olmogo whitepaper

highly secure cloud

The cloud offers appealing conveniences to local server structures; but conventional cloud solutions are vulnerable to attacks and the stored data can be read by third-parties.

olmogo found a way to offer companies 100% privacy, governance and absolute security in storing data, while ensuring that no third party has access to it – not even the provider.

Due to the strict data security measures we implemented in olmogo, administration becomes optimized, streamlined and easy to manage.

highly secure cloud

olmogo enables a completely different approach to storing data in the cloud by following a strict zero information principle: the infrastructure neither knows size, type or actual content of stored data as everything is encrypted, scrambled, and distributed by the client. Even a malicious insider would not have a chance to view your data - it is not even possible to spy the number or type of files you have stored.
Each and every file gets its own individual symmetric key which can be subsequently shared with other olmogo members to allow access for third parties. Access keys are encrypted by the member's public keys so that they can be stored in the olmogo infrastructure. To facilitate key management for your private keys, those are stored and encrypted in a patented way such that only the owner can gain access to the keys using two-factor authentication.
This gives you or your business 100% security, privacy and governance for your data.
Administrative requirements of the infrastructure are lean due to the inherent data security of olmogo, drastically decreasing costs per volume.
Use olmogo as a stand alone solution or as an enhancement for existing services you are already working with like amazon cloud, SAP or others.

philosophy

olmogo has put security and data governance in the center of its design and provides fully encrypted data storage and data transmission using state of the art techniques, securing your data even in the presence of ubiquitous software errors.
Most important that not a provider nor olmogo has access to your information at any point of time. There is no trust center approach or security office you have to trust and rely on.

classic information handling

Using cloud today means to trust a provider. Numerous security issues have been identified by ENISA (European Network Information and Security Agency) - here some examples:

a. loss of governance: the service provider is in charge of security
b. isolation failure: customers can access data of other customers
c. malicious insider: employees of service provider misuse high level privileges
d. insecure or incomplete data deletion upon contract termination
e. subpoena and e-discovery: data is disclosed to unwanted parties

the olmogo approach

In olmogo information is stored with zero information, not only encrypting your data but also scrambling and encrypting meta data such as file size, file type, or even the number of files. A big hassle in today's encryption solution is handling of users' private keys. In one, often chosen solution, users are forced to protect their keys on their own, by encrypting them and distributing them over all necessary devices, leaving them at risk of losing their key (when a non-secure password is chosen) or of losing access to all their data (when the password is forgotten by accident, or the key file is lost). The other solution is creating a master key that can be used to recover all private keys, creating a potentially huge security gap. In olmogo, a patented solution for distributing parts of the key over the infrastructure is chosen such that access to the key can only be gained through a two-factor authentication process and where the infrastructure or an attacker will still not be able to recover valuable key information. Furthermore, passwords are part

of the authentication process only and can be reset if necessary.
What are the answers of olmogo to the above listed security risks of todays cloud solutions?

a. There is no loss of governance at any point of time since the owner of the data is always in possession of the decryption key, and can control, who else may gain access.
b. All your data can only be decrypted by authorized users as encryption keys are also encrypted and isolation failure even of multiple olmogo data units will not result in a breach.
c. The olmogo architecture prevents a breach even with a sniffed password; at worst a malicious insider could manipulate a user key or prevent a login-action the user would notice immediately and that will be logged and evaluated internally.
d. olmogo encryption scrambles and encrypts all data - therefore incomplete data deletion will render no risk
e. olmogo data and meta data are scrambled and encrypted as well. Even disclosed to unwanted parties these data will render useless.

independence from proprietary technology

Important to know that olmogo uses standard encryption technologies and an open-source client API. As systems can be hosted individually, no dependence on olmogo occurs. You as a customer choose the storage place and have access to your information with your keys at any point of time.

olmogo ag

Rosenweg 3
CH-6340 Baar
Phone: +41 41 767 36 38