



RANSOMWARE  
DATA

## RANSOMWARE PROTECTION WITH ICAS FS

iCAS FS is a scale-out platform for the long-term storage of business-critical data. The software-based storage platform is infinitely scalable from 20 TB upwards - and will win you over with its low total costs, easy handling, and high flexibility.

iCAS FS makes compliance and security a top priority - thanks to WORM storage, retention management, encryption, and audit trail.

### Advantages of iCAS FS:

- Cost-efficient: 53% savings compared to the public cloud and you retain control over your data.
- Scalable: Start small, infinitely scalable from 20 TB in one platform.
- Zero-Touch Operation & Managed Services.
- Cloud Experience On-Premise.
- Hardware independent, based on standard hardware.
- Effective protection against ransomware attacks.

### Thanks to long-term immutability and minimal vulnerability, data in iCAS FS is protected against cyber-attacks:

- iCAS FS is a closed, software-based system with a hardened Linux operating system.
- There is no customer-side administrative access to the system. The only external interfaces are protocols such as SMB, NFS, and S3 – and with WORM storage, absolutely all write operations are blocked. Even if malware infects the customer's entire IT infrastructure, the malware has no access to the data in iCAS FS.
- Stored WORM files in iCAS FS cannot be changed, encrypted, or deleted.
- The iCAS FS system is completely administered and monitored by iTernity.
- Encryption at rest, encryption in transit, and encryption of internal cluster communication.
- Data loss due to hardware defects or catastrophes is prevented by using RAID and cluster-wide replication, in conjunction with our self-healing process.
- iCAS FS has been audited and certified by KPMG.