Data Security
DATASHEET

ObjectMatrix

What Data Security Risks Exist?

Sadly, many high-profile news events demonstrate that the risk of data loss comes from: ransomware, spyware, viruses and external hackers; internal hackers and/or disgruntled employees. Other dangers to data come from human error, hardware or software failures.

With Security in Mind, How Can You Better Protect Your Data?

MatrixStore was built from the inside out with data security in mind and provides a great number of benefits over SAN/NAS/scale-out filesystems. If you take digital asset security seriously but don't want to spend your time managing complex cryptography, firewalls and data policies then you'll appreciate that the storage is pre-configured with those core benefits and that individual pools of assets automatically have a high level of security applied.

All this comes built into a nearline storage platform that is integrated directly into many workflows. From securing content at ingest to providing best-of-breed digital preservation throughout and beyond the production process.

Benefits

- Access to MatrixStore is always via an API with a strong user authentication model

- Vaults of data can be made immutable - this can completely protect data from being changed by ransomware attacks, or from being accidentally or maliciously deleted

- This low-level immutability means that many ransomware strategies that bypass gateways (e.g. by loading up in firmware) are protected because the ransomware never has access to the O/S

- User actions are audited - even asset reads can be audited

- Servers are heavily firewalled and can even be hosted on the web

- Data transfer can be made with encrypted protocols and therefore becomes non-sniffable and non-spoofable

- Individual vaults/buckets can have their own admin user

- Unlike complex solutions with multiple software packages and because MatrixStore is cohesive, upgrades of one part of the infrastructure will not accidentally leave security holes in another part

Secure Your Data

Because MatrixStore has strong firewalls, data immutability, optional data encryption, strong user authentication, optional data transmission encryption, and access is always via an API, it already has a strong set of data security protocols with barely any administrator configuration. Such protocols would only exist on a SAN/NAS solution after the installation of multiple software packages – software packages that require updates and upgrades and can be problematic to maintain. MatrixStore can also audit when files are read or deleted so that the culprit for that film that got posted onto YouTube can be more easily tracked down.

- **Built-in firewall**
- **Data immutability**
- **Optional data encryption**
- **Strong user authentication**

- **Optional data transmission encryption**
- **Built-in auditing**
- **Independently security audited**

ObjectMatrix

These are just some of the data security services that come with MatrixStore. Contact us to discover the many other ways our platform can benefit your business!

+44 (0) 2920 382308

sales@object-matrix.com

www.object-matrix.com