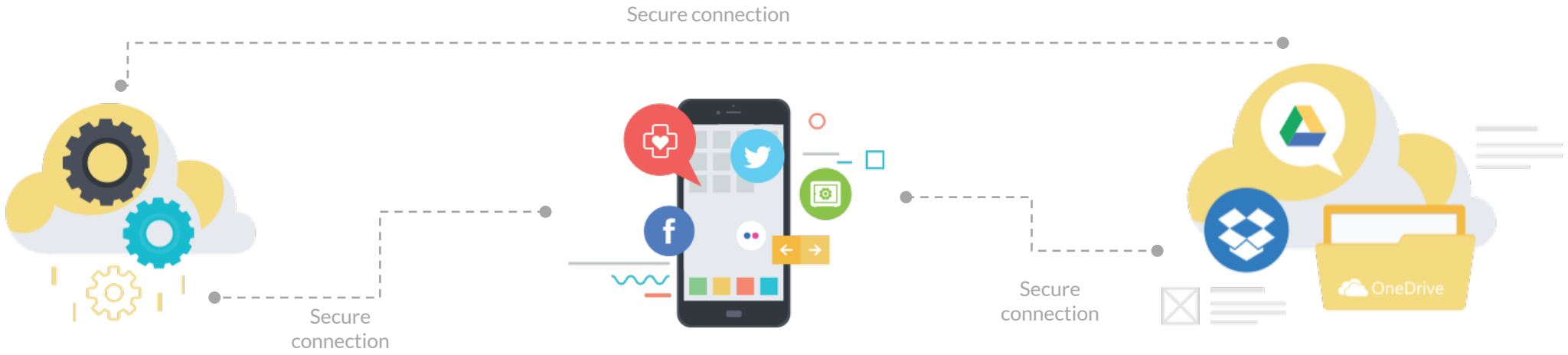
digi.me apps ask the Cloud to fetch your data and store it here in your cloud files, like Dropbox, OneDrive and Google Drive (whichever you choose)

Design | PRESENTATION

system security architecture

The overall solution has been designed to ensure all your data is never passed from one place to another in plain-text, it is always encrypted to a high standard.

Data is only stored in your storage areas, there is no digi.me storage.
All data stored is encrypted



CLOUD PROCESSING

digi.me cloud processing is created on demand and can only be initiated via a request from an authenticated user

APPLICATION

digi.me applications authenticate their user via their password which is used to derive a long cryptographic key that unlocks their credentials stored securely on the device. These security credentials are used to request our secure cloud services

CLOUD STORAGE

You select your own personal cloud storage and all data held there is encrypted and always moved on demand to applications and cloud processing in its encrypted form

Risk | PRESENTATION

the things we design our products against

The attacks on our security will come from people who have the skills, the motivation and resources required to break many security systems, so we design and build our systems to withstand them.

Skilled

We assume all hackers we need to worry about are skilled and aware of the latest security vulnerabilities and attacks occurring in the global market.

Motivated

We expect any hacker to be persistent and motivated sufficiently to stretch our security designs and implementations to the limit.

Resourced

We design and build all our systems to withstand the considerable onslaught possible with modern attacks by people with significant resources available.

Encryption of files and secret keys

It is essential to use high quality encryption methods to secure data, but to also make sure that there are no shortcuts and weaknesses in the methods chosen.

Security of data in flight

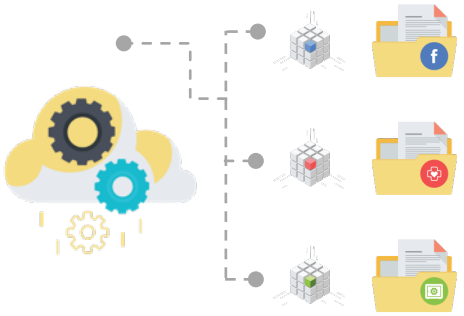
When our apps share data over the internet they always use SSL, the “padlock” connection class you know from your browser. We configure it to only use the highest security settings.

Designed for the onslaught

Modern cloud systems like the ones our app uses, are not just cracked via security breaches, they can be attacked by floods of fake traffic and exploratory connections looking for chinks in their armour. We design and build against all these.

Passwords | PRESENTATION

great passwords are a key to security



LOCKED AWAY

Whenever you run your digi.me app you want all your data to be available. Since your digi.me app stores it for you securely in your cloud you must supply your secret password to unlock the data

ENTER PASSWORD

The secret of good security is good password choice, so it's important you choose a good password that is also easy to remember

60 Seconds
Typical time to hack any file encrypted with simple PINS

"1 2 3 4"

If you choose simple 4-digit passwords then the effort a good hacker will require to crack the encrypted files in your cloud storage will be measured in seconds, it really is not very secure

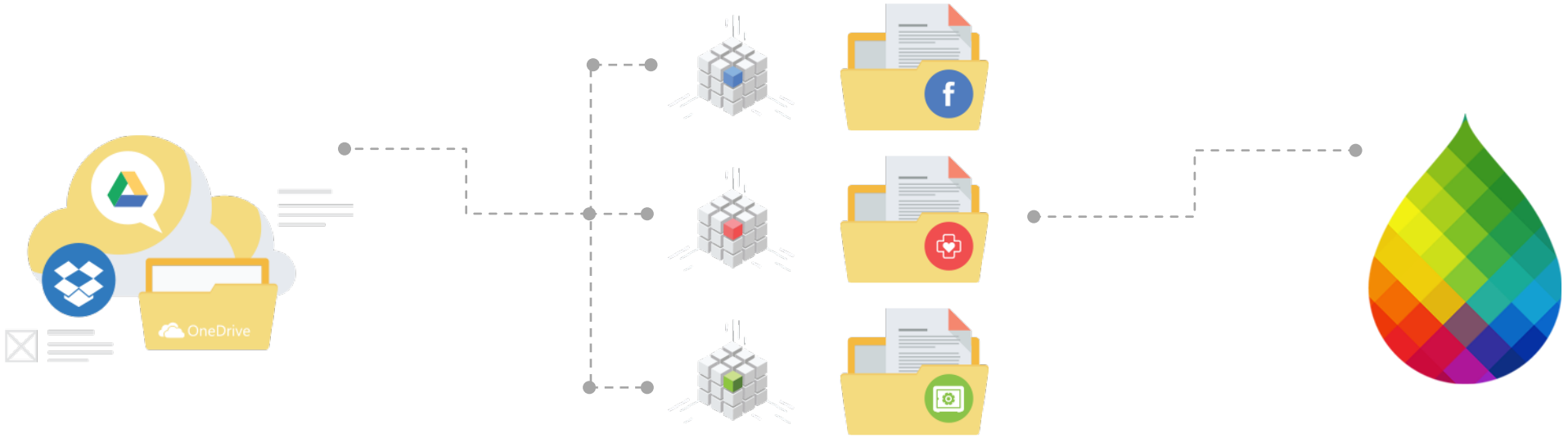
Weeks/Months
Typical time for well resourced hacker to break a single file encrypted with digi.me long word passwords

"MONKEY PERISCOPE"

We allow you to create memorable passwords that have many letters in them and then we use cryptographic algorithms that are proven to generate strong encryption keys that take months or years to crack

Encryption | PRESENTATION

our apps protect your files



SECURE STORAGE

When you use digi.me apps all your data is securely held on the cloud storage service of your choice, whether it is Dropbox, Google Drive, Microsoft OneDrive (or other secure storage services we will add over time). We call this your Personal Cloud or pCloud

UNIQUE KEYS

All the files our software imports from your online data services are stored securely. They are encrypted with a set of keys and ciphers that come from international banking standards

KEY MANAGER

When your digi.me app accesses your files in your cloud storage it is able to decrypt them because your secret keys are secured on your mobile device. It does this by holding them in a protected vault on your mobile that is secured by the digi.me password that only you know

Add a Data Source | PRESENTATION

your data secured on your storage

SELECT SERVICE

When you use our apps you have the choice to select which sources of data you would like your personal digi.me app to collect and manage for you

REQUEST LOGIN

Your app makes a request to your online service so that you can log-in to it and confirm we are allowed to collect the data from it for you

APPROVE digi.me?

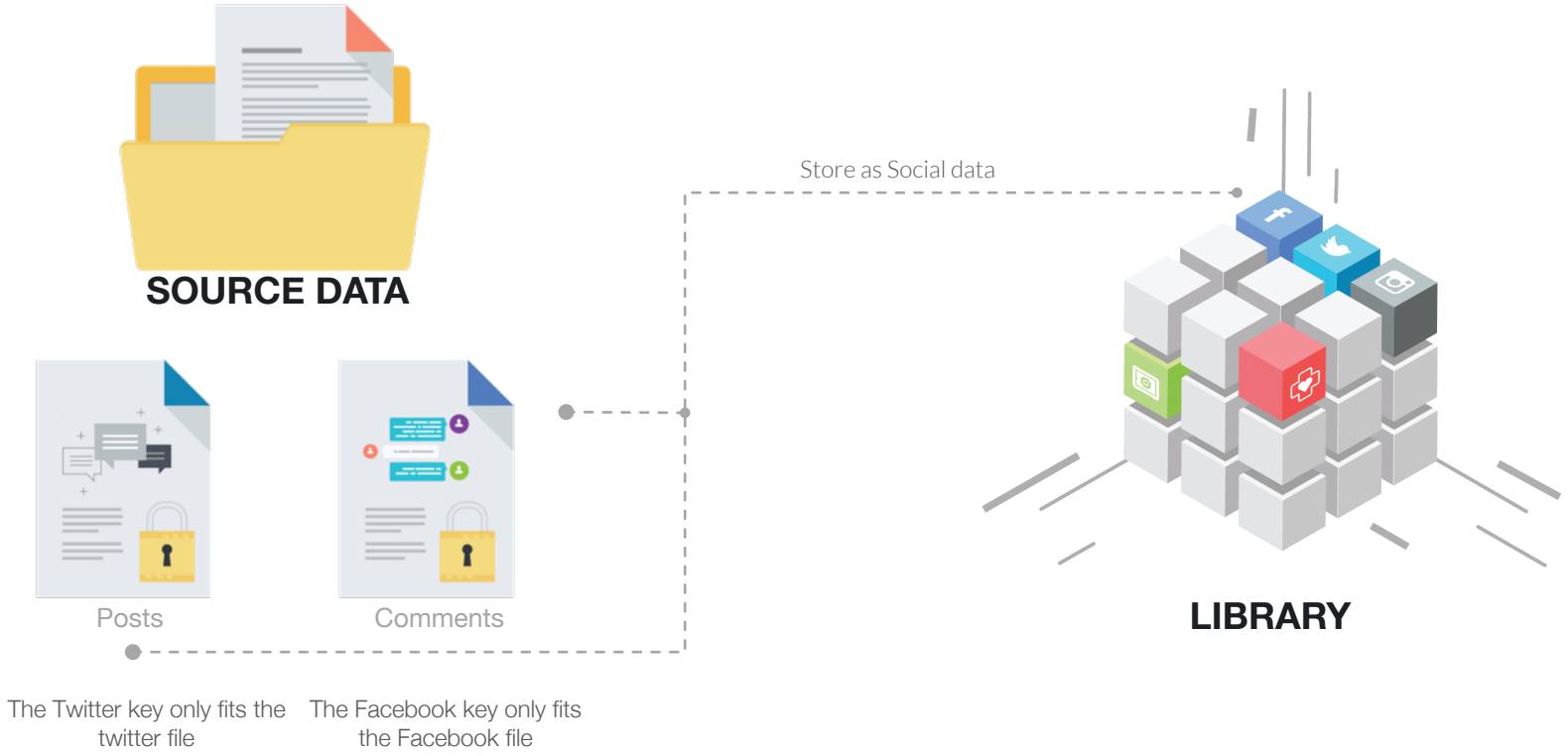
Your app then connects to your favourite online cloud storage library to safely save all your data for you. Its in your storage not ours, because we don't have any

digi.me APPROVED

Your Facebook account allows you to approve apps like digi.me to access it remotely. It issues a special security token that only your digi.me app can use each time it wants to access your social data

Your Data in DataSets | PRESENTATION

all files are encrypted with a unique key



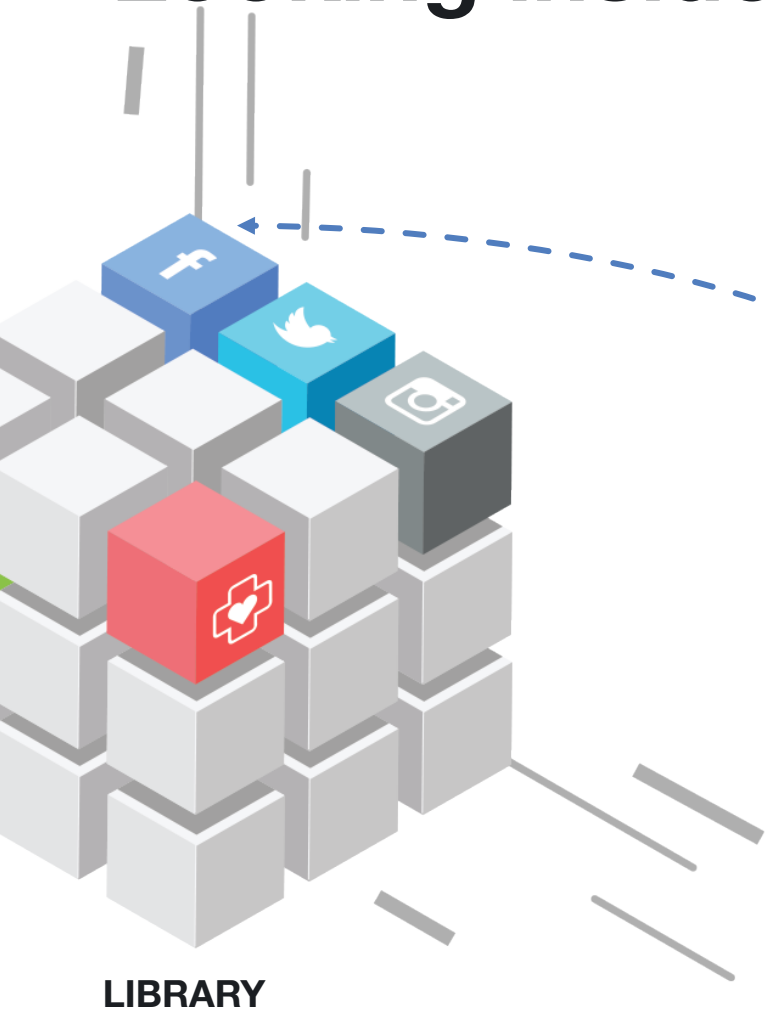
SOCIAL MEDIA : FACEBOOK

Your digi.me files are securely held in your personal cloud storage service and grouped by the dataset they relate to.

All files are encrypted, each with a completely unique and randomised key. This means that if anyone were able to breaks a key, would only ever gets one file. Which means it is extremely hard for anyone to attack and unlock much of your data.

Looking inside the Data | PRESENTATION

all your data is stored in an organised way

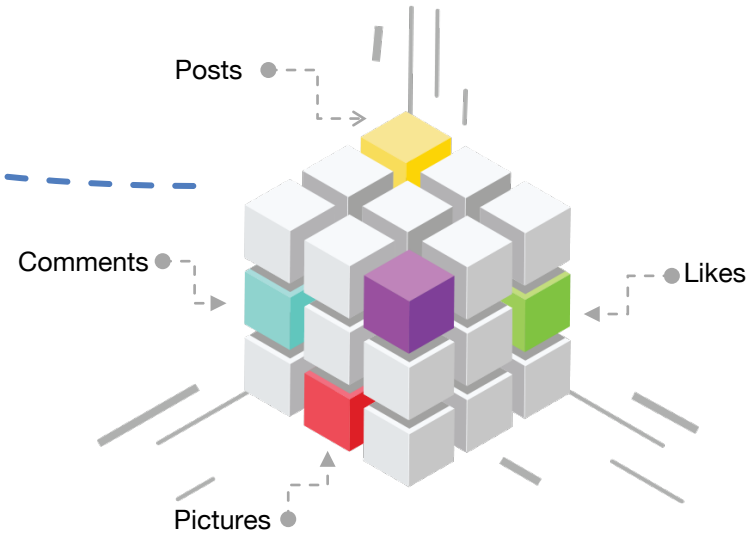


LIBRARY

All your data is collected from external sources and stored in a highly organized way so it can be viewed, searched and shared on demand, according to the type of data required.

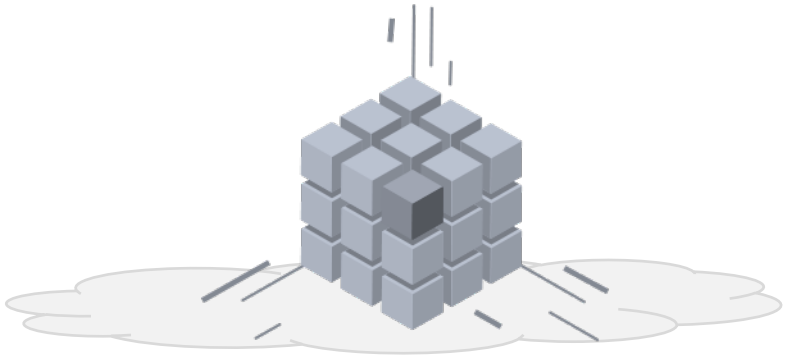
INSIDE YOUR DATA LIBRARY

Inside a social media dataset, we separately store your comments, posts, media and likes. Every dataset is broken down and categorised with standard names, even if Facebook calls a Post what Twitter calls a Tweet and another service calls a “thing”



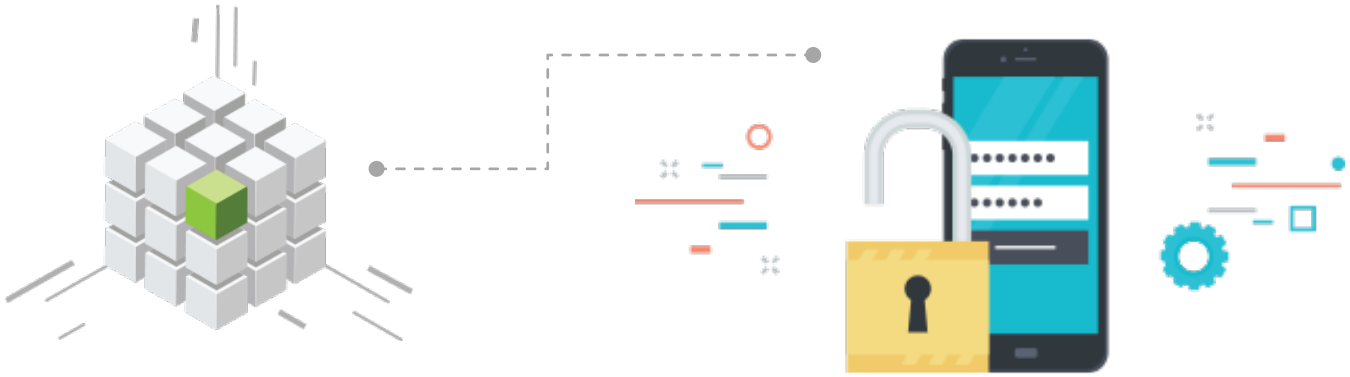
Secured Library | PRESENTATION

the cloud regularly synchronises all your data



ENCRYPTED IN THE CLOUD

All your data is fully encrypted in the cloud. Every file has its own key that can only be unlocked with the secret master key that is unlocked by your password



PASSWORD IS A KEY

When you first open your digi.me app you enter your password to unlock its master encryption key and enable it to then access all the keys it needs to use the storage and synchronisation services

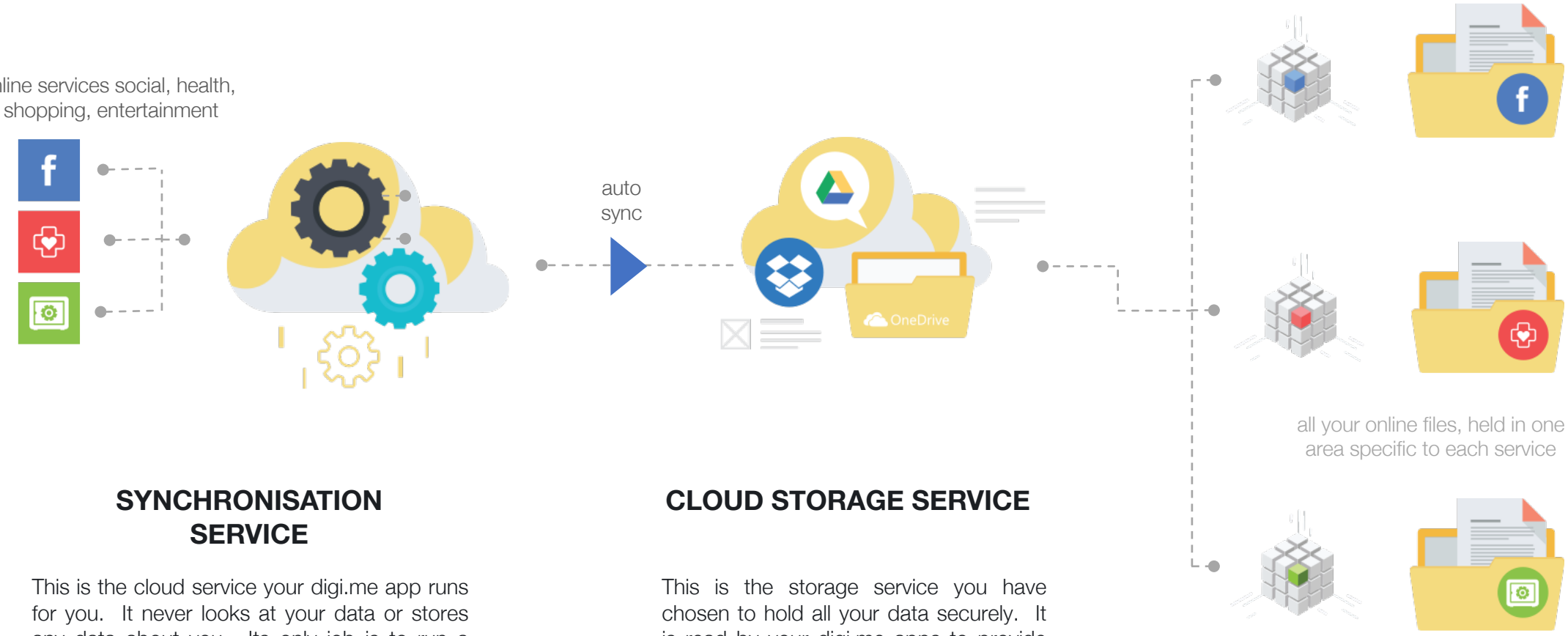
UNLOCK YOUR APP

The app can then internally gets the file keys it needs to open up the online storage where your files are securely held and ensure your digi.me app can access all the encrypted files

Synchronisation | PRESENTATION

the cloud automatically synchronises all your data

all your online services social, health, finance, shopping, entertainment



SYNCHRONISATION SERVICE

This is the cloud service your digi.me app runs for you. It never looks at your data or stores any data about you. Its only job is to run a synchronisation of your data in your online services with all the files you store

CLOUD STORAGE SERVICE

This is the storage service you have chosen to hold all your data securely. It is read by your digi.me apps to provide all the services you need and love

Encrypted | PRESENTATION

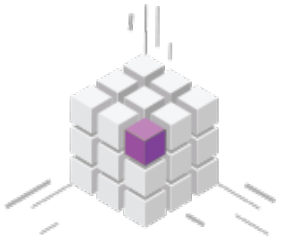
all files are viewed after being decrypted with their unique key

Extracting Encrypted Data

Your digi.me files are securely held in your own cloud storage service and all files are encrypted and decrypted, each with a completely unique key

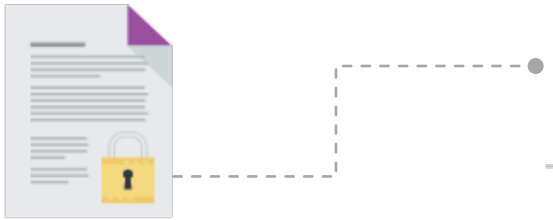
MONKEY PERISCOPE

Your digi.me app must be running and you must have logged in to unlock the encryption keys from the internal storage vault



ACCESS LIBRARY

The password unlocks the key to access the personal cloud library known as the pCloud



ACCESS DATA

The password unlocks the master key to unlock the keys for each document that holds the data you want

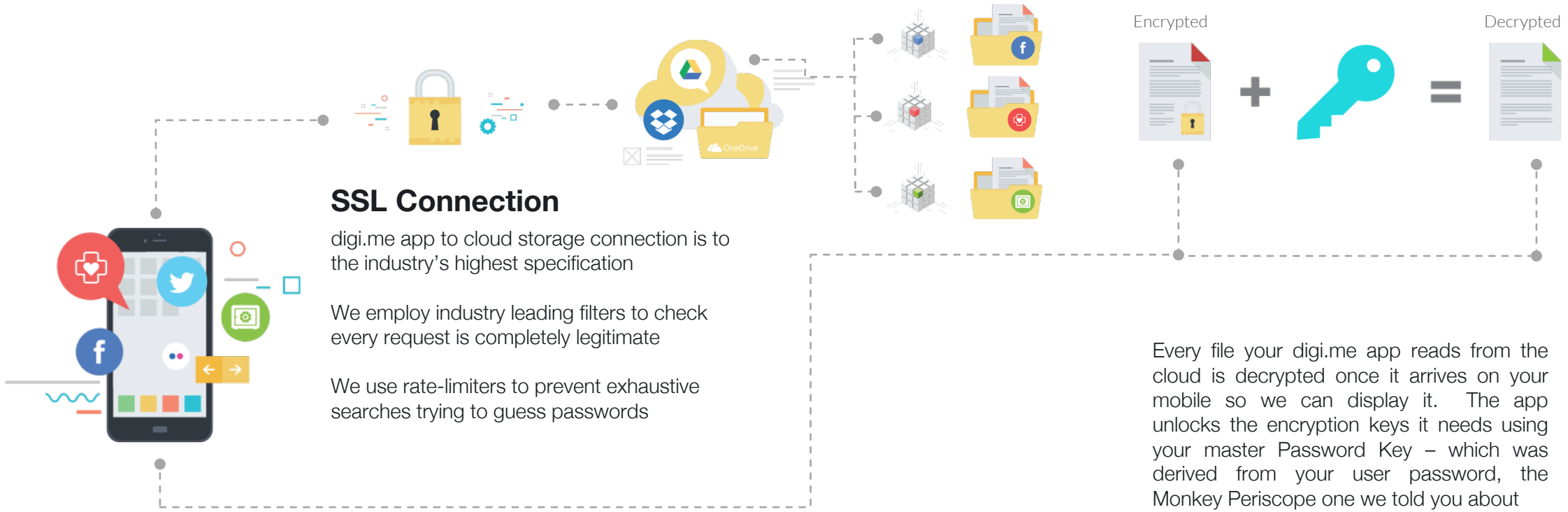
VIEW DATA

The unlocked data is then presented to the application and given a tile or group to display on your screen

Secured | PRESENTATION

all apps use doubly secured SSL connections

When you log-in to digi.me apps they retrieve all your data from the Cloud Storage using a secure connection and the personal data files are also sent over in a fully encrypted form. We use the industry standard ”padlock” connection called SSL and we additionally apply extremely strict filters to ensure every request that reaches our systems is completely valid and is not the result of attackers guessing or trying to brute force our security.



SSL Connection

digi.me app to cloud storage connection is to the industry’s highest specification

We employ industry leading filters to check every request is completely legitimate

We use rate-limiters to prevent exhaustive searches trying to guess passwords

Every file your digi.me app reads from the cloud is decrypted once it arrives on your mobile so we can display it. The app unlocks the encryption keys it needs using your master Password Key – which was derived from your user password, the Monkey Periscope one we told you about

Secured in detail | PRESENTATION

high level details of the security technology we use

AUTHENTICATION
User application authentication via >=12 character passwords and high entropy Key Derivation Functions to limit brute force attack viability. Application authentication via SSL certificates with Verisign Trust Anchor

ENCRYPTION - Asymmetric
High integrity password vaults encrypted with market proven RSA function library, implemented as FIPS compliant 2048bit, with OAEP padding

ENCRYPTION - Symmetric
File encryption via AES-256 by default with optional AES-128 for low-power devices

SSL – Implementation
SSL implementations are exclusively with mature and proven source libraries, using TLS 1.2 and specific control of ECDH curve selection, connections are validated to SSL A+ rating (ref qualys.com SSL validation service) unless limited by external system dependencies

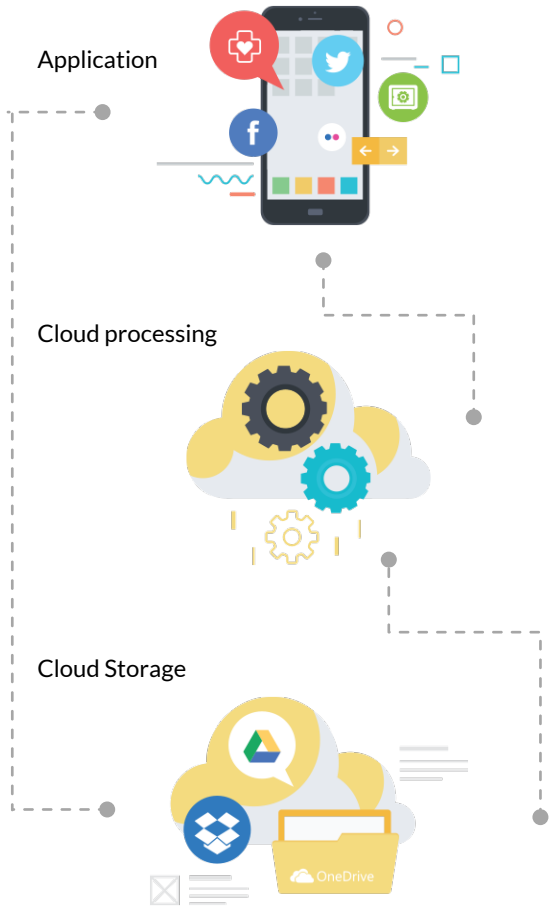
API Integrity
A number of API are exposed to public internet access, we continuously monitor them externally and secure them via strict SSL connection requirements, firewall rules, rate limiters, API filters and transactional design aimed at limited potential for denial of service, spoofing and fuzzing attacks

ENCRYPTION – Key Management
Symmetric file encryption keys are individually sored in encrypted format with the authorised recipient's Asymmetric Encryption PUBLIC key so only secured holders of PRIVATE key can decrypt

Cloud Processing Integrity
All cloud processing is context-free and only functions when provided data access credentials by an authenticated user app via a secure connection request. Personal data is never stored on any discs and all processing threads are destroyed when complete.

Cloud Memory Integrity
All cloud processing has memory to support it and any temporary memory blocks holding user data are encrypted. No memory is copied to disc.

Verification – Signing
Where we pass critical data describing sharing contracts and verifying datasets we use SHA-512 hash functions and X.509 certificates.



THANKS

FOR HEARING OUR STORY

Contact
Gavin Ray - CTO
gavin@digi.me