pixitmedia
by DataCore

Object Matrix

Data Security

Benefits

API-based access for robust content management

Data immutability prevents ransomware attacks and unwanted deletion

Encrypted transfer ensures secure data transmission

Built-in auditing tracks asset reads and deletions and protects against unauthorized access

Simplified security with minimal configuration and cohesive architecture

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?

Object Matrix was designed with data security at its core, providing significant benefits over SAN, NAS, and 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 Object Matrix has you covered. The storage is pre-configured with robust security measures, ensuring individual asset pools automatically benefit from the highest levels of protection.

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.

Secure Your Data

Because Object Matrix 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. Object Matrix 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.

Protection Highlights

- Built-in firewall
- Data immutability
- Optional data encryption
- Strong user authentication
- Optional data transmission encryption
- Built-in auditing
- Independently security audited

Security Features

- Access to Object Matrix 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 Object Matrix is cohesive, upgrades of one part of the infrastructure will not accidentally leave security holes in another part

pixitmedia by DataCore

Pixitmedia by DataCore is a leading provider of intelligent content and metadata management solutions for the media and entertainment industry. Our multi-tier technology combines high-performance access, storage, and archiving with powerful orchestration and AI tools to simplify workflows. Built on an open architecture, Pixitmedia enables seamless collaboration while keeping assets searchable, protected, and available when they're needed. Learn more at **pixitmedia.com**