CAPABILITY BRIEF · 03 / 04

acsense

# Disaster Recovery

Hot standby tenants, one-click failover, and Continuous Resilience Validation for your IAM infrastructure. Recover from any identity disaster with a tested ~10-minute RTO.

Identity is Tier-0 infrastructure. Every employee, application, partner, and AI agent authenticates through it. When an identity tenant goes down, whether from ransomware, a catastrophic misconfiguration, or a provider outage, the entire enterprise stops. No one authenticates. No one works.

Identity providers guarantee their own platform uptime. You own tenant recoverability. There is no native hot standby, no tenant-level failover, and no continuous validation that your identity DR plan holds under real conditions. Acsense closes that gap.

Acsense Disaster Recovery closes the gap. Hot standby tenants kept in continuous sync, automated failover with tested RTO, and Continuous Resilience Validation (CRV) that proves recoverability before disaster strikes.

One platform. Any IDP. Tenant-level disaster recovery that works the same way regardless of which identity provider runs underneath.

**~10 Min**
Tested RTO with automated failover

**Continuous**
Resilience Validation (CRV)

**IDP-Agnostic**
Tenant-level DR, any IDP

> *"Identity providers guarantee their own uptime, not your ability to recover or fail over your tenant. The disaster recovery gap is the single most critical unaddressed risk in enterprise IAM."*
>
> Reflecting the AWS Shared Responsibility Model

**22%** of breaches start with stolen credentials. Credential-based breaches take **246 days** on average to identify and contain. Identity attacks rose **32%** in H1 2025.

SOURCES: VERIZON DBIR 2025 · IBM COST OF A DATA BREACH 2025 · MICROSOFT DIGITAL DEFENSE REPORT 2025

# The identity DR gap: no failover, no validation, no plan

Every enterprise has DR for compute, storage, and networking. Almost none have DR for identity. When the IAM tenant goes down, there is no hot standby to fail over to. No automated switchover. No way to prove, before the disaster, that recovery actually works. Teams discover the gap during the outage itself.

**Identity providers guarantee their own platform uptime.** You own tenant recoverability. There is no native hot standby, no tenant-level failover, and no continuous validation that your identity DR plan holds under real conditions. Acsense closes that gap.

# How Acsense Disaster Recovery works

STAGE 1

### Hot Standby Tenant

A continuously synced replica of your production IAM tenant, ready to take over at any moment.

STAGE 2

### Automated Failover

One-click or automated switchover to the standby tenant. Fast, tested RTO. No manual reconstruction.

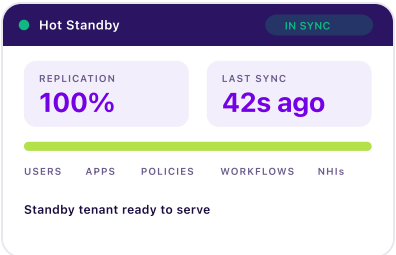
STAGE 3

### Continuous Resilience Validation

Automated tests prove the standby tenant is ready, before disaster strikes. Not a checkbox. A live proof.

# Recovery readiness, validated continuously

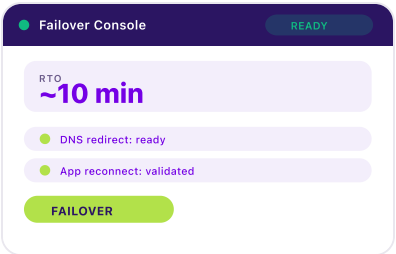
Acsense Disaster Recovery is not a backup you hope works. It is a continuously validated, hot-standby architecture that proves recoverability before disaster strikes. From tenant replication to automated failover to Continuous Resilience Validation (CRV).




## Hot Standby Tenant + Continuous Replication

A full replica of your production IAM tenant, continuously synced and ready to take over. Every user, app, policy, workflow, and NHI binding is replicated. The standby tenant is not a cold backup. It is a live, validated, ready-to-serve copy of your identity infrastructure.

Continuous sync · Full tenant replica · Live standby




## Automated Tenant Failover

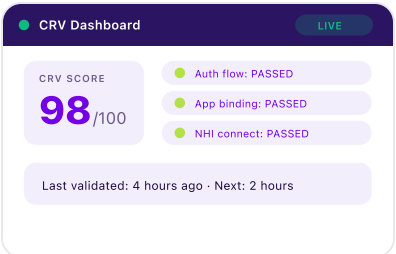
One-click or automated switchover that recovers access, not just the directory. Your users authenticate again, immediately. RTO is tested and validated continuously by CRV, not estimated. No manual reconstruction, no runbook improvisation, no extended outage while the team figures out what to do.

One-click failover · ~10-minute RTO · Orchestrated switchover

## Last-Mile Application Recovery (Coming Soon)

Most identity DR tools stop at the directory. Acsense is building the next layer: automatically updating SAML metadata and application configurations on the recovered tenant so critical apps reconnect without manual reconfiguration. Your users authenticate again — not just to the directory, but to every application that depends on it.

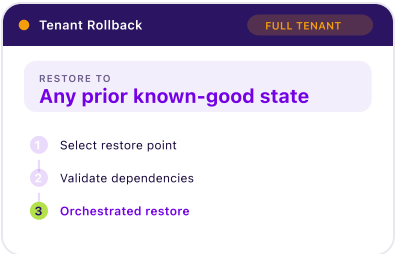
DNS redirect · App reconnection · Session continuity




## Continuous Resilience Validation (CRV)

Automated, non-disruptive tests that prove the standby tenant is ready. CRV validates authentication flows, app bindings, policy enforcement, and NHI connectivity on a continuous schedule. The result is a CRV score: a live, quantified proof of recoverability, updated automatically, not a checkbox or an annual tabletop exercise.

Automated testing · CRV score · Non-disruptive




## Full Tenant Rollback

When failover is not the right response (e.g., the issue is a configuration corruption or insider threat, not a full outage), roll the entire tenant back to any prior known-good state. Dependency-aware, orchestrated, and auditable. Works alongside failover as a complementary recovery path.

Point-in-time rollback · Dependency-aware · Orchestrated

# Real scenarios. Real resilience.

Disaster Recovery operates at the tenant level regardless of which IDP runs underneath. Four scenarios from real IAM environments where the difference between minutes and days is measured in revenue, trust, and regulatory exposure.

WHEN THIS HAPPENS

### Ransomware targets the production IAM tenant

**Acsense:** Automated Failover switches to the hot standby tenant. Authentication continues uninterrupted for the entire enterprise while the primary tenant is remediated.

**Business continuity preserved. Attacker locked out.**

WHEN THIS HAPPENS

### Rogue admin or compromised credential makes mass changes

**Acsense:** Failover to the clean standby tenant removes the attacker's foothold. Full Tenant Rollback restores the known-good state while Tenant Investigation runs in parallel to preserve forensic evidence.

**Clean tenant restored. IR team has a full evidence trail.**

WHEN THIS HAPPENS

### Board asks "can you prove identity DR works?"

**Acsense:** CRV score, updated automatically. Last test: hours ago, not months. Auth flows, app bindings, policy enforcement, all validated. RTO on record.

**Auditable proof of recoverability, not a slide deck.**

WHEN THIS HAPPENS

### Security team needs to investigate what an attacker did without destroying evidence

**Acsense:** Tenant Investigation freezes a forensic snapshot of the compromised state while the clean standby tenant takes over operations. Both happen in parallel.

**Operations restored. Forensic evidence intact. Nothing lost.**

# Why Acsense for Disaster Recovery

### Tested RTO, proven continuously

Not an SLA on paper. A live, validated failover path tested automatically and scored with CRV. The RTO you report is the RTO you can deliver.

### Last-Mile Application Recovery (Coming Soon)

Most identity DR tools stop at the directory. Acsense is adding last-mile application reconnection — updating SAML metadata and app configurations on the recovered tenant automatically. Coming soon.

### Full tenant rollback as a complement

When the issue is corruption or insider threat, not outage, roll the entire tenant back to any prior state. Two recovery paths, one platform.

### NHI & AI agent coverage

Service principals, API tokens, and agent bindings are replicated to the standby tenant and validated by CRV alongside human identities.

### Continuous Resilience Validation

Automated, non-disruptive tests prove the standby tenant is ready. A quantified CRV score, not a checkbox or annual tabletop.

### Hot standby, not cold backup

A continuously synced, live replica of your production tenant. Ready to serve authentication the moment you fail over.

### IDP-agnostic by design

Acsense delivers disaster recovery for your tenant the same way regardless of which IDP runs it. One DR plan, one failover path, one validation score.

## Ready to prove your identity DR plan actually works?

See Acsense Disaster Recovery and Continuous Resilience Validation in action on your IAM tenant.

**Request a demo**

# Built for the IAM admin, and everyone who depends on identity

Disaster Recovery is the resilience guarantee. The platform serves the people who keep IAM running every day, and the leaders who carry the risk when it doesn't.

### IAM Administrators

Your job is to keep IAM running. One-click failover to a hot standby tenant. No manual reconstruction. CRV proves the standby is ready before you need it and tells you your actual tested RTO.

### IT & Operations Leaders

Defined, validated RTO and RPO for identity. CRV produces a quantified readiness score, not an annual tabletop exercise.

### Security & CISO

Ransomware and insider threat resilience for identity. Automated failover removes the attacker's leverage. Auditable DR readiness for regulators and the board.

### AI & ML Leaders

NHI bindings replicated to the standby tenant and validated by CRV. As your NHI surface grows, disaster recovery scales with it.

**CERTIFIED & AUDITED**

- **FedRAMP High** Authorized
- **SOC 2 Type II** Audited by EY
- **ISO 27001** Information Security
- **ISO 27017** Cloud Security
- **ISO 27018** Cloud Privacy

**ABOUT ACSENSE**

Acsense is the IAM Resilience Platform that protects, recovers, and continuously validates enterprise identity infrastructure at scale. The platform delivers Backup & Recovery, Configuration Management, Disaster Recovery, and Compliance & Assurance across Okta and Microsoft Entra ID, from a single purpose-built product. Acsense serves security-first enterprises and federal agencies across financial services, healthcare, critical infrastructure, public sector, and technology globally. Learn more at acsense.com.