Backup Ransomware Readiness Playbook

Purpose

This document provides a **simple and practical** way to check whether backups are actually usable during a ransomware incident. The focus is on answering three basic questions:

1. Can an attacker delete our backups?
2. Can we restore data when we need it?
3. Do we know how long recovery will take?

This playbook is designed to be easy to run by infrastructure teams.

Scope and Safety Rules

- Production data must not be encrypted or destroyed
- No real ransomware or malware is execute
- Tests may be executed in lab, DR (Disaster Recovery), or controlled environments

Threat Assumption

For this playbook, we assume a realistic worst-case scenario:
An attacker has compromised a privileged account (for example, Domain Admin)
The attacker has internal network access & The attacker's goal is to disable or delete backups before deploying ransomware

Step 1: Understand the Backup Environment

Start by clearly documenting how backups actually work in organization:

- Backup software in use
- Where backups are stored
- Where the backup server is located on the network
- What credentials backup jobs use & Which critical systems are protected (AD, file servers, databases, VMs)

This step ensures everyone understands **<u>what must survive an attack</u>**.

Step 2: Test Backup Access Controls

2.1 Administrative Abuse Test

Using a highly privileged account, attempt the following actions:

- Delete existing backups
- Disable backup jobs
- Reduce retention periods

If these actions are possible with a single admin account, backups are at high risk.

Result:

- ❖ PASS: Destructive actions are blocked or strongly restricted
- ❖ FAIL: Backups can be easily deleted or modified

2.2 Credential Isolation Review

Identify how backup jobs authenticate and evaluate whether these credentials would realistically survive a domain compromise.

Classify the authentication method used by backup jobs:

- Domain user account
- Local account on the backup server
- Managed service identity (gMSA or equivalent)

For each backup job, determine:

- Whether the credential has a reusable password
- Whether the credential can be logged into interactively
- Whether the credential is commonly exposed during credential theft (LSASS dump, NTDS.dit, password reuse)

Risk Evaluation：

1) FAIL

Backup jobs run under a **domain user account** with a reusable password, especially if:

- The account is a member of privileged groups &
- The same credential is used for administration or interactive logon
- Compromise of Domain Admin would allow easy reuse of the credential.

2) PARTIAL PASS

Backup jobs run under a **local account**:

- Credential is limited to the backup server
- Password still exists and can be extracted if the backup server is compromised

3) PASS

Backup jobs run under a **managed service identity (gMSA)**:

- No reusable or human-known password exists
- Credential cannot be interactively logged into
- Credential exposure through standard credential theft techniques is prevented
- Usage is restricted to designated backup servers only

Backup credentials should remain usable **even if a privileged domain account is compromised**, and should not rely on credentials commonly targeted by ransomwares.

Step 3: Validate Backup Immutability

Assess whether backup data is protected against deletion, modification, or encryption at the **storage level**, independent of the backup application.

Verify the following controls:

- Immutability or WORM (Write Once Read Many) is enabled on the backup storage
- Retention policies are enforced **outside** of the backup software (storage/object lock level)
- Backup data cannot be deleted, overwritten, or altered before retention expiry
- Administrative access to the backup application does not allow bypassing retention

Ask a single critical question:

Can an administrator delete or alter backups before the retention period expires?

Risk Evaluation :

1) FAIL

Backups are not truly immutable:

- Administrators can manually delete backups before retention expiry
- Retention is enforced only at the backup application level
- Storage-level immutability or object lock is not enabled
- A compromised admin account or ransomware can erase or encrypt backups

2) PASS

Backups are immutable at the storage layer:

- Immutability / WORM is enforced at the storage or object level
- Retention cannot be shortened or bypassed, even by administrators
- Backup data remains intact despite backup server or admin compromise
- Ransomware cannot delete or encrypt backups before retention expiry

Backup immutability must remain effective even if backup administrators or domain privileges are compromised, ensuring recovery is always possible after a ransomware event.

Step 4: Prove Restore Capability

4.1 File-Level Restore Test

Demonstrate that backups are not only present, but they are **actually restorable** within an acceptable timeframe.

Select a random file set and perform the following actions:

- Restore the files to an alternate location (not the original source)
- Verify file integrity (hash, size, content) after restore
- Verify original file permissions and ownership are preserved
- Measure the actual time required to complete the restore operation

Record the **real, observed restore time**, not the estimated or vendor-claimed value.

Risk Evaluation :

1) FAIL

Restore capability is unproven or ineffective:

- File-level restore has never been tested
- Restore fails, is incomplete, or results in corrupted data
- File permissions or ownership are not preserved
- Actual restore time exceeds the defined RTO or business tolerance
- Restore procedures are undocumented or rely on key individuals

2) PASS

Restore capability is proven and reliable:

- File-level restores are successfully completed
- Restored data integrity and permissions are verified
- Restore time is measured and documented
- Restore completes within acceptable RTO limits
- Restore steps are documented and repeatable

Successful backups are meaningless unless restoration is regularly tested and proven under real conditions.

4.2 Full System or VM Restore Test

Prove the ability to recover an entire system or virtual machine following a major failure or ransomware incident.

Select a full system or VM and perform the following steps:

- Restore the system or VM from backup
- Boot the restored system successfully
- Verify operating system stability and accessibility
- Validate critical services and applications are running correctly
- Confirm system usability from an end-user or application perspective

A restore is considered **successful only if the system is fully usable**, not merely powered on or boote

Step 5: Active Directory Recovery Check

Verify that the organization can safely recover Active Directory without re-introducing attacker persistence.

Confirm the following:

- Active Directory is included in backup scope (System State / AD-aware backups)
- Backups exist from **before a potential compromise** (known-good backups)
- Backup retention allows recovery to a clean point in time
- Restore procedures prevent reintroducing compromised ***credentials/objects/backdoors***

Validate that restoring Active Directory will **not**:

- Re-enable attacker accounts or privileges
- Restore malicious GPOs, scheduled tasks, or persistence mechanisms
- Reintroduce compromised passwords or trust relationships

If Active Directory cannot be restored safely, the organization remains exposed even after a full system recovery.

Risk Evaluation :

1) FAIL

Active Directory recovery is unsafe or unproven:

- Active Directory is not included in backups
- No known-good backups exist prior to compromise
- Restore procedures are undefined or untested
- Restoring AD would reintroduce attacker access or persistence
- Password resets, KRBTGT rotation, or post-restore hardening are not addressed

2) PASS

Active Directory recovery is safe and validated:

- AD-aware backups exist and are regularly tested
- Known-good restore points are clearly identified
- Restore procedures include attacker eviction steps
- Compromised credentials and persistence mechanisms are removed
- Post-restore hardening and validation are documented and repeatable

Active Directory is a trust anchor; restoring it incorrectly undermines the entire recovery effort.

Step 6: Network Isolation Review

Make sure the backup environment is kept out of reach from normal users and day-to-day systems, so an attacker can’t easily find or attack it.

Check that:

- Backup servers live on their own network segments, separate from user and production networks
- Backup storage cannot be reached directly from user endpoints or regular servers
- Only systems that actually perform backups can talk to the backup storage
- Management and admin access to backup systems is locked down and not exposed to user networks
- Multi-factor authentication (MFA) is required for anyone administering the backup environment

The goal is simple: even if a user machine or production server is compromised, the attacker should not be able to move into the backup infrastructure.

Risk Evaluation

1) FAIL

The backup environment is too exposed:

- Backup servers share network space with users or production systems
- Backup storage is directly reachable from endpoints
- Backup administration relies only on passwords
- MFA is missing for backup admin access
- A compromised system could realistically reach or damage backups

2) PASS

The backup environment is well isolated and protected:

- Backup servers are placed in dedicated, isolated network segments
- Backup storage is reachable only by authorized backup systems
- User endpoints have no direct network path to backup infrastructure
- Backup administration is protected by MFA

Backups are a last line of defense and should be protected like critical infrastructure.

Step 7: Safe Ransomware Simulation

Validate that the organization can recover from large-scale data impact **without using real malware** or introducing additional risk.

Without deploying any malicious code:

- Simulate mass file changes (for example, bulk renaming or modifying a large set of test files)
- Treat the event as a real incident and initiate the restore process
- Restore the affected data from backups
- Verify data integrity, file structure, and permissions after restore

The objective is to confirm that recovery works **under realistic pressure**, while keeping the environment safe and controlled.

Step 8: Logging and Visibility

Make sure everything that happens in your backup environment is visible, so issues or malicious activity can't go unnoticed.

Check that the following events are logged:

- Attempts to delete backups
- Changes to retention policies or backup configurations
- Restore failures or errors
- Administrative access to backup servers or management consoles

Logs should not just exist , they should be **actively monitored**. Forward them to your SIEM or monitoring system, and ensure alerts are triggered for suspicious activity.

Final Evaluation

At the end of your backup review, summarize each control and assess the overall health of your backup strategy.

For each area, mark it **PASS** or **FAIL**:

- Protection against backup deletion
- Immutability enforcement
- Restore testing (file-level and full system/VM)
- Credential isolation for backup accounts
- Recovery objectives (RTO/RPO) are known, documented, and tested

Then, assign an **overall rating** to reflect the organization's resilience:

Resilient

- All critical controls pass
- Backups are isolated, immutable, tested, and recoverable
- The organization can reliably recover from ransomware or other major incidents

At Risk

- Some controls fail or are incomplete
- Partial isolation, untested restores, or gaps in credential management exist
- Recovery may be possible, but reliability is not guaranteed

High Risk

- Key backup protections fail
- Backups are not recoverable, not immutable, or lack proper testing
- The organization is likely to fail recovery during a ransomware or disaster event

This final evaluation provides a clear snapshot for leadership, showing whether the backup program is truly reliable or needs urgent improvement.