Hardening Enterprise Backups:

The Essential Best Practices Guide

CONTINUITY

Cybercriminals have shifted their focus from just encrypting production environments to targeting the very systems designed to protect them: backups.

While immutability and air-gapping are vital defenses, they’re not foolproof – and when misconfigured or misunderstood, they can create dangerous blind spots. From time spoofing attacks to Active Directory exposure and improperly enforced retention locks, backup infrastructure is increasingly vulnerable to sophisticated threats.

This guide offers a practical blueprint for hardening enterprise backup environments, grounded in proven best practices, vendor recommendations, and real-world attack scenarios.

By following the guidance outlined here, organizations can transform backups from a theoretical last line of defense into a truly resilient and secure asset.

Is Your Immutable Backup Vulnerable to Time Spoofing Attacks?

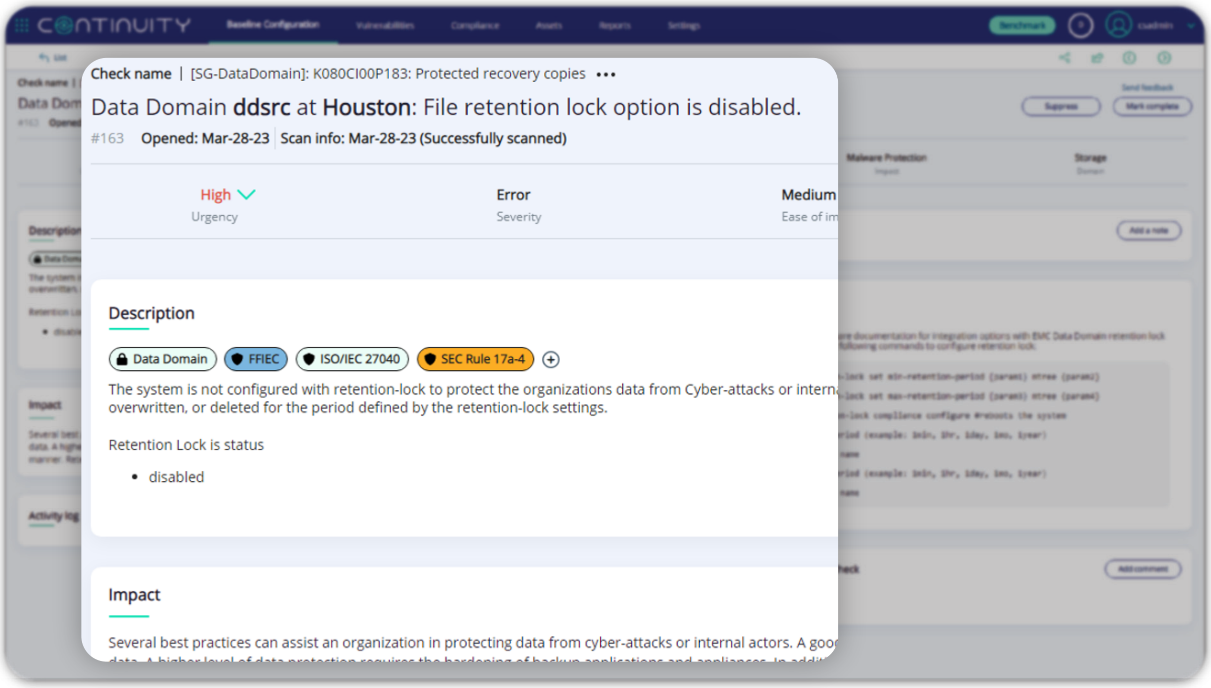
What this is about?

This time-based attack happens when an attacker manipulates insufficiently-secure time sync configuration to trick the backup systems into thinking that “X” number of years have passed, and that the period for immutability has expired. This then allows them to delete, alter or encrypt the data.

It’s not only immutable backups that are vulnerable, but also storage systems and operating systems relying on snapshots for quick data recovery. Time manipulation can force the systems to discard all “clean” point-in-time copies taken prior to an attack.

8 Urgent Things To Do

1. Ensure your Backup software and storage are configured with a trusted time source.
2. Validate the authenticity of the time source.
3. Restrict administrative access in general and specifically for time synchronization administration.
4. Employ a two-person rule (dual authorization) for sensitive changes.
5. Carefully monitor any configuration changes that can directly or indirectly impact time settings.
6. Upgrade and patch your Backup Software and Backup storage to prevent attackers from exploiting vulnerabilities.
7. Restrict consecutive attempts to change the system time.
8. Make sure you're using at least NTPv4, and prefer NTPv5 where and when feasible.



Check name | [SG-DataDomain]: K080CI00P183: Protected recovery copies •••

Data Domain **ddsrc** at **Houston**: File retention lock option is disabled.

#163 **Opened: Mar-28-23** | **Scan info: Mar-28-23 (Successfully scanned)**

High — Urgency
Error — Severity
Medium — Ease of im

Description

Data Domain | FFIEC | ISO/IEC 27040 | SEC Rule 17a-4

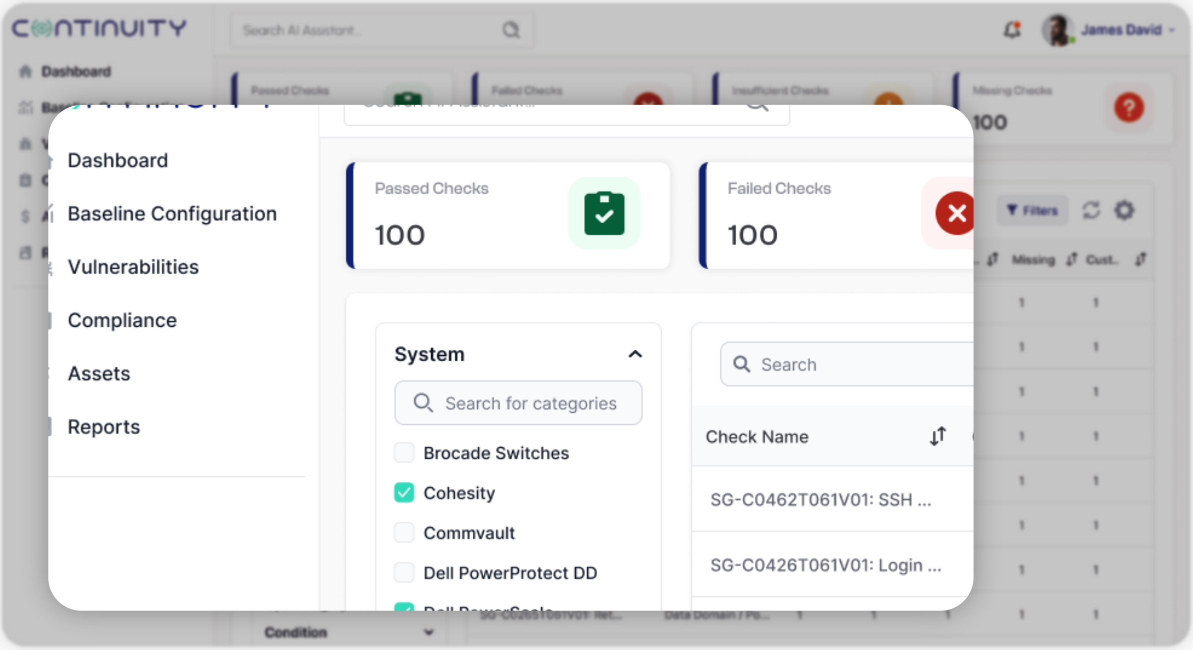
The system is not configured with retention-lock to protect the organizations data from Cyber-attacks or intern
overwritten, or deleted for the period defined by the retention-lock settings.

Retention Lock is status

- disabled

Impact

Several best practices can assist an organization in protecting data from cyber-attacks or internal actors. A goo



Passed Checks 100

Failed Checks 100

Missing Checks 100

System

Search for categories

□ Brocade Switches
☑ Cohesity
□ Commvault
□ Dell PowerProtect DD

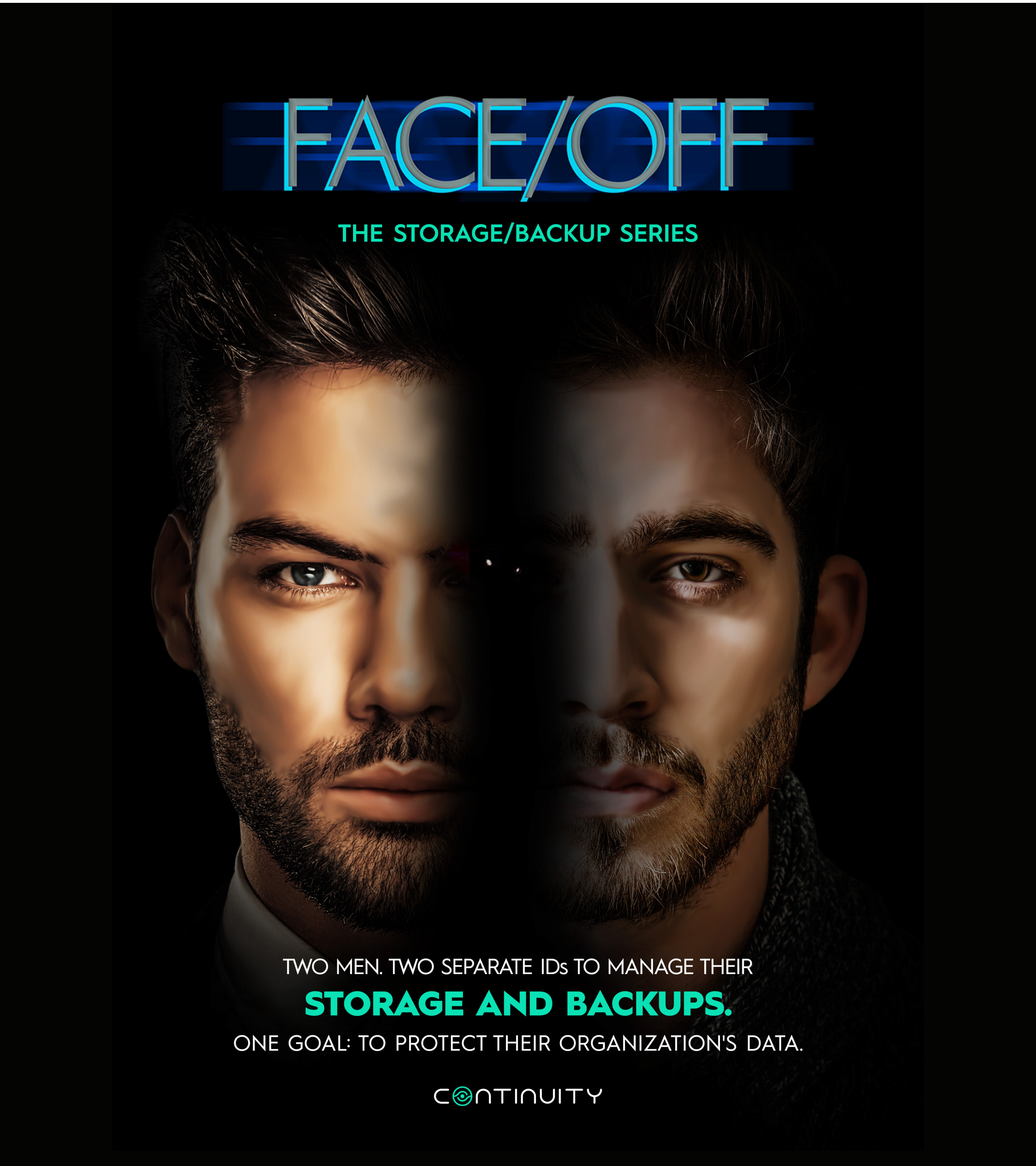
Search

Check Name
SG-C0462T061V01: SSH ...
SG-C0426T061V01: Login ...

To AD Or Not To AD Your Backup System?

That Is The Question.

When it comes to backups, there's an interesting debate as to whether you should connect your backup systems to Active Directory (AD) or not, and for good reasons. *Let's explore this dilemma.*


FACE/OFF
THE STORAGE/BACKUP SERIES
TWO MEN. TWO SEPARATE IDs TO MANAGE THEIR
STORAGE AND BACKUPS.
ONE GOAL: TO PROTECT THEIR ORGANIZATION'S DATA.
CONTINUITY

The Case For Connecting Your Backup to AD

Because it streamlines user and system management, by integrating with AD, your backup system can leverage existing user accounts, group memberships, and organizational unit structures. This not only simplifies the setup process but also ensures that your backups are aligned with the organizational hierarchy.

In addition, utilizing AD integration facilitates automated user authentication and access control, which enhances security.

Backup Admins can leverage AD permissions to control who has access to backup software and infrastructure, ensuring that only authorized personnel can manage and retrieve sensitive information. This centralized management approach also reduces the risk of errors in user provisioning and access, which contributes to a more efficient and secure backup environment.

Without AD, you rely on local user accounts, which are more difficult to control and monitor. In addition, AD integration puts a check in the box of so many regulatory requirements – access control, auditability and more – which assists with compliance.

The Case Against Connecting Your Backup to AD

Because it makes AD a single point of failure for both PROD and Backup (and you don't want that!), if your AD is compromised, an attacker can harm both your production data and backup data, and then all hope is lost.

It helps to ensure that your primary storage systems and backup systems are not managed by the same user accounts – a scenario that would allow a cybercriminal with a compromised user account to corrupt the original data and its backup copies.

Since its your last line of defense, your backups should be as isolated as possible, and prepared for all possible attack scenarios. Nowadays, backup and storage systems offer reasonable access management features – account polices, audit, multi-factor authentication, and more.

Being secure is more important than being compliant!

If you ask us, we vote for #2.

The Backup Immutability
Do's & Don'ts Checklist

Since backups are becoming lucrative targets for cybercriminals, vendors like Cohesity, Commvault, Dell, Rubrik, Veeam and Veritas have responded with new ransomware protection features – including immutability.

With immutable backups, once the data is backed-up, it is fixed and unchangeable. It can never be deleted. Organizations gain an always-recoverable and secure backup, to protect themselves against cyberattacks.

Immutability is an important capability; however, it can lead to a false sense of security if not implemented properly. When misconfigured, it is possible to delete supposedly immutable data, for example, by manipulating time/date settings on the storage device to bypass retention enforcement mechanisms.

One of the best practices by the backup vendors is to ensure immutable backups are configured with retention lock– a parameter that prevents their deletion for a minimum period of time. If retention lock is not configured, cybercriminals can breach the backups by modifying large amounts of data, thereby quickly filling up the backup pools which results in deletion of all existing backups to free up space.

Even when retention lock is enabled, care must be taken to make sure cybercriminals can't fool the backup systems to believe time is passing more quickly than intended. This is referred to as "time spoofing" attacks – where the attacker manipulates insufficiently secure time sync configuration to trick the backup systems into thinking that "X" years have passed.

To give you a helping hand, here's a list of do's & don'ts for your immutable backups:

Do's

- Configure the immutability retention period
- Use secure time synchronization
- Enable two-person rule on immutability related settings
- Consider enabling anomaly detection
- Secure underlying hardware components such as iDRAC, IPMI, BMC, iLO, etc.
- Enable local user MFA
- Limit number of sessions
- Account Login Threshold
- Restrict administrative access
- Create Security Officer
- Disable inactive users
- Harden your backup catalog / repository

Don'ts

- Many vendor solutions offer multiple flavors of immutable backup – some are softer than others. Weaker immutability mode enable users to alter, disable or remove the immutability option altogether – that of course defeats the purpose of immutability – you want to avoid these modes.
- Don't use the same credentials to manage both primary storage and backup systems
- Don't enable unrestricted remote access
- Don't enable unsecure protocols such as FTP, Telnet or plaintext HTTP
- Don't use unrestricted or vulnerable file shares
- Do not allow untrusted hosts to join the Backup domain
- Don't use default passwords

How To Validate The Configuration Of Your Immutable Backups

The integration between backup software and a disk array is crucial for implementing immutable backups. To achieve backup immutability, the backup software needs to leverage the features of the disk array, such as write-once, read-many (WORM) capabilities or snapshots with retention policies.

There is a wide range of configuration details and technicalities that would adversely impact the backup or its immutability. The disk array must also support Write-Once, Read-Many (WORM) capabilities.

In addition, the backup software and the disk array must be compatible and support the necessary features for achieving immutability. Not all backup solutions or disk arrays provide the required functionalities, so compatibility checks are essential. Some pairings may require you to write custom scripts.

Retention values must also be well-coordinated between the backup policy and disk array retention lock settings, otherwise the backup system will attempt to delete the backup before its immutability period is over. This would lead to major confusion when it comes to backup management and reporting.

Jim Brady
CISO at Fairview Health Services

> **Bad actors can gain access to the backup system, change the configuration, and then delete the immutable backups.**
>
> **This is why I believe in the importance of running a ransomware assessment on storage and backups.**

Building a Solid Backup Asset Inventory

Given the importance of backup and recovery systems in any organization, maintaining a comprehensive and up-to-date inventory of all backup infrastructure is critical.

A general-purpose inventory focuses on end-points and servers, but won't correctly capture the full scope of your backup environment. When it comes to an inventory, those of you who have used such data sources know that data quality and completeness is everything.

So what should a backup inventory include?

While not a full listing, here are several things to take into consideration when building an inventory for backup environments:

- Backup UI servers
- Backup Catalog (Repository) databases and servers
- Backup Media servers, data movers or nodes
- Backup Clients
- Backup destinations – disk array
- Backup destinations – tape
- Backup destinations – cloud
- Backup proxy servers
- Backup CLI software installations
- Backup console software installations
- Backup appliances and underlying server hardware
- Backup host servers
- Backup SaaS components
- Backup plugins for primary storage systems (Backup from snapshot)
- Backup plugins for hypervisor
- Backup plugins for databases
- Backup plugins for apps
- Deduplication software components
- Orchestration, Reporting, Analytics and other management software installations
- REST API servers
- SMIS servers
- Key Management software and servers
- Vault & air-gapping devices and/or software installations
- … and more.

Filling The Gap

StorageGuard verifies that your backup systems (from the likes of Cohesity, Commvault, Dell, Rubrik, Veeam and Veritas NetBackup) are hardened, configured according to industry and vendor security best practices, and are not vulnerable:

- Verifies that anti-ransomware features are enabled and configured correctly (e.g., ransomware detection, ransomware isolation, anomaly detection, user behavioral analysis, and AV scanning)
- Verifies that snapshots, replicas, images, and backup sets which are required for recovery from ransomware – are secure, immutable isolated and generally protected
- Verifies that ransomware protection best practices published by storage and backup vendors are implemented
- Validates that data volumes, exports and shares are configured with restricted access and privileges, and according to security best practices
- Allows you to choose the standard sets you wish to comply with, and automating compliance reporting, highlighting gaps, prioritizing risks, and facilitating automated remediation.

To summarize, StorageGuard plays a critical role in your cyber resiliency strategy, by helping you increase usage & adoption of your existing data protection tools – and subsequently get more out of your current investment.

CONTINUITY

www.continuitysoftware.com