

RANSOMWARE
DATA

RANSOMWARE SCHUTZ MIT ICAS FS

iCAS FS ist eine Scale-Out Plattform für die langfristige Speicherung geschäftskritischer Daten. Die software-basierte Speicherplattform ist ab 20 TB grenzenlos skalierbar und überzeugt mit geringen Gesamtkosten, einfacher Handhabung und hoher Flexibilität.

Dank WORM Speicherung, Retention Management, Verschlüsselung und Audit Trail werden Compliance und Sicherheit bei iCAS FS groß geschrieben.

Vorteile von iCAS FS:

- Kosteneffizient: 53% Kosteneinsparung im Vergleich zur Public Cloud und Sie behalten dabei die Hoheit über Ihre Daten
- Skalierbar: Klein starten, unbegrenzt wachsen ab 20 TB in einer Plattform
- Zero-Touch Betrieb & Managed Services
- Cloud Experience On-Premise
- Hardwareunabhängig, basiert auf Standardhardware
- Effektiver Schutz vor Ransomware Angriffen

Dank langfristiger Unveränderbarkeit und minimaler Angriffsfläche sind die Daten in iCAS FS vor Cyber-Angriffen geschützt

- iCAS FS ist ein geschlossenes, software-basiertes System mit gehärtetem Linux Betriebssystem.
- Es gibt auf Kundenseite keinerlei administrative Zugänge zum System. Die einzigen externen Schnittstellen sind Protokolle wie SMB, NFS und S3 – bei WORM Speicherung werden schreibende Operationen ausnahmslos blockiert. Selbst wenn die komplette IT-Infrastruktur beim Kunden von Malware befallen ist, hat diese keinen Zugriff auf die Daten in iCAS FS.
- Gespeicherte WORM-Dateien in iCAS FS können nicht verändert, verschlüsselt oder gelöscht werden.
- Das iCAS FS System wird komplett durch iTernity administriert und überwacht.
- Verschlüsselung at rest, Verschlüsselung in transit und Verschlüsselung der internen Cluster-Kommunikation.
- Einem Datenverlust durch Hardwaredefekte oder Katastrophen wird durch den Einsatz von RAID und der clusterweiten Replikation im Zusammenhang mit dem Self-Healing Verfahren vorgebeugt.
- iCAS FS wurde durch die KPMG geprüft und zertifiziert.