Protecting Unstructured Data

Introducing Anchor for data protection and control.

anchor

Sensitive Data? Anchor It™

Organizations Must Protect Their Data

Much of the sensitive data businesses create is unstructured. In order to ensure against loss, businesses traditionally manage user access via manual processes. Once access is granted, the file is free to travel as requested by the authorized 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. Furthermore, external attackers have been more sophisticated than ever. Ransomware has evolved into Doxware and successful attacks have increased by more than 350% in the last year. With the recent SolarWinds attack, businesses must assume a breach and make sure that network breaches do not result in file losses.

Anchor Your Files

With Anchor, security requirements travel with the file wherever it may go, regardless of email, document management system, cloud, network server, 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 FIPS validated encryption. Examples of anchors can include organizational requirements such as groups or roles, geo-location, and/or connectivity requirements such as organization Wi-Fi, proximity to the user's mobile phone or IoT device. 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, in use and at rest remains encrypted. Users change nothing in the way they work and use applications.

True Ownership & Control Over Data

Using the Anchor administrator console, businesses can easily define a boundary for file access which persists regardless where the files are consumed and without any action by the users. Through this console, any file can be tracked and monitored in a highly granular fashion, including global access patterns and other analytics. Administrators maintain full dynamic revocation control over applications: files remain 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.

Classify Files and Make Rules

Anchor seamlessly integrates with classification solutions. Files are scanned, classified automatically, and subsequently anchored based on their sensitivity level, as per specified by the organization. Integration with a variety of classification engines have been demonstrated. As a result, risks identified are mitigated immediately.

File Security, Simplified

Zero trust - enriched

Set requirements for security by roles, geo-location, Wi-Fi proximity and more.

One-click management

Straightforward deployment. Administrators maintain full control over files with a click.

No change in user workflows

Users access files without a change in their way. Minimal training, no user involvement.

Compliance

CMMC Compliance

The CMMC defines the bare minimum you must have to be allowed to handle CUI. Anchor is the state of the art. Go above and beyond your competition while minimizing cost and complexity.

HIPAA, NIST, GDPR, and Others

Businesses are able to prove a secure breach (i.e, lost data remains encrypted) and do not need to disclose breaches. Full monitoring of all actions taken on data at per-file granularity.

Files & Storage

Granular access controls provide automated and perpetual data governance with or without classification. Encryption and cybersecurity protection is anchored to files wherever they go with complete audit logs.

> " No matter how strong a castle you built around your network, you cannot assume it was not or will not be breached. You should make sure your data remains safe, regardless.
>
> – Emre Koksal, CEO, DAtAnchor

AnchorMyData.com