Who Are We?

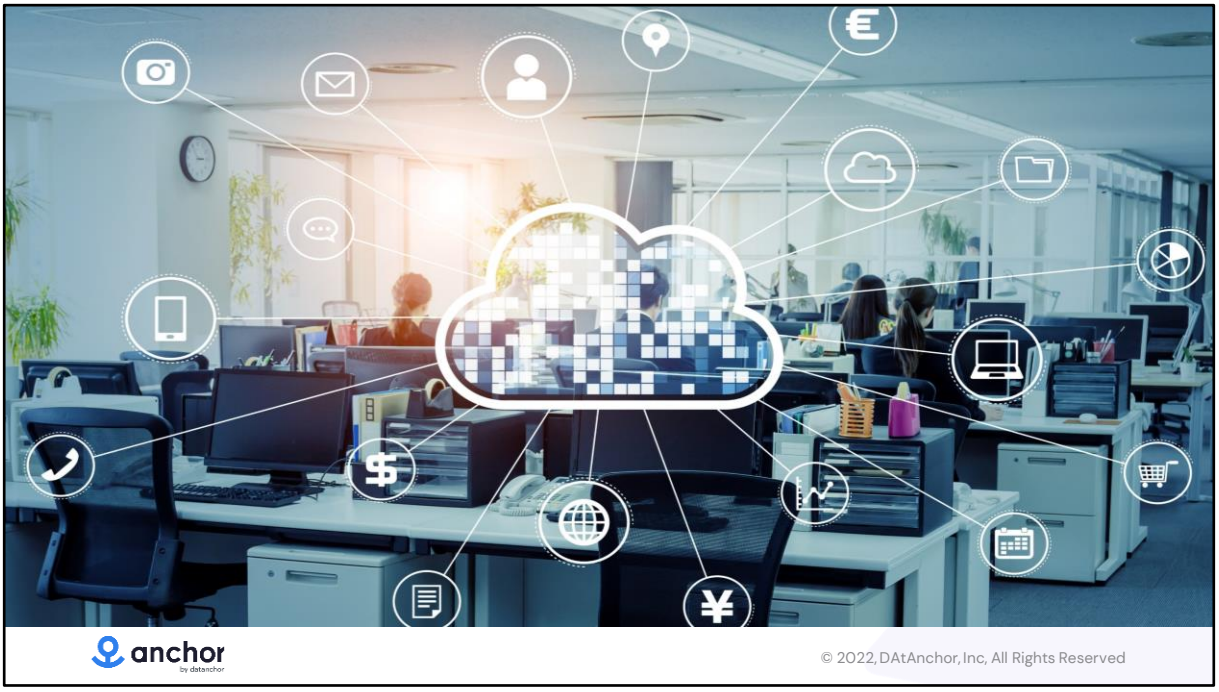
- Based in Columbus, Ohio
- Founded in 2019
- Product came out many years of R&D at The Ohio State University.
- Customers in US DoD, Banking, Insurance, Finance, Muni, Manufacturing, PE, and Retail
- Our mission is to empower organizations to easily and affordably realize the benefits of their information, confidently using and sharing it as needed to do business without fear of it being lost, stolen, or abused.

anchor
by datanchor

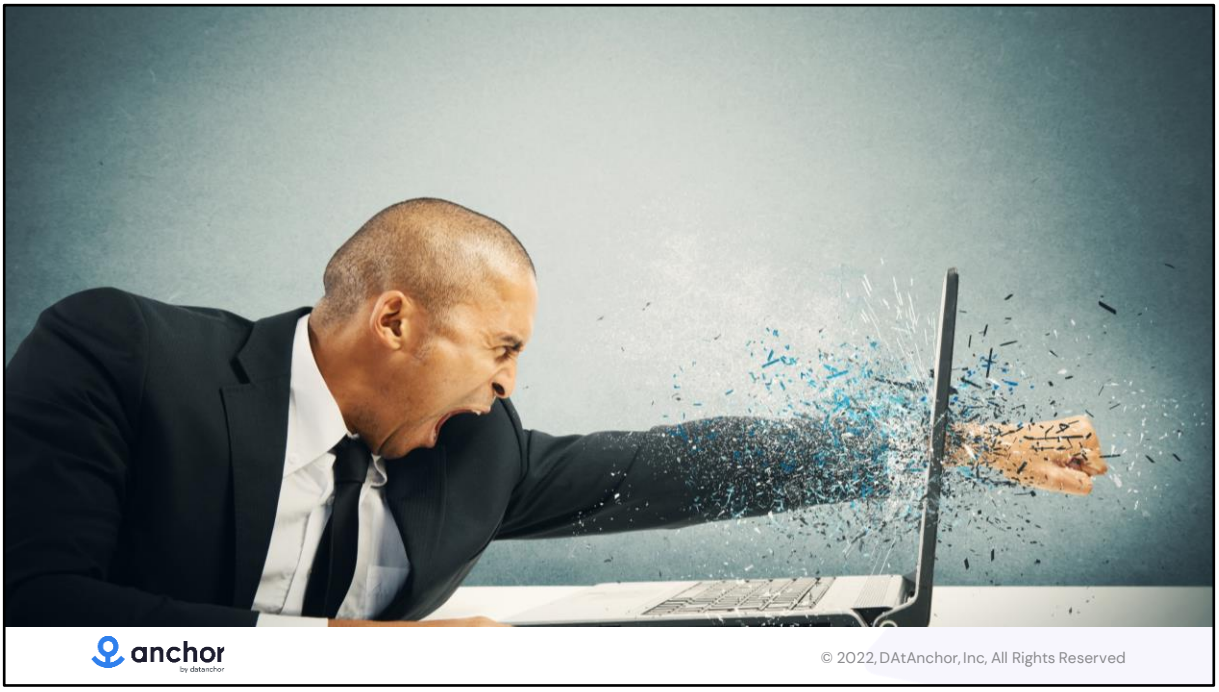
© 2022, DAtAnchor, Inc, All Rights Reserved

Anchor is a zero trust file security platform that enables the complete ownership and control required to prevent data theft, with the transparency and simplicity users demand.

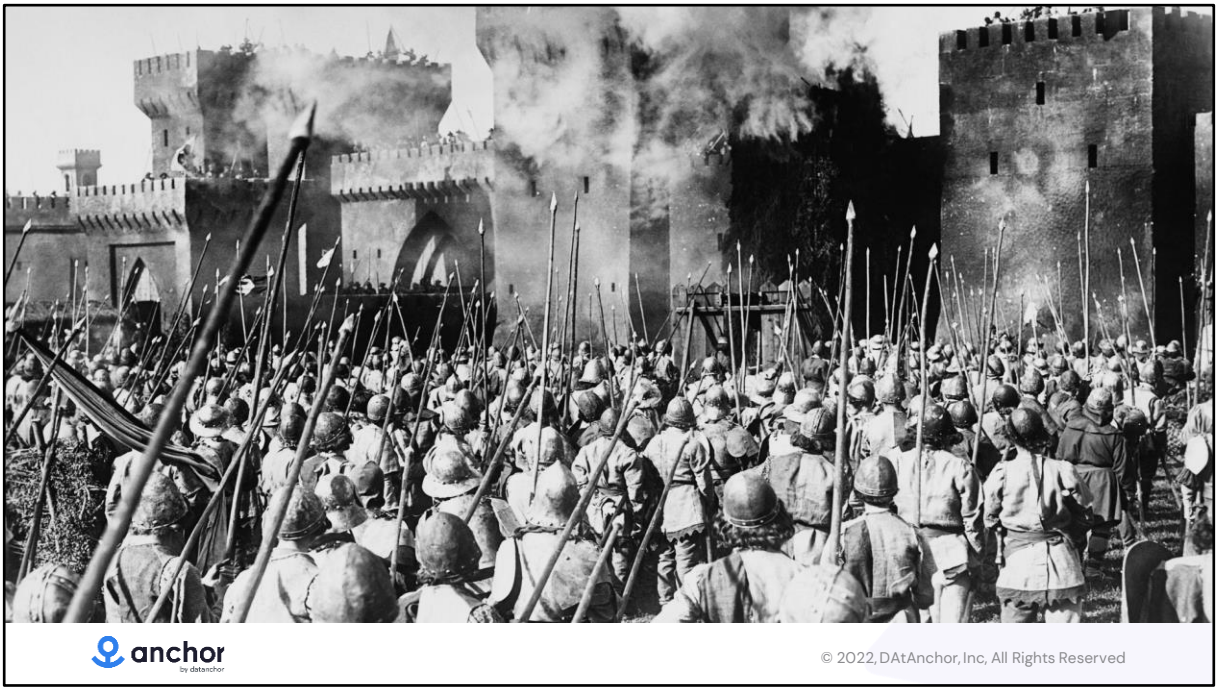
Traditional complicated IT controls, like DLP, focus on locking down networks, devices, and people. But, they have failed to protect data in three major ways. First, they only support some file types, not all.



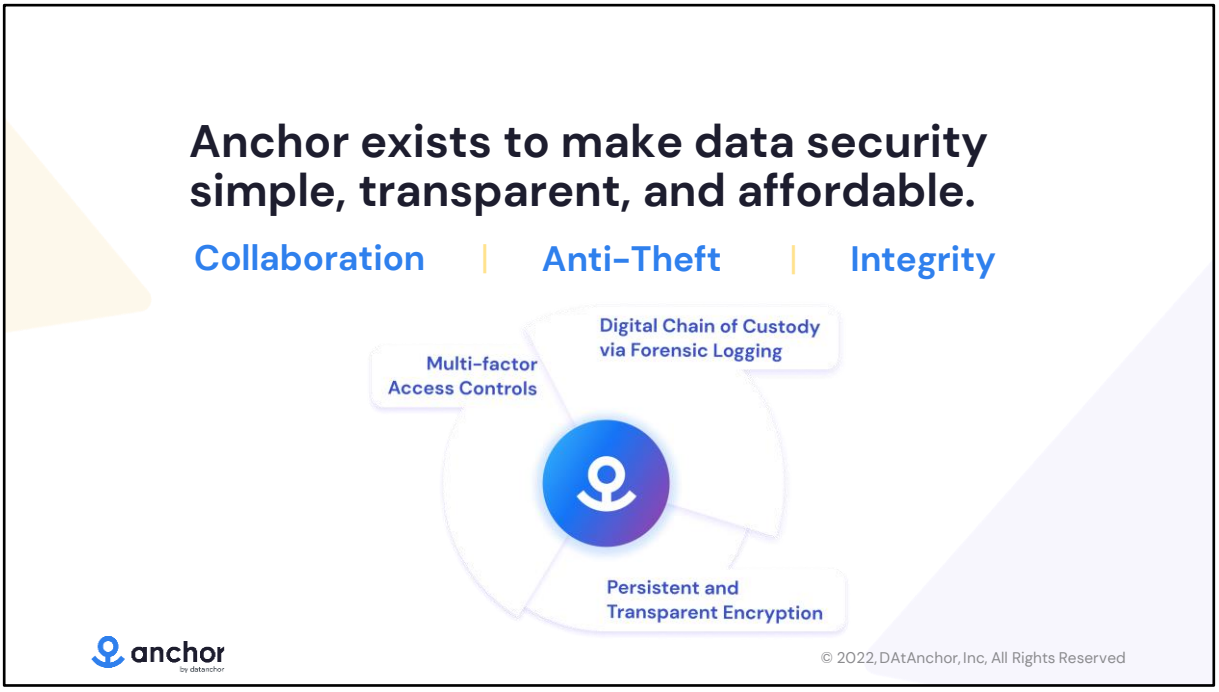
Second, the data is no longer protected once files are moved, shared, or stolen.



And third, these controls get in the way and frustrate business users to the point that they intentionally work around them,



or the business forces IT to dial back the protection, resulting in “security theater.”



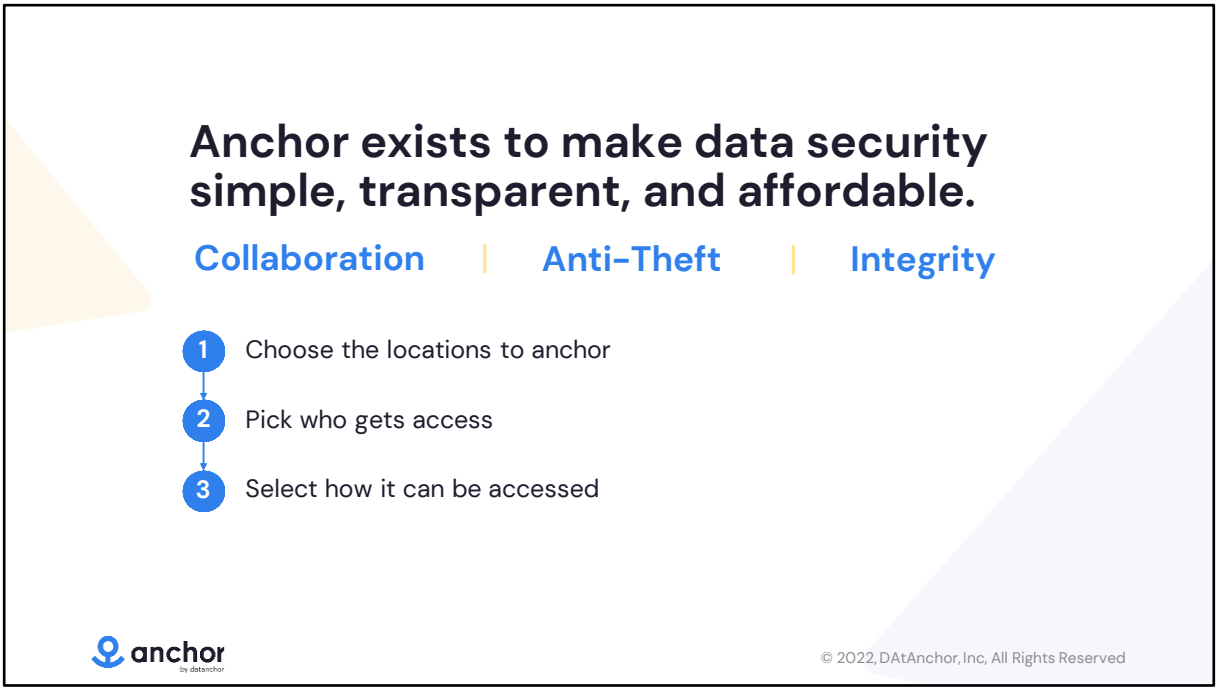
Anchor inverts the equation by baking protection into the data, invisible to the business users (like antivirus) so that files are free to travel and security is out of the way. Simply put, wherever the data goes, it's protected.

<click>

Anchor is a SaaS platform with an endpoint component that bakes protection into your files with a unique

transparent combination of encryption, continuous multi-factor access controls, and a digital chain of custody. Anchor empowers you to maintain control of your files while sharing and collaborating on-premise or in the cloud, including forensic logging and revoking access.

Within minutes, our customers end data theft across their organization by Anchoring sensitive information for all file types, such as source code, corporate documents, and intellectual property (like CAD designs). All without requiring them to change existing IT controls or how their users and applications work today.



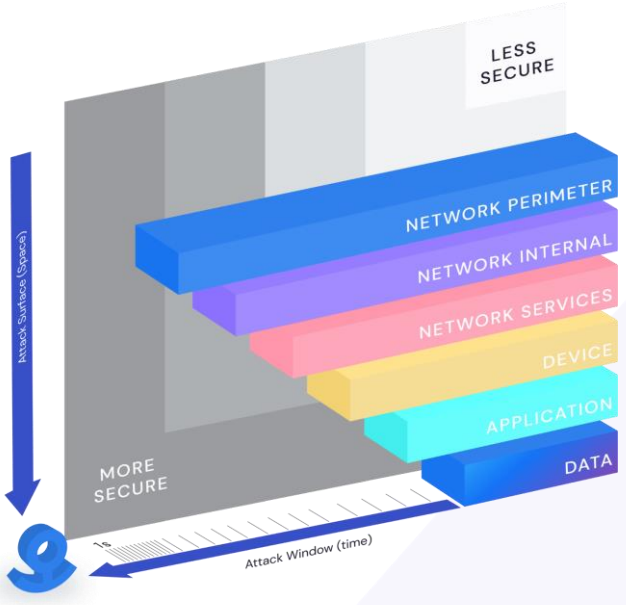
And it really is as simple as 1, 2, 3.

1) What do you want to protect?
2) Who do you want to view or use the data?
3) How do you want them to get it?

Zero Trust Data Centric Security

Maximizes file security, deployment options, and costs while minimizing:

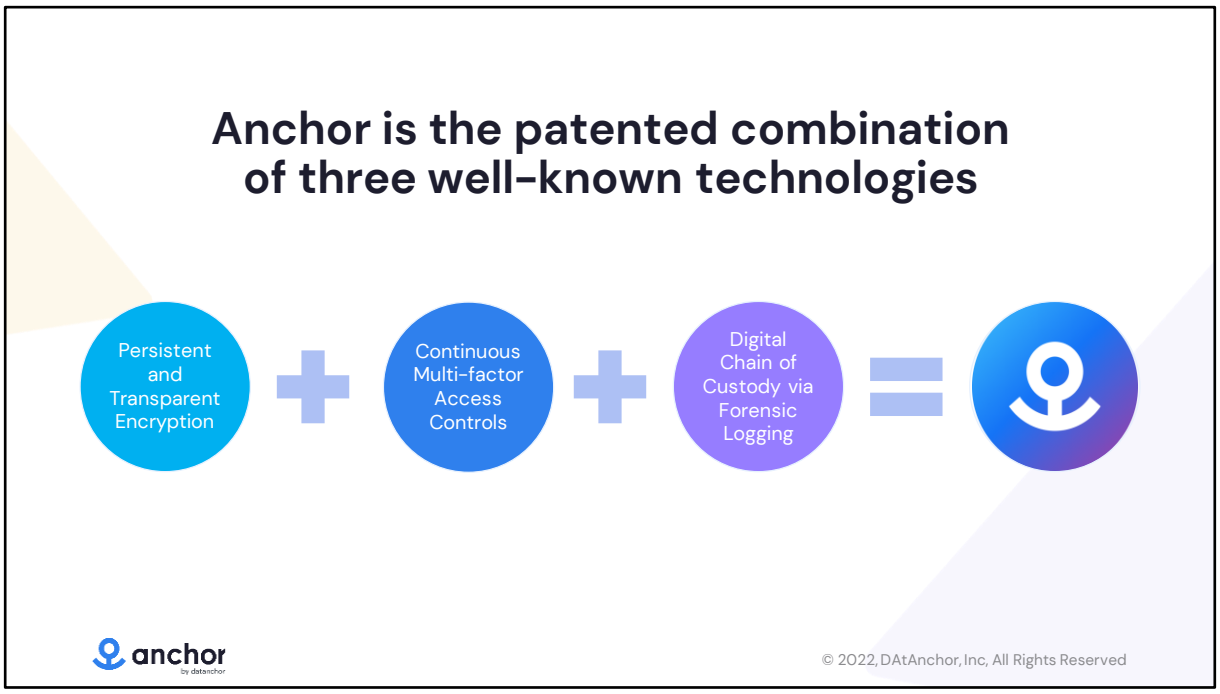
- Attack Surface (Space)
- Attack Window (Time)



anchor by datanchor

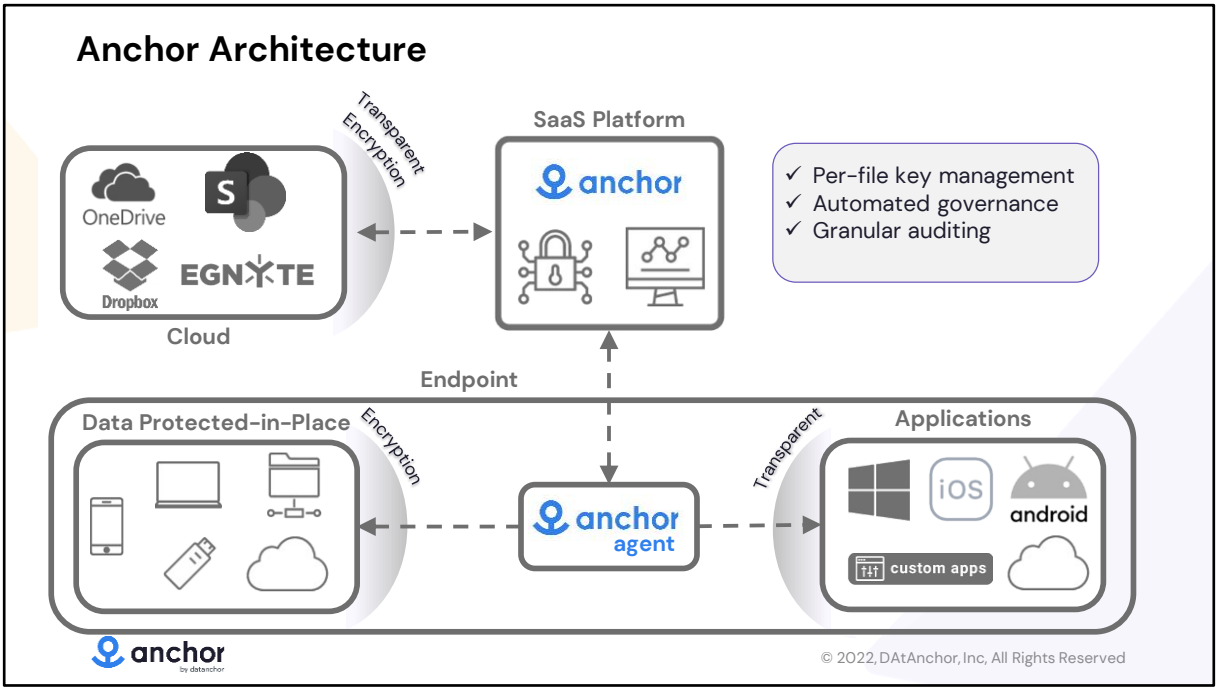
© 2022, DAtAnchor, Inc, All Rights Reserved

And now your data is Anchored and you have implemented Zero Trust Data-Centric Security.



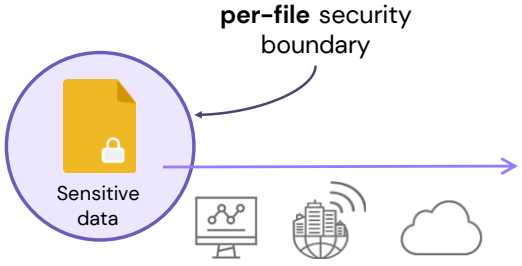
As I previously mentioned Anchor is composed of these three things…

From left to right:
1) We encrypt each file so that it is always protected
2) We use multi-factor access controls enable the right kind of access and
3) We log every single successful access to the files so you know “who is doing what” with your data.



Just so you can get your head around our solution, I want to call you attention to the things in blue:
We have a SaaS component which is where all of the decisions are made,
And
We have an endpoint component that acts as an extension of the devices operating system, working with the existing storage you use today. This is the “worker bee”. This does the work of the encryption and passing the access requests to the SaaS platform.

Persistent Transparent Encryption



Persistent means at rest, in-transit, and in use

Attack surface: **Individual file**

Damage scale: **Single file**

In the Office, At Home, or the Cloud

anchor by datanchor

© 2022, CAtAnchor Inc. All Rights Reserved

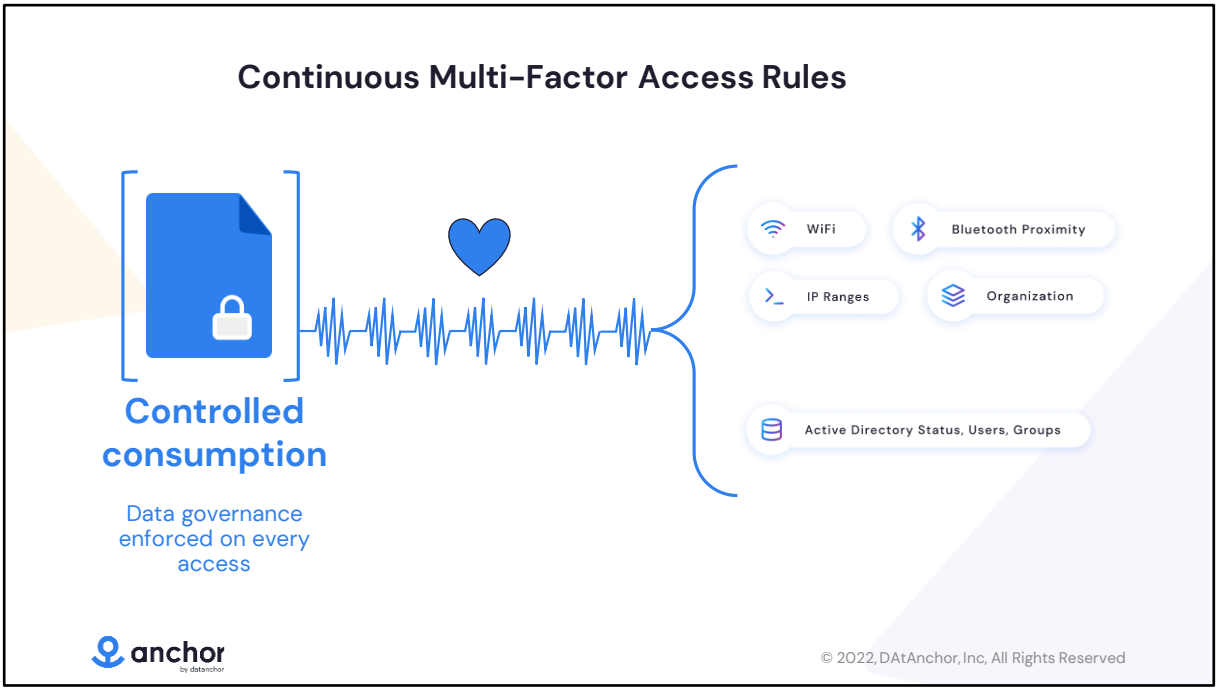
Data is independently FIPS-validated encrypted

Data is self-protecting

Security travels with data!

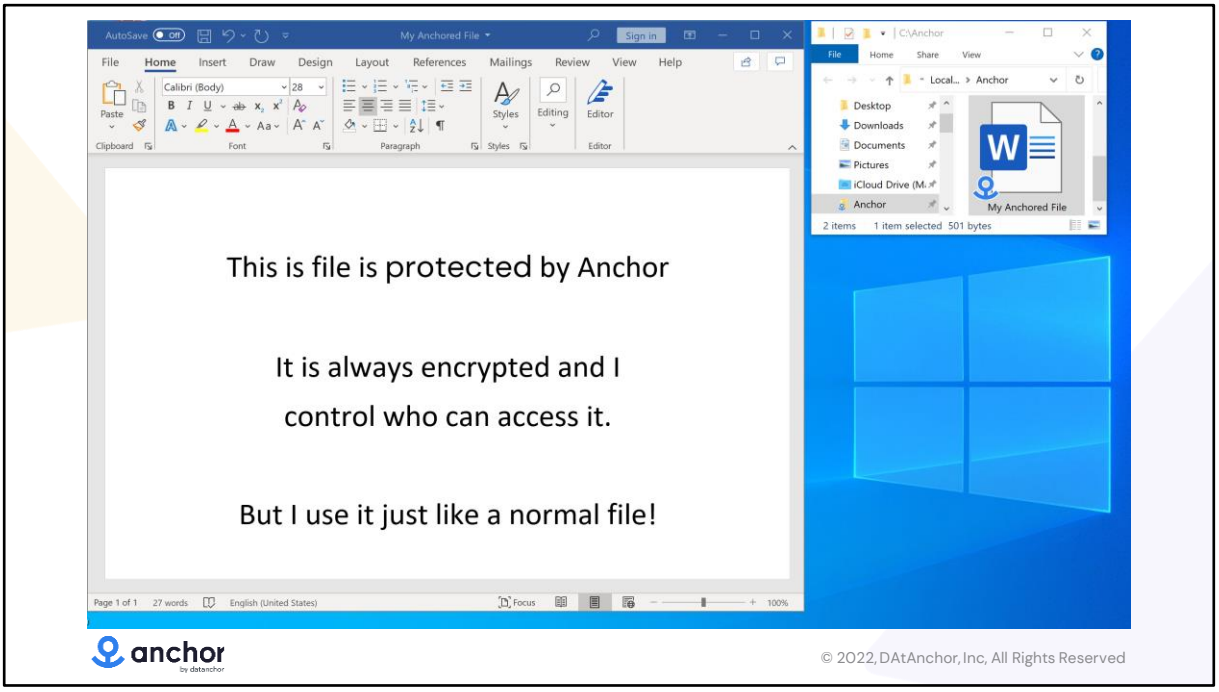
We Anchor data with Transparent and Persistent Encryption

1) Anchored data is encrypted at rest, in transit, and even while in use (saving does not generate plain text)
2) Each file is encrypted, independently. This means each file would have to be individually hacked.
3) We use FIPS-validated encryption, non-proprietary
4) This means that Anchored data is self-protecting and doesn't need to be doubled-encrypted
5) This means the file is protected whether it is on your computer, on a network share, or in the cloud.
6) Even if the files are stolen, they would never be more than cypher text

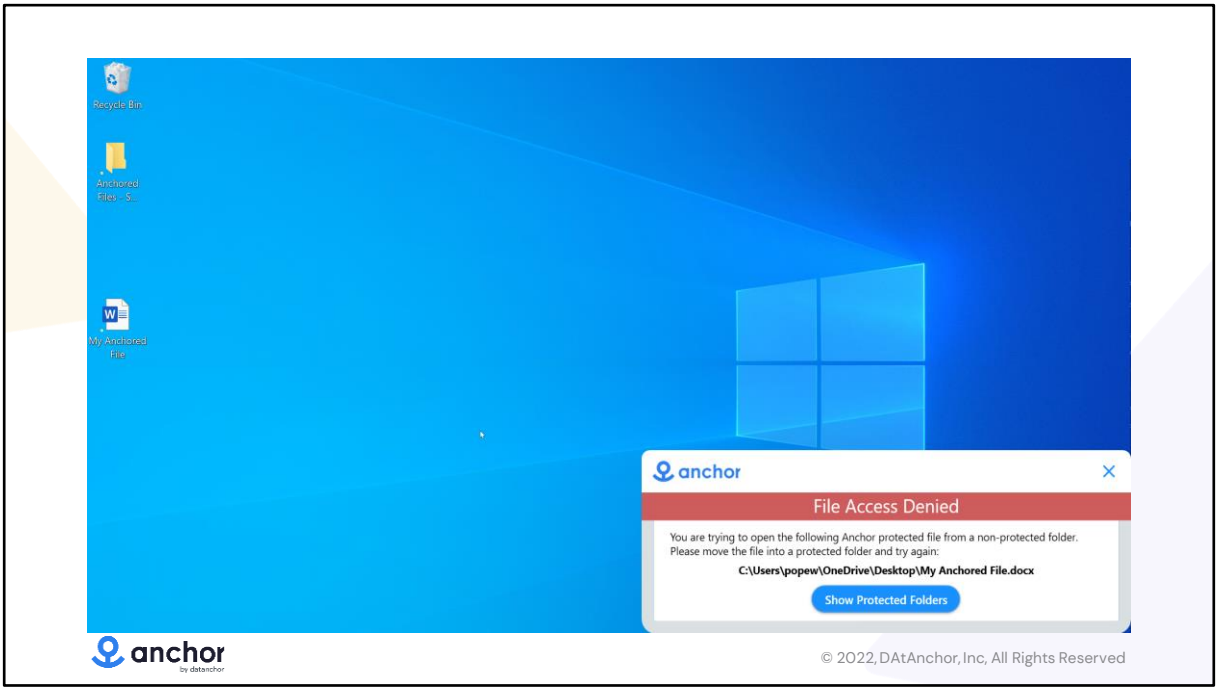


2) Continuous Multi-Factor Access Controls

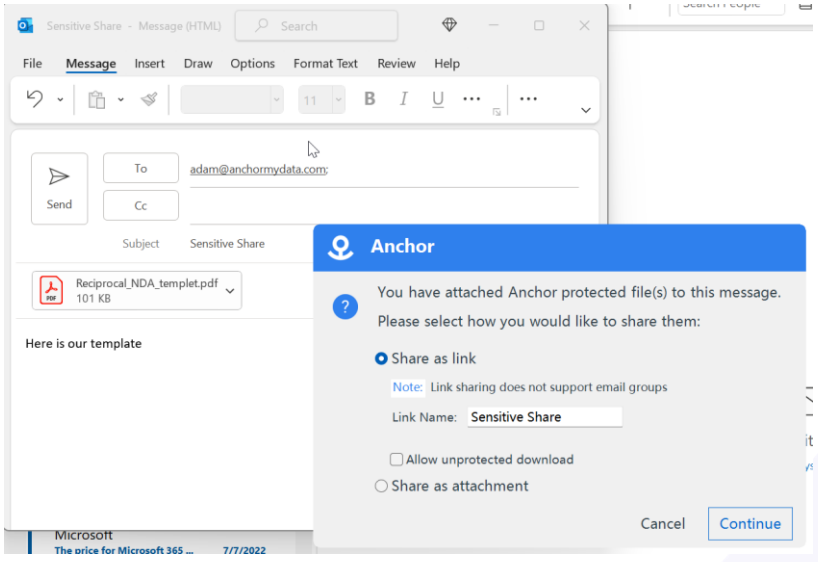
Patented heartbeat technology constantly verifies access rules in real-time based on a myriad of data sources such as Active Directory, IP Ranges, etc. When an access rule is broken, Anchor instantly revokes access. Even while the file is in use. Trust is never assumed, even after a file is open.



And, again, all of this is transparent to the user. They use the same apps in the same manner as they did before.



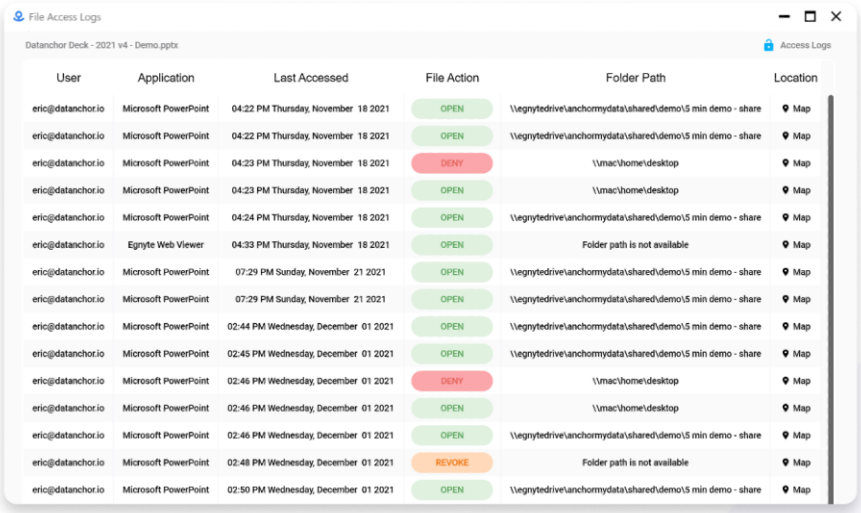
The only time they notice anything is different, is when they break the rules or access is revoked (like for an employee exit).



anchor
by datanchor

© 2022, DAtAnchor, Inc, All Rights Reserved

Chain of Custody – Forensic File Access Logs

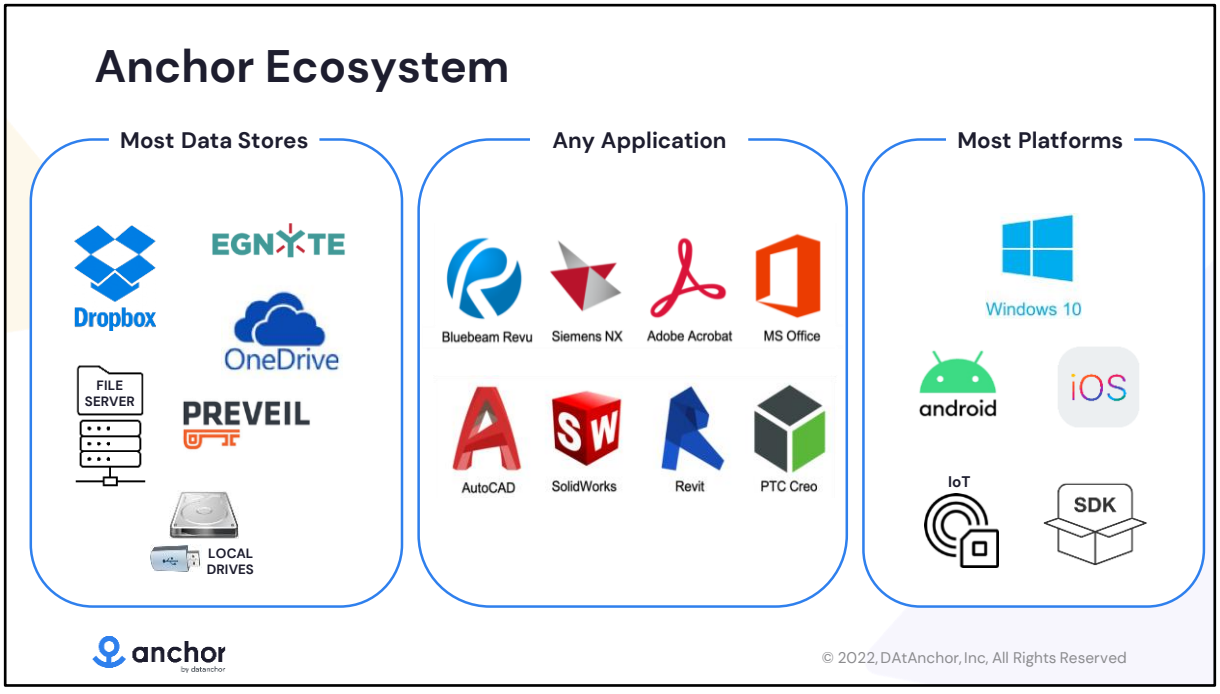


User	Application	Last Accessed	File Action	Folder Path	Location
eric@datanchor.io	Microsoft PowerPoint	04:22 PM Thursday, November 18 2021	OPEN	\\egnytedrive\anchormydata\shared\demo\5 min demo - share	Map
eric@datanchor.io	Microsoft PowerPoint	04:22 PM Thursday, November 18 2021	OPEN	\\egnytedrive\anchormydata\shared\demo\5 min demo - share	Map
eric@datanchor.io	Microsoft PowerPoint	04:23 PM Thursday, November 18 2021	DENY	\\mac\home\desktop	Map
eric@datanchor.io	Microsoft PowerPoint	04:23 PM Thursday, November 18 2021	OPEN	\\mac\home\desktop	Map
eric@datanchor.io	Microsoft PowerPoint	04:24 PM Thursday, November 18 2021	OPEN	\\egnytedrive\anchormydata\shared\demo\5 min demo - share	Map
eric@datanchor.io	Egnyte Web Viewer	04:33 PM Thursday, November 18 2021	OPEN	Folder path is not available	Map
eric@datanchor.io	Microsoft PowerPoint	07:29 PM Sunday, November 21 2021	OPEN	\\egnytedrive\anchormydata\shared\demo\5 min demo - share	Map
eric@datanchor.io	Microsoft PowerPoint	07:29 PM Sunday, November 21 2021	OPEN	\\egnytedrive\anchormydata\shared\demo\5 min demo - share	Map
eric@datanchor.io	Microsoft PowerPoint	02:44 PM Wednesday, December 01 2021	OPEN	\\egnytedrive\anchormydata\shared\demo\5 min demo - share	Map
eric@datanchor.io	Microsoft PowerPoint	02:45 PM Wednesday, December 01 2021	OPEN	\\egnytedrive\anchormydata\shared\demo\5 min demo - share	Map
eric@datanchor.io	Microsoft PowerPoint	02:46 PM Wednesday, December 01 2021	DENY	\\mac\home\desktop	Map
eric@datanchor.io	Microsoft PowerPoint	02:46 PM Wednesday, December 01 2021	OPEN	\\mac\home\desktop	Map
eric@datanchor.io	Microsoft PowerPoint	02:46 PM Wednesday, December 01 2021	OPEN	\\egnytedrive\anchormydata\shared\demo\5 min demo - share	Map
eric@datanchor.io	Microsoft PowerPoint	02:48 PM Wednesday, December 01 2021	REVOKE	Folder path is not available	Map
eric@datanchor.io	Microsoft PowerPoint	02:50 PM Wednesday, December 01 2021	OPEN	\\egnytedrive\anchormydata\shared\demo\5 min demo - share	Map

anchor by datanchor

© 2022, DAtAnchor, Inc, All Rights Reserved

3) Real-time tracking of sensitive data. Audit trails of each request, including physical location. A true chain of custody for digital data.



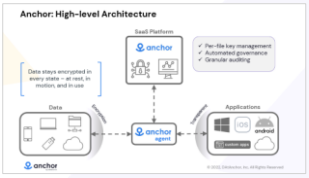
What does Anchor work with?

Anchor Team Pricing

$16
/seat/month

($192/year)

- $4,800 Anchor Platform incl. up to 25 users
- 3-year commitment, annualized fees



anchor
by datanchor

© 2022, DAtAnchor, Inc, All Rights Reserved

Why Anchor?

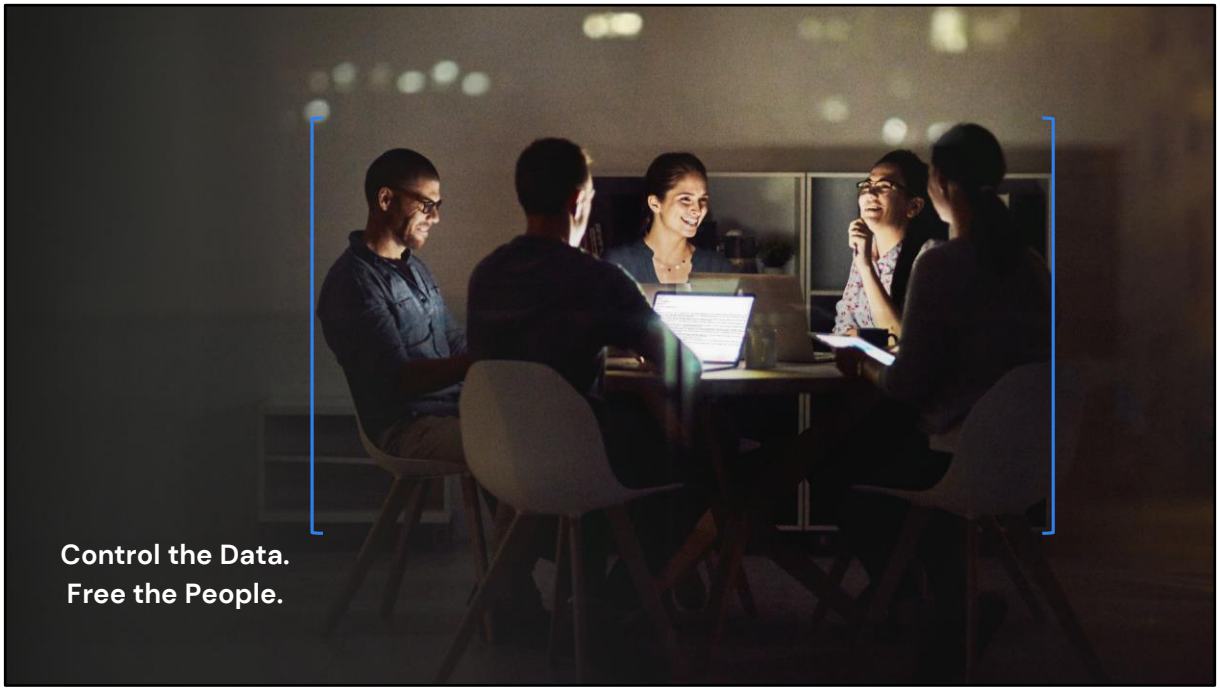
Anchor is a simple, turnkey, **low-cost** way for organizations to achieve state-of-the-art data security **without getting in the way**.

- Protects sensitive data in the face of network breach
- Simplifies data security compliance such as CMMC 2.0
- Seamless for securing flat files (unstructured data)
- **Deployed in under 90 minutes**
- Secures data sharing up and down the supply chain
- Strengthens data security for distributed/remote work
- Plays well with other tools in mixed environments

Anchor brings world-class data security to everyday users.

anchor
by datanchor

© 2022, DAtAnchor, Inc, All Rights Reserved


Control the Data.
Free the People.