SOLUTION BRIEF

MEDIAFLUX®
MADE BY ARCITECTA

Mediaflux® Ripstop

The first line of defence against cyber threats

Are you prepared for a cyber-attack?

Technology is transforming the modern business landscape — not only speeding up innovation and productivity but also widening the door to cyber threats. If your organisation produces, stores, and disseminates interesting and valuable data, it's prudent to assume that external parties are motivated to gain financial advantage by stealing or holding your data to ransom. We are now in a time when hackers are getting more determined and more cunning, and as a result, the incidence of cybercrime will remain a prevalent threat.

Countering cyber security threats is a "game" that will likely never end; organisations need more sophisticated systems to prevent cyber intrusions from happening or detect and respond rapidly with confidence if they do.

Why use Mediaflux Ripstop?

Mediaflux® is a sophisticated data management fabric for modern data enterprises. When Mediaflux is configured in the data path, the system gains additional cyber security protections from Mediaflux® Ripstop, which provides the first line of defence against cyber threats, in most instances preventing an attack in the first place.

Mediaflux Ripstop is designed to cope with the scale and complexity of today's data providing users with a near-perfect data recovery experience.

A recovery point objective (RPO) of near zero

Mediaflux Ripstop uses highly optimized and parallel file scanning to easily traverse and catalogue changes in billions of files and tens or hundreds of petabytes of data offering an RPO very near to zero.

A recovery time point objective (RTO) of zero

Users no longer need to ask IT for help to recover data. They can access and recover to any point in time themselves whenever they want to. They can search for files across the entire space and time continuum with powerful wildcard searching to find and directories no matter when they existed. A recovery time objective of zero is their hands.

www.arcitecta.com | talk@arcitecta.com

Prevention: The first line of defence

There are multiple unique ways that Mediaflux Ripstop prevents contemporary cyber-attacks that hold organisations to ransom from happening.

Tightly controlled attack surface

Having written every protocol from the ground up, Mediaflux minimises the number of network interfaces sitting prey to attackers.

Minimal supply-chain dependencies

Other than the operating system and a Java virtual machine, Mediaflux has no dependency on any third-party software. Arcitecta has written every aspect of the system itself.

Multi-factor at the core

Integrated multi-factor is not only used for authentication (like many systems) but also to verify operations such as deleting important data. Multi-factor includes every protocol, regardless of whether the access is via the API, NFS or SMB filesystem protocols. Mediaflux can configure any operation in the system for multi-factor validation.

Role-based and attribute-based controls

Tightly control the vector and source of access to any data through an extensible and dynamic policy engine.

Secure sharing of data

Share data with external systems using policy restricted access tokens (one-off or multi-use). These tokens help to limit the visible surface of the system.

End-to-end trust

Establish trust between endpoints and exclude untrusted systems and networks by corollary.

End-to-end encryption

The storage and transmission of data are strongly encrypted. For over 15 years, Mediaflux has been deployed on all network classifications from unclassified to top-secret in military environments.

Respond to cyber intrusions that pass the keeper

Even perfect security hygiene can't prevent all attacks – to assume so is hubris. However, suppose there is a compromised pathway, and an attacker does gain entry through the "front door". In that case, system administrators can be confident that Mediaflux Ripstop will kick in second and third lines of defence to minimise and quickly rewind damage.

- WORM – Mediaflux can place expensive (to reproduce) data in the Write-Once, Read-Many state so that it cannot be altered until expiration or cross-approved by select "worm administrators".
- Multi-system replication - Mediaflux can cross-replicate data to different systems, and each system can have varied people managing the life cycle and approvals for those systems. In that way, no individual has full access to all systems. The systems are synchronised in real-time. Deletions are not (immediately) replicated from one system to another.
- A filesystem for every point in time - Mediaflux file systems can record every point in time. If an attack occurs, end-users can simply rewind the file system to the point just before the attack to recover data without requiring assistance from IT.

Accidental Data Loss

This is a form of data loss that many are familiar with. Unlike data failure, where a file is corrupted, data loss occurs when a file is misplaced. The name is a bit of a misnomer as the data still exists somewhere but is inaccessible to the lay user. Nevertheless, the implications of data loss are devastating – especially considering how close within reach that data may have been with the right the tools to recover it.

Mediaflux Ripstop makes finding misplaced data accessible, scalable and easy to use.

How to learn more/ try for yourself

Mediaflux Ripstop is included in every standard Mediaflux Server at no additional cost. To discuss how Mediaflux Ripstop can support your cyber resilience strategy please contact: talk@arcitecta.com