

ASX Announcement

11 August 2022

INVESTOR WEBINAR PRESENTATION

archTIS Limited (ASX:AR9, OTCQB:ARHLF) (archTIS or the Company) is pleased to announce its participation in the ShareCafe Small Cap “Hidden Gems” Webinar, to be held Friday 12th of August 2022 from 12:30pm AEST/10:30am AWST.

Daniel Lai, archTIS Managing Director and CEO, will provide an overview of the Company which is a global provider of innovative software solutions for the secure collaboration of sensitive information.

This webinar is able to be viewed live via Zoom and will provide viewers the opportunity to hear from, and engage with, a range of ASX-listed leading micro/mid cap companies.

To access further details of the event and to register at no cost, please copy and paste the following link into your internet browser:

https://us02web.zoom.us/webinar/register/WN_OYJddCmmQa2ODLAWc1tbfQ

A recorded copy of the webinar will be made available following the event.

A copy of the investor presentation to be delivered during the webinar is attached.

-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: investors@archtis.com

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

Media enquiries

Media & Capital Partners
E: archtis@mcpartners.com.au

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 and the cp. suite of products 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, please visit archtis.com or follow @arch_tis on Twitter.



TRUSTED TO SAFEGUARD THE WORLD'S MOST
SENSITIVE INFORMATION

Investor Presentation



Daniel Lai
Managing Director
& CEO

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.

At a Glance - archTIS



AR9



ARHLF

Data-centric security software that secures information access, sharing and collaboration across the enterprise.

Global Customer Validation & Operations

- Strong Defense and Intelligence customer base
- Marquee global customers
- Co-sell alliances with Microsoft,
- Key partners Thales, Raytheon, ForcePoint, KPMG
- Experienced Executive Team
- Canberra – AUS (HQ) / Boston, MA – US / London – UK

Military-grade Technology

- 2 proven technology products in Kojensi and NC Protect
- Accredited protection layers to “Protected / Top Secret” information and to key Microsoft applications (M365 / Teams)

Strong Market tailwinds

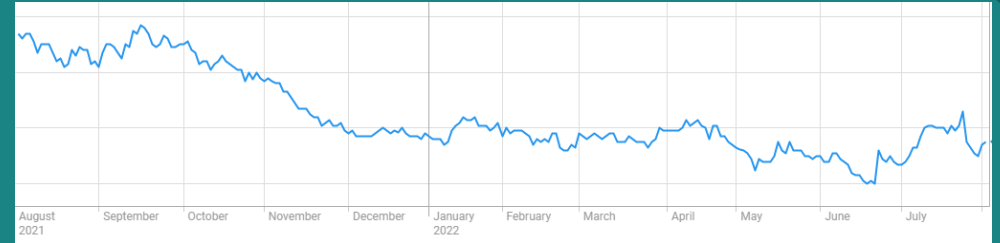
- \$12.5B data-centric security market by 2026 with a 23.1% CAGR*
- Increasing number of data & IP breaches with significant cost
- Remote worker
- Geo-political tensions

At a Glance - ASX:AR9 | OTCQB:ARHLF

Financial (30Jun22 / Unaudited)

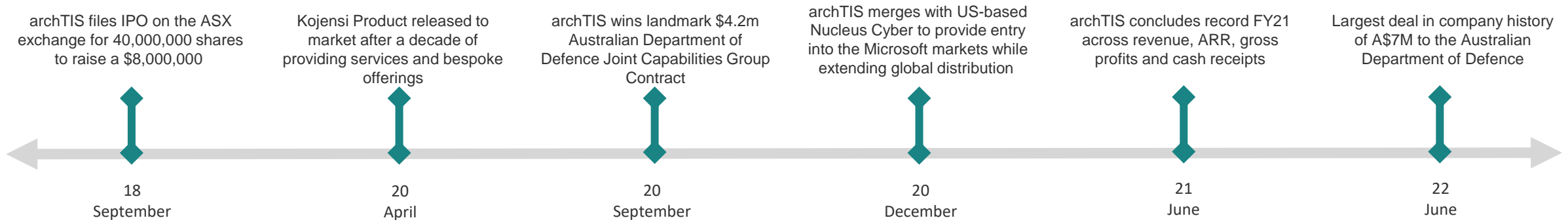
A\$M

Revenue	\$4.6
Licensing	\$2.6
Annual Recurring Revenue	\$3.3
Gross Profit Margin	70.5%
Operating Expenses	\$8.9
EBIDTA	(\$5.6)
Cash / Debt	\$6.5 / \$0



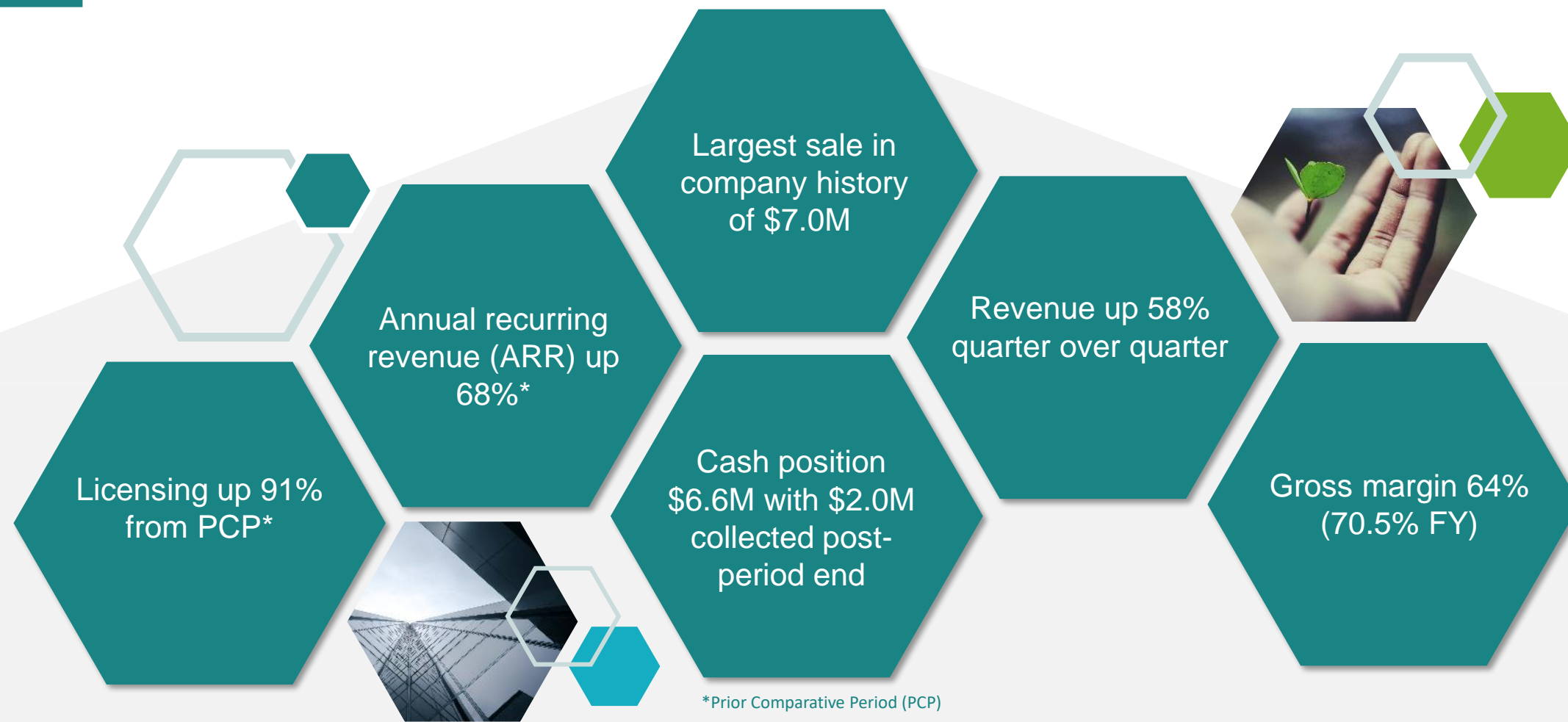
ASX Share Price	\$0.18
12 Month Share Price Range	\$0.10-\$0.39
Shares on Issue	263,803,207
Market Capitalization	\$47.48M
Options and performance rights	16,066,502
Average daily volume (ASX 1-month)	501,477

Company Public History – 2018 | A\$25M raised to date



Q422 Update

Largest Company Deal Builds for Strong FY23



FY23

Outlook Statement



**60% or \$7.5M expected
minimum revenue growth**
(\$4.65M prior)



**Cash receipts expected to be
a minimum of \$9.5M**



**Monthly cash burn expected
to halve in FY23 from prior
year**



The Challenge

Collaboration Challenge:

Malicious & Accidental Insider Threats



The way we work
has changed



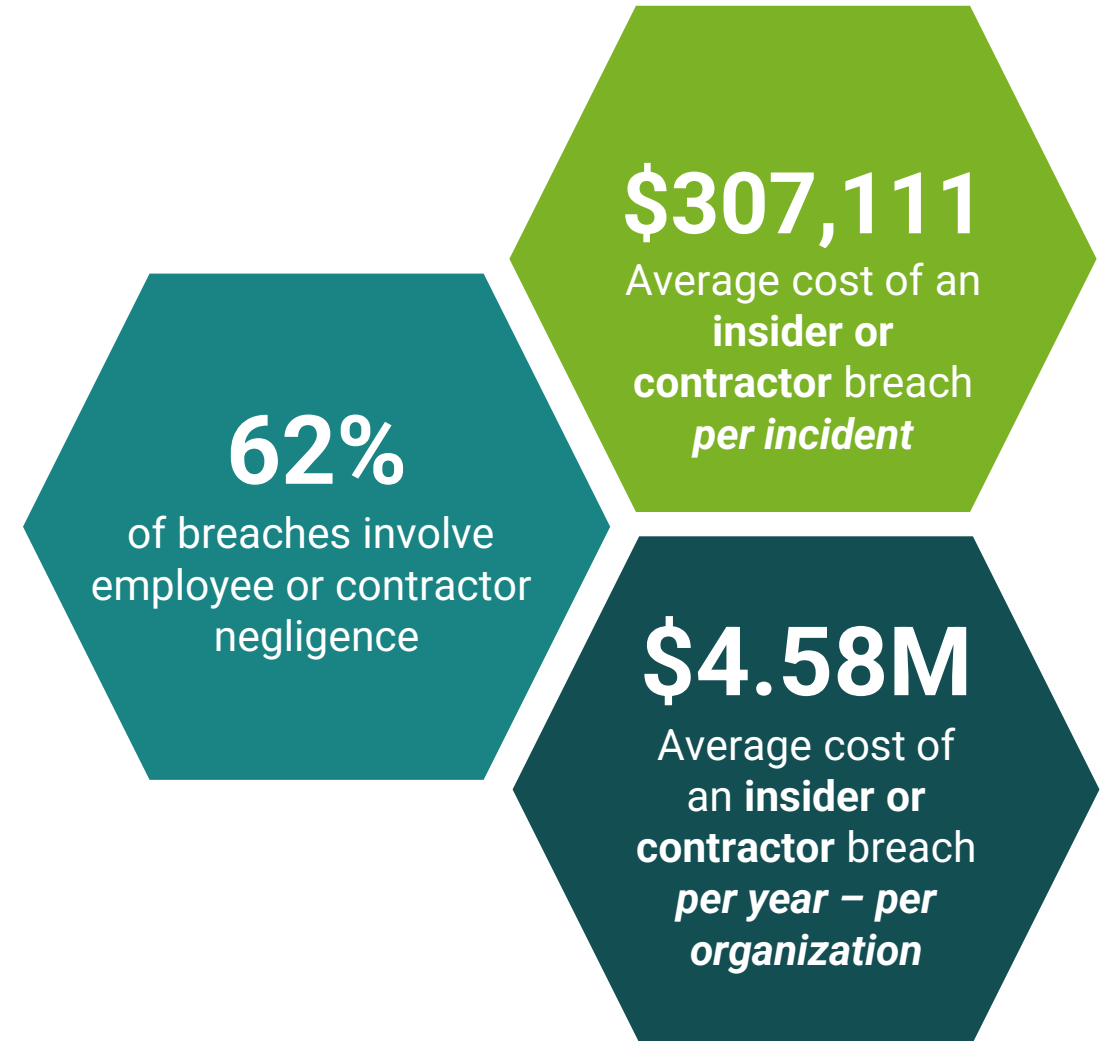
How we access and
share data has changed



Collaboration expanded
cross channel



Traditional Defenses
and protection do not
work



Protection of National Security and Trade Secrets

US\$1 Trillion

TECHNOLOGY AND IIOT > CYBERSECURITY

Tesla Sues Former Employee for Allegedly Stealing 26,000 Confidential Files

The employee allegedly stole the files remotely and transferred them to his personal Dropbox account.

USA TODAY

Facebook CEO Mark Zuckerberg breaks his silence as Congress demands answers after whistleblower testimony

TECH • F-35

Hackers Stole Restricted F-35 Data From an Australian Contractor



China theft of technology is biggest law enforcement threat to US, ...
Christopher Wray says China using 'any means necessary', with Chinese theft of US trade secrets costing '\$300bn-\$600bn a year'

www.theguardian.com

Australian securities regulator latest to suffer file sharing breach

26 January 2021 1 2 0

The Australian Securities and Investments Commission (ASIC) has suffered a cyber security breach related to its use of the Accellion file sharing software which was recently at the centre of a similar incident at the Reserve Bank of New Zealand.



Aircraft-Maker Bombardier Breached by Accellion FTA Hackers

CYBER RISK JANUARY 14, 2021 / 8:57 PM / UPDATED 2 MONTHS AGO

New Zealand central bank governor apologises after cyberattack resulted in serious data breach

By Reuters Staff

3 MIN READ



Info of 27.7 million Texas drivers exposed in Vertafore data breach

Vertafore blames incident on human error after user data was stored on an unsecured external storage service. The files were accessed by an external party.



Data breach at Mitsubishi may have exposed prototype missile design

WATCH NOW

Japan has launched an investigation into the potential exposure of confidential missile data in the wake of a cyberattack on Mitsubishi Electric Corp.



Military-grade Technology

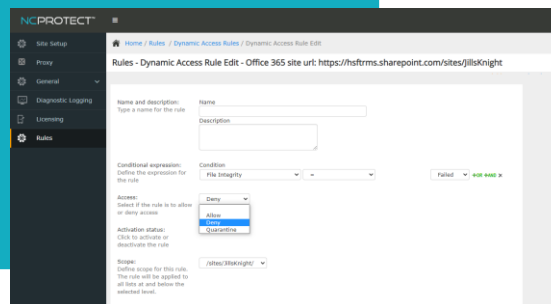
Our Products and Customers

Product Innovation

NCPROTECT™

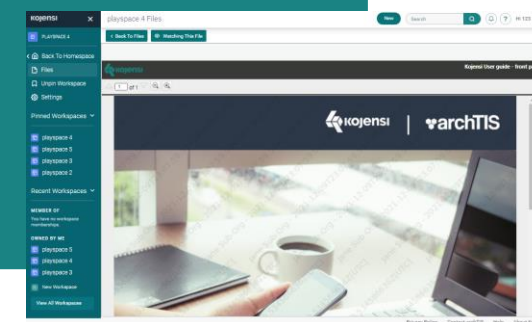
DYNAMIC ACCESS & DATA PROTECTION FOR MICROSOFT 365 & FILE SHARES

- Discover, classify and secure sensitive information
- Prevent data loss, misuse and human error
- Audit and report for compliance



SENSITIVE & CLASSIFIED INFORMATION - SHARED SECURELY

- Share sensitive and classified files securely
- Accredited secure document collaboration platform
- Enforce zero trust with attribute-based access control (ABAC)
- Multi-Level Security Platform



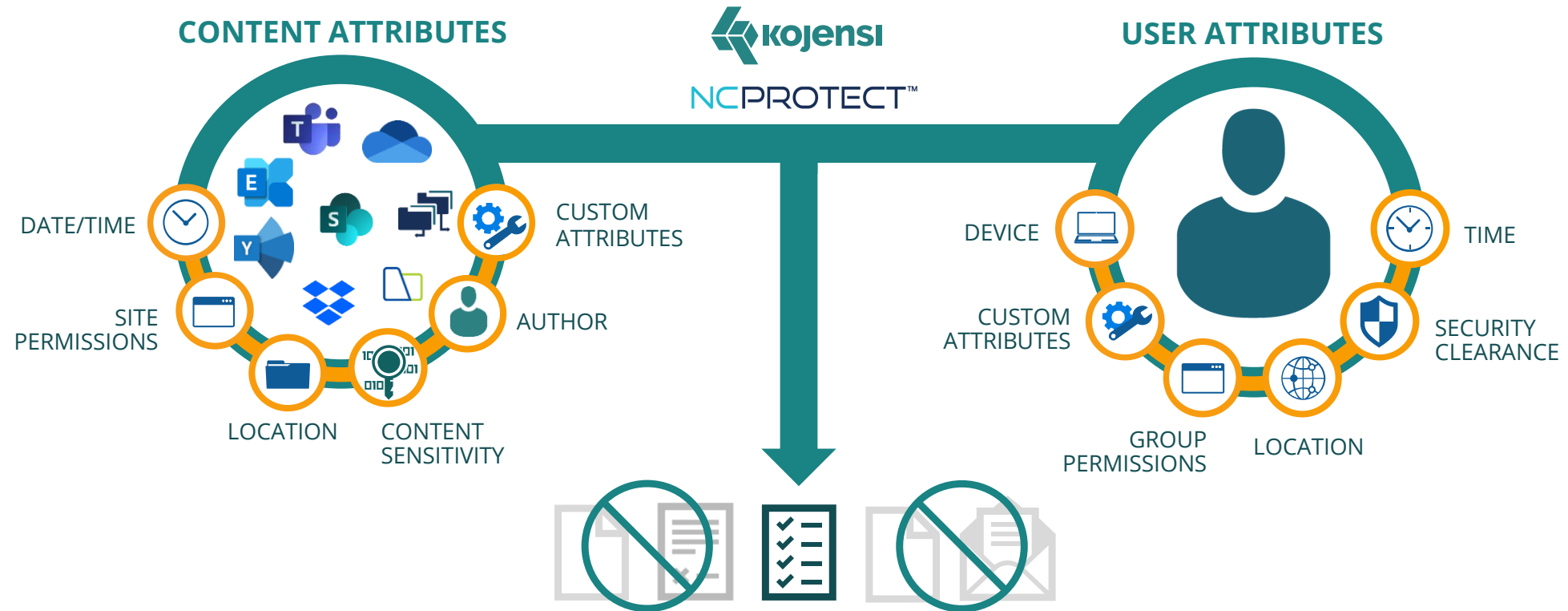
**IDENTIFY, CLASSIFY &
SECURE SENSITIVE DATA**

**PROACTIVELY BLOCK &
PROTECT INFORMATION**

**AUDIT & REPORT FOR
COMPLIANCE**

Key Technology Drivers

Dynamic Context Driven Policy Enforcement



What a user sees when viewing and searching for files

Whether a user can open, edit, copy or download a file

If a file is encrypted when saved, copied, or emailed

If a dynamic watermark should be applied to a file

If a file can only be viewed in a secure application

What actions are enabled in the Microsoft UI

Marquee Customers & Partners

Our customers span the globe, operating in a broad range of industries and deal with sensitive data

Americas



Europe Middle East & Africa



Asia Pacific



BalladHealth



CORNING

Gallagher

Cogentrix

First State Investments

wyzetalk

SINGAPORE POWER

toteboard
Giving Hope. Improving Lives.

THE UNIVERSITY OF ADELAIDE AUSTRALIA

DARPA

NIH
Center for Scientific Review



BGW
Berufsgenossenschaft für Gesundheitsdienst und Wohlfahrtspflege

Deutsche Post
DHL



Australian Government
Attorney-General's Department

Australian Government
Department of Defence

Australian Government
Office of the Australian Information Commissioner

ECCLESIASTICAL
INSURANCE YOU CAN BELIEVE IN

CareFirst

Raytheon

NORTHROP GRUMMAN

aws

KPMG

leidos

LOCKHEED MARTIN

Microsoft

NORTHROP GRUMMAN

NUTANIX

Raytheon Australia

THALES

VAULT
Australia's Secure Cloud Specialist

Market Validation Across Defense

THE AWARD \$7M (incl GST)

LICENSING

\$3.4M

ARR 2yr period

SERVICES & HARDWARE

\$3.6M

ADDITIONAL OPTION YEAR

OUTLOOK (ex GST)

FY23

\$5.0M

Annual licensing:

\$1.65M

Services & Hardware:

\$3.3M

FY24

\$1.5M

Annual licensing:

\$1.5M

FY23

Cash receipts:

\$7M

KOJENSI ON-PREMISES

\$7M Award

Largest sale in company history

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



Australian Government

Department of Defence

Referenced Case Study

Australian Department of Defence



Australian Government
Defence



CHALLENGES

Needed a more effective way to secure the collaboration and sharing of files and prevent accidental data loss while maintaining need to know principles and controlling the releasability of files in SharePoint.



SOLUTION

NC Protect™ for SharePoint



RESULTS

- Dynamically control access to classified information with ABAC policies
- Enforces 'need-to-know principles' for classified data
- Reduced the level of IT effort required for multi-coalition information sharing
- Created a repeatable solution for managing information access and security across the DIE



“ 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



Our Business Model

Develop scalable annual recurring revenue via license sales

Strategic Focus

Deep and focused



Government & Defense



Manufacturing

Prevent Accidental / Malicious Data Leaks

- Restrict what users can do with files: download, copy/paste, email, etc.
- Prevent oversharing and accidental sharing and/or access to files, messages and chat with internal and guest users across M365 apps
- Hide sensitive files from unauthorized users
- Add dynamic watermarks

Enforce Regulatory Compliance

- Restrict access to and flow of information between individual or groups of individuals for SEC, GDPR...
- Flexible Information Barriers allow users to chat and collaborate on permitted projects/topics, but block restricted ones
- Enforce global data privacy and handling regulations
- ITAR / CUI / CMMC

Control Teams Internal & Guest Access

- Control what content guests can see content in a Team or channel based on their user profile
- Automatically restrict guest data access and limit file usage / actions
- Team owners can apply default security to teams and channels
- Toggle private channels on/off
- Coalition forces separation

Audit Activity & Permissions

- User activity, information protection and permissions reports
- Plug at-rest permissions gaps for sensitive files
- Find and fix incorrect app level at-rest permissions
- Identity and associated permissions are no longer a single point of failure

ARR Go-to Market Strategy

Diversified Customer Base / High Margin / Stickiness



Gov & Defense

Kojensi Enterprise On-premises

- Securing “Protected / Top Secret” information
- Government Agencies | Defense Industrial Base
- Enterprise Direct | Large System integrators | MSFT Co-sell
- ASP: \$500k–6M per annum | Users licenses: Over 5,000

Enterprise

Kojensi Enterprise On-premises & NC Protect Enterprise

- Secure Collaboration | Supply Chain Risk Management (C-SCRM)
- Government Agencies | Corporate Enterprises over 5,000 staff
- Regional Direct | System Integrators | MSFT Partners | MSFT Co-sell
- ASP: \$50–500k per annum | Users licenses: 500–5,000

Corporate SME

Kojensi SaaS & NC Protect

- Secure Collaboration
- SME under 5,000 | State & Local Gov (SLG) and Higher Education (HE)
- Inside direct | Channel Resellers (MSFT / Security partners)
- ASP: \$10–50k per annum | User licenses: 1-500

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 / Raytheon
- ForcePoint / Optiv





EXECUTING ON STRATEGIC GROWTH

GOVERNMENT Defense & DIB OPPORTUNITIES

Leverage Australian prior successes
in key government agencies and
Defense industrial entities

LEVERAGE KEY PARTNERSHIPS

Microsoft, Thales, Raytheon and
global reseller channel

CONTINUOUS PRODUCT INNOVATION

Embrace Zero-trust security
architecture across ABAC
technologies for data-centric offerings

Why Invest Now

Who should have access
to data and when

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

- ✓ Good Value
- ✓ Repeatable Growth
- ✓ Industry-leading Partners & Customers
- ✓ Strong Market Tailwinds
- ✓ Global Distribution





Level 3 , 10 National Circuit
Barton ACT 2600 Australia

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

www.archtis.com

 **[@arch_tis](https://twitter.com/arch_tis)**

Q&A

daniel.lai@archtis.com

+61 419528061