USE CASE

Securing your data in the cloud, while maintaining full control in-house.

Key Customer Concerns

- Theft of data in the cloud
- Lack of confidence in the security of cloud providers
- Risk of cloud provider breach exposing data
- Unauthorized access to data due to misconfiguration
- Cloud provider insider threat
- Limited data security responsibility and liability of cloud service provider

Ubiq Benefits

- Secures data in the cloud, while maintaining full control of encryption keys
- Protects all of your sensitive data, in transit and at rest
- Devalues data in the event of a breach, minimizing impact
- No disruption to existing user workflows
- Easy to design and administer data access policies
- Granular control over file access including protection from sysadmins
- Fully integrated key management
- Delivers “always-on” compliance

Contact us to learn more!
www.ubiqsecurity.com

THE SITUATION

The cloud provides organizations with an incredible amount of flexibility and efficiency and has radically changed the way organizations think about and deliver IT services across every major industry. The rapid growth and adoption of the cloud has also led to exponential growth of data, and with that, come new risks.

If you use the cloud today, then you are well aware of the “shared responsibility model,” which is a fancy way of saying, the responsibility over the security of your data is on you, not the cloud provider. Yes, the cloud provider is responsible for a baseline level of infrastructure security, but you (the customer) are responsible for securing your data (in their infrastructure).

There have been frequent examples of confidential and personal identifiable information (PII) being exposed and stolen, caused by insufficient security measures or avoidable misconfigurations. Some caused by mistakes as simple as misconfiguring a cloud instance as public or not encrypting a database or sensitive files and folders.

CHALLENGES

Organizations often don’t understand that the burden of data security remains with them, even though their data is in the cloud. It’s nearly the same level of significant implementation of security controls as on-premise data storage, but often overlooked due to misunderstandings in responsibility or a rush to adopt the cloud.

Alarmingly, today, 80% of data stored in the cloud is unencrypted. The majority of organizations continue to store sensitive data in the cloud without implementing appropriate security controls. Encryption should be a fail-safe, so even when data is stolen by the bad guys or inadvertently exposed, it remains worthless.

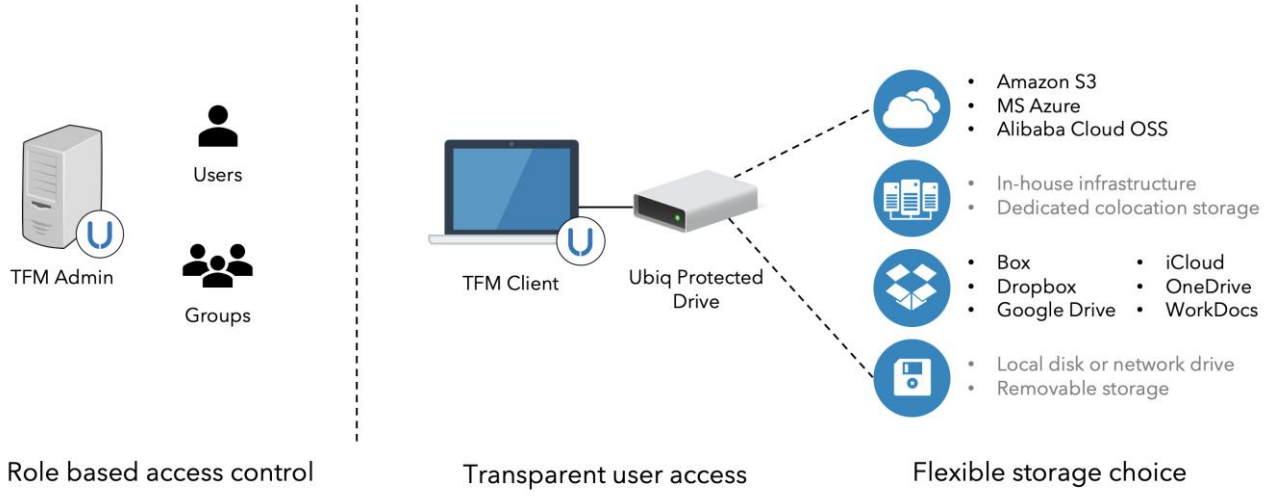
Of the organizations that do secure their data in the cloud, most leverage cloud provider encryption capabilities. An easy start, but ultimately the keys stay with the provider. Would you leave your safety deposit keys with your bank manager?

UBIQ

SECURING YOUR DATA WITH UBIQ TRUSTED FILE MANAGER

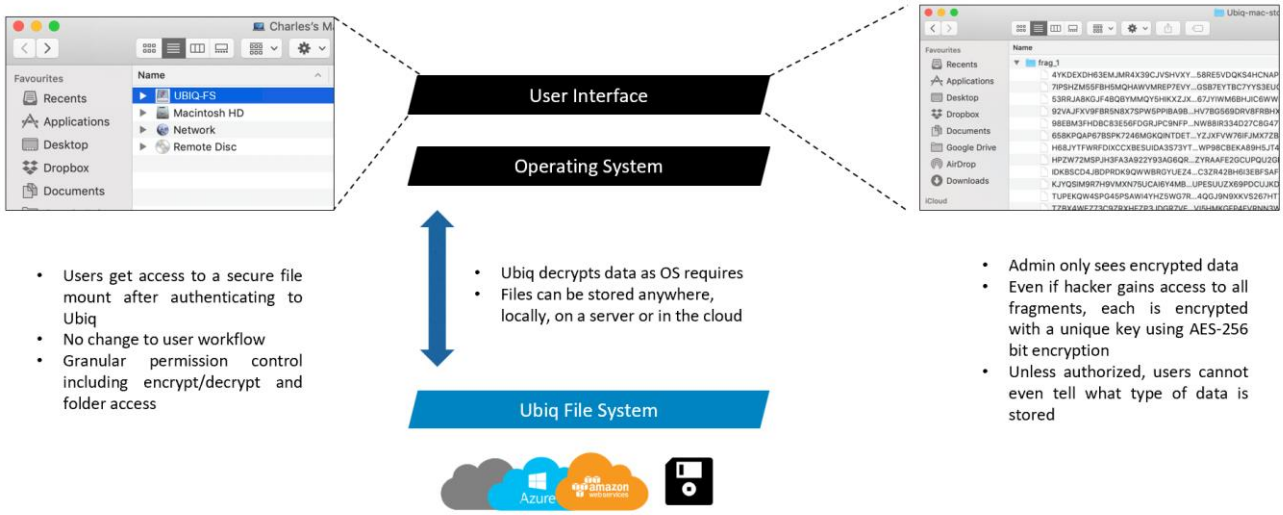
Ubiq TFM provides the flexibility to securely store your data on premise, in any cloud, or a combination of both, while maintaining full control of the encryption keys and access control in-house. Not only can you maintain a ubiquitous encryption scheme for your on-premise and cloud data, but you drastically reduce your reliance on server-side cloud provider encryption services. Most importantly, users can work with data stored in the cloud as if it resided on a local drive, while, unbeknownst to them, the data is transparently and automatically protected in the background. Productivity is maintained as users just work as per normal – with no changes to workflow or user behavior. It provides a transparent user experience to create and secure data files of any type at the point of inception.

TRANSPARENT, SECURE CLOUD AND/OR ON-PREMISE DATA STORAGE



Data is automatically fragmented and encrypted leveraging the Ubiq security model and stored in a single, or number of, assigned repositories. Administrators manage which repositories users can store data to and users simply drag and drop their data in folders via their local machine. TFM also 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 is also completely software based and consists of a very lightweight client software application and GUI for management and administration. The diagram below demonstrates just how simple, secure and transparent the user experience is.



To find out more about our Trusted File Manager or to request a demo, visit www.ubiqsecurity.com

All rights reserved by Ubiq Security, Inc.