



TRUSTED TO SAFEGUARD THE WORLD'S MOST
SENSITIVE INFORMATION

Investor Update

Q422 (JUNE) QUARTER



Daniel Lai
Managing Director
& CEO



Kurt Mueffelmann
Global COO
& US President

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 a cyber security technology 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.

Q422 Update

Largest company-deal builds for Strong FY23

Largest sale in company history of \$7.0M	Revenue up 58% quarter over quarter	Annual recurring revenue (ARR) up 68% with licensing up 91% from PCP
Strong cash position at quarter end of \$6.6M with additional \$2.0M collected post-period end	Monthly cash burn expected to halve in FY23 from prior year	Accelerated growth outlook for FY23 in revenue and cash receipts

***Q4 FY22 Highlights Relative Prior Comparative Period (PCP)**

Q4 Overview – Driving Tactical Execution

	FY22-Q4*	FY21-Q4
(A\$'000)		
Licensing Revenue	691	361
Services Revenue	667	1,765
Equipment Revenue	-	133
Total Revenue	1,358	2,259
Annual Recurring Revenue	3,257	1,939
% Increase on prior comparative period	68%	
Gross Margin for quarter	64%	66%
Underlying OPEX	2,939	2,305

*Unaudited results

Licensing revenue up
91%

Record ARR up 68% on PCP

Gross Margin 64%
(70.5% FY)

Stable Operating Expenses

Cash of \$6.5M with \$2M additional
collections post-close

Market Validation Across Defence

The Award \$7M (incl GST)



Outlook (ex GST)



Referenced Case Study: Australian Dept of 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

Additional Quarterly Customers

Low churn / High revenue & cash predictability

100% Account growth – Kojensi SaaS

- Northrop Grumman and SAP Australia renewed and expanded their use of Kojensi SaaS
- *Network growth effect* of Kojensi SaaS across AUS higher-educational institutions
- Secure collaboration with Defence

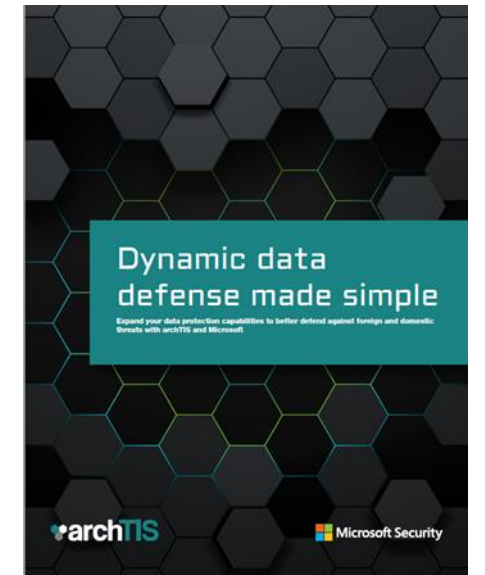
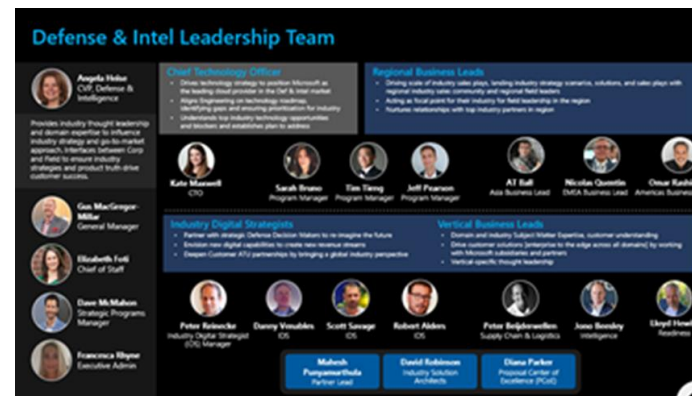
Geographical partner expansion

- I-Sprint, a new Singapore partner procured a 3-year customer for NC Protect (M365)

- The **U.S. Department of Health and Human Services**, is the nation's medical research agency — making important discoveries that improve health and save lives for safeguarding collaboration across the agency.
- A **global IT distributor** of computer and IT components in the world to secure customer and intellectual property agreements across File Share systems.
- US-based **energy conglomerate** protecting strategic M&A documents across M365
- One of the largest **US real estate management** companies protecting the collaboration of financial information through NC Protect's secure web viewer and dynamic watermarking features in SharePoint on-prem.
- A **Middle Eastern government agency** for atomic and energy securing scientific, research and governmental entity collaboration.
- One of the **largest healthcare insurance providers** in the US.
- **European specialist developer** and provider of advanced healthcare technologies for protecting intellectual property and creating information barriers between supply chain trading partners.

Continued Microsoft Expansion

- Expanding Pipeline
- Eurosatory
- E-Book co-marketing campaign
- Global presentations
 - Sales force
 - Partner kick-off - Inspire
- Executive Briefings (CTO / CVP)



Azure Commercial & Government Marketplace Offers LIVE

The screenshot shows the Azure Commercial Marketplace page for 'NC Protect for Microsoft 365 Applications (Office, SharePoint, OneDrive, Exchange & Teams)' by archTIS. The page features a blue header with the Microsoft logo and navigation links. The main content area includes a product overview, a 'Get It Now' button, and a list of key advantages. A large image of the NC Protect logo is also visible.

Microsoft | Azure Marketplace | Apps | Consulting Services | Search Marketplace

Products > NC Protect for Microsoft 365 Applications (Office, SharePoint, OneDrive, Exchange & Teams)

archTIS

NC Protect for Microsoft 365 Applications (Office, SharePoint, OneDrive, Exchange & Teams)

archTIS

Overview | Plans + Pricing | Ratings + reviews

Get It Now

Categories
Identity
Security

Support
Support
Help

Legal
License Agreement
Privacy Policy

Advanced sensitive information protection that's simple, fast and scalable

NC Protect from archTIS leverages Microsoft security investments to protect sensitive and classified information against data loss and insider threats with data-centric security that is simple, fast and scalable across Microsoft 365 applications including Teams, SharePoint Online, Exchange, OneDrive and Office.

By combining Microsoft Information Protection (MIP) labels with NC Protect's dynamic attribute-based access control (ABAC) and protection policies to control access, usage and sharing, customers benefit from expanded data protection and control over collaboration and sensitive/classified information to meet security and compliance needs across Microsoft collaboration apps.

Key Advantages:

- Leverage MIP labels in combination with other file and user attributes to dynamically adjust access and data protection.
- Control what users can see, how they can use and share information, and with whom at the file, message and chat level using granular attributed-based access and sharing control (ABAC).
- Get unique security capabilities to: enforce secure read-only access, hide sensitive files from unauthorized users, trim the application ribbon, and apply dynamic personalized watermarks.
- Redact sensitive or confidential information, such as keywords or phrases, when viewed in Word, Excel, PowerPoint and PDF files or when the file is presented in the NC Protect secure reader.
- Encrypt or restrict attachments sent through Exchange Email.
- Integrate user activity and protection logs with SIEM tools including Microsoft Sentinel for further analysis and downstream actions.

Trusted to safeguard the world's most sensitive information

Experience less data loss, misuse, and accidental sharing, and ensure compliance with NIST and CMMC requirements with fast, simple, and scalable advance information protection from NC Protect.

Learn more

- NC Protect Overview
- NC Protect for M365 & SharePoint
- NC Protect for Teams
- NC Protect Resources
- Customer Case Studies by Industry
- Data Sheet
- Technical Specifications
- How do I deploy NC Protect from Azure Marketplace?

Azure Commercial Marketplace

https://azuremarketplace.microsoft.com/en-us/marketplace/apps/nucleuscyber.nc_protect_m365?tab=Overview

The screenshot shows the Azure Government Marketplace page for 'NC Protect for Microsoft 365 Applications (Office, SharePoint, OneDrive, Exchange & Teams)' by archTIS. The page features a blue header with the Microsoft Azure Government logo and navigation links. The main content area includes a product overview, a 'Create' button, and a list of key advantages. A large image of the NC Protect logo is also visible.

Microsoft Azure Government | Search resources, services, and docs (G+)

Home >

NC Protect for Microsoft 365 Applications (Office, SharePoint, OneDrive, Exchange & Teams)

archTIS

archTIS

NC Protect for Microsoft 365 Applications (Office, SharePoint, OneDrive, Exchange & Teams)

archTIS

Plan

NC Protect for Microsoft 365 - Azure ... | Create

Overview | Plans + Pricing | Usage Information + Support

Advanced sensitive information protection that's simple, fast and scalable

NC Protect from archTIS leverages Microsoft security investments to protect sensitive and classified information against data loss and insider threats with data-centric security that is simple, fast and scalable across Microsoft 365 applications including Teams, SharePoint Online, Exchange, OneDrive and Office.

By combining Microsoft Information Protection (MIP) labels with NC Protect's dynamic attribute-based access control (ABAC) and protection policies to control access, usage and sharing, customers benefit from expanded data protection and control over collaboration and sensitive/classified information to meet security and compliance needs across Microsoft collaboration apps.

Key Advantages:

- Leverage MIP labels in combination with other file and user attributes to dynamically adjust access and data protection.
- Control what users can see, how they can use and share information, and with whom at the file, message and chat level using granular attributed-based access and sharing control (ABAC).
- Get unique security capabilities to: enforce secure read-only access, hide sensitive files from unauthorized users, trim the application ribbon, and apply dynamic personalized watermarks.
- Redact sensitive or confidential information, such as keywords or phrases, when viewed in Word, Excel, PowerPoint and PDF files or when the file is presented in the NC Protect secure reader.
- Encrypt or restrict attachments sent through Exchange Email.
- Integrate user activity and protection logs with SIEM tools including Microsoft Sentinel for further analysis and downstream actions.

Trusted to safeguard the world's most sensitive information

Experience less data loss, misuse, and accidental sharing, and ensure compliance with NIST and CMMC requirements with fast, simple, and scalable advance information protection from NC Protect.

Media

More products from archTIS

- archTIS**
- NC Protect Data Connector for Azure Sentinel
- archTIS
- Azure Application
- Get advanced user insight, audits and alerts with NC Protect's Azure Sentinel integration

Azure Gov Marketplace

https://portal.azure.us/#create/nucleuscyber.nc_protect_m365nc-protect-azure-marketplace-plan



Reaching up to support employee causes to build a better global community

Recipient Name: **Oz Harvest**

Overview of Cause:

They rescue food from going to landfill and repurpose it and donate to charities to help feed people in need.

What it Means to Nominee:

Food Relief for individuals and charities

Education - food Waste program aims to reconnect all Australians to the value of food and make food waste a thing of the past.

The Environment – Food waste is responsible for 8-10% of global greenhouse gases





Executing on Strategic Growth

Government Defence & DIB Opportunities

Leverage Australian prior successes in key government agencies and Defence 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

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
(\$880k decreasing)

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



Global Distribution



Industry-leading Partners & Customers



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



@arch_tis

Q&A

Company Enquiries

Daniel Lai

Managing Director, archTIS

E: investors@archtis.com

Investor Relations

NWR Communications

sam@nwrcommunications.com.au