Okta To Entra ID Migration Security Parity Framework – A Checklist for CISO

A structured leadership decision guide for CIOs, CISOs, and security stakeholders — ensuring your Conditional Access posture on Day 1 in Entra ID is at least as strong as what you had in Okta.

"The fastest way to lose trust in an Okta to Entra ID migration is security regression."

1. Pre-Migration: Go / No-Go Gate

Critical

Authoritative Security Baseline

Leadership must confirm a verified current-state inventory before any migration work begins. You cannot achieve parity with an unknown baseline.

- **Export every Conditional Access policy from Entra ID with state, exclusions & last-modified date.**

  Use Microsoft Graph API or CA Insights Workbook. Flag any policy in Report-Only or Off state — these do not enforce.

- **Inventory all Okta sign-on policies, app-level policies, and adaptive MFA rules.**

  Map each Okta policy concept (sign-on rule, network zone, device trust, group membership trigger) to its Entra ID equivalent before migration planning begins.

Exclusion groups created for "temporary pilot" scenarios routinely persist for years. A group with 847 members - including compromised service accounts - is a real pattern found in enterprise assessments. Audit before migration, not after.

- **Document every CA exclusion group — enumerate members and validate justification.**

  Stale exclusion groups are the #1 MFA bypass risk. Each member must have a current, documented, time-limited reason for exclusion.

- **Confirm no users are enabled for legacy per-user MFA in the Entra admin center**

  Legacy per-user MFA conflicts with Conditional Access policy enforcement. Verify Enabled and Enforced fields are clear before configuring CA policies.

- **Identify all applications integrated via Okta — SAML, OIDC, and proprietary connectors.**

  Custom SAML/OAuth configurations require manual reconfiguration in Entra. Each integration must be catalogued with its MFA requirement and current access rule.

- **Obtain executive sign-off that baseline assessment is complete before proceeding to migration design.**

  This is a formal governance gate. The CIO or CISO must attest that the parity gap inventory has been completed and reviewed.

2. MFA & Conditional Access Parity Design

Critical

"MFA methods and Conditional Access policy models do not map 1:1 between Okta and Entra ID. Every leadership decision here directly determines whether your security posture improves or regresses."

- **Define Authentication Strength policies — differentiate MFA methods by privilege tier.**

  Not all MFA is equal. FIDO2 / Certificate-Based Auth for Tier-0 Admins. Microsoft Authenticator with number matching for standard users. Eliminate SMS OTP for all privileged operations.

- **Map every Okta network zone to a Named Location in Entra ID — validate IP ranges are current.**

  Stale named locations grant trusted status to ranges no longer under organizational control. Each IP range must be verified against current network infrastructure before migration.

⚠ **COMPLIANCE DEVICE FALSE FLOOR**

Device compliance in Intune is evaluated at policy assignment time, not continuously. A device compliant at 9AM can fail by noon and still hold an active session token. Configure session controls explicitly to close this gap.

- **Translate Okta device trust rules to Entra device compliance via Intune integration.**

  Entra ID uses Intune compliance policies in place of Okta Device Trust. Hybrid Joined and Entra Joined device paths must be separately designed and validated.

- **Design session control policies to enforce continuous compliance re-evaluation.**

  Session controls must be explicitly configured — sign-in frequency, persistent browser session restrictions, and continuous access evaluation (CAE) — to close the compliance gap between assignment and runtime.

- **Design Conditional Access policies for Workload Identities (service principals)**

  Machine identities often operate outside human-centric CA policy scope. Inventory all service principals and application registrations; apply location and risk controls via Workload Identity CA (Entra ID P2).

- **Define Cross-Tenant Access and B2B guest identity policies**

  External partner and guest identities traversing the tenant boundary are a common parity gap. Explicitly define inbound and outbound trust settings for MFA claims and device compliance.

- **CIO/CISO joint sign-off on target CA policy architecture before staging begins**

  The CA policy architecture document must be reviewed and approved at leadership level.

3. Policy Validation Without Enforcement Risk

High

“Report-Only mode is critical for impact testing — but Report-Only policies provide zero enforcement. Leadership must govern the transition from staged to enabled policies explicitly.”

- **Stage all CA policies in Report-Only mode and run CA What-If simulations for each user population**

  Use the Entra CA What-If tool monthly during staging to validate that policy intent matches runtime behavior before any cutover.

- **Establish a formal Report-Only → Enabled promotion checklist with sign-off requirements**

  Every Report-Only policy must have a documented promotion plan. Policies must not remain in Report-Only mode past the staging window without documented leadership exception.

⚠ **REPORT-ONLY MODE TRAP**

Policies appearing in the CA policy list in Report-only mode show up in access reviews and look like enforcement but they don’t run. Many organizations discover post-breach that critical policies were staged and never promoted. Require exceutive attestation on all promotions.

- **Execute a controlled pilot with select users — validate MFA flows, app access, device compliance paths**

  Pilot population should span all user types: admins, standard users, guests/B2B, service accounts, mobile users, and legacy application users.

- **Confirm parallel Okta authentication is maintained during pilot — dual-run before full cutover**

  Both identity systems must operate in parallel during pilot to allow rollback without user impact. Define the parallel-run window duration in the migration plan.

- **Document and resolve all MFA friction points and policy gaps surfaced during pilot**

  Pilot findings must be formally tracked, each gap assigned a resolution owner, and re-tested before proceeding to wave migration.

4. Phased Cutover with Parity Checkpoints

Critical

“Wave-based migration minimizes blast radius. Each wave requires a security parity checkpoint — a verified comparison of enforcement coverage before and after the wave — before the next wave proceeds.”

- **Define migration waves by risk profile: start with low-privilege users, progress to admins last.**

  Privileged identities (Global Admins, PRA, Security Admins) should be migrated in the final wave — after all parity issues have been identified and resolved in earlier waves.

- **Run a parity checkpoint after each wave — compare Okta enforcement coverage to Entra enforcement**

  The parity checkpoint is a structured comparison: for every migrated user and app, verify the Entra CA policy is applying equivalent or stronger controls than the Okta policy it replaced.

- **Configure alerts on all CA policy changes — any modification triggers security team notification**

  Policy drift during migration is a significant risk. Real-time change alerting on Conditional Access policies must be active before cutover begins.

- **Ensure 24/7 support coverage and a real-time health dashboard are in place for each cutover window**

  Identity system cutovers require around-the-clock coverage. The health dashboard must surface MFA failures, CA policy errors, and sign-in anomalies in real time.

- **Maintain a tested rollback procedure for each wave — including Okta re-federation steps.**

  Rollback is not theoretical — it must be tested. Define the precise steps to re-federate Entra ID to Okta for each application category and validate the procedure before cutover.

- **Disable corresponding Okta MFA policies for migrated users to eliminate double-prompting.**

  Once Entra CA is enforcing MFA for a user or app, set the corresponding Okta sign-on policy to Inactive to avoid dual-MFA prompts. Coordinate the timing precisely.

5. Exclusion Hygiene & Authentication Uplift

High

“Migration creates new exclusion debt. Leadership must mandate operational hygiene programs immediately post-cutover — before the exclusions created during migration calcify into permanent attack surface.”

- **Initiate exclusion hygiene sprint within 30 days of final wave cutover.**

  For every CA exclusion group created during migration: enumerate current members, validate justification, remove stale entries. Implement Entra ID Access Reviews for ongoing automated cadence.

- **Enforce phishing-resistant MFA for all Tier-0 privileged identities.**

  Global Administrators and Privileged Role Administrators must authenticate with FIDO2 security keys or Certificate-Based Authentication. SMS OTP is not acceptable for these roles under any circumstance.

- **Enable Privileged Identity Management (PIM) for all admin role assignments.**

  Replace standing privileged access with just-in-time role activation via PIM. This is an immediate security uplift opportunity above Okta's native privileged access model.

- **Validate all Named Location IP ranges against current network infrastructure.**

  Named locations migrated from Okta network zones must be re-validated against live network topology. VPN ranges, office IPs, and cloud egress addresses change — verify all ranges are current and organizationally controlled.

- **Enable passwordless authentication pathways — FIDO2, Windows Hello, Microsoft Authenticator.**

  Post-migration is the optimal window to accelerate passwordless adoption. This capability exceeds what was available in Okta and represents a direct security ROI on the migration investment.

6. Board-Ready Continuous Verification

Ongoing

“Parity is not a migration deliverable — it is an ongoing governance discipline. These items define the operational program that keeps your CISO's board narrative accurate and defensible.”

- **Deploy Entra ID CA Insights Workbook and Microsoft Secure Score as operational dashboards.**

  These must be reviewed weekly by the security operations team — not surfaced only at quarterly reporting cycles. Policy coverage gaps surface here before they become incidents.

- **Run CA What-If simulations monthly to validate policy intent matches runtime behavior.**

  Simulate sign-in scenarios for admin users, guest/B2B users, mobile users, and service principals monthly. Document results as evidence of continuous parity verification.

- **Establish quarterly exclusion group review as a mandated security operations procedure.**

  Automate via Entra ID Access Reviews. Any exclusion group whose review lapses must be automatically flagged to the CISO. No exclusion should survive more than 90 days without re-validation.

- **Enable Identity Protection risk-based Conditional Access — user risk and sign-in risk policies.**

  Activate Microsoft's 78 trillion daily security signal advantage. Risk-based CA automatically challenges or blocks anomalous sign-ins — this capability exceeds standard Okta Adaptive MFA and represents a strategic security gain towards Zero Trust Architecture.

- **Text Box 2, TextboxPrepare a board-ready parity attestation narrative — evidence-based, not assertion-based.**

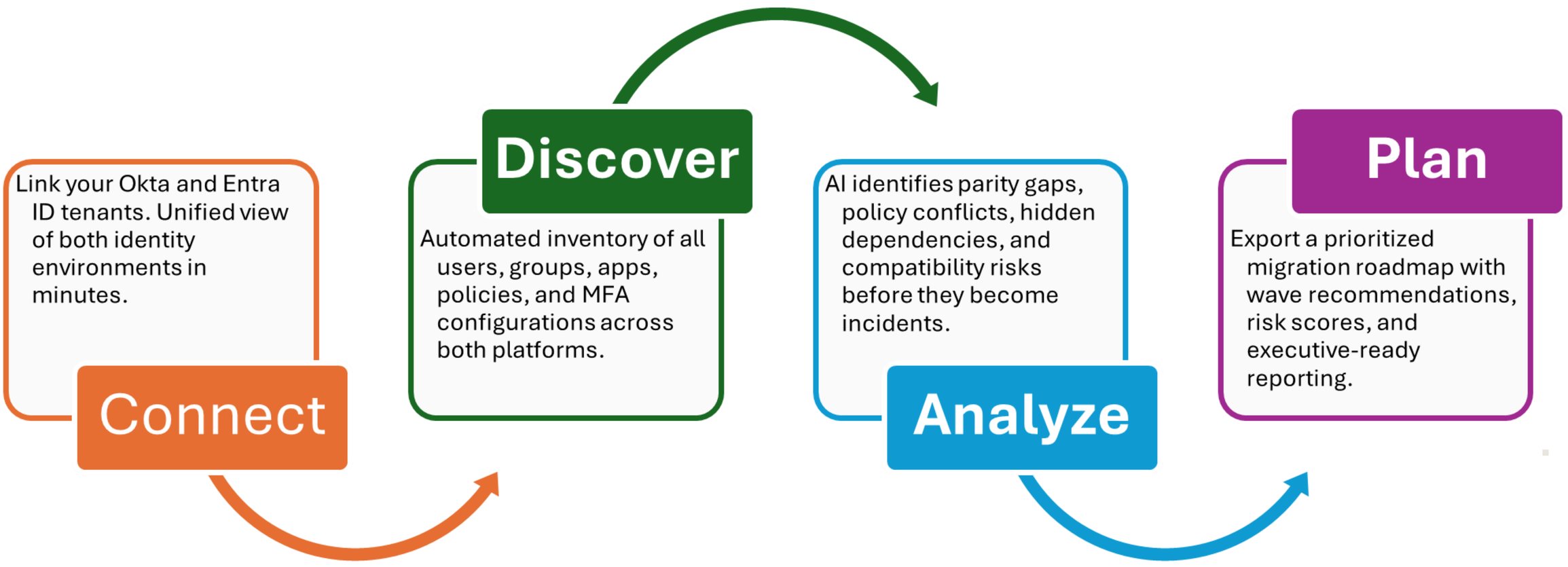
  “We have MFA" is no longer sufficient. The board narrative must include: CA policy coverage percentage, exclusion count and trend, authentication strength distribution, and last verified What-If simulation date.

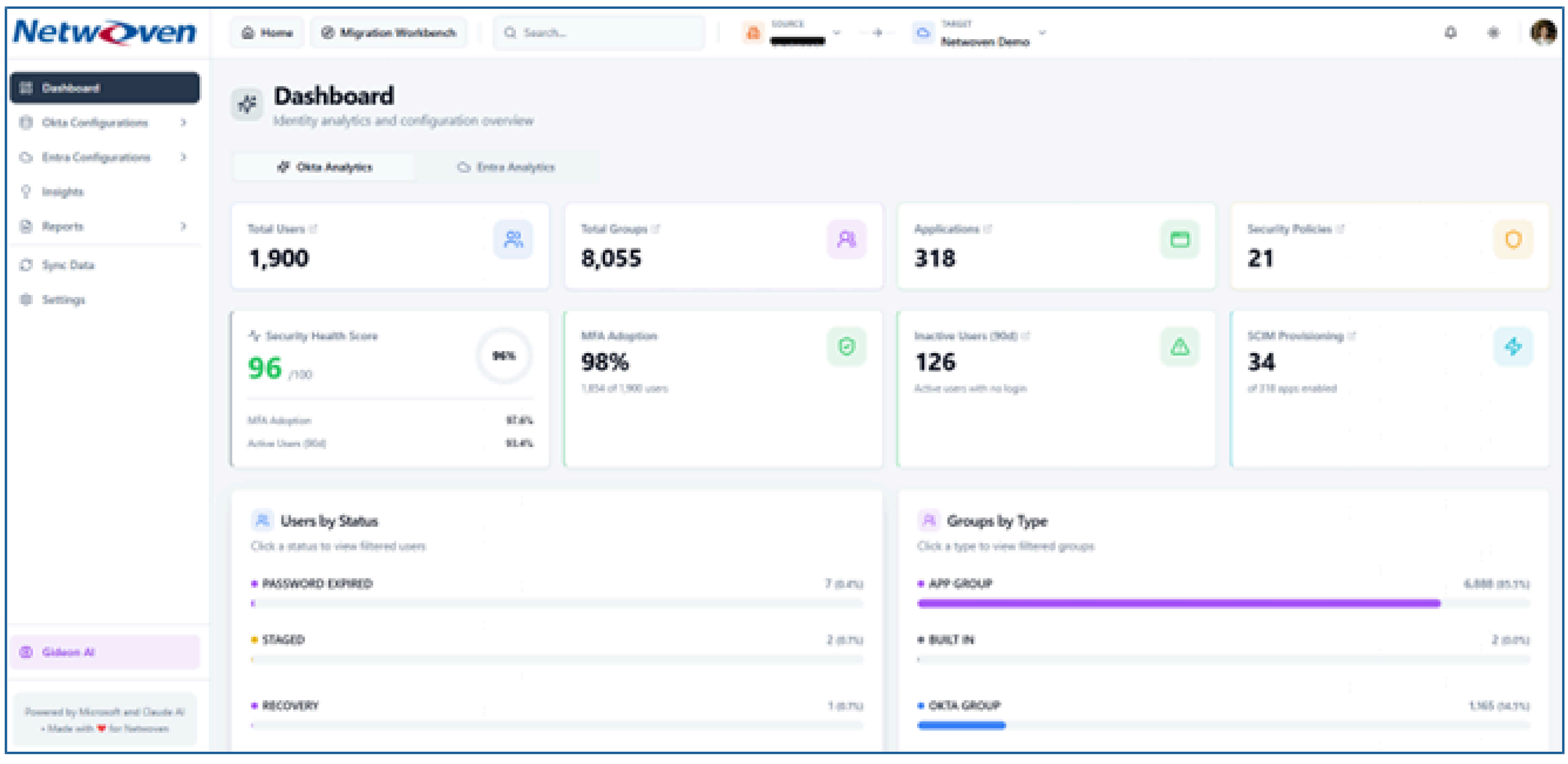
Stop Auditing Spreadsheets.
Let AI do the Discovery

Every checklist item above demands evidence — not assertion. Netwoven's AI Discovery Workbench is the engine that makes this checklist answerable in hours, not weeks — automating the discovery, analysis, and parity mapping that typically consumes 2–4 weeks of manual spreadsheet work.

"Reduce discovery time by 80%. Eliminate migration blind spots. Get a data-driven migration plan — before you commit to a single cutover wave."

How it works - 4 Steps

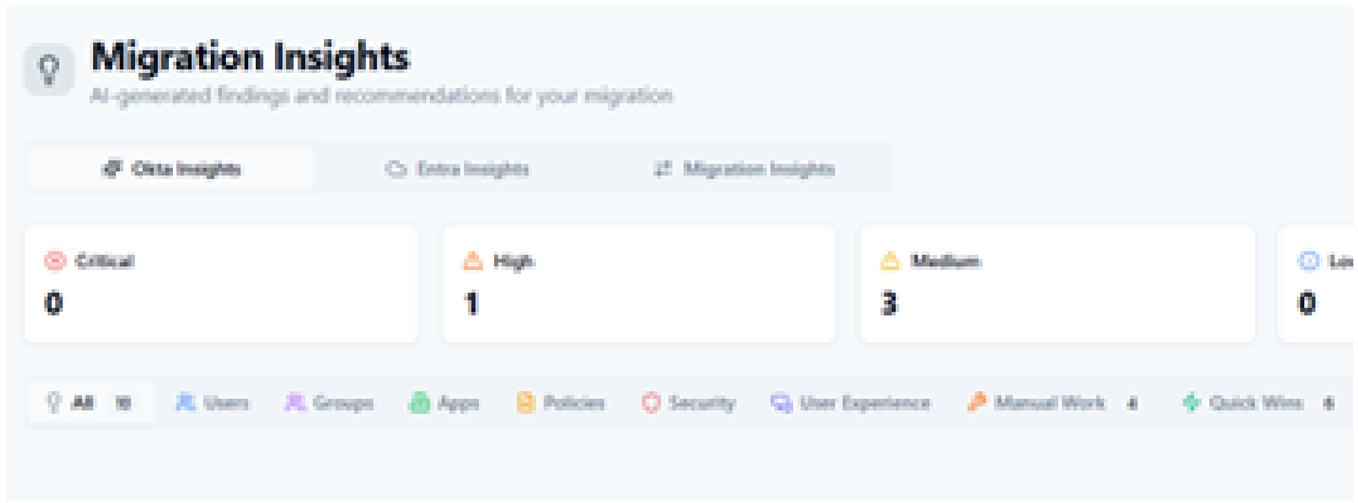


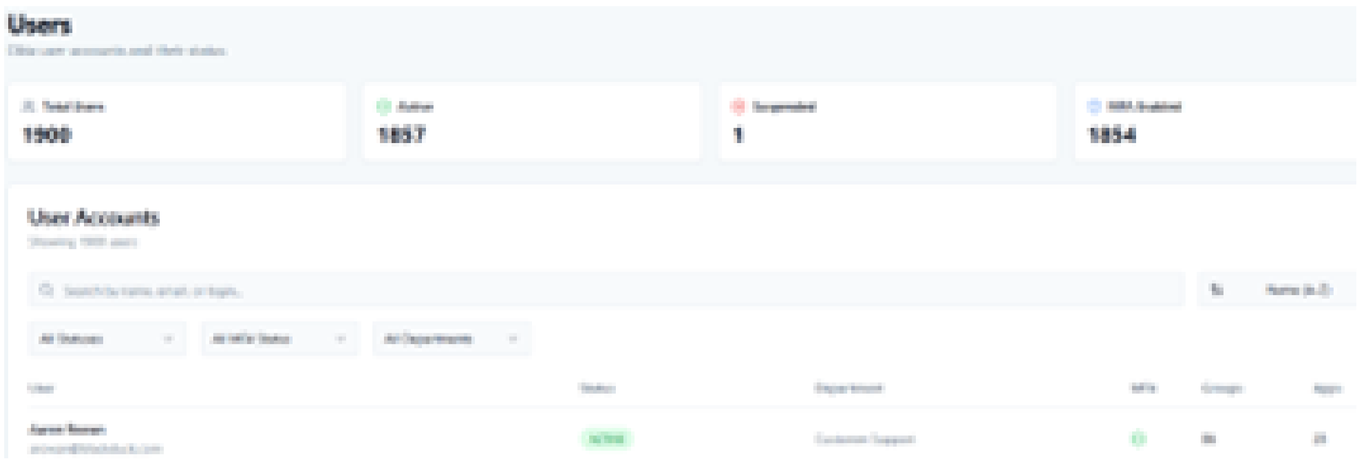


Core Capabilities

Tenant Analysis

Connects to both Okta and Entra environments simultaneously, providing the unified identity landscape view required for Phase 1 baseline.



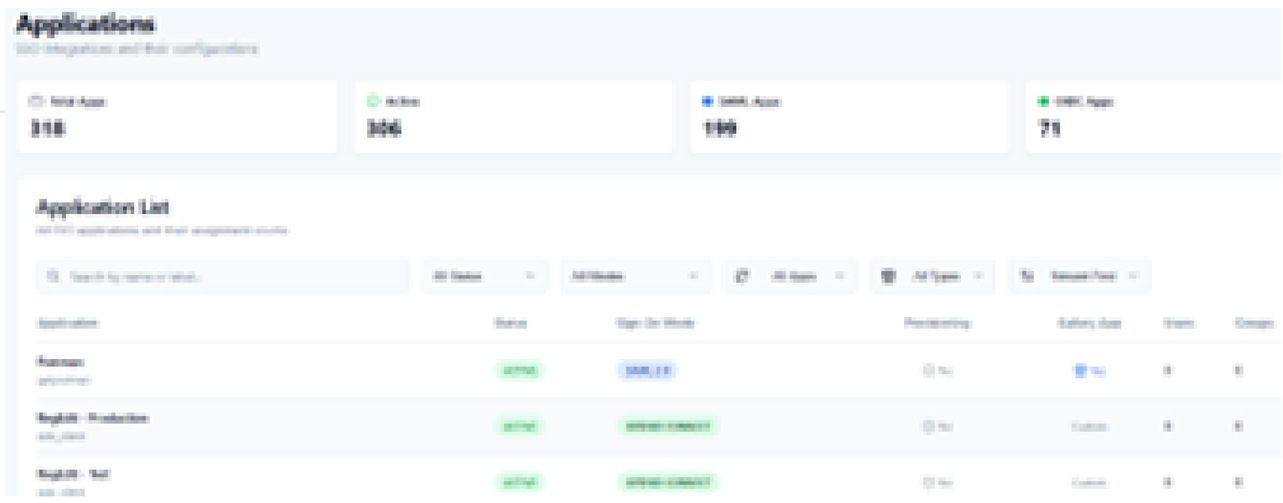


User & Group Discovery

Automatically inventories all users, groups, and membership relationships — including the exclusion group enumeration your Phase 1 governance gate demands.

Application Mapping

Intelligently maps Okta-integrated SAML, OIDC, and proprietary apps to Entra ID equivalents with compatibility recommendations and SSO reconfiguration flags.

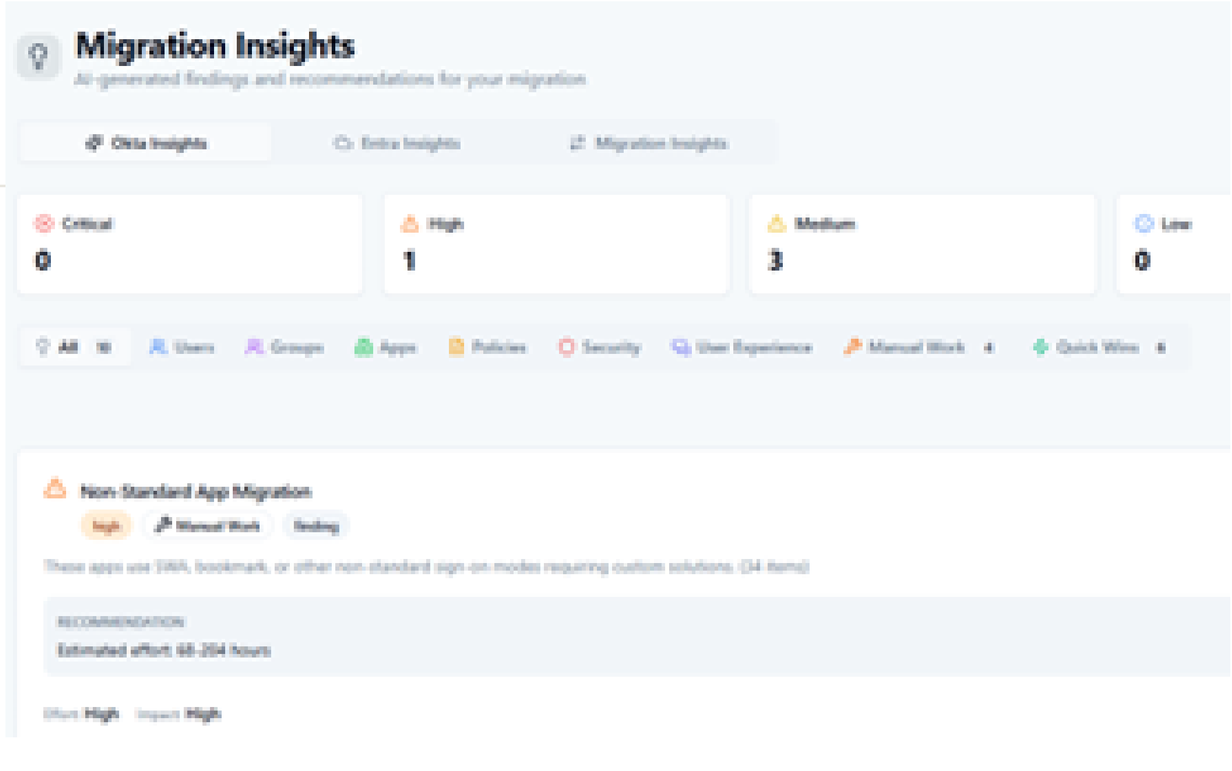


Policy Analysis & Parity

Reviews authentication policies, MFA configurations, and Conditional Access rules to identify the exact parity gaps your Phase 2 design decisions must close.

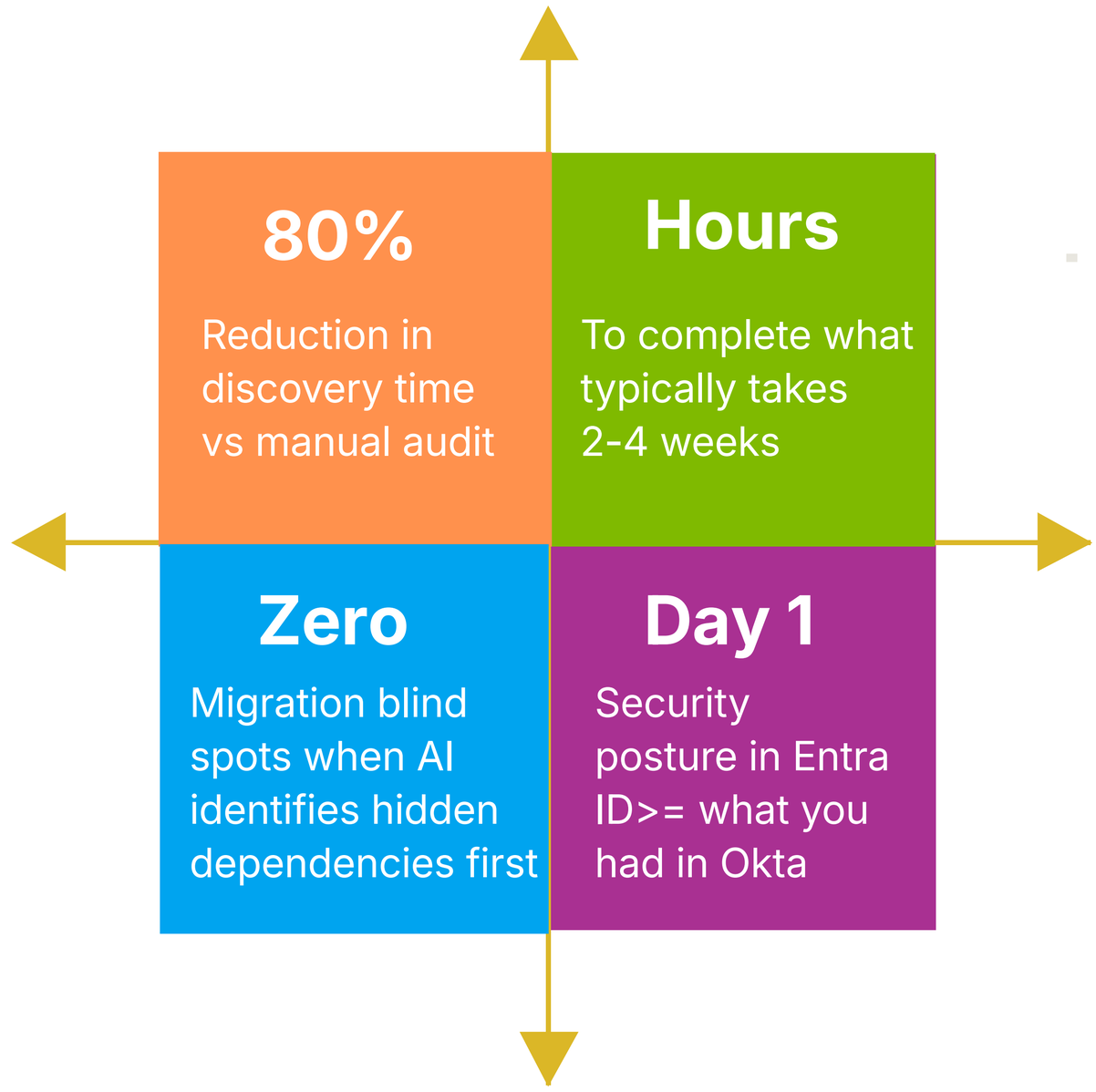
AI-Powered Insights

Ask natural language questions about your migration environment. Get instant, actionable answers — no more digging through reports or waiting for analyst turnarounds.



Enterprise-Grade Security

Built on Microsoft Azure with Entra ID authentication. Your discovery data stays within your security perimeter — compliant, encrypted, and access-controlled.



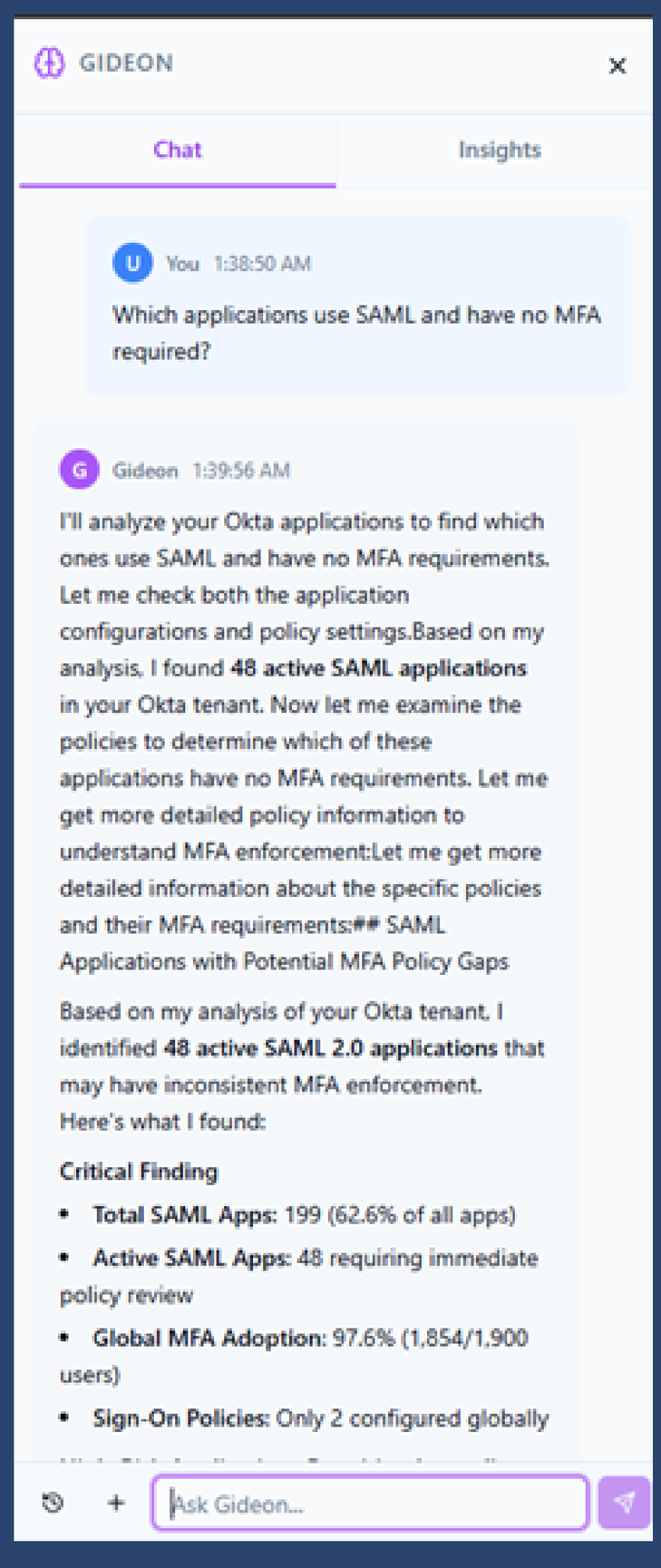
Gideon AI

Your Interactive AI Assistant

Ask Your Migration Data Anything

No more waiting for analyst reports. The Workbench's built-in AI assistant lets CISOs, migration architects, and leadership ask plain-English questions about their identity environment — and get immediate, evidence-based answers that directly inform your Phase 1 through Phase 6 decisions.

From "which apps are MFA-exempt in Okta today?" to "show me all exclusion groups with more than 50 members" — your parity gap inventory is a conversation, not a spreadsheet marathon.



Customer Story

Learn how a venture capital firm modernized its security posture by migrating from OKta to Entra ID, streamlining identity management and application access with stronger MFA—delivered with minimal disruption. Read the **full case study**.

Microsoft Solutions Partner
Security
Specialist
Identity and Access Management
Information Protection and Governance

Microsoft Solutions Partner
Microsoft Cloud
Microsoft Intelligent Security Association
Microsoft

"Our experience working with the Netwoven team was excellent. They demonstrated a high level of expertise and admirable quality of work which helped us solve any challenges that occurred during the migration process and assisted us in the timely completion of the project. I'm extremely satisfied with the smooth execution of the project and the overall outcome achieved."

Joaquin Alvarez

Senior Director, Relay GSE

Next Steps

Talk to an IAM Expert

Schedule a Discovery Session

Next Steps

Click **here** to learn more about Netwoven security and other services.Feel free to contact us to discuss your security priorities.

+1 877 638 9683

info@netwoven.com

netwoven.com

About Us

We shepherd organizations safely through the cloud transformation journey by unravelling complex business problems. By partnering with us, our clients securely collaborate globally, improve business operations, build new products and solutions with deeper insights, and reduce cyber security risks.