SOLUTION BRIEF

UBIQUITOUS DATA SECURITY

Secure any type of data, on any device, anywhere… without impacting performance.

HIGHLIGHTS

- PATENTED SINGLE SOLUTION
  100% pure software solution protects data everywhere: server, cloud, endpoint, application, & IoT – protected by multiple, granted patents!
- EXTREMELY LOW OVERHEAD
  Our solution causes virtually NO performance impact or latency to systems – even on single core machines – hello IoT!
- LIGHTWEIGHT AND FLEXIBLE
  Available as a software application or embeddable into existing applications and devices (via SDK) – super tiny at 14-30mb!
- DEVALUE STOLEN DATA
  Our patented techniques render stolen data useless to the bad guys.
- ENTIRELY TRANSPARENT TO THE CUSTOMER EXPERIENCE
  Device or end user. No one knows we're there!
- TRANSMISSION AGNOSTIC
  Operates over Internet Protocol (IP), cellular, microwave, or satellite.
- DIVERSE ENCRYPTION SUPPORT
  Out-of-box we deploy AES 256-bit encryption, or any encryption suite of your choice.

Contact us to learn more!
www.ubiqsecurity.com

A BETTER APPROACH TO DATA SECURITY

Old-guard, perimeter-centric models are no longer effective. Organisations are no longer bound by four walls, and a moat outside your castle won't stop the flying monkeys or stop the wrath of a disgruntled groundskeeper.

But you already know that. What you're trying to figure out is how do you protect your most valuable digital asset – your data. The problem is, you have data everywhere – cloud, endpoints, file servers, databases, applications, edge devices, IoT, etc. – and securing it requires multiple, disparate, complex, and resource-intensive "point products."

HERE'S WHY YOU SHOULD CARE ABOUT WHAT WE HAVE TO SAY

Ubiq has developed a patented, 100% data security software solution that secures any type of data, on any device, anywhere… without impacting performance or user experience. Yes. No impact. No joke.

FRAGMENTING
DISASSOCIATING
ENCRYPTING
DISPERSING

Ubiq developed and patented an **asynchronous multithreading** technique, which allows us to exploit available compute on a system, without impacting system performance. We then leverage this technique with our data security model, which involves a 4-step-process to secure any data type:

1. Fragmentation
2. Disassociation
3. Encryption
4. Dispersion

Each fragment (and you can make as many as you like) is encrypted with its own unique encryption key (AES 256 out-of-box) and can be stored separate from the other fragments. If an encrypted fragment is intercepted in-transit or accessed at-rest, it is nearly impossible for the bad guys to make any use of it. They don't know what data type it is or if it represents all or just a small portion of the data. This renders the stolen data fragments useless.

Fragments can also be transmitted across multiple channels – IP, satellite, radio, or microwave – to the same destination or multiple destinations.

Hot tip! Ask for a demo, it's much easier to see it in action.

SECURITY WITH BENEFITS

Ubiq not only provides robust data protection but maintains customer experience with its low latency and transparent operations. Users can keep using existing tools and workflows while their data is secured in the background. You no longer have to compromise system performance, speed, or high costs when adding security to your environment.

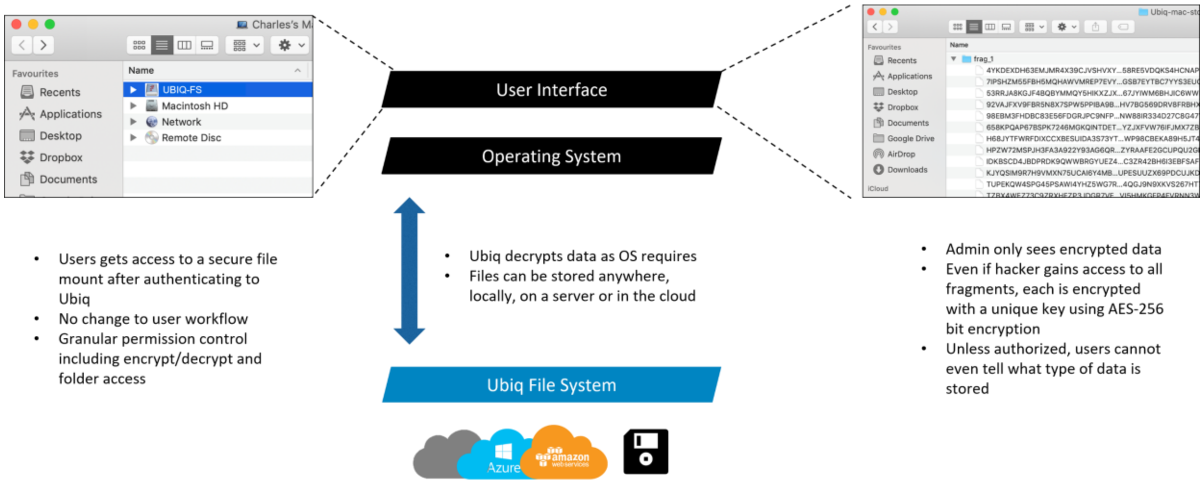
AVAILABLE IN TWO FLAVORS

Depending on your requirements and environment, Ubiq offers two options – an out-of-the-box software application, Trusted File Manager (TFM) or a Software Development Kit (SDK), which can integrate into existing applications or IoT devices from day one.

TRUSTED FILE MANAGER (WINDOWS, MAC, CLOUD)

The Trusted File Manager (TFM) works to protect the files being accessed by staff and other recipients of unstructured file data. It provides a transparent user experience, seamlessly integrating into existing workflows to create and encrypt data files at inception.

Data is automatically fragmented and encrypted using the Ubiq encryption process and. TFM gives administrators the ability to enforce data governance policies and least privilege access to ensure that users only have access to the data they need to do their job. TFM can also remove access to the secured files from system administrators further enforcing separation of duties and minimizing potential leakage.


Charles's M
Favourites
Recents
Applications
Desktop
Dropbox
Documents
Name
UBIQ-FS
Macintosh HD
Network
Remote Disc
User Interface
Operating System
Ubiq File System
Azure
amazon web services
Ubiq-mac-sto
Favourites
Recents
Applications
Desktop
Dropbox
Documents
Google Drive
AirDrop
Downloads
iCloud
Name
frag_1
4YKDEXDH63EMJMR4X39CJVSHVXY...58RE5VDQKS4HCNAP
7IPSHZM55FBH5MQHAWVMREP7EVY...GSB7EYTBC7YYS3EU
53RRJA8KGJF48QBYMMQY5HIKXZJX...67JYIWM6BHJIC6WW
92VAJFXV9FBR5N8X7SPW5PPIBA9B...HV7BG569DRV8FRBH
98EBM3FHDBC83E56FDGRJPC9NFP...NW88IR334D27C8G47
658KPQAP67BSPK7246MGKQINTDET...YZJXFVW76IFJMX7ZB
H68JYTFWRFDIXCCXBESUIDA3S73YT...WP98CBEKA89H5JT4
HPZW72MSPJH3FA3A922Y93AG6QR...ZYRAAFE2GCUPQU2G
IDKBSCD4JBDPRDK9QWWBRGYUEZ4...C3ZR42BH6I3EBFSAF
KJYQSIM9R7H9VMXN75UCAI6Y4MB...UPESUUZX69PDCUJKD
TUPEKQW4SPG45PSAWI4YHZ5WG7R...4QGJ9N9XKVS267HT

- Users gets access to a secure file mount after authenticating to Ubiq
- No change to user workflow
- Granular permission control including encrypt/decrypt and folder access

- Ubiq decrypts data as OS requires
- Files can be stored anywhere, locally, on a server or in the cloud

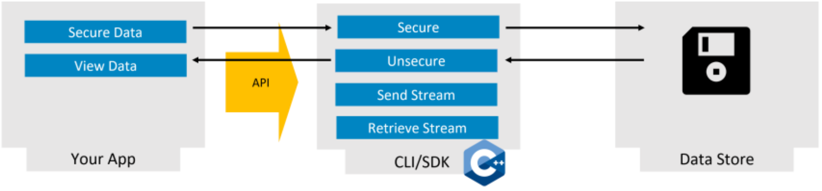
- Admin only sees encrypted data
- Even if hacker gains access to all fragments, each is encrypted with a unique key using AES-256 bit encryption
- Unless authorized, users cannot even tell what type of data is stored

SDK (ANDROID, WINDOWS, LINUX)

The Ubiq SDK allows you to leverage our core technology to efficiently secure digital data of any type.

With the Ubiq SDK, you can engineer solutions that:

- Encrypt data and store it anywhere the device can access local disk or cloud storage
- Retrieve and decrypt Ubiq protected data
- Stream data securely from A to B in real-time (including live video)
- Create a secure remote access function
- Restrict access to Ubiq protected data
- Securely encrypt and decrypt files within a local or remote filesystem



Add security to any applications.

Robust set of APIs to protect files

Flexibility to use any data store: locally or in the cloud

To find out more about Ubiq or to request a demo, visit www.ubiqsecurity.com

SDK FOR IoT – GET IT EMBEDDED

Security is key for IoT to succeed in the future and to fulfill its full potential. However, it is often forsaken due to business needs – time to market and costs. Rather than focus on infinite number of potential attacks, Ubiq helps secure data on IoT devices. Manufacturers don't need to invest into more expensive engineering resources or component and can instead implement Ubiq quickly with our SDK.

The Ubiq SDK allows for data security to be embedded at the manufacturing level, ensuring that security is built-in from conception.

- Transmit sensor data to fog computing infrastructure or the cloud
- Send remote commands or sensor data securely with <1ms latency
- Store data locally on disk without fear of physical theft
- Create trusted command & control channel
- Authenticate devices to the network