

IAM RESILIENCE PLATFORM

BUILT FOR THE ERA OF MACHINE IDENTITY

Your identity infrastructure, resilient by design.

Acsense is the **IAM Resilience Platform**: protecting, recovering, managing, and continuously validating enterprise identity infrastructure. IDP-agnostic by design. Built for organizations that cannot afford identity downtime.

Gartner Cool Vendor · Identity-First Security

Gartner Hype Cycle · IAM Backup & Data Protection

Backup &
Recovery

Configuration
Management

Disaster
Recovery

Compliance &
Assurance

Millions

of Identities Protected

~10^{min}

Full tenant RTO and RPO

7+

Regulatory frameworks mapped
automatically

The IDP keeps you online. The Identity Control Plane keeps you operational.

Your IDP handles authentication. It won't recover your tenant from ransomware, detect configuration drift, or continuously validate your security posture.

FOUR RISKS EVERY ENTERPRISE IAM TEAM CARRIES TODAY

01

Configuration drift goes undetected for hours or days

Access policy changes, MFA requirement gaps, and permission misconfigurations accumulate silently. By the time they surface, the blast radius is wide and the rollback window is gone.

02

A corrupted or locked tenant halts the entire organization

Ransomware targeting identity infrastructure, accidental bulk deletions, or a misconfigured admin policy can lock every user out simultaneously. Native IDP tools offer no full-tenant recovery path.

03

Compliance evidence is fragmented across tools and tenants

SOC 2, ISO 27001, DORA, NIS2, and NIST SP 800-53 controls require continuous identity assurance. Without automated mapping, teams spend weeks assembling evidence manually for every audit cycle.

04

Non-human identities create invisible attack surface

Service accounts, API tokens, and machine identities proliferate faster than they are audited. Overprivileged NHIs are the most common initial access vector in enterprise identity attacks.

The bottom line: Protecting, recovering, and continuously validating your identity infrastructure requires a dedicated resilience layer. Acsense is the Identity Control Plane.

Four modules. One Identity Control Plane.

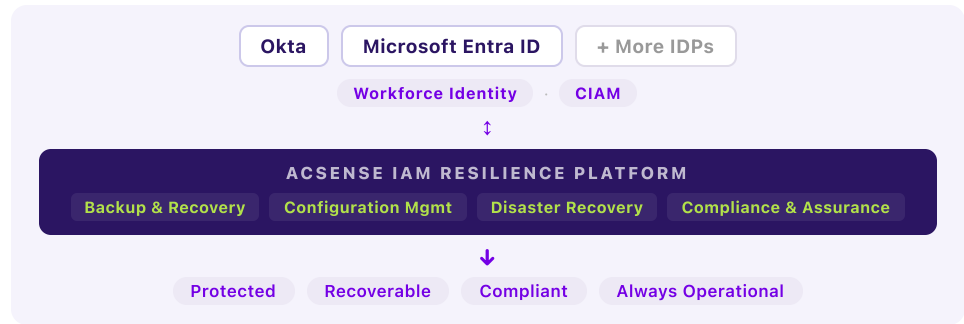
Acsense brings backup, configuration control, disaster recovery, and compliance assurance under a single operational layer for Okta and Entra ID. Each module is built for enterprise scale and designed to work as a unified system.



Most organizations think they are protected once everything is in the cloud. This is a misconception. Compliance and regulations require a backup tenant for significant and critical assets like Okta.

Lior Zagury, Director of Global IT — Monday.com

What Acsense covers



1

Backup & Recovery

Continuous automated backups of your entire Okta and Entra ID tenant. Granular object-level restore or full-tenant recovery with a complete audit trail of every change.

— Full tenant recovery in approximately 10 minutes

2

Configuration Management

Track every IAM configuration change with full attribution. Clone tenants for testing, promote changes across environments, and map dependencies before you commit.

— Complete change audit trail with role attribution

3

Disaster Recovery

Standby tenant infrastructure with one-click failover. Continuously validates your recovery posture so your RTO is a tested reality, not a theoretical target.

— Continuous Resilience Validation built in

4

Compliance & Assurance

Real-time drift detection mapped to SOC 2, ISO 27001, DORA, NIS2, APRA, FISMA, and NIST SP 800-53. NHI audit trails included across both IDPs.

— Drift detected in 10 minutes across both IDPs

Built for IAM resilience.

Non-human identities now outnumber human identities in the enterprise, and attackers are targeting identity infrastructure directly, not just endpoints. When it fails, every user, app, and workflow goes down with it. Most identity protection tools were not built for this. Acsense was.

01

The Identity Control Plane for enterprise IAM resilience

Every competitor is a backup vendor, a data protection vendor, or an ITDR vendor that added identity as a module. Acsense is the only product purpose-built for IAM resilience across both Okta and Entra ID, with unified configuration management, disaster recovery, and compliance and assurance in one platform.

IAM Resilience category creator

02

Continuous Resilience Validation means your RTO is tested, not promised

Other solutions document a recovery process. Acsense continuously runs that process against your live environment so that when you need to invoke disaster recovery, you already know it works.

Tested RTO, not theoretical

03

Unified compliance baseline across Okta and Entra ID

Most tools cover one IDP. Acsense maps both Okta and Entra ID to seven regulatory frameworks simultaneously, with continuous drift detection and audit-ready evidence for every audit cycle.

SOC 2, ISO 27001, DORA, NIS2, APRA, FISMA, NIST SP 800-53



GET STARTED

See IAM Resilience in action.

Request a demo at acsense.com



Protect. Recover. Remain Operational.