



THE **ACTIVE DIRECTORY** RECOVERY PLAYBOOK

Everything you need to know about detection, containment, and clean restore.

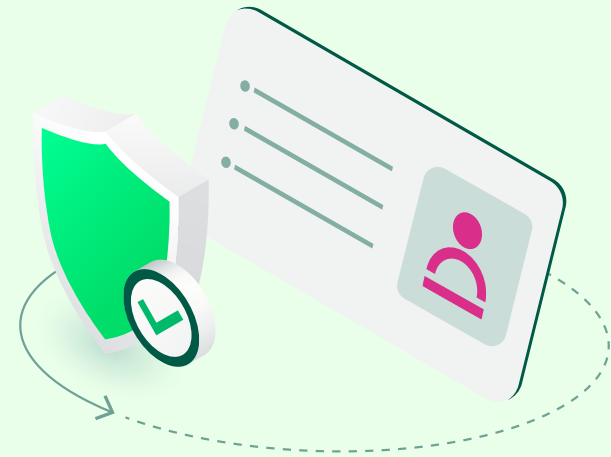
COHESITY

CONTENTS



Executive summary	3
Section 1: Why AD recovery isn't like any other restore	4
Section 2: Understanding the AD-centric kill chain	5
Phase 1: Initial access and reconnaissance	5
Phase 2: Privilege escalation and AD takeover	6
Phase 3: Persistence (planting backdoors inside AD)	7
Phase 4: Lateral movement and data exfiltration	8
Phase 5: Deployment and encryption	8
Section 3: Building Your AD Recovery Runbook	9
1. Prepare and harden	9
2. Detect and respond	10
3. Investigate before you restore	10
4. Recover	11
5. Learn from and continue to strengthen identity resilience	11
Section 4: Sample tabletop AD recovery drill	12
Roles and sample drill scenario	12
Success criteria and after-action report outline	13
Section 5: Recovery readiness self-assessment	14
Ready to start strengthening your identity resilience?	15
Appendix	16
Full MITRE ATT&CK reference table and glossary	16

EVERY RECOVERY STARTS IN THE SAME PLACE: CAN YOUR PEOPLE LOG IN?



Identity is core to your Minimum Viable Company (MVC), the smallest set of systems and services your business needs to keep operating after an attack.

Email, ERP, file shares, applications, and even the tools your own incident response team uses to coordinate all depend on identity working first. Recovering data means nothing if nobody can authenticate to reach it. Identity isn't just any workload you recover; it's how you get your business back up and running.

Nine out of ten cyberattacks now involve identity and access management systems. Cohesity CERT (Cyber Event Response Team) finds on-premises Active Directory present in 95% of the incidents it responds to. Once an attacker owns AD, they own everything it grants access to, and everything downstream stops with it.

This playbook covers everything identity, backup, and security practitioners need to plan an AD recovery. It will help you understand:

- ✓ Why AD recovery is uniquely complex and challenging
- ✓ What a real attack lifecycle looks like against Active Directory
- ✓ Why standard backup-and-restore breaks down against it
- ✓ How to build and drill a recovery runbook that survives contact with a real incident
- ✓ How to run your own tabletop exercise
- ✓ How to assess your team's identity recovery readiness

WHY AD RECOVERY ISN'T LIKE ANY OTHER RESTORE



Most disaster recovery thinking treats every workload the same way: back it up, restore it, move on.
But AD isn't just another database or NAS workload. It's uniquely challenging and complex for several reasons.

1

Restoring data isn't restoring trust.

A conventional restore brings back files. An AD restore brings back the system that decides who is allowed to touch every other system. If the restore includes a compromised credential, a malicious Group Policy Object (GPO), or a persistence mechanism the attacker planted, you haven't recovered. You've just reinfected yourself with a clean-looking file structure.

2

The blast radius is the whole environment, not one workload.

AD is the authoritative source for authentication and authorization across on-prem infrastructure, and in hybrid environments it typically feeds Entra ID and/or Okta through directory sync. A botched or incomplete AD recovery doesn't just fail to fix AD; in a hybrid environment, it can propagate bad state into every downstream identity provider (IdP) and application that trusts it.

3

Speed and integrity are in tension, and integrity has to win.

A fast restoration to an untrusted state isn't a win. Multiple industry incident-response teams report environments where the technical recovery is fast, but forensic validation is skipped or rushed. The environment is compromised again within hours because the same accounts, permissions, and backdoors were faithfully restored along with the legitimate data.

This is why an AD recovery runbook must be built around specialized people, processes, and technology purpose-built for identity workloads.

UNDERSTANDING THE AD-CENTRIC KILL CHAIN

You can't prepare or successfully execute an AD recovery if you don't know how an attacker gets in or how much they've compromised your AD. Let's start by understanding what the AD-centric kill chain looks like. Ransomware operators targeting AD generally follow a five-phase pattern.

Phase 1: Initial access and reconnaissance



Attacker objective: Establish a foothold, then map the environment before touching AD directly.

Key TTPs (MITRE ATT&CK)	Technique
T1078	Valid Accounts: stolen credentials reused for legitimate access
T1087.002 / T1069.002	Domain Account & Group Discovery: mapping privilege paths
T1482	Domain Trust Discovery: identifying inter-domain trust relationships

The attack rarely starts inside AD. Entry typically comes through a side door: spear phishing, exploitation of an exposed VPN or RDP endpoint, credential stuffing against a public-facing portal, or a supply-chain compromise through a trusted partner. Once a foothold is established, tools like BloodHound, SharpHound, and ADRecon can map delegation paths, privileged group memberships, and domain trust relationships within minutes, quickly surfacing Domain Admins, Enterprise Admins, overprivileged service accounts, and objects with misconfigured ACLs.



How this affects AD recovery

This phase doesn't damage anything yet, but it tells the attacker exactly which accounts and trust relationships are worth targeting next. Active Directory's attack surface here isn't one misconfiguration; it's a decade of inherited configurations, forgotten delegations, and permissions granted for convenience. Proactive hardening of your AD infrastructure is critical to remediate gaps in your identity's attack surface.



Phase 2: Privilege escalation and AD takeover



Attacker objective: Move from “has a foothold” to “owns the directory.”

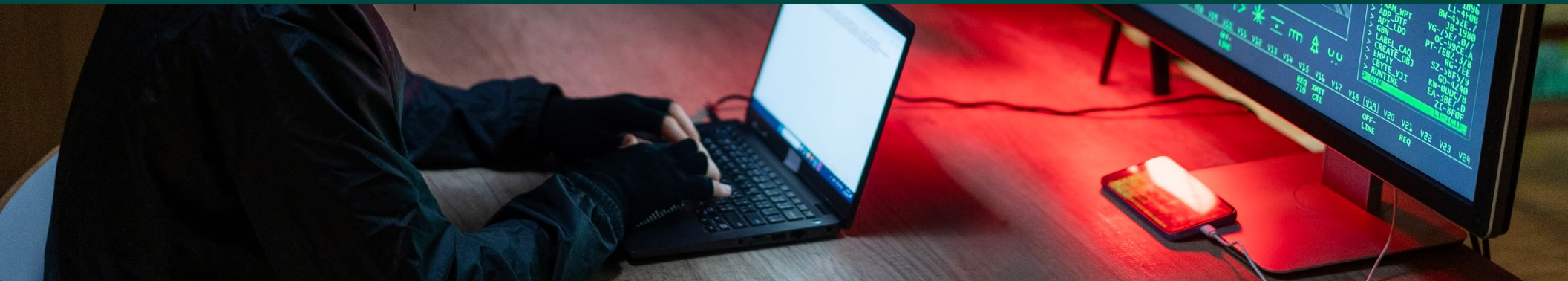
Key TTPs (MITRE ATT&CK)	Technique
T1558.003	Kerberoasting: offline cracking of service ticket hashes
T1558.001	Golden Ticket: forging Kerberos tickets after krbtgt hash compromise
T1003.006	DCSync: impersonating a DC to extract all AD password hashes
T1068	Exploitation for Privilege Escalation: ZeroLogon, noPac, PrintNightmare

This is the hinge point of the whole attack. Once the krbtgt account is compromised, the attacker can forge Golden Tickets: valid Kerberos tickets for any account, any service, with an arbitrary lifetime. At that point, Active Directory is fully under adversarial control.



How this affects AD recovery

If a runbook doesn’t include a mandatory krbtgt password reset (performed twice, respecting the domain’s replication interval) as a recovery step, a Golden Ticket forged in this phase can survive a routine password reset elsewhere in the environment. Advanced identity threat detection and response (ITDR) tools like Cohesity Identity Resilience can detect and remediate DCShadow, Golden Ticket, and Kerberoasting attacks at this phase, rolling malicious actions back before the incident becomes a full-blown recovery effort.



Phase 3: Persistence (planting backdoors inside AD)



Attacker objective: Guarantee re-entry even after AD is “restored” and the incident is believed to be resolved.

Key TTPs (MITRE ATT&CK)	Technique
T1207	DCShadow: rogue DC replicating malicious changes with no audit trail
T1556.001	Skeleton Key: master password injected into DC LSASS processes
T1178	SID-History Injection: invisible Domain Admin rights on an innocuous account
T1222.001	AdminSDHolder ACL Modification: auto-propagation of malicious rights

This is the least visible phase, and the most dangerous one for incident response teams. Before triggering encryption, sophisticated attackers embed persistence mechanisms directly into the structure of Active Directory itself. These backdoors are engineered to survive partial restores and password resets: the application layer can be fully recovered while the directory remains compromised and the attacker’s access remains intact.



How this affects AD recovery

This phase is the single strongest argument in this entire playbook for why “restore from backup” is not the same thing as recovery. See Section 1.

Phase 4: Lateral movement and data exfiltration



Attacker objective: Extract data before triggering encryption.
This creates the leverage behind double extortion.

Key TTPs (MITRE ATT&CK)	Technique
T1021.001 / T1021.002	RDP & SMB: lateral movement using stolen credentials
T1567.002	Exfiltration to Cloud Storage: data staging via Rclone, Mega



How this affects AD recovery

By this phase, the incident is no longer just an availability problem; it's a data-loss and disclosure problem. Runbooks need a forensics/legal track running in parallel with technical recovery, not bolted on afterward.

Phase 5: Deployment and encryption



Attacker objective: Detonate and cause as much disruption as possible to force a ransomware payment or cause chaos.

Key TTPs (MITRE ATT&CK)	Technique
T1486	Data Encrypted for Impact: mass encryption of files and volumes
T1490	Inhibit System Recovery: deletion of VSS shadow copies
T1485	Data Destruction: destruction of network-accessible backups
T1484.001	GPO Modification: ransomware deployment pushed via Group Policy

With persistence established and data staged, the signal is given. Group Policy Objects are used to push the ransomware payload across the entire domain simultaneously. Now the same infrastructure the organization relies on for management becomes the delivery mechanism for the attack.

BUILDING YOUR AD RECOVERY RUNBOOK

A recovery runbook isn't a single document you write once. It's five connected disciplines, each of which maps directly back to a phase of the kill chain in Section 2.

1 Prepare and harden

Close the gaps attackers rely on in Phase 1 before they're exploited:

- Inventory and audit MFA coverage on every Tier 0 account (Domain Admins, Schema Admins, Enterprise Admins)
- Review for least privilege: flag excessive Domain Admin group membership and stale delegations
- Identify and remediate stale, orphaned, or dormant privileged accounts
- Identify Kerberoastable service accounts (weak or crackable SPN configurations)
- Verify backup immutability and air-gap configuration
- Confirm recovery has been tested and RTO validated within the last 90 days – not assumed



2 Detect and respond

Traditional, rule-based security tooling is not built to catch identity-specific attacks: compromised credentials can look exactly like sanctioned behavior. Detection needs to be identity-specific and continuous to catch malicious behaviors in Phases 2 and 3:

- Monitor GPO changes, group membership changes, and Tier 0 asset changes in real time, not on a periodic scan cycle
- Specifically hunt for the four Phase 3 persistence techniques (DCShadow, Skeleton Key, SID-History injection, and AdminSDHolder ACL abuse) since these are the mechanisms engineered to survive a naive recovery
- Contain compromised accounts and sessions as surgically as possible to avoid an unnecessary full production shutdown

3 Investigate before you restore

This is the most important step in making sure your recovery doesn't lead to persistent reinfection from the backdoors attackers leave in Phases 3 and 4.

- Confirm root cause and full blast radius: how did the attacker get in, what did they touch, which Phase 1–3 techniques were used
- Treat this as an explicit go/no-go gate: do not initiate recovery until forensics has confirmed the extent of persistence mechanisms present
- Document the investigation and evidence trail; this is also exactly what insurers and auditors will ask for after the fact (a maintained audit trail with a minimum retention period is a standard requirement across most carriers)



4 Recover

Once an attacker has detonated the malware and encrypted your AD in Phase 5, you'll need to be able to recover quickly and cleanly to meet both RTO and RPO targets.

- Sequence identity sources correctly. In hybrid environments, restore Active Directory first as the authoritative identity source before re-establishing sync to Entra ID or Okta. Recovering pieces independently risks syncing a compromised or incomplete state back out to the cloud identity layer.
- Reset krbtgt twice. This invalidates any Golden Tickets forged during Phase 2 and is non-negotiable regardless of what else the recovery plan includes.
- Plan DC and domain recovery order explicitly. A runbook should define the sequence in which domain controllers and domains come back online across a multi-domain forest: not assume a single restore operation covers the whole environment.
- Validate before declaring "recovered." A system that is back online is not the same as a system that is clean. Recovery is complete only once forensic validation confirms no persistence mechanisms survived.

5 Learn from and continue to strengthen identity resilience

Continuous learning and improvement are fundamental parts of any security discipline. After any incident, you'll want to learn from what happened, adjust your process, and evaluate your technology to continue strengthening your identity resilience.

- Re-audit ACLs and privileged group membership post-recovery before declaring the environment trusted
- Feed after-action findings into what still needs to be hardened across your identity infrastructure
- Re-test recovery capability on a defined, recurring cadence: recovery readiness is a program, not a one-time project



SAMPLE TABLETOP AD RECOVERY DRILL

Reading a runbook and executing one under pressure are different skills. The only way to know if a recovery plan works is to drill it before an attacker forces the question. Here is an example of a tabletop AD recovery drill to reference and test with your own team.

Roles

Role	Responsibility
Executive Sponsor (CISO/CIO)	Sets success criteria for the drill and signs off on outcomes
SecOps Lead	Validates detection, alerting, and response workflows during the exercise
ITOps / AD Admin	Owns deployment, configuration, and execution of the recovery drill itself

Sample drill scenario

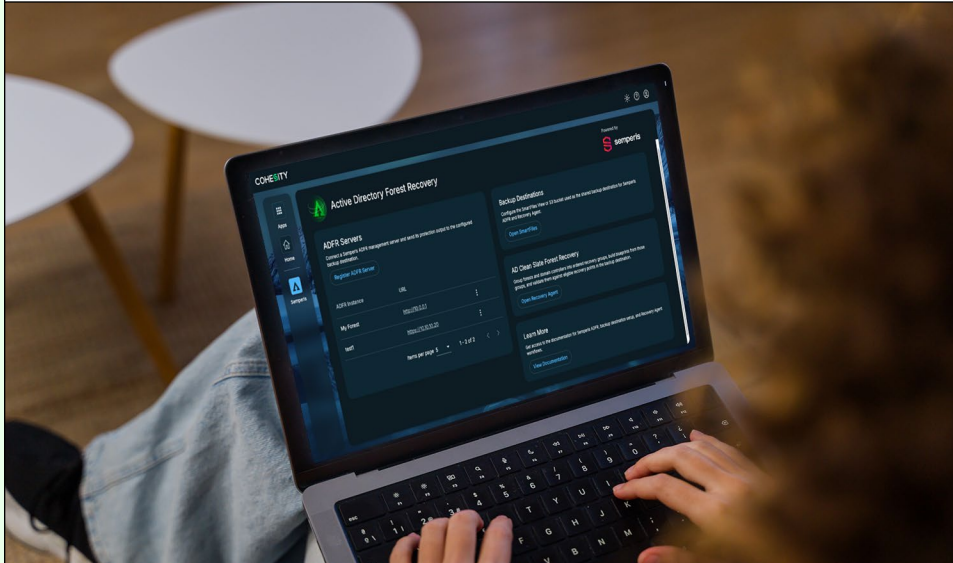
Use the kill chain phases from Section 2 and adjust timing to fit a half-day or full-day exercise.

Inject	Kill chain phase	Scenario detail
Hour 0	Phase 1	A phishing email delivers initial access; a foothold is established on a standard workstation
Hour 6	Phase 1	SIEM/logging shows anomalous LDAP enumeration consistent with BloodHound-style reconnaissance
Day 2	Phase 2	Evidence surfaces that the krbtgt hash was compromised and a Golden Ticket was likely forged
Day 3	Phase 3	Logs show replication traffic inconsistent with known DCs: potential DCSshadow activity
Day 3 + 4hrs	Phase 4	Large outbound data transfer detected to an external cloud storage endpoint
Day 3 + 18hrs	Phase 5	A GPO push is detected across the domain; ransomware detonates on file servers
Day 3 + 19hrs	Recovery	Recovery is formally initiated

SUCCESS CRITERIA

Score the exercise against these dimensions rather than treating it as pass/fail:

- **Time to detect** each inject, measured against the timestamp it occurred
- **Time to contain** once the team recognized an active incident
- **Time to clean recovery** with forensically validated clean state
- **Did the team catch persistence mechanisms** before declaring the environment trusted, or only after a second compromise?
- **Could the response team communicate and coordinate** without relying on the compromised identity environment?



AFTER-ACTION REPORT OUTLINE

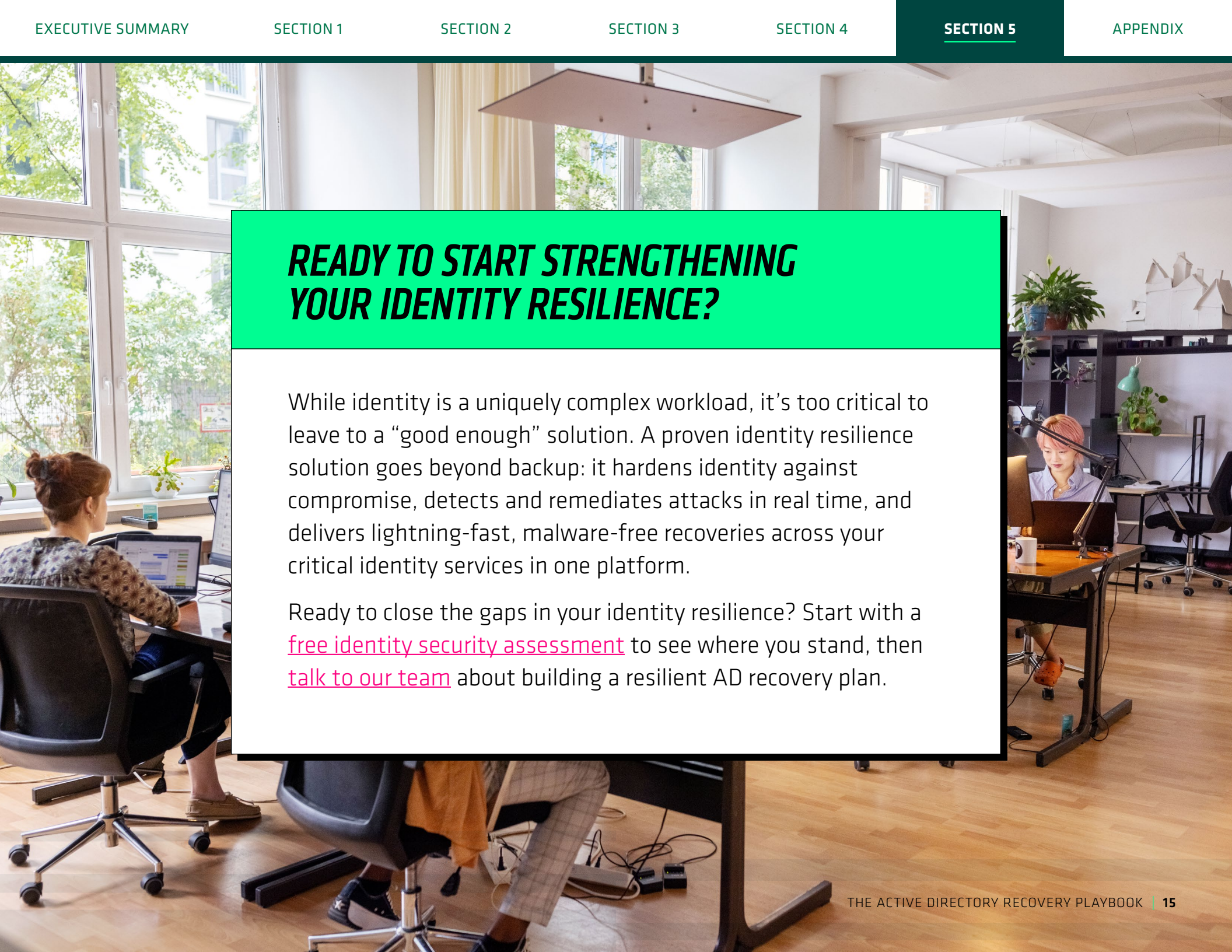
1. Incident timeline (actual vs. detected vs. contained)
2. Detection gaps (which injects were missed or caught late, and why)
3. Containment effectiveness
4. Recovery time vs. target RTO
5. Recovery point vs. target RPO
6. Persistence mechanisms found on first pass vs. found only on review
7. Action items to continue to harden the environment and strengthen identity resilience

RECOVERY READINESS SELF-ASSESSMENT

Use this as a working checklist for your AD recovery program, regardless of tooling:

- ☐ Immutable, isolated backup of AD data, decoupled from production credentials and infrastructure
- ☐ Ability to recover AD data independent of the underlying server OS
- ☐ Ability to perform recovery without dependency on internet connectivity or external cloud services
- ☐ Support for both granular (object/attribute) recovery and full forest recovery from the same workflow
- ☐ Coordinated, parallel recovery across multiple domain controllers and domains, not a strictly serial, one-DC-at-a-time process
- ☐ Full audit trail of AD changes (actor, timestamp, source, attribute) independent of native AD/Entra logging limits
- ☐ Forensic capability to identify persistence mechanisms and malicious changes, not just diff detection
- ☐ Administrative and infrastructure separation between identity recovery systems and general backup/recovery systems (Tier 0 isolation)
- ☐ Defined, tested hybrid recovery workflow spanning AD and connected cloud IdPs (Entra ID, Okta)
- ☐ Communication/coordination infrastructure for the response team that doesn't depend on the identity systems being recovered
- ☐ Ability to detect identity-based attacks (Golden Ticket, DCSync) and automatically remediate them in real time
- ☐ Ability to validate that identity recovery is malware-free

If you answered “no” to any of these, your business is at risk.



READY TO START STRENGTHENING YOUR IDENTITY RESILIENCE?

While identity is a uniquely complex workload, it's too critical to leave to a "good enough" solution. A proven identity resilience solution goes beyond backup: it hardens identity against compromise, detects and remediates attacks in real time, and delivers lightning-fast, malware-free recoveries across your critical identity services in one platform.

Ready to close the gaps in your identity resilience? Start with a [free identity security assessment](#) to see where you stand, then [talk to our team](#) about building a resilient AD recovery plan.

APPENDIX

Full MITRE ATT&CK reference table

Phase	ID	Technique
1. Initial access & reconnaissance	T1078	Valid Accounts
	T1087.002 / T1069.002	Domain Account & Group Discovery
	T1482	Domain Trust Discovery
2. Privilege escalation	T1558.003	Kerberoasting
	T1558.001	Golden Ticket
	T1003.006	DCSync
	T1068	Exploitation for Privilege Escalation
3. Persistence	T1207	DCShadow
	T1556.001	Skeleton Key
	T1178	SID-History Injection
	T1222.001	AdminSDHolder ACL Modification
4. Lateral movement & exfiltration	T1021.001 / T1021.002	RDP & SMB
	T1567.002	Exfiltration to Cloud Storage
5. Deployment & encryption	T1486	Data Encrypted for Impact
	T1490	Inhibit System Recovery
	T1485	Data Destruction
	T1484.001	GPO Modification

Glossary

- **Golden Ticket:** A forged Kerberos ticket-granting ticket, created once an attacker has the krbtgt account hash, granting access to any account or service with an arbitrary lifetime.
- **DCSync:** A technique in which an attacker impersonates a domain controller to extract password hashes for any account in the directory.
- **DCShadow:** A technique where an attacker stands up a rogue domain controller to replicate malicious changes into AD without generating a normal audit trail.
- **Skeleton Key:** Malware injected into a domain controller's LSASS process that installs a master password, granting the attacker authentication as any user.
- **SID-History Injection:** A technique that grants an account invisible elevated (often Domain Admin) rights by manipulating its SID history attribute.
- **Kerberoasting:** Requesting Kerberos service tickets for accounts with weak service passwords, then cracking them offline to recover credentials.
- **krbtgt:** The Active Directory service account whose password hash underpins the Kerberos ticket-granting system; compromising it enables Golden Ticket attacks.
- **Tier 0:** The set of accounts and systems (Domain Admins, Enterprise Admins, domain controllers, etc.) whose compromise means full control of the identity environment.

READY TO START STRENGTHENING YOUR IDENTITY RESILIENCE?

GET YOUR FREE ASSESSMENT

COHESITY

cohesity.com | 1-855-214-3133

© 2026 Cohesity, Inc. All rights reserved. Cohesity, the Cohesity logo, SnapTree, SpanFS, DataPlatform, DataProtect, Helios, and other Cohesity marks are trademarks or registered trademarks of Cohesity, Inc. in the US and/or internationally. Other company and product names may be trademarks of the respective companies with which they are associated. This material (a) is intended to provide you information about Cohesity and our business and products; (b) was believed to be true and accurate at the time it was written, but is subject to change without notice; and (c) is provided on an "AS IS" basis. Cohesity disclaims all express or implied conditions, representations, warranties of any kind. 6100037-00110-2026