

Secure Identity.
Trusted Data.
Agentic Intelligence.



TRUSTED IDENTITY INTELLIGENCE FOR THE AGENTIC ENTERPRISE

One Customer. Many Systems. One Trusted Identity.

COMPLEXITY SIMPLIFIED. IDENTITY MASTERED.



RELIO Executive Summary

The trusted identity foundation for governed agentic action

RELIO is an enterprise customer identity security, mastering and intelligence platform designed to resolve fragmented customer and party records into trusted, explainable Golden Identities - then use governed intelligent agents to investigate exceptions, recommend remediation and support controlled action.

01 One Trusted Identity

Unify customer and party identities across CRM, portals, registries, authentication platforms and legacy systems.

02 Explainable Resolution

Show why records match, conflict or remain uncertain, with evidence and source traceability.

03 Agentic Investigation

Use specialised agents to investigate duplicates, data-quality issues and reconciliation exceptions.

04 Governed Action

Apply human approval, policy controls and audit trails before sensitive changes are executed.

Why RELIO

Reduce identity fragmentation and manual reconciliation while creating a trusted context layer that both people and enterprise AI agents can safely use.

About Subject Matter Experts

SUBJECT MATTER EXPERTS - EXPERTISE • INSIGHT • IMPACT

Subject Matter Experts (SME), a registered business name of SAFAAN GROUP PTY LTD, is an Australian technology business established in 2013. SME focuses on enterprise customer identity, data mastering, data quality, reconciliation, integration and security-focused technology solutions.

SME develops RELIO to help organisations move from fragmented identity records and manual exception handling toward trusted identity intelligence and governed automation.

Customer identity & party mastering	Entity resolution & duplicate investigation	Data quality & reconciliation
Enterprise integration	Security, governance & audit	Agentic identity intelligence

The Flagship Use Case

One Customer. Many Systems. One Trusted Identity.

The problem is not simply that customer data exists in multiple systems. The problem is that enterprises often cannot confidently determine whether different records represent the same real-world person or organisation, which attributes should be trusted, and what should be corrected when systems disagree.

CRM Different names, identifiers, contacts and status	Customer Portal Different names, identifiers, contacts and status	Registry A Different names, identifiers, contacts and status	Registry B Different names, identifiers, contacts and status	Authentication Different names, identifiers, contacts and status	Legacy Different names, identifiers, contacts and status
1 Resolve Link records that represent the same real-world party.	2 Master Create a governed Golden Identity with source traceability.	3 Explain Show evidence behind match, survivorship and conflict decisions.	4 Investigate Agents gather context for duplicates, mismatches and anomalies.	5 Act Recommend or execute policy-approved remediation with audit.	

Business outcome

A trusted, explainable identity layer that reduces manual investigation and gives downstream applications and AI agents consistent identity context.

The Customer Identity Challenge

Why this problem becomes more important in the AI era

01 Duplicate identities

The same customer appears multiple times with different spellings, identifiers or contact details.

02 Conflicting attributes

Systems disagree on email, mobile, address, status or relationship information.

03 Manual reconciliation

Data and operations teams use SQL, spreadsheets and manual investigation to resolve exceptions.

04 Disconnected relationships

People, organisations, trusts and account relationships are difficult to understand across systems.

05 AI trust gap

AI agents can make poor decisions when they receive inconsistent identity context.

06 Governance risk

Automated changes without evidence, approval and traceability create operational and compliance risk.

RELIO Agentic Identity Intelligence Architecture

EXPERIENCE & ENTERPRISE AGENTS	Search • Steward Workbench • APIs • MCP-ready tools • Enterprise applications
AGENTIC IDENTITY INTELLIGENCE	Identity Resolution Agent • Duplicate Investigation Agent • Data Quality Agent • Reconciliation Agent • Relationship Intelligence Agent • Identity Risk Agent
IDENTITY INTELLIGENCE	Matching & scoring • Survivorship • Conflict analysis • Relationship graph • anomaly/risk signals • explainability
TRUSTED IDENTITY CORE	Golden Identity • Party & Relationships • Identifiers • Contacts • Consent • Source traceability
GOVERNANCE & SECURITY	Tenant isolation • RBAC • approvals • audit trail • policy controls • encryption patterns

Design principle: deterministic identity controls remain authoritative. Agents reason over governed data and invoke approved tools; sensitive master-data changes can require human or policy approval.

Agentic Identity Intelligence

Specialised agents focused on measurable identity operations

01 Identity Resolution Agent

Investigates candidate matches, gathers evidence and recommends merge / no-merge decisions.

02 Duplicate Investigation Agent

Compares suspected duplicates and explains similarities, conflicts and uncertainty.

03 Data Quality Agent

Finds incomplete, inconsistent or suspicious identity data and proposes governed corrections.

04 Reconciliation Agent

Compares Golden Identity with connected systems and investigates mismatches.

05 Relationship Intelligence Agent

Analyses person, organisation and trust relationships to surface inconsistencies or unusual patterns.

06 Identity Risk Agent

Combines identity quality, conflict and anomaly signals into explainable risk indicators.

Roadmap discipline: agent capabilities should be introduced progressively and validated against accuracy, explainability, cost, latency, security and client-specific governance requirements.



Core Product Capabilities

01 Customer & Party Mastering

Govern source mappings, precedence and survivorship.

02 Golden Identity

Maintain an enterprise identifier with source traceability.

03 Entity Resolution

Detect, score and resolve candidate duplicate identities.

04 Party & Relationships

Represent people, organisations, trusts and relationships.

05 Data Quality & Reconciliation

Identify and investigate missing, conflicting and mismatched data.

06 Agentic Identity Intelligence

Use specialised agents for investigation, recommendation and governed remediation.

07 Security & Governance

Support tenant isolation, RBAC, approvals, audit and controlled change.

08 API & Agent Integration

Expose secure APIs and agent-consumable tools for enterprise workflows.

Security, Governance & Human Control

Agentic automation must remain evidence-based and governed

01 Identity & Access

Enterprise authentication integration, MFA support and role-based access control.

02 Tenant Isolation

Logical tenant boundaries and controlled access to tenant-specific identity data.

03 Agent Permissions

Constrain which tools, records and actions each agent can access or invoke.

04 Human Approval

Require steward approval for ambiguous or high-impact mastering decisions.

05 Auditability

Record evidence, recommendations, approvals, tool calls and material changes.

06 Explainability

Trace identity outcomes and agent recommendations back to underlying source evidence.

Client-specific validation: final controls, certifications, regulatory mappings and autonomous-action boundaries should be validated for each customer environment.

Why RELIO

Focused positioning rather than generic MDM or generic AI

Customer question	Traditional approach	RELIO focus
Who is this customer across systems?	Rules, manual stewardship or broad MDM implementation	Trusted Golden Identity with source traceability
Why were these records matched?	Scores or steward investigation	Evidence-based, explainable resolution
What does not agree?	Reports, queues and manual reconciliation	Continuous conflict and reconciliation intelligence
What should we do next?	Human analysis and hand-off	Agent recommendation with governed action
Can enterprise AI trust the identity context?	Depends on upstream data quality	Governed identity context exposed through secure APIs / tools

RELIO proposition

Turn fragmented enterprise identities into trusted, explainable and actionable identity context - for people, applications and governed AI agents.

Discovery-to-Agentic Pilot Path

1 Discover Identify systems, identity pain points, manual reconciliation effort and target business outcome.	2 Assess Profile records, duplicates, identifiers, relationships and data-quality issues.	3 Resolve Configure matching, Golden Identity, survivorship and explainability.
4 Agent Pilot Introduce one controlled agent use case - e.g. duplicate investigation or reconciliation.	5 Measure Compare accuracy, steward effort, cycle time, exception reduction and governance outcomes.	6 Scale Expand integrations and automation only where measurable value and controls are proven.

Recommended first agentic pilot: duplicate investigation or cross-system reconciliation. Both are tightly bounded, evidence-rich workflows where RELIO can demonstrate value without granting broad autonomous write access.



Let's Solve Your Identity Challenge.

SUBJECT MATTER EXPERTS

Operated by SAFAAN GROUP PTY LTD

1800 800 555

subjectmatterexperts.com.au

Start with a focused discovery session to identify where fragmented identities, duplicate records, inconsistent data and manual reconciliation are creating operational, security or AI-readiness risk.

REQUEST A DISCOVERY SESSION

RELIO product capabilities and agentic roadmap are subject to implementation scope, validation and client-specific architecture and governance.