Security at a Glance

A plain-language overview for IT and security teams

What is ThematIQ?

ThematIQ is Allen + Clarke's human-led, AI-assisted thematic analysis system for qualitative text data. It is used to securely process large volumes of qualitative material (e.g., submissions, open-text survey responses, stakeholder feedback and interview transcripts) and produce structured, traceable thematic outputs.

ThematIQ is delivered by Allen + Clarke and built in partnership with Qamcom NZ. Qamcom is the specialist technology partner responsible for the system's engineering, security design, and technical operation. Qamcom is a research and technology company with deep expertise across hardware, software and systems development, including artificial intelligence.

What this sheet is (and isn't)

This document is designed to show that ThematIQ is a controlled, engineered system with security built in, not an ad hoc or consumer AI tool. It is not intended to replace formal security assessment processes. We expect and welcome direct IT/security questions and will provide detailed responses as needed.

Who uses and operates ThematIQ?

Allen + Clarke operates ThematIQ as part of delivery: configuring the analytical approach, conducting human verification and QA, and being accountable for outputs. Outputs are provided via existing, approved client channels (e.g., SharePoint or other agreed secure transfer methods).

Qamcom built and operates the ThematIQ technology platform, including the security controls and monitoring. Qamcom's role is to ensure the system is engineered and run to a standard suitable for high-scrutiny use cases and sensitive qualitative datasets.

Security design principles

ThematIQ has been designed to meet the UK NCSC's Cloud Security Principles. Additionally, ThematIQ uses only sovereign processing – all data is processed and stored in-country (NZ-hosted for NZ data; AU-hosted for AU data where required).

Key ThematIQ security features

For more information or project specific security features please contact Officenz@allenandclarke.com

Project-specific environments and data handling	Environments are time-bound and decommissioned at project completion, including the removal of project infrastructure and data as agreed. Customer data is not used for training. Data is encrypted in transit and on disk
Strict access control	Individual user accounts with multi-factor authentication (MFA). Accounts are created and managed by designated administrators only. Role-based permissions ensure staff only access the projects and datasets required for their work.
In-country hosting	Deployments are hosted in-country, including all AI processing (NZ for NZ data; AU for AU data where required) to support sovereignty expectations.
Closed processing environment	The system is designed to avoid uncontrolled external data sharing. No third-party services are used in the storage and processing of data.