# READI+One Identity

## Complete Connectivity, Automation, and Governance

## Beyond the Catalog

The disconnected application problem is not a catalog problem. It is a platform problem. READI gives your team the ability to build any connector fast, extending One Identity Manager governance to the applications that no pre-built catalog will ever reach.

## The Challenge

One Identity Manager is a category leader in identity governance and administration. It excels at connecting applications with modern APIs, standard protocols, and pre-built connectors.

Yet every enterprise has a significant number of applications that remain outside the reach of native connectivity. Legacy systems with no APIs. Win32 desktop tools. Niche SaaS platforms without pre-built connectors. Line of business applications with proprietary interfaces. Mainframe environments that have not been reviewed in years.

These disconnected applications are not marginal. They often hold the most sensitive access, serve critical business functions, and have accumulated years of ungoverned accounts and entitlements. They represent the largest unresolved risk in most identity programs.

> **One Identity governs what it can see. READI ensures it can see everything.**

## The Business Impact

### Identity-Based Attack Exposure

Most breaches now start with compromised identities, not hacked systems. Disconnected applications harbor stale accounts, excess privileges, and unmanaged contractor access that attackers actively exploit. If these identities are not governed, they are not protected.

### Incomplete Certification Coverage

Auditors and compliance teams cannot prove who has access to what when a significant portion of the application portfolio is invisible to One Identity. Certification campaigns cover only the applications that are connected, creating a false sense of assurance. The applications most likely to harbor excessive or orphaned access are precisely the ones that remain unmanaged.

## READI complements One Identity by:

- Connecting applications outside the native connector catalog
- Cleansing and normalizing identity data before governance
- Automating complex, multi-step identity workflows
- Enabling custom remediation beyond standard IAM operations
- Providing full audit trails for every automated action

### Persistent Compliance Risk

Regulatory frameworks including SOX, HIPAA, PCI-DSS, and GDPR require organizations to demonstrate control over access to sensitive systems. Disconnected applications create enforcement gaps that surface during audits, lead to findings, and require expensive remediation.

### Stalled Security Initiatives

Zero trust and least-privilege programs depend on comprehensive visibility. When a substantial number of applications sit outside governance, these strategic initiatives cannot deliver their intended protection. Blind spots persist, and the organization cannot enforce consistent policy across its full environment.

## Why Native Connectivity Alone Is Not Enough

One Identity Manager is a powerful platform for governing applications across its native connector ecosystem. It provides lifecycle management, certification, and policy enforcement for applications it can connect to through APIs, standard protocols, and pre-built connectors.

However, native onboarding depends on those connectors, standard protocols, or supported integration patterns. For the long tail of disconnected applications, there is no native connector to accelerate. These applications require a different approach entirely.

**This is where READI complements One Identity directly:**

| Capability | One Identity | READI Extends With |
|---|---|---|
| Application discovery | Lifecycle governance for applications with native connectors and standard protocols. | **Connectivity to applications with no APIs, no connectors, and no standard protocols.** |
| Onboarding speed | Pre-built connector deployment for supported applications. | **No-code connector configuration for any application, including legacy and custom systems.** |
| Integration methods | Native connectors and standard protocols. | **API, file, ODBC, and AI-powered computer vision via Smart Connector.** |
| Provisioning depth | Automated provisioning for natively connected applications. | **Bidirectional provisioning workflows for disconnected applications, including complex multi-step operations.** |
| Governance reach | Full lifecycle governance for applications within the native connector ecosystem. | **Extends governance to the full long tail of disconnected, legacy, and custom applications.** |

> **Native connectivity governs the applications One Identity can reach. READI extends that reach to applications it cannot.**

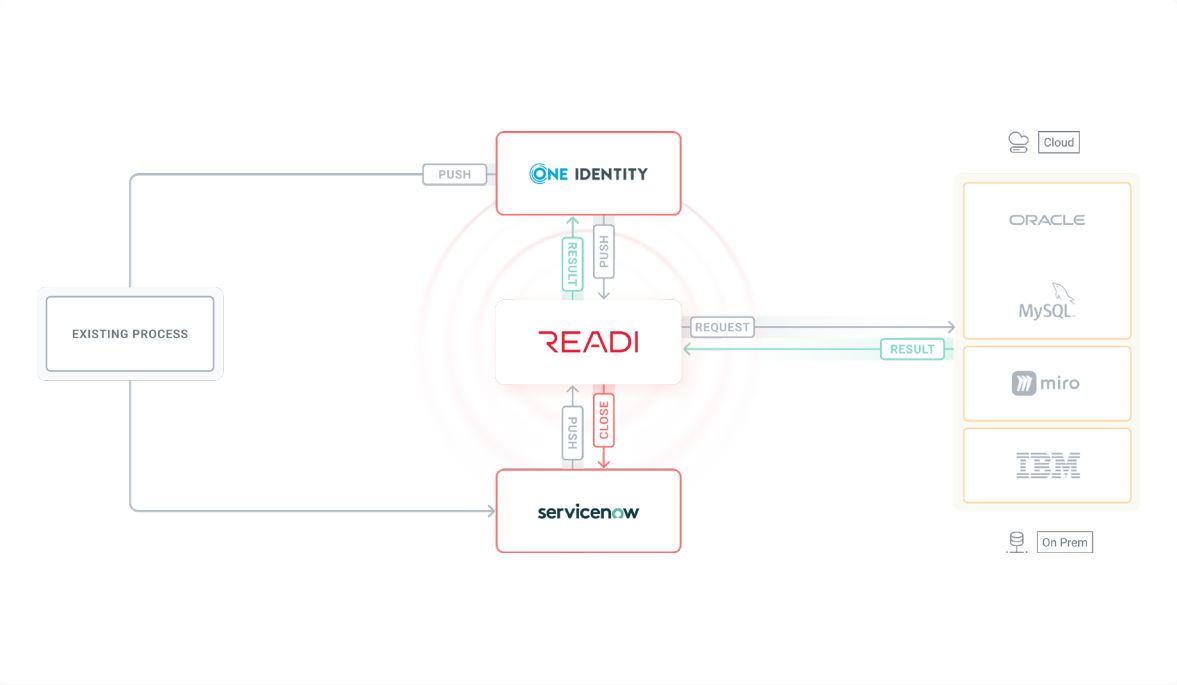
## The READI Approach

READI serves as a foundational layer between your applications and One Identity Manager. It abstracts the complexity of application connectivity, cleanses and normalizes identity data, and delivers governed, accurate identity information to One Identity for policy enforcement and certification.

READI connects applications through multiple integration methods, matching the right approach to each application's capabilities:

| Integration Method | Description |
|---|---|
| API Connectors | Direct integration with applications that expose REST, SOAP, or other API endpoints. |
| File-Based Connectors | Structured import and export of files, with midstream transformation and cleansing. |
| ODBC Connectors | Direct database connectivity for applications where identity data can be queried from underlying databases. |
| Smart Connector (AI) | AI and computer vision for applications with no APIs, no database access, and no file exports. Smart Connector interacts with the application UI the way a human would. |

Regardless of the integration method, identity data flows through Connector Studio for mapping, normalization, and enrichment before being stored in Atlas, READI's unified identity directory. From Atlas, clean, structured identity data is synchronized to One Identity Manager.



## Smart Connector: The Last Mile of Connectivity

The most difficult connectivity challenges involve applications that offer no APIs, no database access, and no file exports. Line-of-business applications, legacy systems, and custom internal tools are often the oldest, most sensitive, and most deeply embedded systems in the enterprise. They are also the applications that accumulate the most ungoverned access over time.

READI Smart Connector solves this problem using computer vision and large language models to interact with application interfaces the way a human operator would. Smart Connector navigates web applications, LOB applications, Win32 desktop tools, and legacy terminal environments to extract and update identity data without requiring any changes to the source application.

## Smart Connector vs. Generic RPA

Robotic process automation tools can interact with application UIs, but they were not designed for identity governance. They have no concept of users, roles, or entitlements. Their automations are brittle, hard-coded to pixel coordinates, and break when UIs change. They lack the audit trails, credential governance, and RBAC controls that identity programs require.

Smart Connector is fundamentally different. It uses computer vision and LLM intelligence rather than scripted coordinates. It is configured in plain English rather than recorded macros. And every action it takes is governed, audited, and tied to the identity lifecycle.

## Automation Beyond Governance

READI automates identity-related processes that extend beyond what One Identity handles natively. One Identity follows best practices for identity governance, which works well for standard lifecycle events. But enterprises frequently have processes that cannot be changed or do not fit standard governance patterns.

READI provides the flexibility to automate these processes. Examples include setting out-of-office reminders during leave events, archiving or wiping hard drives as part of offboarding, reclaiming software licenses when access is revoked, and executing multi-step provisioning workflows that span multiple disconnected systems.

## How Smart Connector Works

### No-code configuration

Instructions are written in plain English. No scripting, no pixel coordinates, no brittle recorded sequences.

### Computer vision navigation

Smart Connector sees and interprets the application UI visually, adapting to layout changes without breaking.

### Identity-first design

Unlike generic automation tools, Smart Connector is purpose-built for identity operations. It understands users, accounts, roles, and entitlements.

### Full audit trail

Every action is logged, governed by RBAC, and backed by centralized credential management.

## Business Outcomes

### Complete Governance Coverage

Connect the full long tail of disconnected applications to One Identity. Access certifications, policy enforcement, and audit evidence extend across the entire application portfolio, not just the fraction with native connectors.

### Reduced Audit Risk

Demonstrate control over sensitive systems that were previously invisible to your governance program. Reduce audit findings related to incomplete application coverage, orphaned accounts, and stale access.

### Faster Application Onboarding

Bring new applications under governance in days rather than months. READI's no-code configuration and AI-powered connectivity eliminate the need for custom development and specialized engineering for each new application.

### Automated Lifecycle Processes

Replace manual joiner, mover, and leaver processes for disconnected applications with automated, governed workflows. Reduce offboarding delays, eliminate orphaned accounts, and ensure consistent policy enforcement.

### Stronger Security Posture

Close the visibility gaps that undermine zero trust and least-privilege initiatives. With comprehensive access data across all applications, security teams can enforce consistent policy and detect excessive access wherever it exists.

### Bidirectional Provisioning

Go beyond read-only data extraction. READI updates records in disconnected applications based on changes in One Identity, ensuring real-time synchronization during attestation, certification, and lifecycle events.

## In A Nutshell

READI extends One Identity governance across all applications, eliminating blind spots, reducing audit risk, and accelerating onboarding. By automating lifecycle processes and enabling real-time, bidirectional provisioning, organizations achieve complete visibility, stronger security, and consistent policy enforcement at scale.

## Why READI

**IGA-Complementary:** READI extends the reach of One Identity Manager. It does not compete with or replace your existing One Identity investment.

**Native-Connectivity-Complementary:** READI works alongside your native connector ecosystem to close governance gaps, connecting applications beyond the native catalog and enabling richer provisioning workflows.

**Multiple Integration Methods:** API, file, ODBC, and AI-powered computer vision. The right approach for each application, managed from a single platform.

**No-Code Configuration:** Connector Studio, Bot Studio, and Smart Connector all provide no-code or low-code interfaces that reduce dependence on specialized engineering.

**Data Quality Built In:** Midstream normalization and cleansing ensure your IGA receives accurate, structured identity data, not the raw, inconsistent data that clogs onboarding pipelines.

**Governed by Design:** Centralized credential management, RBAC, full audit trails, and deterministic execution across all connectors and automations.

**Identity-First:** Every component of READI is purpose-built for identity governance. This is not a general-purpose automation platform adapted for identity use cases.

**A CISO gets fired not for being breached. They get fired for not knowing. 'We couldn't connect that system' is not a defense, it's a confession."**

READI extends the reach of your existing IGA platform, without replacing it, by connecting any application through multiple integration methods, including APIs, files, ODBC, and AI-powered automation. Built with an identity-first approach, READI combines no-code configuration, centralized governance, and embedded data quality to deliver accurate, structured identity data while reducing complexity and reliance on specialized engineering.

## About READI

READI is the identity foundation that removes connectivity and complexity barriers, enabling IGA platforms to deliver complete governance across all applications. With a unique no-code and AI-driven connectivity approach, READI rapidly integrates virtually any system, including disconnected, unstructured, and legacy applications that lack modern APIs.

READI complements IGA platforms; it does not compete with them.

**Scan for more information on**
www.readibots.com | LinkedIn



READI