Identity Resilience
Proof-of-Concept (POC) Toolkit

Prove how you can detect, withstand, and recover from identity-based cyberattacks with your environment and your team.

1 What an identity resilience POC delivers

A structured, guided evaluation that proves (in your own environment) how Cohesity Identity Resilience can help you secure your critical identity infrastructure across every stage of the attack lifecycle.

You'll walk away with:

- Proof that your identity infrastructure can be recovered in hours, not days or week
- Live detection and remediation of active threats through advanced continuous monitoring
- Actionable steps to close gaps/address vulnerabilities in your identity environment
- Post-breach forensics that surface and removes backdoors to prevent reinfection

2 Who's involved

Our team

- **Cohesity Account Executive**
  Owns the engagement, commercial scope, and success criteria. Your single point of contact for all engagements.
- **Cohesity Sales Engineer**
  Technical lead. Maps your environment to the Cohesity Identity Resilience solution and coordinates the POC with our identity resilience specialist, end-to-end.
- **Identity Specialist**
  Drives the POC from the technical perspective for identity recovery and threat detection testing.

Your team

- **Executive Sponsor (CISO/CIO)**
  Sets success criteria. Signs off on outcomes and requirements for business case.
- **SecOps Lead (and identity lead if one exists)**
  Validates detection, alerting, and response workflows. Responsible for identity security day-to-day.
- **ITOPs / AD Admin**
  Responsible for deployment, configuration, and identity recovery drills and identity infrastructure maintenance.

3 The process

Phase	1. Align	2. Stand-up	3. Prove	4. Review
Approximate time	~1 week	~1-2 weeks	~1-2 weeks	~1 week
Core deliverables	Confirm scope, success criteria, and stakeholders. Define what "proven" looks like.	Deploy to lab or non-production tenant. Connect AD and/or Entra ID. Get ready with all the POC environment requirements.	Run the POC with the team covering critical capabilities: detect risky changes and execute a clean recovery.	Walk through findings. Document and evaluate outcomes based on success criteria. Answer questions and discuss next steps.

4 Fast-start checklist

- [ ] **POC/NDA agreement in place**
  POC and NDA terms signed and countersigned. Confirm with your account team what is necessary before the start of a POC.
- [ ] **Name point of content for internal stakeholders**
  One lead from IT team, one from security and/or identity team
- [ ] **Define the success criteria**
  Understand what "proven" means and what outcomes you're looking to test in a POC for your key internal stakeholders.
- [ ] **Align with executive sponsor**
  Review criteria with and make sure that executive sponsor is engaged and in agreement with what outcomes the POC should accomplish
- [ ] **Schedule kickoff call with the Cohesity team and your internal stakeholders**
  Meet to understand the expectations, process, and core team who will be working with your team throughout the POC process.
- [ ] **Test environment access**
  Work with your Cohesity team to ensure that you have the right POC lab environment requirements in place.

Ready to start? Contact your Cohesity Account Executive to scope your Identity Resilience POC.

COHESITY