How Fasoo Improves Cloud Security

en.fasoo.com/blog/how-fasoo-improves-cloud-security

The enterprise is moving to the cloud to ease collaboration for partners and employees. The cloud enables work-from-home and hybrid working models and enhances productivity.

But the cloud is vulnerable to human error and misguided settings, putting your data at risk of unauthorized access. According to Gartner, preventable misconfigurations and end-user mistakes cause more than 99% of cloud breaches. Cloud providers use a flavor of security. But data needs its own protection.

What's the risk of storing data in the cloud?

End-users share Dropbox links and credentials from personal smartphones via Wi-Fi hotspots. They email documents to friends and unauthorized third parties. You'd no more send your data out into the world without policies, access controls, and encryption than send a child out into the cold without a coat. But if you leave security to the cloud, who knows where your data ends up.

Amazon S3 buckets include unlimited storage. But weak settings leave default credentials intact, granting limitless access to criminal hackers who automatically search and exploit bucket links. When criminal hackers kidnap your files, cloud cyber defenses seldom follow behind. You need centralized control with enterprise security that wraps your data and sticks with it.

Enterprises work with many cloud providers, passing data from one environment to the next, one job to the next. You may have some visibility when you pass data directly to the cloud. But what happens when that cloud routes your data to other cloud environments for processing? It's one thing to entrust your child to someone *you* know; it's another to let them hand her off to someone *they* know.

Cloud providers may offer security policies, identity and access controls, and encryption for data in transit and at rest. But those stop short where the cloud ends, leaving your intellectual property (IP) open to theft by criminal hackers and exploitation by unscrupulous competitors.

How do I protect my sensitive data in the cloud?

Enterprise Digital Rights Management (EDRM) eases moving to the cloud, binding location-agnostic security controls to unstructured data. EDRM embeds encryption, persistent IDs, and access control policies with sensitive documents. Your custom controls travel with your files into unmanaged, unsecured environments.

EDRM maintains data governance policies and controls on your confidential documents whether you move them to Salesforce, Box, Microsoft Azure, or AWS. You can track documents in and beyond the cloud, maintain access controls, and change granular permissions and privileges at any point using centralized policy management.

You don't have to care what cloud has your data; EDRM keeps it safe when cloud security fails. If the cloud provider has a breach, so what? EDRM maintains the security policies, controls, and enforcements you've set in motion, no matter who has your data.

You can ease moving to the cloud by mitigating your risk. The Discovery Classification Tool (DCT) identifies old, redundant, and obsolete data. You can delete obsolete files and duplicates and archive data you must keep, reducing your attack surface, data management requirements, and cloud costs. Then use EDRM to apply policies and encryption to the data you use, and move it to the cloud.

Chat with the Fasoo team and discover how your peers deploy Enterprise DRM in the cloud.