ENCRYPTION AT REST (EAR) EXPLAINED

What is Encryption at Rest?
EAR is the technology that encrypts data before it is stored in hard drives for network share or folder location.

EAR is one of the most important tools to fight against data breaches or technology theft.

What does Encryption at Rest with ScaleMatrix do?

There are many ways cyber terrorists can gain access to your data, or sometimes it could be human error, like misplacing a hard drive. In either case, EAR can help protect your data if these incidents occurred.

THERE ARE 2 TYPES OF DATA THAT REQUIRE ENCRYPTION:

Data at Rest
- Files and folders in your Network
  - Not used on a regular basis
  - Used only when working on them
  - Stored in a location within the Network
  - EAR required

Data in Motion
- Active data accessed from a Browser Page, or an OS Dedicated Program
  - Data is usually encrypted already by these programs

Why do you need Encryption at Rest (EAR)?

Encryption at Rest is an important step in data security as it ensures the data is secure down to the storage medium. By using EAR, you increase protection against physical theft and lost hard drives.

How does ScaleMatrix Implement Encryption at Rest (EAR)?

ScaleMatrix offers you SAN access called ScaleStor delivered in three different IOP Performance tiers for Copper or Fiber Networks.

Make Encryption at Rest a high priority in your organization's data protection plan.

Reach out with questions or ask for a complementary data protection evaluation at

protection@scalematrix.com