# Never Lose Data Even if Passwords are Compromised

## *ioFABRIC's Behavior-Based AI Ensures Your Data isn't Corrupted or Deleted by Ransomware*

## Executive Summary

ioFABRIC software tamper-proofs your backups guaranteeing you will not be held hostage by cyber criminals even if your passwords are compromised. ioFABRIC learns how your applications interact with file systems, and then restricts bad behavior. It uses machine reasoning, a combination of machine learning and an expert system, to analyze file system activity to learn behavior patterns. ioFABRIC uses learnt behaviors to prevent bad behavior from destroying data. The unique behavior-based functionality monitors, alerts, and protects your backups from suspicious activity. The system auto identifies the important backup files and then adds file locking and snapshot policies to maximize protection, both for short term (recovery) and long term (regulatory) requirements.

The rise of ransomware is due to unsecured backup files—making your entire company vulnerable—because you cannot restore your files or systems after a malicious employee act or a ransomware attack. If companies could quickly recover from backups, they would never pay a ransom. A common myth is that frequent snapshots or write-once technology will solve the issue, but it will NOT. Frequent snapshots will take frequent images of corrupted data, and WORM (write once, read many) technology is not compatible with most backup software nor financially viable because of the exponential storage requirements. This is why ransomware is a growing billion-dollar industry regularly hitting major companies, but you can stop it from blackmailing your company with ioFABRIC.

ioFABRIC is the first company to solve this problem. ioFABRIC software works with all backup software protecting your backup files from malicious or accidental corruption. ioFABRIC uses industry-first technology to identify your important files, take behavior-based snapshots immediately after each close, retention lock the snapshots, and then retention lock the file after the backup application has completed all updates to the file. This completely eliminates the window of vulnerability left with time-based snapshots. ioFABRIC is the perfect defence against simple or complex threats, including ransomware.

# Overview

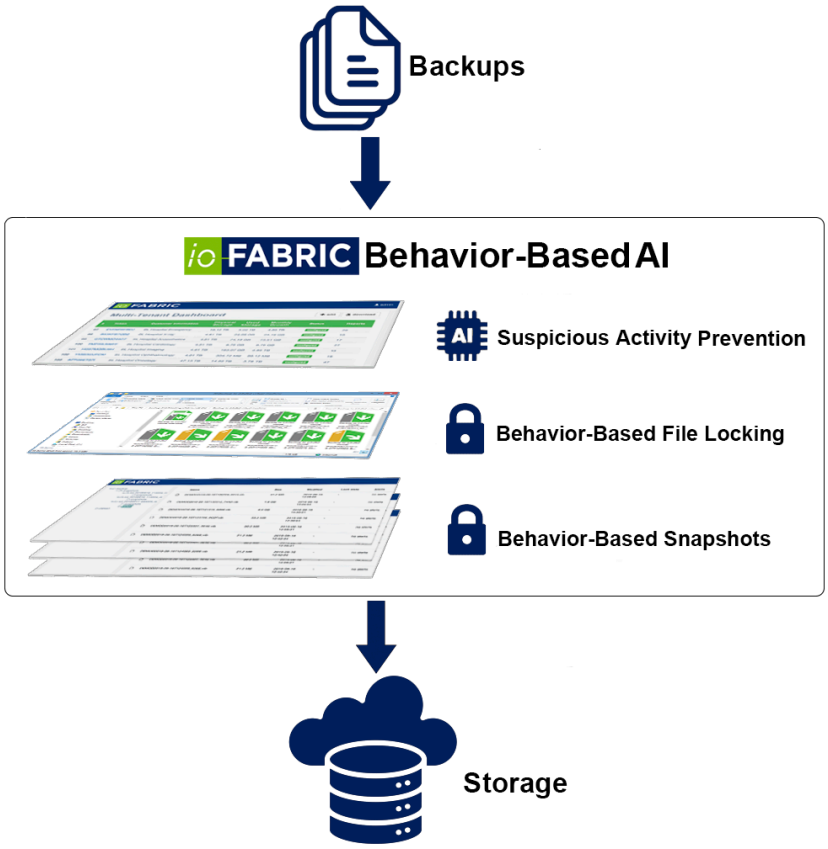
## Why Current Approaches to Ransomware are Not Working

Malicious employees and ransomware all pose a significant risk to your security. Ransomware will spread inside your company, encrypting or deleting your files, damaging multiple systems – all from a single user mistake. If ransomware only destroyed your computer files and you could quickly recovery from your image-based backups, you would never pay a ransom. Criminals are aware that destroying backups is crucial for blackmailing companies. They also know that current backup targets are not designed to withstand cyber-attacks. The cold reality is that cybercriminals only have to get through your defences once to get paid. Backups files, your last defence, need to be better protected and the myth that regular file systems and snapshots solve the problem needs to be dispelled. Snapshots have been around for decades and if they solved the problem, we would not be hearing about million-dollar payouts or municipalities being shut down for days.

The standard defence of regular snapshots or even WORM technology does not solve the problem. Frequent snapshots, such as every day, hour or minute offer a false security because they only solve half the problem. Snapshot solutions do not ensure the data in the files has not been deleted or modified before it is snapped. It's easy for a hacker to modify or delete backups, with stolen backup user credentials, between the time they are written, and the time they are snapped. A hacker only needs to lurk on your network and destroy/alter backups over time as they occur. Also, the storage systems' snapshots themselves are not protected from being deleted once the cyber criminals have stolen the admin credentials. WORM technology isn't feasible for two reasons: because backup vendors did not write their programs to be compatible with write-once file compatibility and unviable because of the exponential data growth.

## How ioFABRIC Works

ioFABRIC replaces or enhances your existing NAS with a physical or virtual secure NAS that prevents malicious data destruction. The principal use case against ransomware is to use ioFABRIC as a secure backup target. As your backup software writes files into the ioFABRIC appliance they are immediately snapped, made immutable, and then retention locked. ioFABRIC's security policy guarantees files can be recovered.



## ioFABRIC Features

**Suspicious Activity Prevention** identifies and blocks unusual or suspicious behavior. Alerts of these events occur in real time.

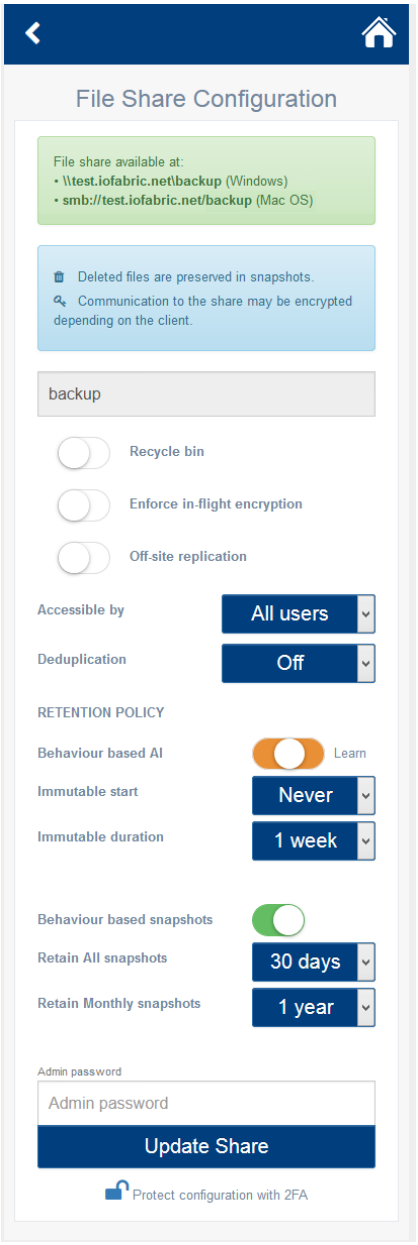
**Behavior-Based File Locking** ensures your data is tamper-proof. This locking makes your files immutable which is an extra layer of security that cannot be undone even by admins or hackers.

**Behavior-Based Snapshots** capture the data and state of the ioFABRIC system immediately after a backup is written so the data is accurate and recoverable.

**Offline Replication** provides an immutable copy of your data at a second site.

**Hardened Security** with a built-in firewall, two-factor authentication and AI to analyze behaviors.

**Centralized Management** provides enterprise or managed service providers, a single interface to manage, monitor and receive alerts from multiple appliances




# Feature Summary

ioFABRIC makes your backups tamper-proof so you will never lose data. It works with all backup vendors protecting the important and sensitive data files immediately after they are written. This allows fast recovery from a secure backup as well as long-term retention of important data. Locked data can never be destroyed but ioFABRIC software goes even further into real time inspection, alerting, and prevention of unusual behavior or suspicious activity.

ioFABRIC's retention policies are for files in the datacenter and the cloud. The security policies use three complementary processes to provide tamper-proof backups: behavior-based file locking, behavior-based snapshots with retention locking, and suspicious activity prevention. Not even admin credentials can destroy existing data until the locks on files and snapshots have expired.

## Suspicious Activity Prevention

As the backup application writes to the file system, ioFABRIC learns behaviors. ioFABRIC will then predict patterns as well as what files are important and need to be preserved versus what files are temporary and will be deleted. Predicting behaviors is important to differentiate backup use from suspicious activity as file behaviors are unique to different backup vendor implementations. ioFABRIC uses machine reasoning to predict what files are important, if the file is allowed to be modified, and exactly when the backup has finished writing so it can be immediately secured. Important files are snapshotted, and retention locked against tampering. Trying to modify an important file will either result in the request being rejected and alerted or allowed and alerted depending on the files state in its life cycle. For example, if a backup files life is over and it is expected to be deleted but is instead moved or modified, then along with the alert is a read-only location of the previous file data to undo the operation.

## Behavior-Based File Locking

Behavior-Based File Locking learns behaviors and locks immediately after the file has been written to ensure that files cannot be tampered with. No one, regardless of their file permissions, can destroy a backup file while it is locked. Some backup applications open and write their data, others take a less direct process. The tamperproof period is the duration of the file lock and is manually set. It is possible to learn this, but it would take multiple periods (i.e. a week retention would require 3 weeks to learn) so it is operationally faster and simpler to manually set this time. The file lock duration is the amount of time files are tamper-proof. Older files are generally unlocked prior to automated backup removal and no longer tamper-proof.

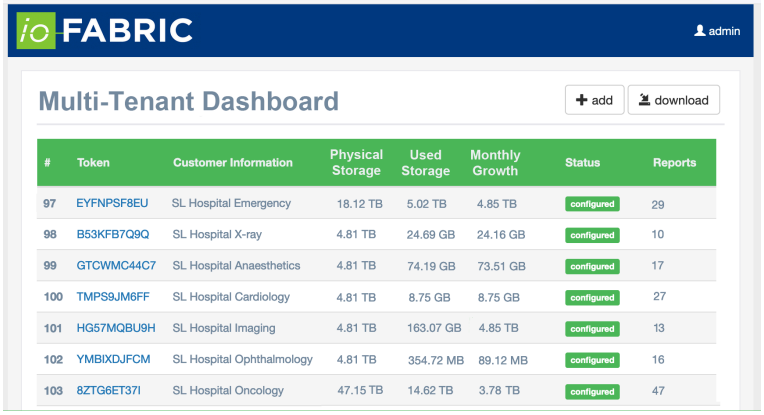
## Behavior-Based Snapshots and Retention Locking

The writing of a backup file is a deterministic process but there are a set of backup files written over days or weeks that are needed to properly restore a system. Data in a backup file must be secured immediately after it is written to ensure reliable recovery. ioFABRIC creates a snapshot of the entire file system after each file is written. These snapshots are then retention locked to prevent deletion. The individual files are also retention locked, so the snapshot taken after the entire backup job has completed is consistent.

File Locking retains the state of a file at a point in time, whereas Snapshot Locking retains the state of the file system at a specific point in time. Snapshots are taken after it detects each file has been written, after the backup job completes, and every day. Each snapshot is locked according to the policy. It is not possible to manually delete a snapshot—they must age out which prevents ransomware from tampering with your backups.

## Multiple Appliances: Centralized Management, Monitoring and Altering

ioFABRIC's multi-tenancy dashboard allows centralized management of 100s to 1000s of appliances from a single plane of glass. Each appliance has a low touch setup that involves powering on the appliance and entering a key/password to activate. The appliance then communicates with the Multi-Tenancy Dashboard to authenticate and receive its pre-set configuration. The configuration can also be done on the appliance and only takes minutes. For deployment into existing environments, the backup application needs updating to use ioFABRIC as its target. This deployment, including configuring the backup application, can be completed in 5 to 10 minutes.




## Offline Replication of Snapshots

Replication is an optional protection step, usually done offsite, for traditional site disasters. ioFABRIC maintains a replicated copy of data, unmounted on a second appliance which requires two-factor authentication to provide read-only access.

# Conclusion

ioFABRIC software uses three core security processes: behavior-based locking, behavior-based snapshots and suspicious activity prevention to tamper-proofs your backups. It is available as a virtual or physical appliance that can be configured quickly.