# SOLVING SENSITIVE/CLASSIFIED INFORMATION SHARING & COLLABORATION CHALLENGES WITH KOJENSI

*How the Kojensi Platform Delivers ABAC-Enabled Multi-Level Security Out-of-the-Box*

archTIS

# TABLE OF CONTENTS

# EXECUTIVE SUMMARY

The archTIS Kojensi platform addresses the long-standing challenge of how to securely collaborate on and share sensitive and classified information within and between organisations.

Originally developed as a bespoke system for a Defence agency, Kojensi is now commercially available as a cloud service or as an on-premises platform. The platform enables the secure creation, collaboration, storage and sharing of sensitive or classified information. It uses Attribute-Based Access Control (ABAC) to automate highly granular management of access rights between users and data.  It delivers secure information sharing through its security-driven architecture and features, and uses an 'access policy engine' to mediate the attributes of users, workspaces, organisations, and the data itself, to dynamically allow or prevent access.

This white paper describes the business problem and use case that Kojensi addresses, and provides an overview of the technology and the security model. It will show how the SaaS Kojensi platform enables Government and Defence agencies and the Defence Industry to collaborate and share sensitive information with partners (public and private), suppliers and other agencies and corporates, while maintaining high levels of trust and security.

# DEFENCE AND SUPPLY CHAIN INFORMATION SHARING CHALLENGES

It has been apparent for many years that air-gapped networks and tight perimeter security are fine, so long as you do not want to share information across domains (Cross-Domain Solution (CDS)), or do not want to easily share data of differing security classifications with users of different security clearances. The goal of achieving this is often referred to as Multi-Level Security (MLS).

As the need for connectivity, sharing and collaboration grows in Defence, government and the corporate sector, and the supply chains that link them, so does the need for platforms to deliver such sharing in a secure manner.  To date platforms seeking to achieve MLS have been bespoke and costly, taking a long time to deliver, and still being limited to a defined population of users, with limited scope to extend to new networks or new users.

This is what Kojensi delivers. It was developed as a bespoke solution to meet an Australian Defence need. That bespoke solution has evolved to become a commercially available solution to allow organisations of all sizes to be able to quickly stand-up a secure information collaboration and sharing platform. Unlike spending millions to build and manage your own information sharing system, Kojensi enables secure, compartmentalized collaboration out of the box for less time and money.

# HOW NEW INFORMATION SECURITY MODELS PROVIDE A SOLUTION

In today's global environment, defence and the complex industry supply chains that enable these operations blur the traditional lines of geography and locality. Even more so as we collaborate and share information daily with our partners, suppliers, subcontractors, and our clients, using numerous combinations of information systems and media.

In the defence industry, sensitive information handling comes with mandated comprehensive controls. System owners must ensure their systems enable and enforce these controls to meet requirements. However, the task of balancing effective security whilst still enabling information sharing in these complex environments is difficult.

Dynamic policy enforcement and Multi-Level Security (MLS) methodologies provide the means to ensure that separation and protections are in place for contextual access to information without hindering authorized collaboration, whilst also stopping unauthorized access and sharing – a must to meet defence and industry supply chain requirements.

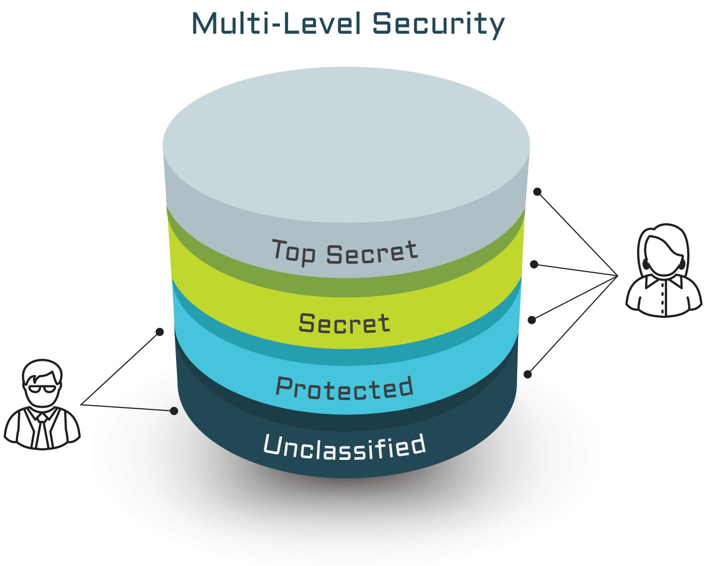
## Multi-Level Security (MLS)

A security classification is the hierarchical category assigned to information and material that identifies the degree of damage that unauthorised disclosure or compromise would cause to a nation, generally regarding military or other government business. The classification denotes the degree of protection and control required for the storage, transmission, and utilisation of the information.

Alongside security classification is a compartmentalisation layer of separation and associated control requirements. These are sometimes referred to as codeword, sensitive, or compartmentalised, and can include releasability caveats or rules around the sharing or dissemination of that information artefact.

All systems have security boundaries, whether logical and enforced, or ephemeral and inadvertent. A security boundary naturally exists wherever two different "security domains" (which could be a set of security requirements, control objectives, or even handling characteristics) come together for some reason. It can be between classifications, between compartments, between organisations, between networks, between systems, or even between nations.

This sort of complexity means that we need the ability to measure and enforce contextual security, with rules or policies that are defined, required, and applied – also referred to as "dynamic policy enforcement" that can provide assurance which can be independently verified by a security assessor.



An MLS capability (system, platform, or environment) allows information at different classifications to be stored and accessed within a single security domain, while enforcing different access policies and compartments dynamically depending on context, with the assurance that the separation is effective.

MLS provides an organisation with the ability to:

- Enable custodians to label and tag their content creations in the system.
- Control and release information to individuals/devices/locations that meet the contextual rules.
- Enable dynamic policy enforcement and dynamic access controls to information.
- Enforce contextual controls based on labels, tags, and other attributes.
- Enable granular controls to apply either between or inside security domains.

By adding controls like Attribute-based Access Control (ABAC), MLS becomes even more effective. When utilising ABAC as the dynamic policy enforcement method you can provide granular access control at the most appropriate context. These attribute controls can be expressed as a key=value pair (for example [Nationality=Australian], [Location=Canberra, Australia], or [Organisation=archTIS]). By dynamically measuring the attributes of the user or device and aligning it to the rules of access for the information, ABAC can be an effective way to ensure only the right people, in the right context, can get access to the right information, at the right time.

### Combining MLS and ABAC

MLS combined with the dynamic capabilities of ABAC can enable and support complex information sharing challenges and offers several benefits to:

- Increase the accuracy, provenance and speed of getting the right information to the user, within multiple operational and security contexts.
- Improve access management of compartmentalised information, within contextual constraints.
- Assist to collapse networks and reduce the number of systems that users have to interact with, including potentially within deployed scenarios.
- Enable multi-national information sharing within mission related network environments, potentially improving interoperability and effectiveness.
- Enable files and documents to be rapidly created and shared respecting the owner defined security rules.

## ACHIEVE ABAC-ENABLED MULTI-LEVEL SECURITY EASILY WITH KOJENSI

Kojensi is a highly secure, multi-level security platform for the secure sharing and collaboration of sensitive and classified files. It is available as either a cloud or an on-premises solution, depending on an agency or organisation's specific security requirements.

It looks at a file's attributes such as security classification, organisation and country releasability, and matches them with a user's comparable credentials, such as clearance, organisation and nationality, to determine who is able access, edit and download a file. Once access permissions have been assessed and granted, users of Kojensi can create, share files and co-author documents in real-time. All in a secure and intuitive platform that ensures sensitive information is only accessed by those who need-to-know, and is invisible to those who don't.

The Kojensi platform provides the security controls to help compliance with information protection obligations, in an MLS environment. Kojensi provides an assured and accredited SaaS solution to store, share and collaborate both internally and with supply chain, partners, and clients on information up to Australian PROTECTED.

Kojensi delivers several key capabilities and functions, including:

- An ABAC-based MLS platform that enables user driven workspaces and communities of interest (COIs).
- User controlled allocation and invitation of personnel to COIs.
- The ability for users to create, modify and upload documents and files, using metadata releasability tags.
- Editing and co-authoring via an easy to use interface that enforces and respects the access rules.
- The ability for authorised users to modify document and file metadata, to narrow or increase user access.
- The mapping and management of bi-lateral and multi-lateral agreements related to handling of sensitive data to support multi-national information sharing.

For Microsoft users, archTIS NC Protect product enables comparable capabilities for granular ABAC-based control of application data in SharePoint (Online and on-premises), Teams, Exchange and OneDrive.

**Multi-Level Security combined with the dynamic capabilities of ABAC can enable and support complex information sharing challenges**

### How Kojensi Works: The Attribute Based Access Control (ABAC) Approach

Librarians have used tags and metadata forever to catalogue and retrieve books and documents. Library users have certain permissions, as do books and documents. Matching the two sets of permissions enables the librarian to determine whether, and for how long, a book can be borrowed, by a particular user.

In the IT industry such use of metadata tags to manage access is referred to as Attribute-Based Access Control or ABAC which applies a comparable book/data centric approach to IT data and documents:

- Users have attributes that they bring with them when they seek to access data.
- Data has access/permission attributes as to what, when, who and how access can be granted.

All that is then needed is for the librarian or in Kojensi's case, the built-in policy engine, to check/match the credentials of the user, and the attributes of the document (which can be automatically defined or uniquely specified by the creator). Access is then either granted or denied, along with other permissions such as rights to edit, print, download, or whatever constraints the document/data creator wishes to apply and have enforced.

## KOJENSI SECURITY ARCHITECTURE OVERVIEW

### Secure Architecture

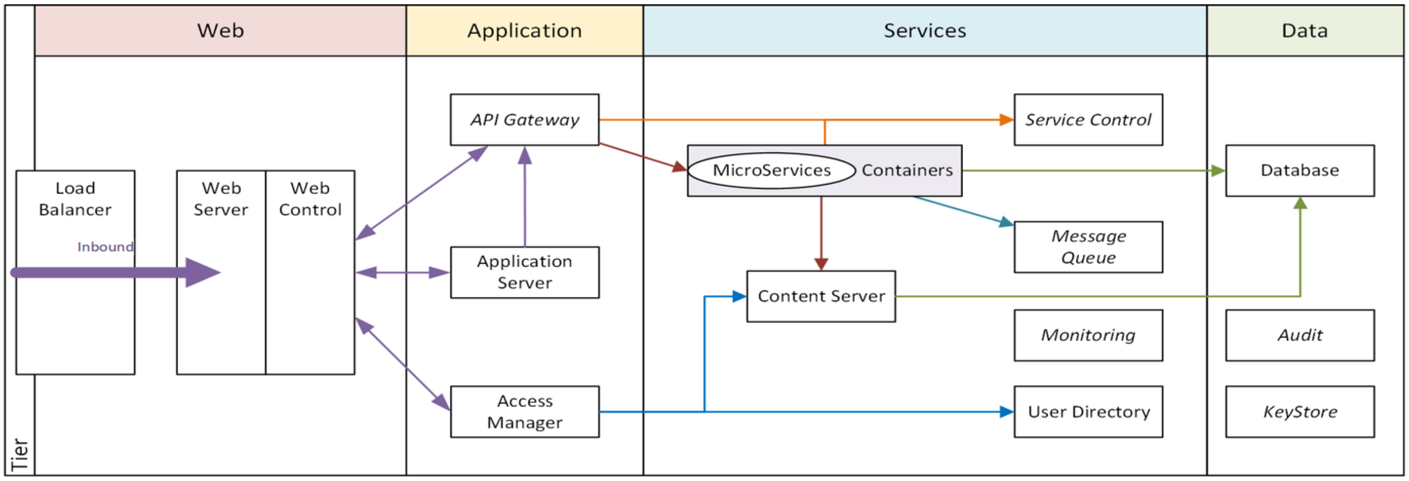
Kojensi is a secure and trusted platform for sharing sensitive and classified files and document collaboration. It employs ABAC policies to ensure only authorized users have access to information under the right conditions and controls what they can do with that information.

Organisations no longer need to add layers of security as an afterthought, which slows productivity and complicates processes. With Kojensi, users can create, co-author, and share documents in real-time, all in a secure and intuitive platform that empowers collaboration and is highly secure-by-design.

Kojensi was designed with security as the primary consideration, within each component and at all layers.

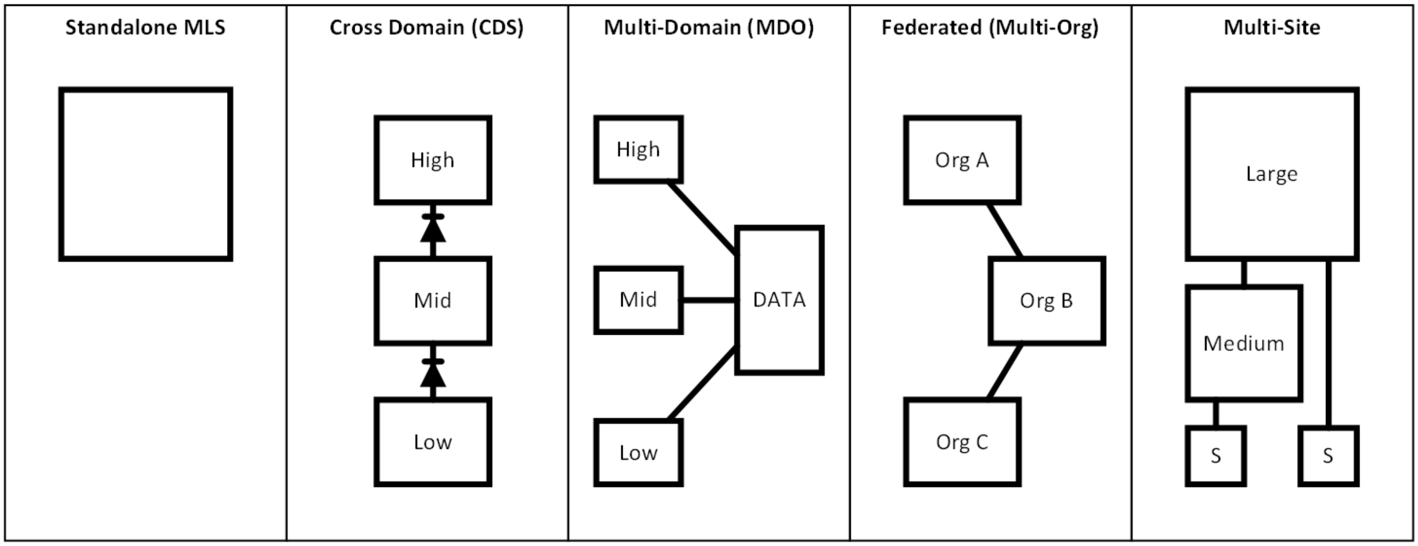
Kojensi applies a consistent set of security principles and controls across the four-tier layers of the architecture – Web, Application, Services and Data

Each layer has separate controls, as well as logical isolation from the higher and lower layers using network, port and component separation and segmentation.



## Implementation Modes

Kojensi has been designed to be implemented and operated in multiple different scenarios, including as an accredited SaaS platform, in a standalone or isolated model, as well as in providing policy enforcement across security boundaries, whether in a Multi-Level Security, Cross-Domain, Multi-Domain, Federated, or Multi-Site:



## Data-Centric Security Model

The Kojensi ABAC Security model was defined after consideration of over 200 use cases. Information elements (attributes) were chosen that provide the broadest applicability and compliance with the least number of configured items to reduce complexity.

For access to a resource, all the attributes and rule sets configured must be checked and validated prior to access being granted.

Each action request is checked immediately, with validation occurring in near real-time so if an attribute or rule changes then the chosen combination is in effect straight away.

At a high level, the key attributes that Kojensi can use for security controls include:

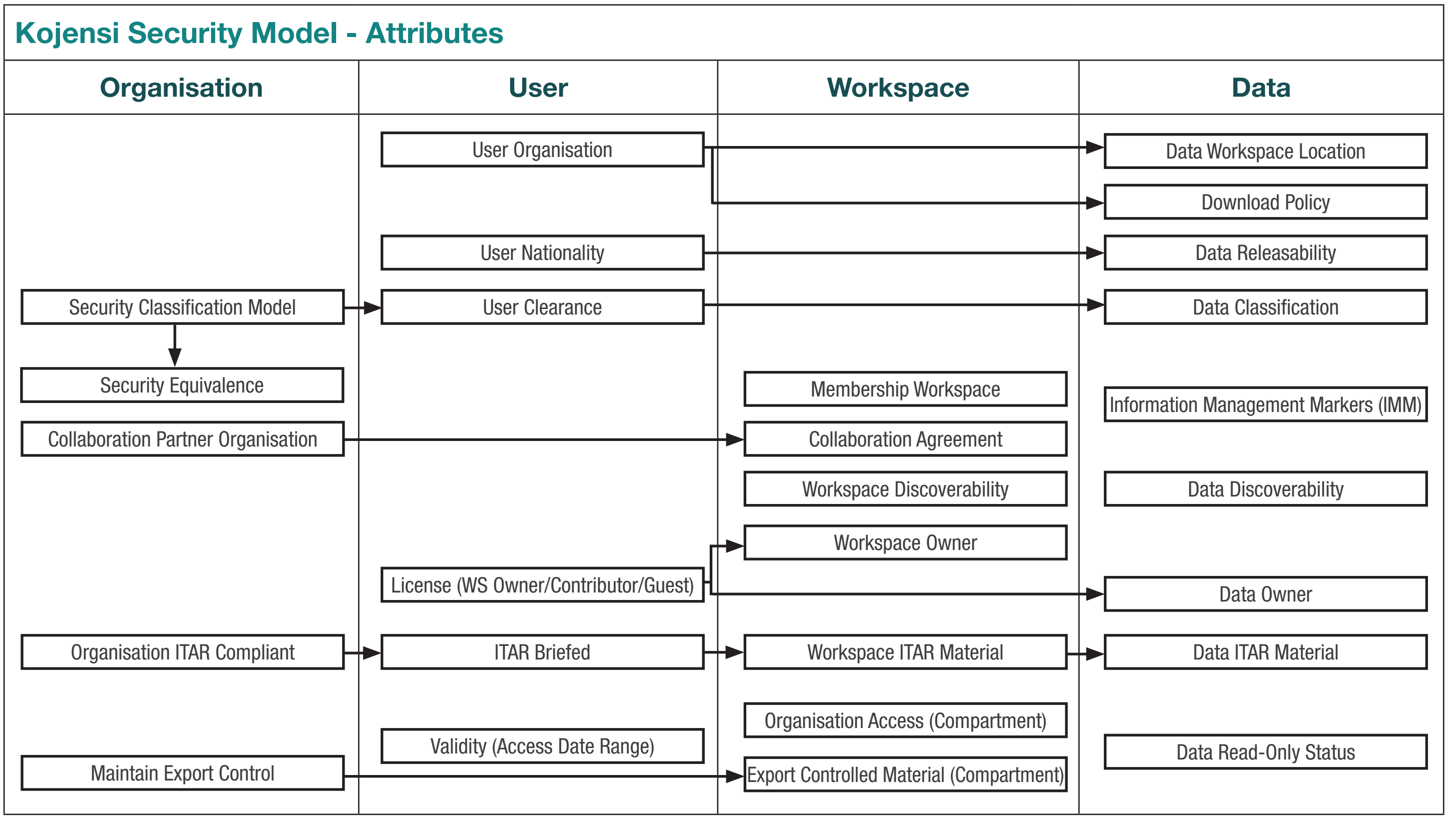
- User nationality
- User security clearance
- Organisation
- Invitation to community of interest (workspace)
- Export control (e.g., International Traffic in Arms Regulations (ITAR) / Export Administration Regulations (EAR) information)
- Object security classification, and
- Information handling rules.

The various combinations of this list facilitate a broad range of complex information sharing scenarios.

## Security Attribute Model Diagram

Kojensi also utilises a set of logical rules that can further enforce multiple layers of security beyond those described above, enabling a truly granular technical security model.

A diagrammatic view of the granular Kojensi security model is as follows:



### Kojensi Technical Security Attribute Model

Kojensi uses multiple elements as attributes for the security model, with each attribute considered as part of the ABAC decision flow. These may include:

| Type | Attribute / Element |
|---|---|
| User Element | User Organisation |
| User Element | User Nationality |
| User Element | User Clearance |
| User Element | Licence (Workspace Owner / Contributor / Guest) |
| User Element | Validity (Access Date Range) |
| User Element | ITAR Briefed |
| Workspace Elements | Workspace Owner |
| Workspace Elements | Membership to Workspace |
| Workspace Elements | Organisation Access (Compartment) |
| Workspace Elements | Collaboration Agreement |
| Workspace Elements | Workspace ITAR Material |
| Workspace Elements | Export Controlled Material (Compartment) |
| Workspace Elements | Workspace Discoverability |
| Data Element | Data Owner |
| Data Element | Data Workspace Location |
| Data Element | Data Read-Only Status |
| Data Element | Data Classification |
| Data Element | Data Releasability |
| Data Element | Information Management Markers (IMM) |
| Data Element | Data ITAR Material |
| Data Element | Data Discoverability |
| Data Element | Data Download Policy |
| Organisation Element | Security Classification Model |
| Organisation Element | Security Equivalence |
| Organisation Element | Collaboration partner organisation |
| Organisation Element | Organisation ITAR Compliant |
| Organisation Element | Maintain Export Control |

Other attributes can be added or defined.

## Kojensi User Security Roles

Kojensi also applies a dynamic role-based structure, allowing for separation of system administration and information access. A key benefit of this is that administrators no longer require the highest level of clearance, and can manage the system and data to keep the system running optimally, without having access to the sensitive contents itself. The model is described in the following table:

| GROUPING | ACTION | ARCHTIS SUPPORT | ARCHTIS ADMIN | ORGANISATION OWNER | ORGANISATION LOCAL ADMIN | WORKSPACE OWNER | USER (CONTRIBUTOR) | USER (VIEWER) | Object Owner |
|---|---|---|---|---|---|---|---|---|---|
| ADMINISTRATION | Monitor System Status | Y | | | | | | | |
| | Restart Servers and Applications | Y | | | | | | | |
| | Respond to System Alerts | Y | | | | | | | |
| | Deploy code updates | Y | | | | | | | |
| | System Management | Y | | | | | | | |
| | Setup Templates | | Y | | | | | | |
| | Set Policy Options | | Y | | | | | | |
| | Set Performance Metrics | | Y | | | | | | |
| | Restore Backups | | Y | | | | | | |
| ORGANISATION | Setup Organisations | | Y | | | | | | |
| | Create Org Admin and Owners | | Y | | | | | | |
| | Reset Organisation Local Admin | | Y | | | | | | |
| | Set Organisation Values and Security | | | Y | | | | | |
| USER MANAGEMENT | Reset User Password | | | Y | Y | | | | |
| | Create and Manage Users | | | Y | Y | | | | |
| | Reset User Password | | | Y | Y | | | | |
| | Set User Roles | | | Y | Y | | | | |
| | Create and Manage Users | | | Y | Y | | | | |
| WORKSPACE MANAGEMENT | Create Workspace | | | | | Y | | | |
| | Invite Users | | | | | Y | | | |
| | Approve User Request | | | | | Y | | | |
| | Assign Workplace Security | | | | | Y | | | |
| | (within Org Security) | | | | | Y | | | |
| | Set Discovery | | | | | Y | | | |
| | Reassign Workspace rights | | | | | Y | | | |
| | View Workspace Users | | | | | Y | Y | Y | |
| | See Notifications | | | | | Y | Y | Y | |
| OBJECT MANAGEMENT | Access Object | | | | | Y | Y | Y | |
| | View Comments | | | | | Y | Y | Y | |
| | Add Comments | | | | | Y | Y | | |
| | Create and Edit Object | | | | | | | | Y |
| | Set Object Security | | | | | | | | Y |
| | Set Object Releasability | | | | | | | | Y |
| | Set Object Discovery | | | | | | | | Y |
| | Delete Object | | | | | | | | Y |

## Infrastructure Security

### Infrastructure Independent

Kojensi is infrastructure independent, able to be deployed into almost any modern x86 based infrastructure model. Kojensi has been deployed as a managed service (SaaS), via dedicated instances into cloud provider infrastructure, and into high-assurance environments requiring on-premises deployment inside secure environments on different hypervisors and technology stacks.

### Operating System Security

The virtual machine operating system on which Kojensi is built is CentOS 7 Linux, as well as using Docker for containerisation of certain components and microservices.

From Kojensi version 2.0 onwards, these security configurations are based on the STIGs (Security Technical Implementation Guide) for RedHat Enterprise Linux (RHEL), combined with technical controls expected for Australian Government ISM (Information Security Manual) compliance.

### Search & Discoverability Security

Kojensi uses the well-established capabilities of Elasticsearch, a distributed, RESTful search and analytics engine that has been implemented to provide the core search functionality for the solution.

Users do not have direct access to the Elasticsearch capability as it is isolated from any user-accessible endpoints, and all search activity is logged for auditing purposes.

The search engine has been configured and structured to support and enforce the Kojensi ABAC model to all search results via the Kojensi application.

The filtering leverages the Kojensi master data store and session-based credentials to dynamically filter the results based on:

- Security Clearance
- Releasability
- Organisation
- Nationality, and
- Discoverability.

As all access to the search functionality is provided through the Kojensi application, only searches meeting security criteria are permitted to execute and only results that meet the ABAC rules are returned.

Data can be selectively excluded from all indexing and search results by the information owner/custodian, by changing the object's Discoverability status.

## SUMMARY

For Defence, Defence Industry and Intelligence who need the ability to share sensitive and classified information internally and with partners and clients, Kojensi is a proven and accredited MLS classified information sharing and document collaboration platform. It enables collaboration and sharing while managing the compliance and security obligations of sensitive information. Rather than building an expensive bespoke solution to manage an organisation's information sharing needs, Kojensi is a commercial product that delivers secure, compartmentalized collaboration, as a cloud service or an on-premises platform, through a per user subscription license.

CONTACT US FOR MORE INFORMATION OR TO BOOK A DEMO:

**www.archtis.com/contact**

## ABOUT ARCHTIS LIMITED

archTIS Limited (ASX:AR9) is a provider of innovative software solutions for the secure collaboration of sensitive information. The company's award-winning data-centric information security solutions protect the world's most sensitive content in government, defence, supply chain, enterprises and regulated industries through attribute based access and control (ABAC) policies. archTIS products include Kojensi, a multi-government certified platform for the secure access, sharing and collaboration of sensitive and classified information; and NC Protect for enhanced information protection for file access and sharing, messaging and emailing of sensitive and classified content across Microsoft 365 apps, Dropbox, Nutanix Files and Windows file shares. For more information visit archtis.com.  Follow us on twitter @arch_tis

archTIS

archtis.com | info@archtis.com

**Australia | United States | United Kingdom**