

30 May 2024

archTIS to Present at Henslow Defence and Security Conference

archTIS (ASX:AR9, OTCQB:ARHLF), a global provider of data-centric solutions for the secure collaboration of sensitive information, today announced that it will be presenting at the Henslow Defence and Security Conference at the Radisson Blu Plaza Hotel in Sydney on 30 May.

The national security landscape has shifted significantly in recent years. A combination of the Russia-Ukraine war, AUKUS alliance, China-Taiwan tensions and conflict in the Middle East has resulted in a major re-think of Australia's security posture. These events have created a significant opportunity for Australian companies to contribute to and benefit from this new paradigm.

Kurt Mueffelmann, Global COO and US President of archTIS will present on behalf of the Company. He will discuss the market drivers around the securing of sensitive information and collaboration from the battlefield to the boardroom, outline recent product innovations and customer wins that support annual revenue growth and move toward cash flow neutrality while wrapping up with key strategic drivers within the business.

-ENDS-

Authorised for issue by order of the Board of Directors.

For further information please contact:

Company enquiries

Daniel Lai
CEO and Managing Director, archTIS
E:

Media enquiries

Irena Mroz
CMO, archTIS
E: irena.mroz@archtis.com

archTIS US Investor enquiries

Viriathus Capital
E: beverly.jedynak@virithus.com

archTIS Interactive Investor Hub

<https://investors.archtis.com/>

The archTIS Investor Hub is an online portal for investors to read and interact with our announcements and updates. You can ask questions and add comments, which our team can respond to where possible.

About archTIS Limited

archTIS Limited (ASX:AR9, OTCQB:ARHLF) is a global 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, SharePoint on-premises, Nutanix Files and Windows file shares. For more information visit archtis.com or follow [@arch_tis](https://twitter.com/arch_tis) on X.



TRUSTED TO SAFEGUARD THE WORLD'S
MOST SENSITIVE INFORMATION

Investor Presentation

ASX:AR9 / US-OTC:ARHLF



Kurt Mueffelman
COO & US President

The logo for archTIS features a stylized globe composed of blue dots and lines, centered in the background. The text 'archTIS' is overlaid on the globe. 'arch' is in white, and 'TIS' is in a teal color. To the left of the text is a small icon consisting of three dots: a teal one at the top, a white one in the middle, and a grey one at the bottom.

archTIS

archTIS: A Snapshot

Global provider of data-centric solutions for the secure collaboration of sensitive information



Daniel Lai
CEO AND MANAGING DIRECTOR

Extensive industry experience in successfully delivering outcomes as part of a senior executive team to both government and commercial organisations.



Kurt Mueffelmann
GLOBAL COO & US PRESIDENT

30+ years of technology leadership, with 5 successful shareholder exits (2x Deloitte Fast 500 CEO), provides proven strategies for scaling go to market efforts and achieving hyper revenue growth.



Andrew Burns
CFO

Andrew Burns brings more than 25 years of experience in executive, commercial and financial leadership, driving sustainable business transformation and profitable growth. Former CFO of The Citadel Group (Miles Jakeman)

Simplified Data Integration & Security at Scale

Data Sources



archTIS Solutions



End-Use



Unstructured Data



Operational Database



Application Database



Application APIs



Data Warehouse / Data Lakes



IoT



Data Orchestration



Policy Orchestration



Governance



Metadata



Data Centric Security



Dashboards



Reports



Analytics



Viewing/Editing



Discovery

Our solutions help solve for

1) Who should have access to data and when

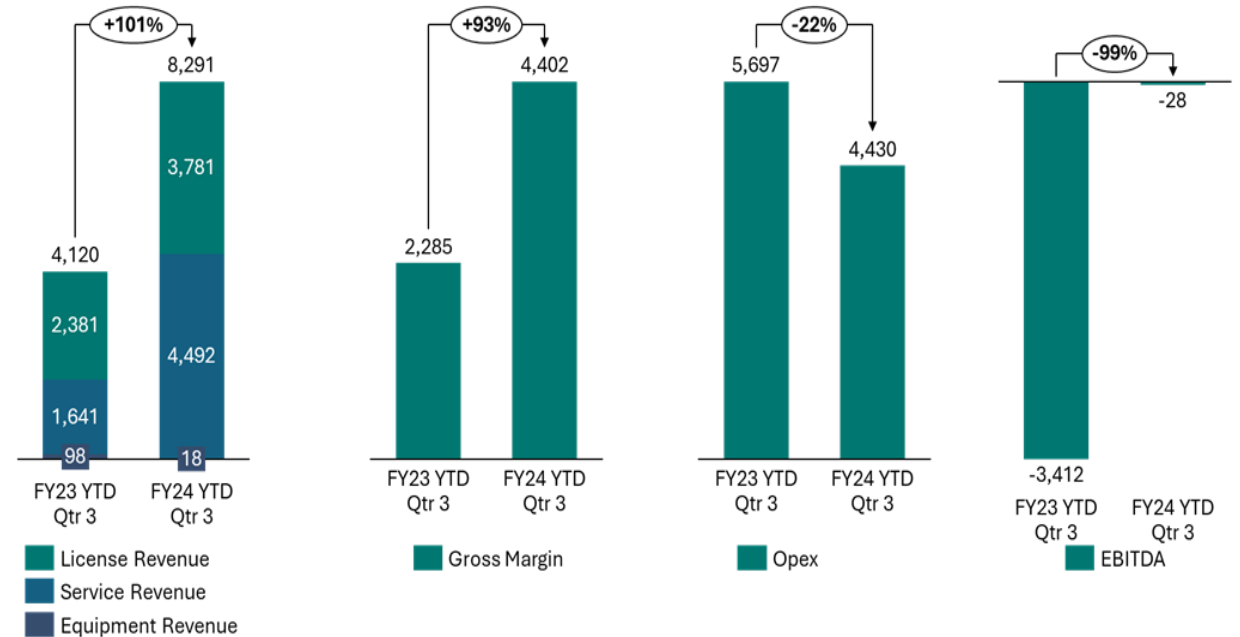
2) What users should be able to do with it once they have access

Equity and Financial Overview

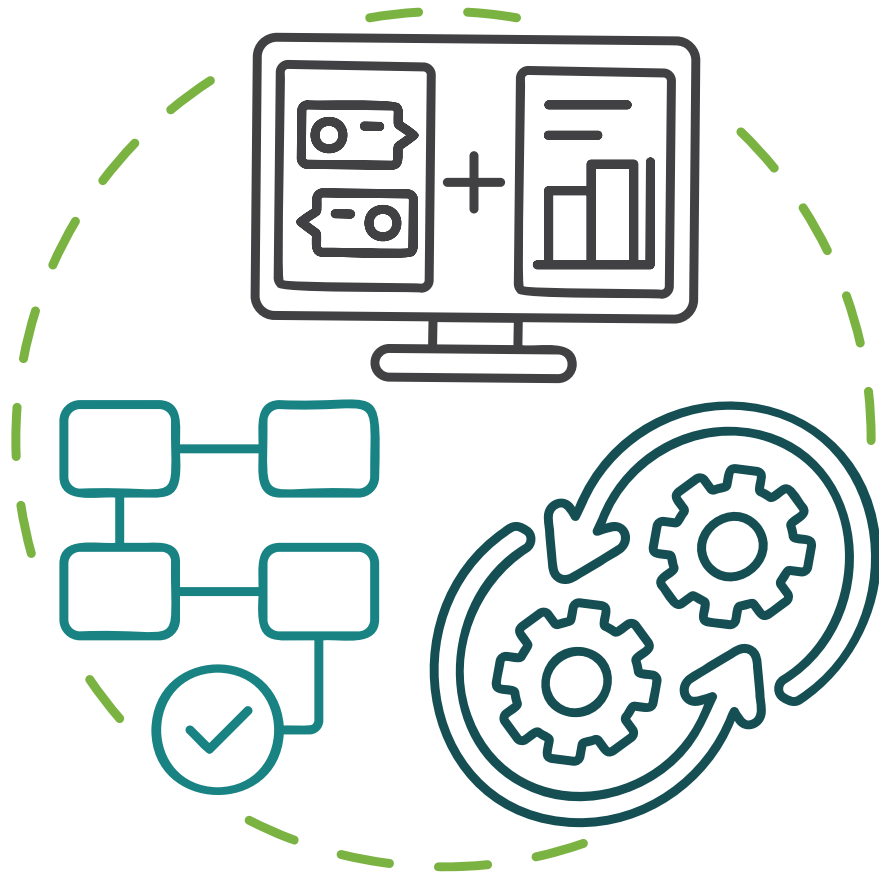
Key metrics

- ASX:AR9 / US-OTCQB:ARLF
- ~A\$27.5M market cap
- 280M o/s shares
 - Management / Board – 22%
 - Top 50 shareholder – 52%
 - AUS / US institutional investors

FY24 YTD (Q3)



The Customer Challenge



- Sensitive and classified data is voluminous and siloed, spread across multiple systems and formats.
- To extract value data must be consolidated and enriched to support operational and analytical workloads.
- Integration and aggregation of sensitive/classified data must be controlled and governed against strict compliance requirements.
- Current generation products are cumbersome and resource-intensive.

Can't take the network with you....data is the key

Data is the new Crown Jewel

\$300B Joint Fighter project



The Risk: Compliance Violations & Fines

ITAR

- Carries a civil penalty of US \$1 million+ per violation
- Violators can be 'debarred' or lose the ability to export goods.
- Criminal penalties of up to 20 years in prison.

EAR

- Criminal penalties of up to US \$1 million in fines per violation and up to twenty years imprisonment.
- Civil penalties, also referred to as administrative penalties, can be either \$300,000 per violation or twice the transaction value, whichever is greater.

FLIR \$30 million for exports and re-exports by FLIR to FLIR AB of ITAR-controlled defense articles and technical data to foreign person employees.

Honeywell \$13 million for unauthorized exports and retransfers of ITAR-controlled technical data in the form of engineering files to several countries across three continents.

Bright Lights USA \$400,000 for the transfer of unauthorized ITAR-controlled defense components and technical data to foreign persons in China.

VTA Telecom Corporation (VTA) \$1,869,372 fine under EAR and a 3-year administrative debarment under ITAR for six unauthorized exports on the USML made or attempted to Vietnam.

Seagate fined \$300 million for EAR violations and placed under a 3-year ITAR debarment for exporting hard disk drives to Huawei Technologies.

Airbus SE \$3.9 billion in fines for ITAR violations and misconduct, and foreign bribery.

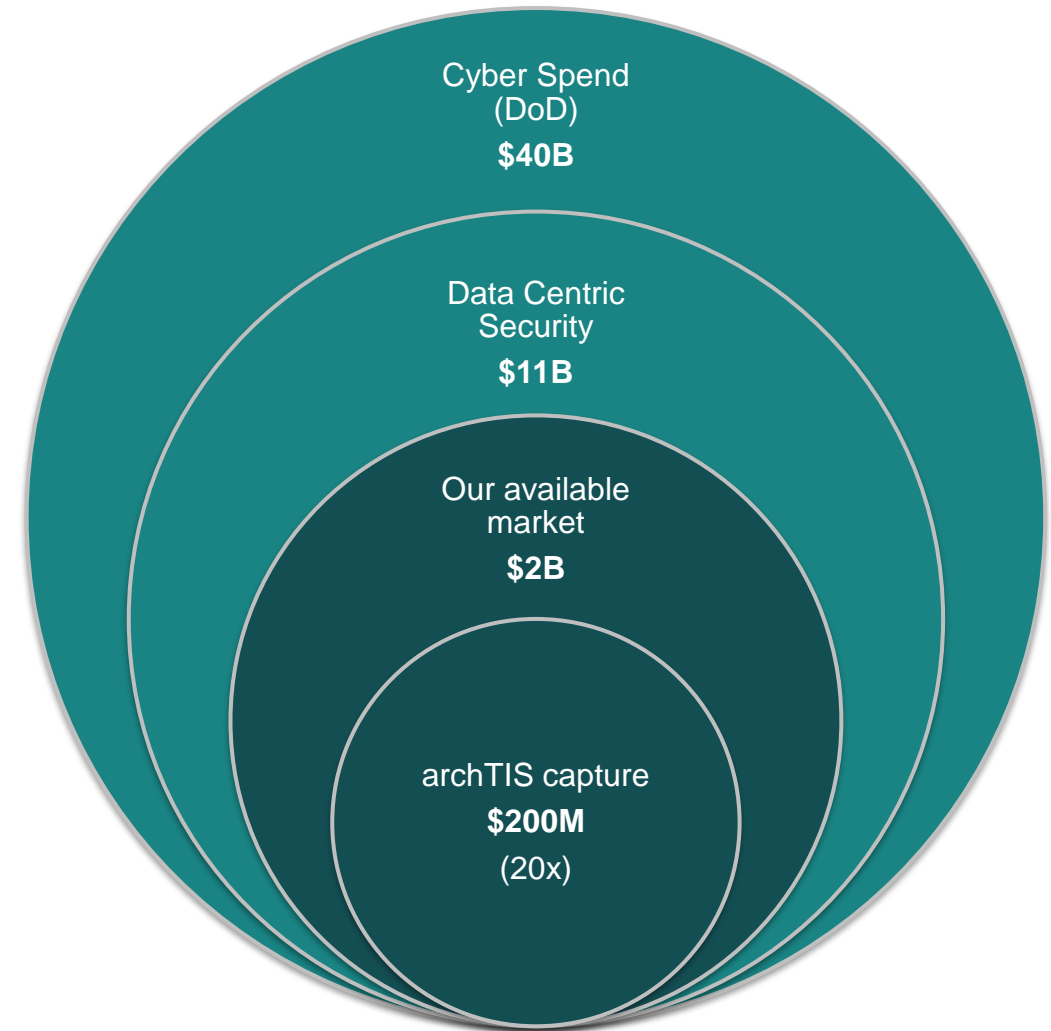
3D Systems \$20,000,000 for ITAR violations.

Under AUKUS-related laws, information breaches will be **fined up to \$31 million, while individuals face up to 25 years in jail.**

Total Addressable Market

*Data-centric security (DCS)
part of the broader and growing
cyber security market (\$225B)*

- Focused on servicing the defence & intelligence markets
- Core customers: Coalition defence & intelligence agencies, Global defence industrial base (DIB)
- First mover / early-stage competition
- Emerging DCS sub-markets:
 - ✓ Attribute-based access controls (ABAC)
 - ✓ Policy orchestration
 - ✓ Data fabric



Our Solutions

A Data Centric Security solution for every data sharing problem

NCPROTECT™

DYNAMIC ACCESS & DATA PROTECTION FOR MICROSOFT 365, SHAREPOINT & FILE SHARES

- Discover, classify and secure sensitive information
- Prevent data loss, misuse and human error
- Enforce zero trust with Attribute Based Access Control (ABAC) and data protection policies
- Audit user file access and interactions for security and compliance reporting
- Maintain control of encryption keys in M365 with Bring Your Own Key (BYOK) Support

kojensi

POLICY-BASED ACCESS CONTROL FOR SENSITIVE & CLASSIFIED DATA

- Compartmentalized military-grade classified information collaboration and file sharing
- IRAP assessed and accredited up to PROTECTED
- Control access and sharing with data-centric ABAC policies, including security classification, country, organization and releasability
- Audit all user interaction and changes made to files, workspaces and other administrative tasks

archTIS®

TRUSTED DATA INTEGRATION

STRUCTURED DATA INTEGRATION, SECURITY & POLICY ORCHESTRATION

- Adds Zero Trust Data Centric Security capabilities to structured data access
- Source and integrate data from multiple authoritative data sources based on access context
- Centrally author and apply access control policies for security and compliance across data transactions with minimal user impact
- Enable seamless information and data collaboration with multiple third parties
- Enables speed of relevance for decision-making



The archTIS ABAC Advantage

Security is built around the combination of **User, Environmental and Resource Attributes** to approve or deny access and apply data protection – in real time

In the Office

Sensitivity: Confidential

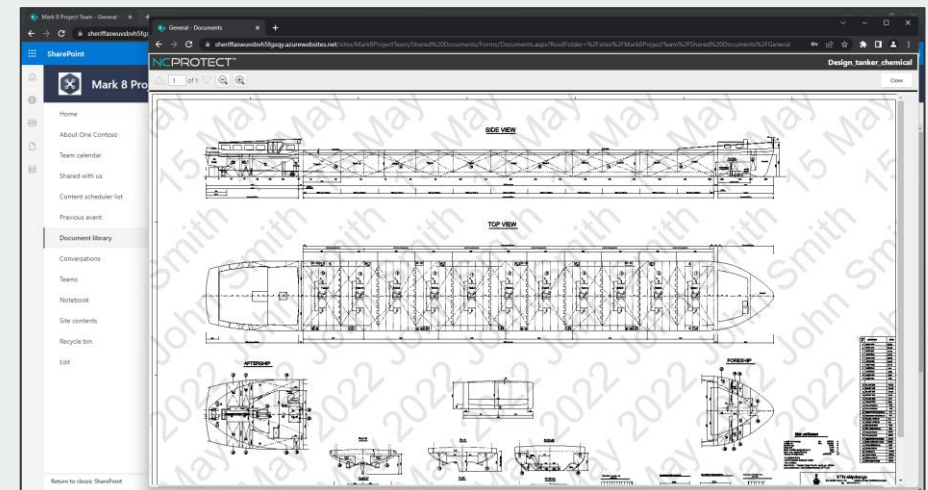
Location: Office

Approve Access



VS.

Public Transportation



Customer Validation

A\$15M Sold to Date



Australian Government

Defence

KOJENSI ON-PREMISES NC Protect

Military-grade secure access,
collaboration and sharing of classified
and sensitive information.



Australian Government
Department of Defence






“ With NC Protect we can increase our collaboration by automatically controlling access to classified information. Before NC Protect, we had to lock everything down so very few users could access content to the extent that it inhibited our ability to collaborate with our coalition partners in theatre. ”

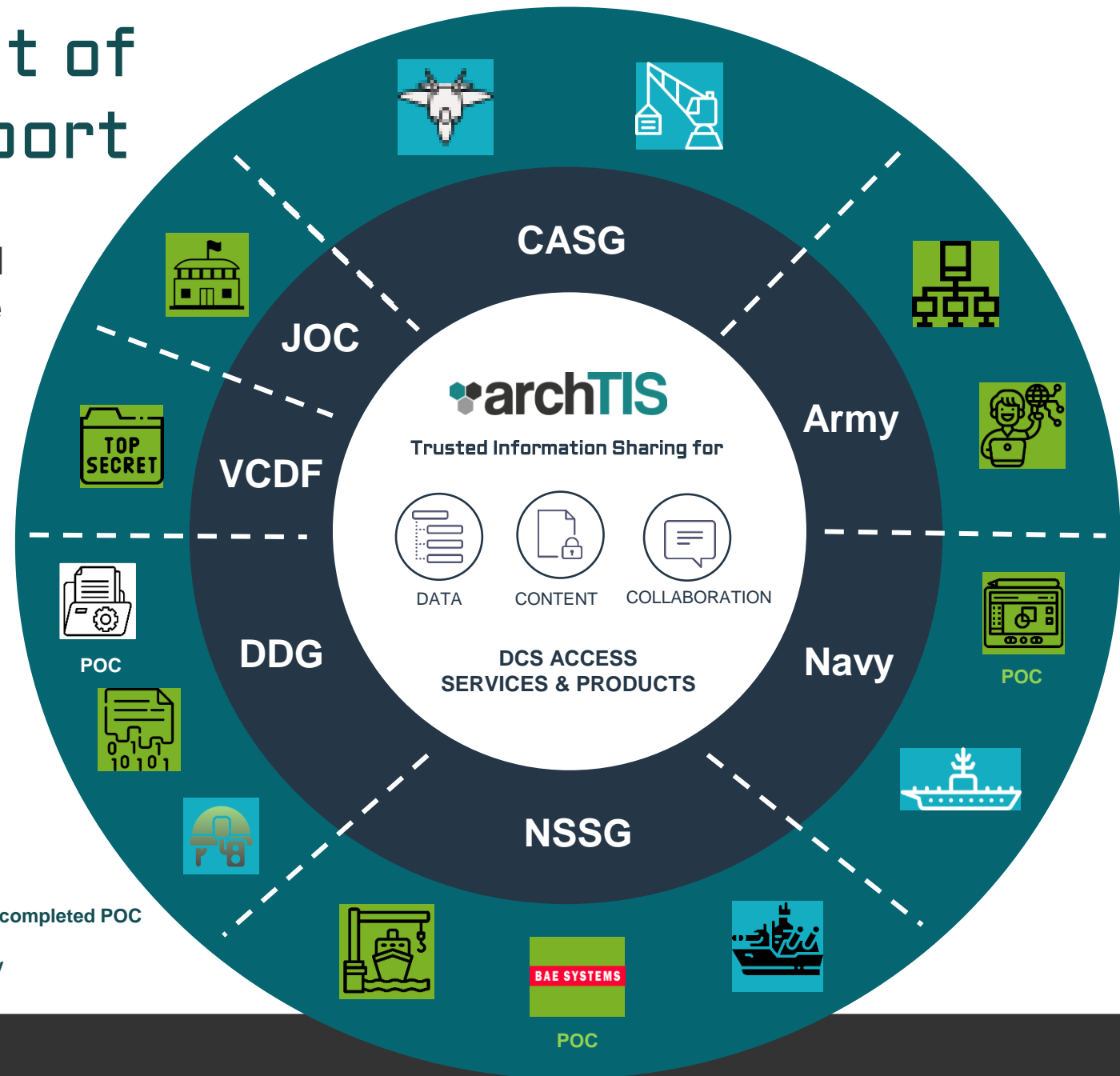
Brigadier General Warren Gould
Director General Systems and Integration,
Department of Defence

Australian Department of Defence Progress Report

The premium provider of Policy Enforced Access Management products to Defence

- Active in **six out of ten** key divisions of Defence
- Defence Strategic Review (DSR) restructure is nearing completion
- Services are part of the journey to educate and demonstrate value for licences
- Enterprise licence vs Whole of Defence licence

-  In Progress
-  Won / Successfully completed POC
-  Current Opportunity

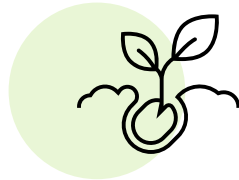


Sales Journey across Emerging Market



Initial Sales Process

Identify need requirements, return on investment, compelling events and success criteria over life of solution offering.



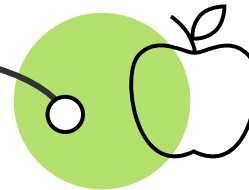
PoC / Services Engagements

Established term limited PoC with success criteria and assumed commercial purchase upon completion Leverage domain expertise for services to drive license.



Licensing Sale & Deployment

Add additional licensing sales to core (90-180 days) to drive higher percentage of licensing against services.



Annual Recurring Renewals

Deliver annual subscription to drive enterprise value of customer and increasing licensing margin.

Global Distribution Strategy

Direct Regional Presence

- Apac – Canberra
- Americas – Boston
 - USFED- DC
- EMEA - London

Global Reseller Channel

- System / Defense integrators
- Value Added Partners
 - Microsoft certified
 - Security / Vertical
 - Trusted Advisor Relationship

Strategic Alliances

- MSFT Co-sell
- DIB's - Thales / Fujitsu



Microsoft Partnership

Microsoft
Partner

Member of
Microsoft Intelligent
Security Association



- Distribution
 - Microsoft Co-Sell Ready
 - Available in Azure Marketplace
- Technology integration
 - Member of the invite-only Microsoft Intelligent Security Association (MISA)
- Industry Recognition
 - Microsoft Security Excellence Awards Compliance & Privacy Trailblazer Finalist

“

Our Aerospace and Defense Industrial Base customers and partners are actively seeking a product that can help meet zero-trust requirements for M365, especially in respect to demonstrating compliance with the new defense standards for the secure and handling of information. **The innovative capability from archTIS makes it seamless to leverage a data-centric, zero-trust practices for information security and data handling.**

”

Richard Wakeman

Chief Architect

Aerospace & Commercial Defense

Microsoft

Strategic Drivers

Driving toward \$150M - \$200M market cap over the next 24-36 months built upon annual recurring software revenue and supporting services

- ✓ Good Value
- ✓ Repeatable Growth through ARR
- ✓ Industry-leading Customers & Partners
- ✓ Innovative Technology Solutions
- ✓ Strong Market Tailwinds





Level 3 , 10 National Circuit
Barton ACT 2600 Australia

1300 ARCHTIS
+61 2 6162 2792
+61 419 528 061

www.archtis.com

X @arch_tis

Q&A

kurt.Mueffelman@archtis.com
+1 603 568 4499

Disclaimer

No Warranties

Disclaimer

The material in this presentation has been prepared by archTIS Limited (“**Company**”).

This presentation may not be reproduced, redistributed or passed on, directly or indirectly, to any other person, or published, in whole or in part, for any purpose without prior written approval of the Company. The material contained in this presentation is for information purposes only.

This presentation is not an offer or invitation for subscription or purchase of, or a recommendation in relation to, securities in the Company and neither this presentation nor anything contained in it shall form the basis of any contract or commitment. Any offering of any of the Company's securities to Australian persons will be subject to Australian securities laws. The distribution of this document in jurisdictions outside of Australia may be restricted by law, and persons into whose possession this document comes should inform themselves about, and observe, all such restrictions.

This presentation is not financial product or investment advice. It does not take into account the investment objectives, financial situation and particular needs of any investor. Before making an investment in the Company, an investor or prospective investor should consider whether such an investment is appropriate to their particular investment needs, objectives and financial circumstances, seek legal and taxation advice as appropriate and consult a financial adviser if necessary.

This presentation may contain forward-looking statements that are subject to risk factors associated with data-centric cyber security business. Forward looking statements include those containing such words as "anticipate", "estimates", "forecasts", "should", "could", "may", "intends", "will", "expects", "plans" or similar expressions. Such forward-looking statements are not guarantees of future performance and involve known and unknown risks, uncertainties, assumptions and other important factors, many of which are beyond the control of the Company. It is believed that the expectations reflected in these statements are reasonable, but they may be affected by a range of variables and changes in underlying assumptions which could cause actual results or trends to differ materially. The Company does not make any representation or warranty as to the accuracy of such statements or assumptions.

This presentation has been prepared by the Company based on information currently available to it. No representation or warranty, express or implied, is made as to the fairness, accuracy, completeness or correctness of the information, opinions and conclusions contained in this presentation. To the maximum extent permitted by law, none of the Company or its subsidiaries or affiliates or the directors, employees, agents, representatives or advisers of any such party, nor any other person accepts any liability for any loss arising from the use of this presentation or its contents or otherwise arising in connection with it, including without limitation, any liability arising from fault or negligence on the part of the Company or its subsidiaries or affiliates or the directors, employees, agents, representatives or advisers of any such party.