SECURITY STORY

WE NEVER SEE, TOUCH NOR HOLD YOUR DATA

CTO Office | www.digi.me

another Engineering Briefing

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

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

cloud computing power that fetches all your online data for you

CLOUD STORAGE

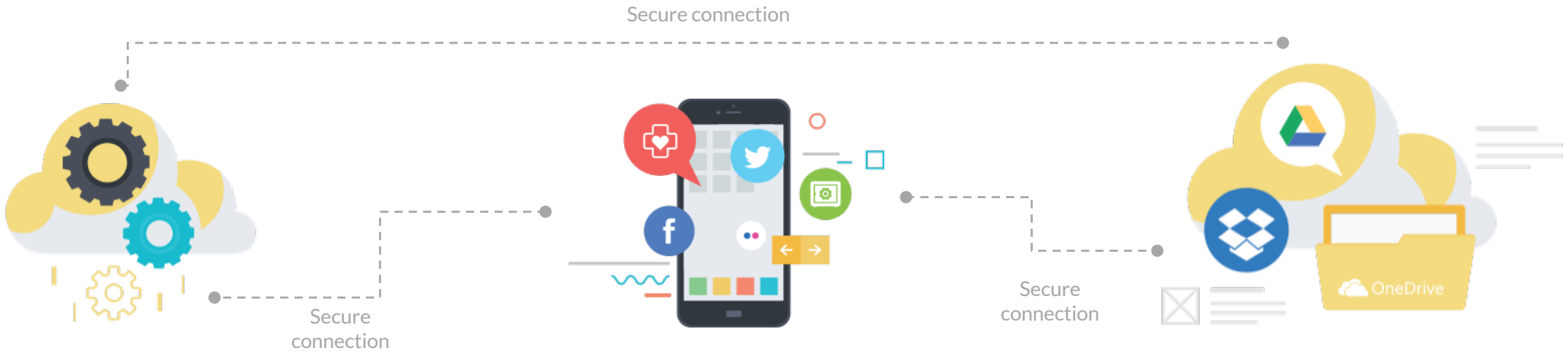
digi.me apps ask the Cloud to fetch your data and store it here in your cloud files, like Dropbox, OneDrive and Google Drive (whichever you choose)

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 with a long high-entropy password and unlock the credentials stored securely on the device to request external services

CLOUD STORAGE

You select your own cloud storage and all data held is encrypted and moved on demand to applications and cloud processing in 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

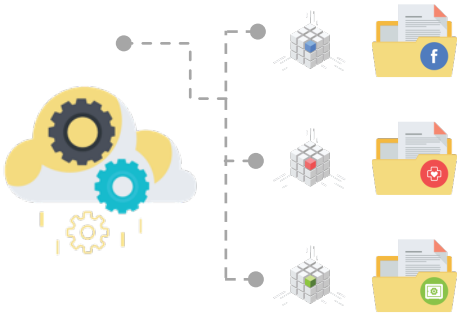
When our apps share data over the internet they always use SSL, the “padlock” connection class you know from your browser. We configure it to only use the highest security settings.

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

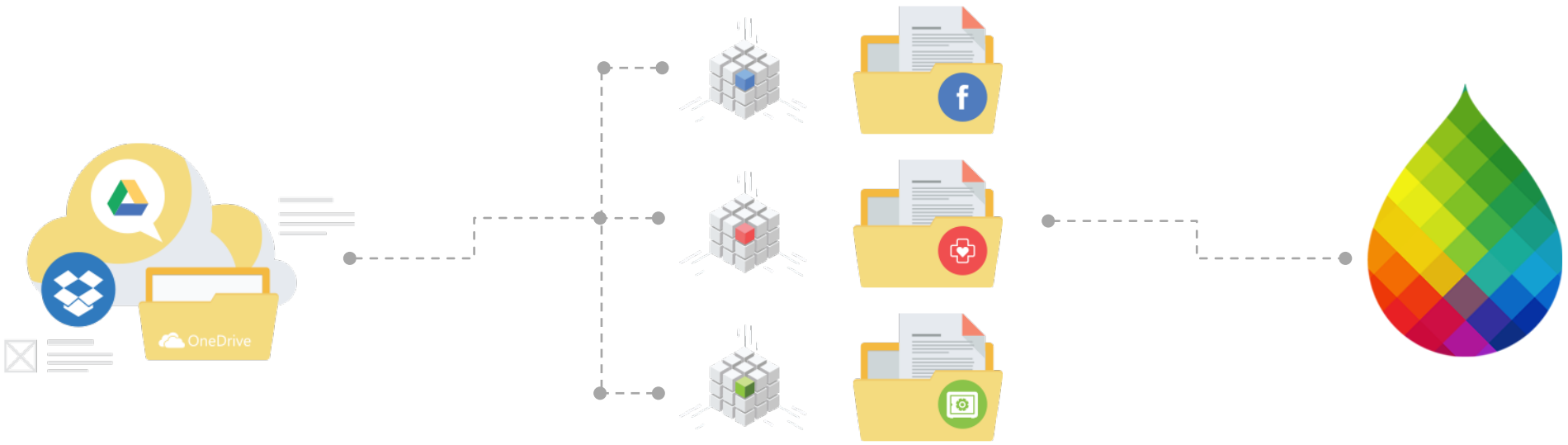
Weeks/Months
Typical time for well resourced hacker to break a single file encrypted with digi.me long word passwords

MONKEY PERISCOPE

We allow you to create memorable passwords that have many letters in them and we use cryptographic algorithms that are proven to generate 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)

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 a 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

Make Request

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

Request Approval

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

Security Profile

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

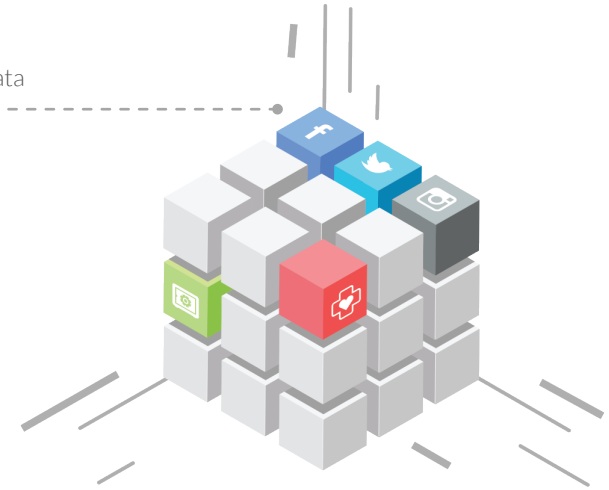
Getting DataSets | PRESENTATION

all files are encrypted with a unique key

Posts

Comments

Store as Social data



LIBRARY

The Twitter key only fits the twitter file

The Facebook key only fits the Facebook file

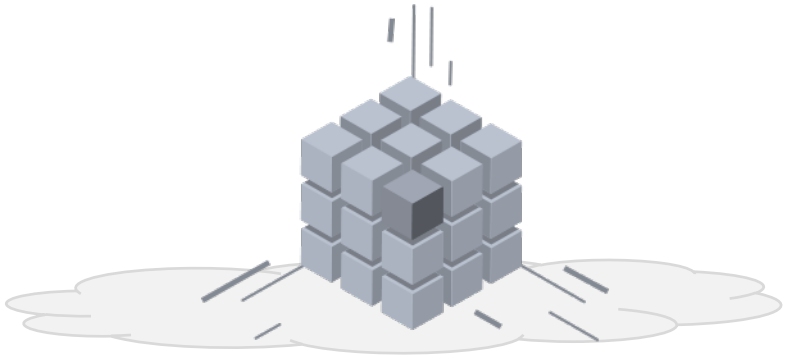
SOURCE DATA

SOCIAL MEDIA : FACEBOOK

Your digi.me data is securely held in your own cloud storage service in encrypted files, each with a completely unique key. This means that anyone who ever breaks one key, only ever gets one file. Which means it is extremely hard for anyone to attack and unlock all your data.

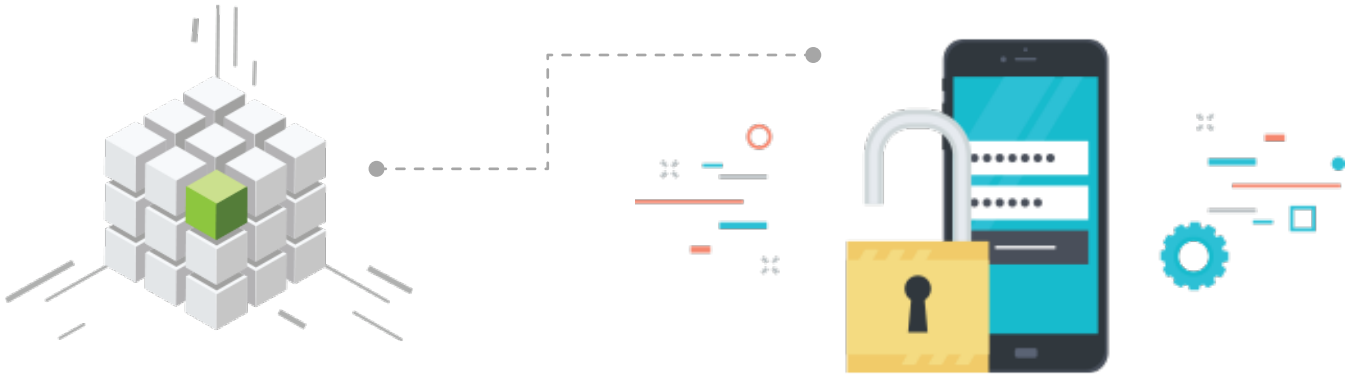
Secured Library | PRESENTATION

the cloud 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

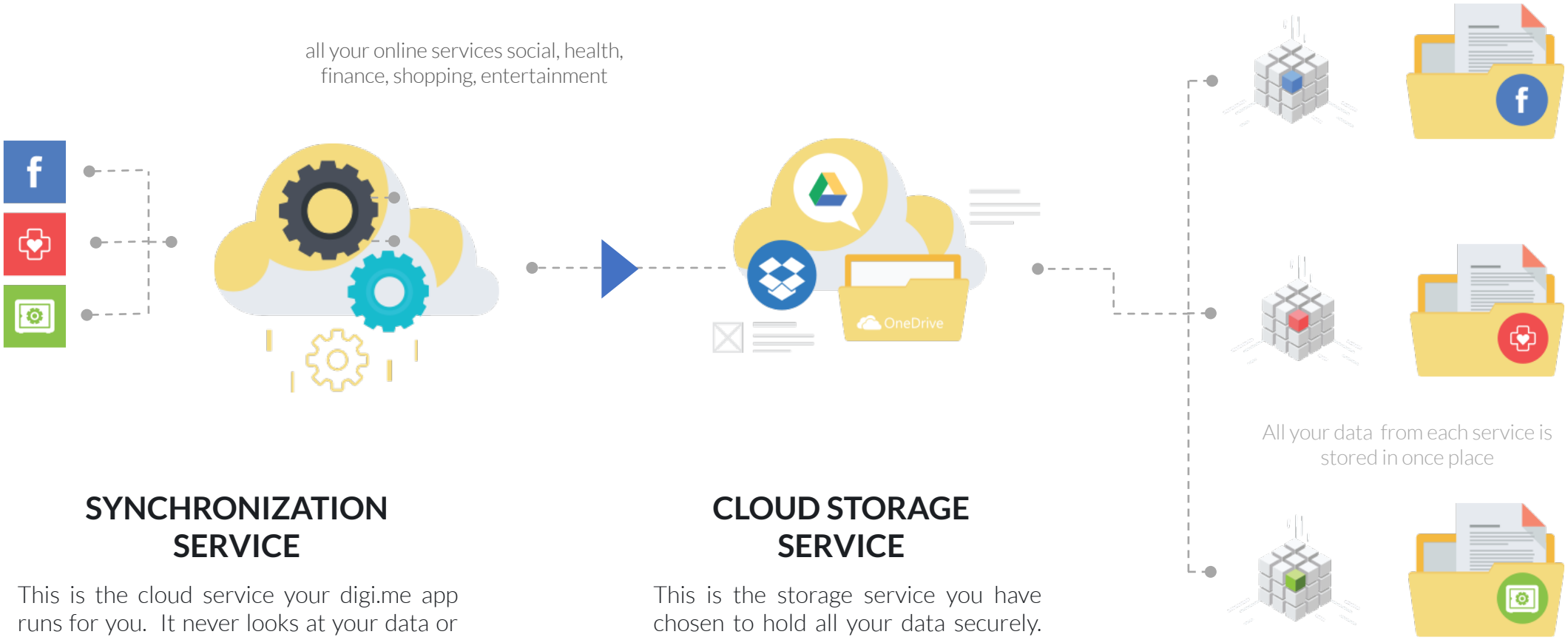
digi.me

skunkworks.digi.me
everything below the pixels

Synchronisation | PRESENTATION

the cloud synchronises all your data

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



All your data from each service is stored in once place

SYNCHRONIZATION 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

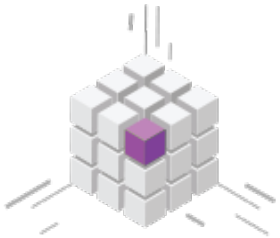
all files are viewed after being decrypted with their unique key

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

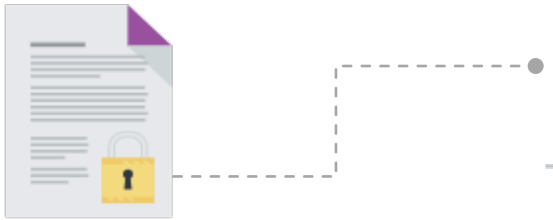
MONKEY PERISCOPE

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 pCloud library



ACCESS DATA

The password unlocks the key to unlock the key for the documents that hold the data you want

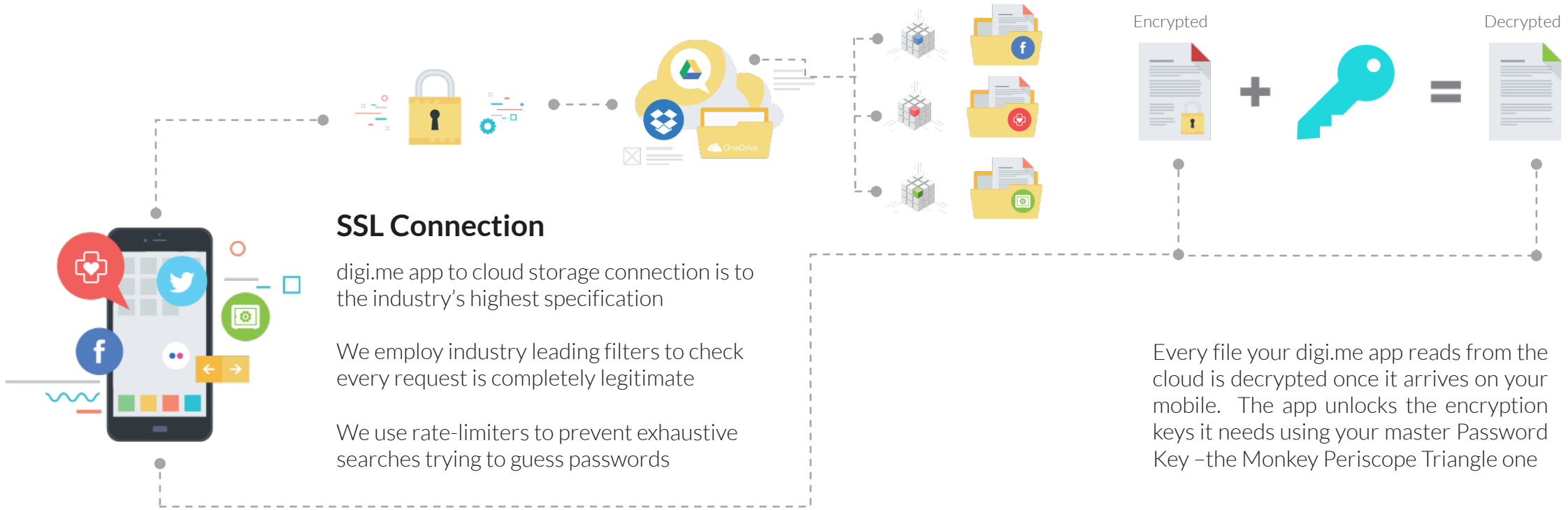
VIEW DATA

The unlocked data is then presented to the application

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. The app unlocks the encryption keys it needs using your master Password Key –the Monkey Periscope Triangle one

Security Model | PRESENTATION

Our Products Must be Proven

Our systems are independently tested regularly and monitored continuously for changes and weaknesses

THREAT MODEL

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.

SECURITY REQUIREMENT

Firewalled
All remote access must be via commercial firewall (Checkpoint) and integrated threat monitoring and profiling (Splunk)

Strict SSL
We require all SSL implementations to use Pinned Certificates from trusted root authorities and all HTTPS connections to explicitly control known configuration risks (including ECDH curve selection, header controls and Cypher Suites)

Rate Limited
We require all API access to data request services to be rate limited to prevent brute force and fuzzing attacks

We assume all major attack tools and methods will be used, including but not limited to:

- Man in the middle (MITM), SQL injection and interlocution
- Certificate forgery and replay attacks
- Volume (denial of service) attack and brute force/fuzzing attacks
- Application reverse engineering and corruption
- Known vulnerability profiling

Swagger Definitions
We require that all public facing API are protected by strict Swagger definitions that explicitly define valid inputs in full RegEx format.

Authentication
We require all API access to be via valid user identifiers

Encryption
We require strong key management RSA-2048 and strong crypto (AES-256) for file content encryption. This includes any encrypting databases on devices and memory databases in cloud services

Crypto code libraries
We require all crypto libraries used in implementation to be from proven sources that have been hardened by significant time in pubic use.

Crypto verification
We require all crypto based code elements to be verified by a full suite of known good and bad content.

Deployment verification
We require all deployed crypto/security components to be verified live in use via acceptance test AND continuous verification of certificates and open network services

THANKS

FOR WATCHING

Visit Us

www.digi.me