DAtAnchor

Organizations Must Control their Data

In order to ensure against data loss, businesses traditionally restrict user access to applications and files to a selected trusted circle of employees. Once access is granted, the data is free to travel as requested by the user. This data protection method does not guard against the bad actor who gains access to systems, nor does it prevent the nearly 70% of employees that leave a company with data.

Anchorize your data

With DAtAnchor, security requirements travel with the file wherever it may go, regardless of email, document management system, cloud, application platform or whether the file was taken on a USB drive. It works by attaching security requirements, or "Anchors", to the file itself rather than placing unrestricted files in a secure folder or location. These Anchors are a set of boundary requirements for access that must be met in order to unlock the file from military-grade encryption. Examples of Anchors can include organizational requirements such as groups or roles and/or geo location parameters such company Wi-Fi proximity, proximity to the user's mobile phone or IoT device for two-factor authentication. This security process is made completely transparent to the end user such that sharing of data between authorized parties is easily and safely facilitated without the worry of data loss as data in transit, use and at rest remains encrypted. Users change nothing in the way they work and use applications.

True business control and ownership over data

Using the DAtAnchor administrator console, businesses can easily define a boundary for file access which persists regardless where the data travels and without any action by the users. Through this console, any piece of data can be tracked and monitored in a highly granular fashion, including global access patterns and other analytics. It is here that applications are blacklisted and whitelisted for additional protections. Administrators maintain full dynamic revocation control over applications and files such that data will become encrypted while in use should an Anchor be violated. Furthermore, rules around strong encryption and key management are fully automated, saving tremendous time when compared to traditional, manual data governance practices.

Increase collaboration while reducing risk

Employees, contractors and partners exchanging data within the security parameters set by DAtAnchor will never know it is there, enabling a freer exchange of data without the risk of sensitive data loss.

Organizational Data Control

File security wherever, whenever
Set requirements for security by roles, geo-location, Wi-Fi proximity and more

Total control over your data
Administrators maintain full dynamic control over files and data with a click

Fully-automated safety features
Save time over data governance with industry grade settings built-in

Dynamic Compliance

HIPAA Compliance
Works with your existing HIPAA compliance solutions and communication platforms, further complementing protection against human errors and external threats

GDPR Compliance
Businesses are able to prove a secure breach (i.e, lost data remains encrypted) and do not need to disclose breaches to data owners per GDPR

Files & Storage
Granular access controls provide automated and perpetual data governance. Encryption and cybersecurity protection is anchored to the data wherever it goes

"If you look at a data breach, you can always find a human error or an adversarial action at it's core. DAtAnchor is the answer to data exchange without the risk of sensitive data loss."

— Emre Koksal, CEO, DAtAnchor