anchor

Anchor for Ransomware Protection

A powerful offensive weapon in your cyber defense strategy

Defending against traditional ransomware means frequent, offline backups. But with doxware – the most harmful type of ransomware attack – attackers not only hold your sensitive data hostage, but also threaten to release it to the public if the ransom is not paid.

It's time to turn the tables on attackers. It's time to Anchor your data.

Any organization – large or small – is at risk. Ransomware attacks are often directed at specific industries, such as manufacturing, healthcare, finance, and energy. Nation states typically target the infrastructure of cities, municipalities, and utilities.

6%
of companies receive their data back after a doxware attack.

Ransomware threat growing exponentially

"Ransomware is now a primary threat for businesses and, with the past year or so considered the "golden era" for operators, cybersecurity experts believe this criminal enterprise will reach new heights in the future." ZDNET

Stop ransomware in its tracks

The best defense is a good offense

By Anchoring your data, you protect it using the same method ransomware attackers and "doxers" use to lock up your data.

Anchor is a quick and easy-to-deploy SaaS solution that delivers frictionless data security, working invisibly like antivirus solutions. The sensitive data in your files is encrypted and access controlled, so even if a breach occurs and attackers steal your files with Anchored data, they can't use that data against you.

With Anchor, all your sensitive data is impervious to attack, and at a price that won't break the bank.

Simple
Setup in minutes

Transparent
No impact to user experience

Affordable
Simple pricing, volume discounts

Bullet-proof
Military-grade FIPS-validated encryption

How Anchor for Ransomware Works
Your data is bullet-proof

Anchor's simple and transparent data security neutralizes ALL your external threats. After a ransomware or doxware attack, the exfiltrated files will be useless, as they will appear as ciphertext because they are outside the access rules. Since the stolen data is encrypted, the reporting requirements under most compliance regulations will no longer apply.

For further peace of mind, Anchor secures the data decryption keys offsite and never saves them with the data. You, and only you, will be capable of decrypting your files.

Take pride in knowing you protected your confidential information from would-be doxers using the same method they used to make you a victim.

Anchor security architecture
A patented combination of technologies

- Persistent & transparent encryption
- Multi-factor access controls
- Digital chain of custody via forensic logging

Streamline incident response

Responding to attacks can be costly. When data is Anchored, just the click of a button generates a log of every successful file access within seconds.

Anchor your data today.
Contact Us.

8000 Walton Parkway
Suite 224
New Albany, OH 43054

Hello@AnchorMyData.com
www.anchormydata.com