

archTIS Limited

(ASX: AR9, OTCQB: ARHLF)

Equity | Australia

November 1, 2021

VIRIATHUS[®]

Marco Rodriguez, CFA

+1 212 380 6200

Research Analyst

marco.rodriguez@virithus.com

Company Description:

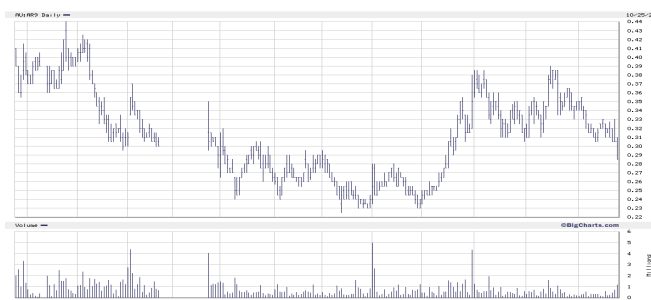
archTIS designs, develops, and markets software solutions and services for secure information sharing and collaboration globally. The company's flagship solutions, Kojensi and NC Protect, enables organizations to share and collaborate on files in a secure space. Kojensi allows the sharing of sensitive and classified information securely, while NC Protect provides dynamic access and data protection for Microsoft 365 applications and file shares.

Informational Report Highlights:

- Large and expanding target market.** The data-centric security market is expected to grow at a 23.1% CAGR to US\$9.8B by 2026. Driving growth is an increasing number of high-cost data breaches, an increase in cloud-based data security needs, coupled with the need to better secure remote employees' work and access to information.
- Unique technology underpins patented software platform and drives differentiation.** archTIS differentiates itself from other security companies by employing a security method called Attribute Based Access Control (ABAC). ABAC is a security model that allows individuals to define rules to control who accesses information, and under what conditions. The ABAC enforces zero trust at the perimeter and at the data layer. Importantly, the security platform is patent protected.
- Proven technology platforms poised to take market share.** archTIS' data-centric cyber security software enables secure information sharing and inter-organization collaboration anywhere and on any platform. Kojensi is a multi-government certified platform for the secure access, sharing and collaboration of sensitive and classified information, and NC protect provides dynamic access and data protection for Microsoft 365 applications and file shares.
- Global sales network and key strategic partnerships to drive growth.** archTIS' distribution strategy is based on a solid foundation of direct sales, indirect sales through key channel partners, and strategic alliances. Key strategic alliances include Microsoft, that co-sells NC Protect, and Thales S.A., and Raytheon.
- Solid FY21 performance drives cash flows and solid balance sheet.** archTIS' business model is based on driving annual recurring revenue (ARR) from licensing its software solutions. Importantly, in FY21 the company saw record breaking financials results that included y/y revenue, ARR, and EBITDA growth of 743%, 681%, and 44%, respectively. Furthermore, the company saw cash receipts from customers increase 846% y/y and a cash balance of AUD\$12.7M as of June 2021.

Financial Data (AUD):

Share Price:	0.285
Market Capitalization (mln):	67.76
Shares Outstanding (mln):	233.67
Float (mln):	164.8
Average Volume (90 Day approx.):	0.529
52 Week Range:	0.225 – 0.44
Exchange:	ASX



Recent Milestones:

- Acquisition of Cipherpoint Technology assets & customers adds to archTIS' rapidly growing annual recurring revenue, global distribution, and industry-leading intellectual property.
- archTIS expands global operations in Europe, Middle East, and Africa.
- archTIS begins quoting its ordinary shares on the US based OTCQB.
- archTIS successfully completes merge with Nucleus Cyber. The merger immediately expands archTIS' global footprint, creates product diversity, and increases cross-selling opportunities.
- archTIS secures landmark AUD\$6.18M contract with Australian Department of Defense.

Corporate Contact Information:

archTIS Limited
 Level 3, 10 National Circuit
 Barton, ACT 2600 Australia
 Kurt A. Mueffelmann
 Global COO / US President
 Email: investors@archtis.com

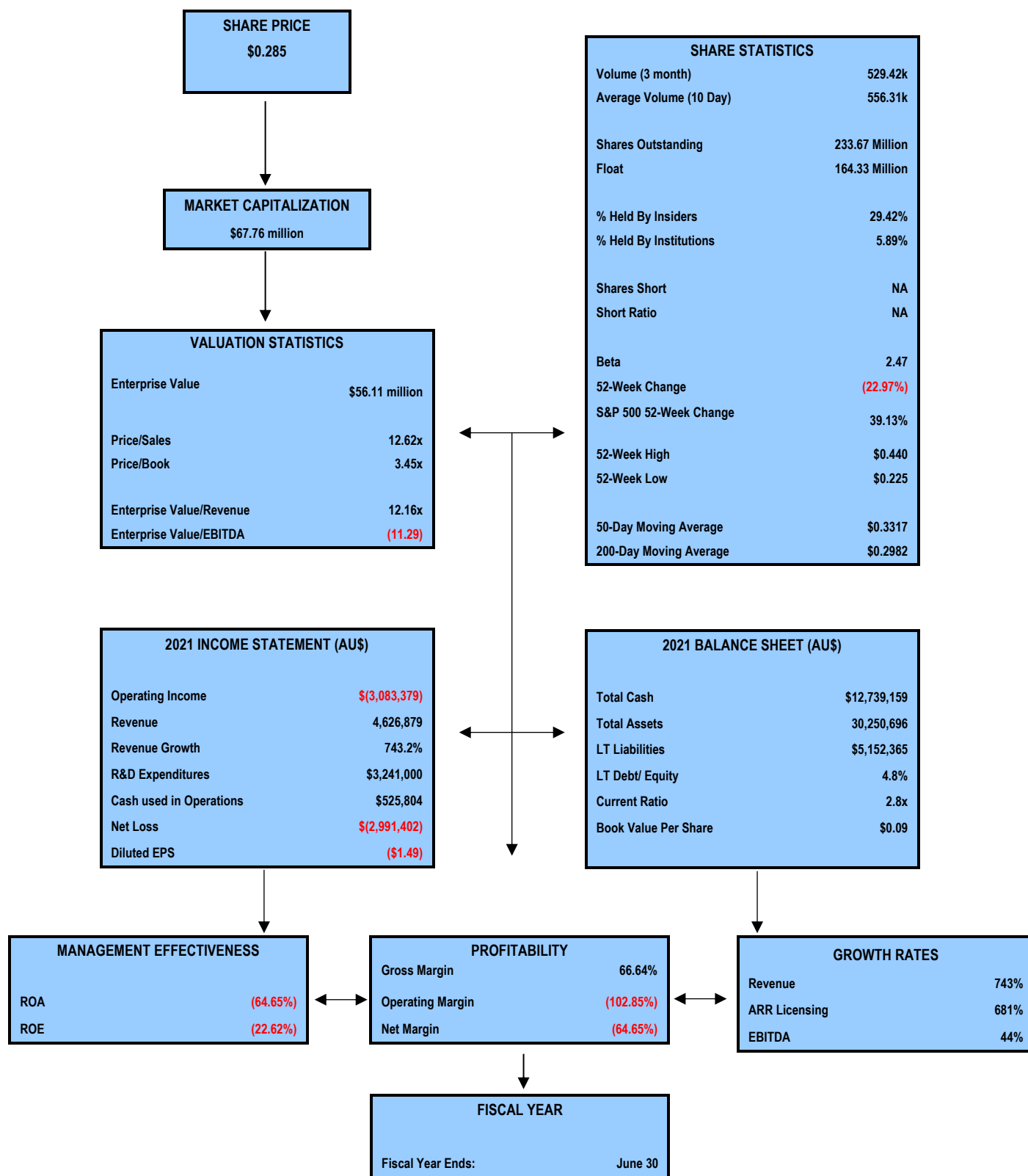


Balance Sheet (AUS)	June 2021
Cash	12,739,159
Assets	30,250,696
Shareholders' Equity	19,642,975
Non-Current Liabilities	5,152,365
NCL to Equity Ratio	4.8%

P&L Data AUS (000)	2020	2021
Revenues	549	4,627
R&D Expenditure	0	3,241
Pre-tax Loss	3,725	3,334
Net Loss	3,725	2,991
EPS	(2.94)	(1.49)

Cash flow: (AUS) (000)	2020	2021
From Operations	2,838	526
From Investing	4	104
From Financing	2,015	10,625
Cash Acquired		331
Net Change in Cash	827	10,327

Financial Metrics



archTIS Limited
(ASX: AR9, OTCQB: ARHLF)

Table of Contents

Company Description:1
Milestones:1
Informational Report Highlights:1
Financial Metrics:2
Company Overview:4
Product & Services Overview5
Technology Overview:7
Business Strategy & Model:9
Sales & Marketing Strategy:10
Market Overview:12
Management Team:14
Competition:16
Investment Risks:19
Summary:20
Financial Statements: 22
Disclaimer:26

Company Overview

archTIS is trusted to safeguard the world's most sensitive information.

archTIS Limited is a provider of innovative software solutions for the secure collaboration of sensitive information. The Company's data-centric, information security solutions protect the world's most sensitive content in government, defense, supply chain, enterprises, and other regulated industries through a unique attribute-based access and control (ABAC) policies. The company's products include:

- Kojensi
 - A multi-government certified platform for the secure access, sharing, and collaboration of sensitive and classified information.
- NC Protect
 - For enhanced information protection for file access and sharing, messaging, and emailing sensitive and classified information/content across Microsoft 365 applications, Dropbox, Nutanix Files, and Windows file shares.

archTIS is an Australian based company that was established in 2006, however its product was not commercialized until early 2019. The company has over 15 years of experience delivering information security solutions within the highest security levels of the government and defense, as well as enterprises.

Exhibit 1: archTIS Company Timeline



archTIS (architected trusted information sharing) vision is to be the company that the world trusts with its most sensitive information.

archTIS' vision is to be the company that the world trusts with its most sensitive information. In fact, the company's name is an abbreviation for "architected trusted information sharing." This phrase, trusted information sharing, came out of a US Senate commissioned report into the events of 9/11. The report discovered that a lack of trust, and infrastructure, prevented the sharing of information between law enforcement, border protection, and intelligence services to prevent the 9/11 attacks. archTIS saw this as a global problem and was founded to solve this issue.

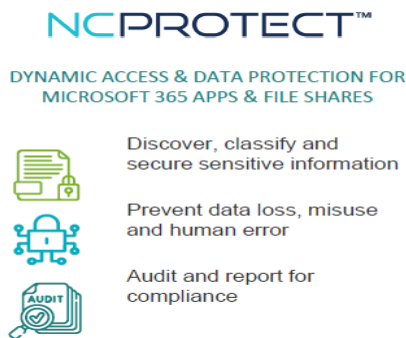
archTIS went public via an IPO in September 2018 and is listed on the Australian Securities Exchange. In early 2019, the company launched its first commercial offering, Kojensi.

Product & Services Overview

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

archTIS' software solutions are patented, data-centric cyber security software that enables secure information sharing and inter-organization collaboration anywhere and on any platform. archTIS' software solutions 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 sensitive and classified content across Microsoft 365 apps, Dropbox, Nutanix Files, and Windows file shares.

Exhibit 2: archTIS' Software Solutions



Through its September 2021 acquisition of Cipherpoint Technology, the company added the IP to cp.Protect and cp.Discover. cp.Protect is an advanced SharePoint on-premises data encryption solution while cp.Discover is a data discovery and classification platform. Both products complement archTIS' NC Protect solutions.

Kojensi

Kojensi is a proven and accredited software platform delivered as software-as-a-service (SaaS). This multi-level, collaboration software platform allows government and industry to create and share highly classified information. Through the use of Attribute Based Access Control (ABAC), the user can define policies around who can access information and under what conditions. The ABAC enforces zero trust at the perimeter and at the data layer. Importantly, the security platform is patent protected.

Users of Kojensi can create, share files, and co-author documents in real-time, all in a secure and intuitive platform. Key attributes of Kojensi include:

- ✓ **Secure Documents** – Documents and files access are controlled by attributes including security classification, country, and organizational releasability.
- ✓ **Ensure Compliance** – It is hosted locally by an ASD-certified protected cloud providers. Kojensi is also PSPF and ISM compliant.
- ✓ **Increase Productivity** – It provides a suite of collaboration features, each designed to improve productivity.
- ✓ **Collaboration With Anyone** – Allows the user to securely share large files and collaborate between and within organizations.

Importantly, the Kojensi platform has three separate applications that include:

- **Kojensi Cloud Service** – Hosted in a protected cloud, the service enables private and public sector organizations to share and collaborate on files in a secure space.
- **Kojensi Enterprise** - Hosted on-premises or in a private cloud, Kojensi Enterprise allows for multi-level, multi-coalition and multi-domain collaboration on information classified up to Top Secret.
- **Kojensi Field** – Deployed on ruggedized equipment. Kojensi field allows military, government, aid and emergency service workers to collaborate in the field.

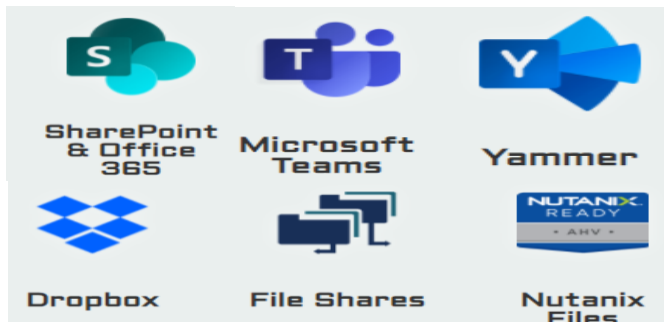
One platform, Three Applications

NC Protect allows organizations to secure all its collaboration with a single solution.

NC Protect

NC Protect provides advanced data-centric security for collaboration applications including Microsoft Office, 365, SharePoint online, and on-premises, OneDrive, Teams, Yammer, and Exchange emails. Additionally, the software platform supports Nutanix files, Dropbox, and Windows File Shares.

Exhibit 3: NC Protect Solutions



The software platform discovers, classifies, and secures unstructured data including files, messages, and chat content. Access and security are dynamically adjusted based on real-time comparison of user context and file content to make sure that users’ access, use, and share files according to a business’s regulations and policies.

Importantly, the software platform is both content and context aware and can automatically find, classify, and secure data on-premises, in the cloud, and in hybrid environments. As such, NC Protect offers advanced information protection to proactively stop insider threats. Additionally, the platform secures data at rest, or in motion, to protect it as users and partners collaborate across different communication channels. Important features of NC Protect includes:

Dynamic, granular information protection without the complexity.

- **Discovery, Classification & Tracking** – It locates and classifies all sensitive and confidential data (PII, IP, HIPAA, HR/Board docs etc.) using one set of rules for one-to-multiple on-premises, cloud, or hybrid environments. You can encrypt or quarantine documents when required.
- **Prevent Data Loss, Misuse, and Human Error** – Dynamic security that adjusts access, usage and sharing rights for files, charts, and messages based on real-time comparisons of user context and file content to enforce regulations and policies. The software also takes advantage of advanced features such as secure viewer and dynamic security watermarks.
- **Audit & Report for Compliance** –Tracks user activity and the application of NC Protect encryption and security. Additionally, the software has alert features for non-compliant or risky user behavior that allows an organization to act before an incident occurs. Lastly, auditing and reporting features allow an organization to prove compliance with regulations.

Exhibit 4: NC Protect

NC Protect
In-transit Protection Across Microsoft Apps
Simpler. Faster. Cheaper.



IDENTIFY, CLASSIFY & SECURE SENSITIVE DATA	PROACTIVELY BLOCK & PROTECT INFORMATION	AUDIT & REPORT FOR COMPLIANCE
--	---	-------------------------------

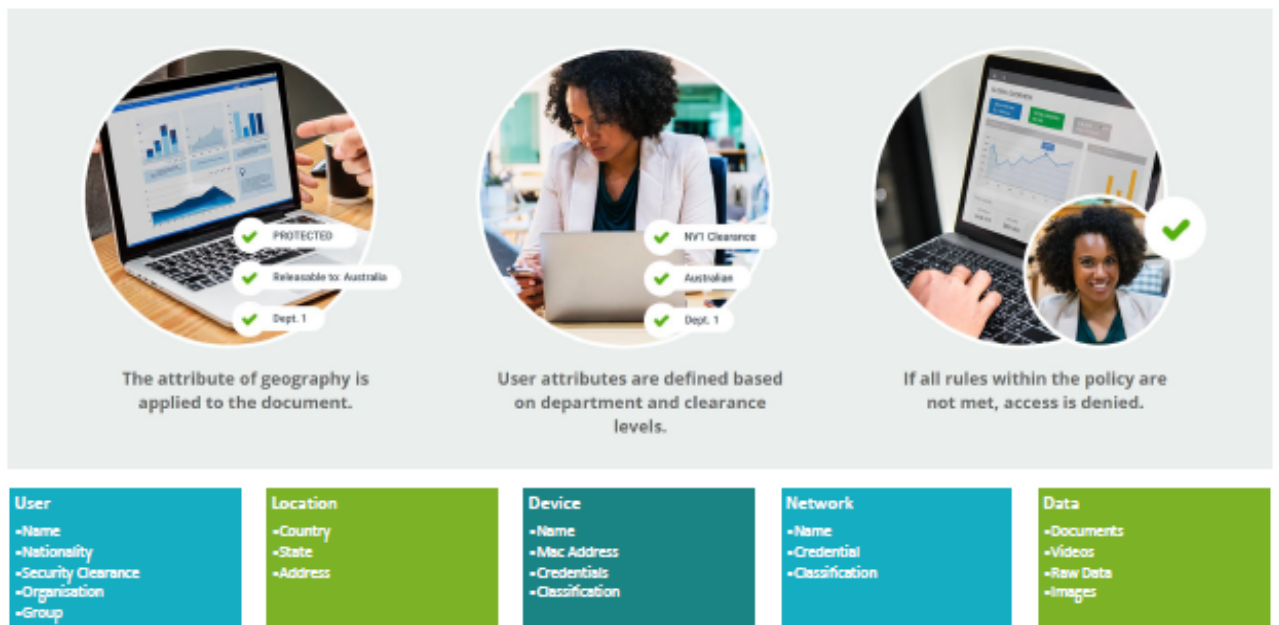
Technology Overview

Attribute Based Access Control (ABAC) underpins all of archTIS' products and services

archTIS differentiates itself from other security companies by employing a security method called Attribute Based Access Control (ABAC). ABAC is a security model that allows individuals to define rules to control who access information, and under what conditions.

As a result, the right people access the right information, at the right time. More specifically, the ABAC model works by applying attributes to documents and users. A dictionary of attributes is thus created to build precise access control policies.

Exhibit 5: How ABAC Works



We note that there are many cyber security firms which produce firewall, antivirus, anti-intrusion, or other anti-threat software solutions. But archTIS' solution is different because it protects an organization's information. Its policy enforcement or attribute-based access control allows the archTIS' software to present information in context of people's risk profile, and who, and where they are.

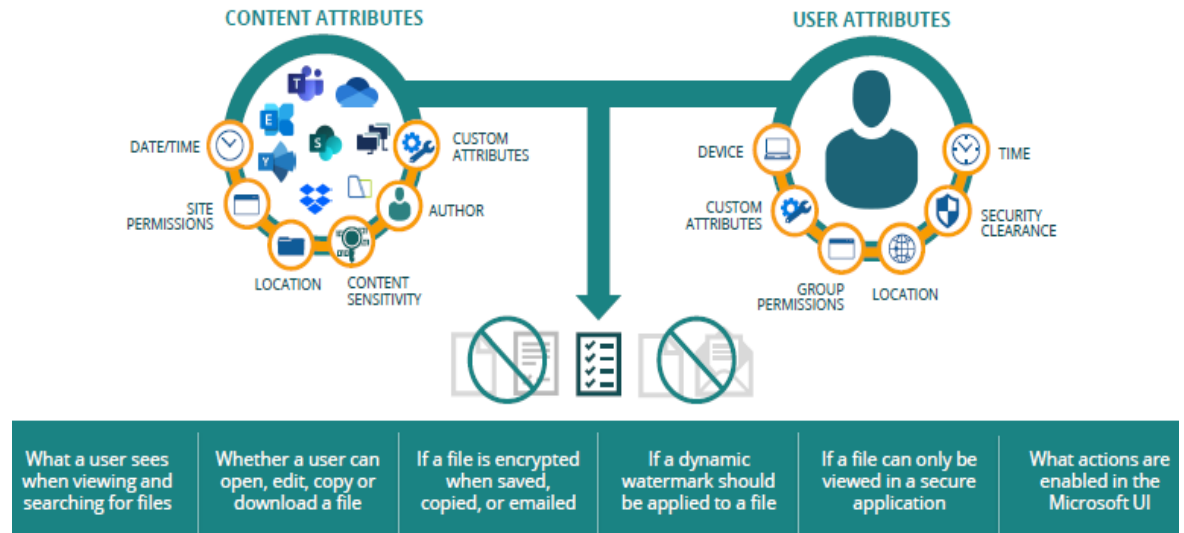
archTIS' ABAC automatically adjusts access and security policies using these real-time, attribute-based access and sharing control to:

- ✓ Limit what a user sees when viewing and searching files
- ✓ Control whether a user can open, edit, copy, or download a file
- ✓ Control if a file is encrypted when saved, copies, or emailed
- ✓ Determine if a dynamic watermark should be applied to a file
- ✓ Force a file to be viewed in a secure, read-only application
- ✓ Apply document expiration to limit access

The ABAC methodology ensures secure information access and sharing across government and industry.

This level of security allows governments, defense sector organizations, and public organizations to safely share and collaborate on information and ensure that the conditions set on access and sharing are enforced.

Exhibit 6: Real-time Access & Sharing Control of Information



Business Strategy & Model

archTIS’ is well positioned to be trusted to safeguard the world’s most sensitive information.

archTIS’ goal is to be the company that the world trusts with its most sensitive information. As such, the company is focused on unlocking the potential of an information-driven world by enabling trust. archTIS expects to achieve this mission by leading the world in developing and applying new security models and distributed security platforms that enable people, governments, and corporations to share and collaborate on their most valuable and sensitive information/content.

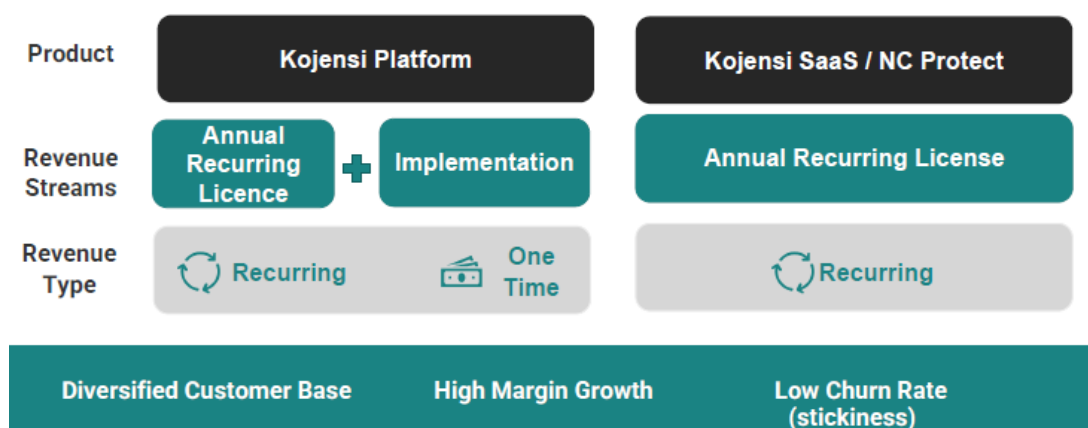
The company has also outlined its current strategic focus and outlook along three parameters including:

- 1. Financial**
 - a. Aggressively continue to drive triple digit recurring growth through annual recurring revenue
 - b. Aspirational gross margins at 70% or higher
 - c. Approach cash-flow neutral
- 2. Sales & Marketing**
 - a. Leverage key Australia government and defense wins into other regions
 - b. Focus on capturing global market share in more highly regulated industries
 - c. Expand global direct sales distribution to multiply pipeline volume
 - d. Continue significant alliance opportunities with Microsoft
- 3. Products & Operations**
 - a. Deliver product superiority across a data-centric approach to drive new customers and ensure low churn
 - b. Explore key acquisition opportunities of complementary technologies
 - c. Provide an innovative, exciting, and enjoyable experience for staff, partners, and customers

Business model is focused on driving annual recurring revenue.

The company’s business model is centered on driving annual recurring revenue. archTIS’ receives an upfront annual contract and associated licensing fees and recognizes this revenue over the period of the contract. Importantly, and as outlined in the business strategy, archTIS is driving a diversified customer base to eliminate any concentration in long-sales cycle government contracts. Additionally, because these are software sales, archTIS’ should be able to deliver high gross margins. And archTIS’ is targeting low-churn rates through the inherent stickiness of its software that is designed to protect the world’s most sensitive information.

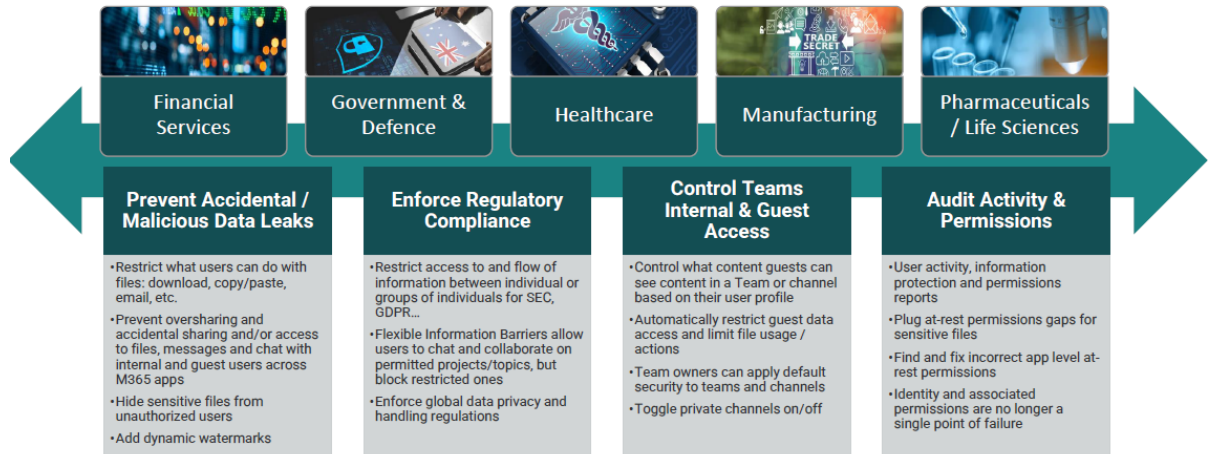
Exhibit 7: Annual Recurring Revenue Model



Sales & Marketing Strategy

archTIS is targeting industries with sensitive and highly regulated data. As a result, the company is targeting industries that include Financial Services, Government & Defence, Healthcare, Manufacturing, and Pharmaceuticals/Life Sciences. Given its differentiated software capabilities to secure information, it provides these industries with the ability to (1) prevent accidental/malicious data leaks; (2) enforce regulatory compliance; (3) control teams internal and guest access; and (4) audit activity and permissions.

Exhibit 8: archTIS' Target Markets



Following these target markets, archTIS' has closely aligned its licensing model with its product offerings and mapped those products to its target markets, key use cases, distribution channels, and opportunity size. Below in Exhibit 9, we illustrate the company's go-to market strategy.

Exhibit 9: Go-To-Market Strategy



Global distribution strategy supported by direct sales, global channel partners, and key strategic alliances.

archTIS' distribution strategy is based on a solid foundation of direct sales, indirect sales through key channel partners, and strategic alliances. archTIS' direct regional presence is spread through Asia Pac, the America's and EMEA. The company's indirect channel includes various system/defense integrators, and value-added resellers that are Microsoft certified, focused on the security vertical, and has a trusted advisor relationship with its customers. Enhancing the company's channel partnerships includes its strategic alliances with Microsoft, that co-sells NC Protect, and Thales S.A., and Raytheon.

Exhibit 10: Global Distribution Platform and Strategy



Merger with Nucleus Cyber immediately expanded archTIS' global footprint

Importantly, archTIS' merged with US based Nucleus Cyber in FY21 (announced Oct'20; closed Dec'20). The merger expanded archTIS' market opportunity and enabled the company to scale up through the expansion of a global sales distribution network, increased sales pipeline, and additional key alliance partnerships.

Cipherpoint acquisition is immediately accretive and further expands archTIS' global distribution platform

Additionally, in September 2021, archTIS' acquired Cipherpoint Technology's assets and customers. While the acquisition adds to the company's growing annual recurring revenue, and industry leading intellectual property, it also expanded archTIS' global distribution platform by expanding its presence in Europe (Cipherpoint's HQ) and Singapore, adding reseller NTT Data, and adding several government and defense agency customers.

Exhibit 11: Customer and Partners



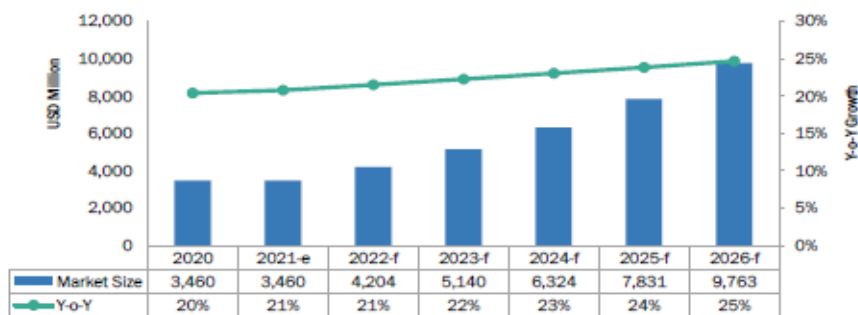
Market Overview

Data-Centric Security Market

On a daily basis, enterprises and government entities generate mountains of data in multiples formats, including structured (data that conforms to a data model; think databases), semi-structured, and unstructured (video, email, images, social media, PDFs). According to Accenture, almost 80% of data in enterprises is comprised of unstructured data. What’s more, Gartner forecasts this type of unstructured data is growing at 25% to 50% per year. Compounding the growth in data volume and variety, has been the dispersion of this data across on-premises and cloud IT environments. This explosion in data, the need for enterprises to collaborate on files/data/projects, coupled with an upsurge in the global growth of a remote workforce, is creating large challenges to enterprises to protect its valuable data from security breaches.

As a result of the above, data-centric cyber security solutions are gaining in popularity as a comprehensive way to protect strategic data to meet compliance protocols, and lock-guard the most critical/sensitive information. Importantly, data-centric solutions are concerned with privacy and security of data rather than the security of networks, endpoints, and applications. Given the growing instances of cyberattacks and data breaches, data-centric security solutions represent an essential tool in security portfolios.

Exhibit 12: Data-Centric Security Market Forecast

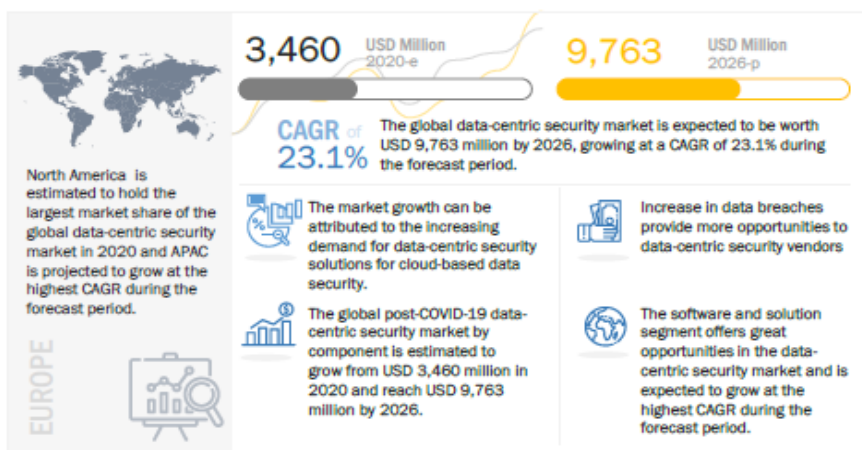


e: estimated; p: projected

Source: Secondary Research, Expert Interviews, and MarketsandMarkets Analysis

On a regional basis, North America is estimated at 35% of the total market, followed by Europe at 28%, Asia Pacific at 21%, Latin America at 11%, and the Middle East/Africa at 5%. Markets and Markets expects growth rates over the above forecast period in North America and Europe to grow at CAGRs of 20.2% and 25.0% respectively. APAC, Latin America, and MEA are expected to show CAGRs at 26.2%, 21.9%, and 19.1%, respectively.

Exhibit 13: Market Overview



Source: MarketsandMarkets Analysis

Global data growth is exploding, with unstructured data nearly 80% of total data, and growing at 25% to 50% per year.

The global data-centric security market is expected to be US\$9.8M by 2026, growing at a CAGR of 23.1%.

Drivers of data-centric security market include:

- ✓ Increasing usage of cloud IT environments
- ✓ Increasing compliance regimes and regulations
- ✓ Increasing risk of enterprise data exploitation due to big-data, machine learning, and AI

As such, the need to authentication users, maintain access controls, and encrypt data, should all drive the need for data-centric cyber security solutions such as archTIS’.

Cloud Adoption

Cloud infrastructure and adoption is growing. Furthermore, due to COVID-19, adoption of cloud technology accelerated as much of the world settled into a work-from-home model as social distancing became a necessity. According to commentary from Gartner in April 2021, world-wide spending on public cloud services is forecasted to grow 23.1% in 2021 and reach a level of US\$332.3B. Furthermore, Gartner predicts a 5-year CAGR of 16.1% until 2025. While this accelerated digital adoption is a positive to global enterprises, it also presents significant challenges.

With data growth exploding, coupled with cloud adoption, and increasing numbers in the remote workforce, data can flow anywhere and everywhere in the cloud. Enterprises of all sizes are finding an increasing need to secure its data in the cloud.

Heightened Regulations

Compliance regimes and increased regulations are at the forefront. All organizations must monitor, analyze, and get alerts on data access and movement of data that can potentially jeopardize the organization’s compliance with regulations. Increasing regulations, such as GDPR (General Data Protection Regulation (EU)), HIPAA (Health Insurance Portability & Accountability Act), PCI DSS (payment card industry data security standard), are all examples of the heightened regulatory environment around data protection and safeguarding data privacy. Noncompliance with regulations could result in significant monetary fines and brand/reputational damage.

Data Leaks

As mentioned, data creation is exploding and creating a need for organizations to store it. And most of this data is unstructured data that now resides or is pulled from the cloud. With an increasing amount of unstructured data, organizations are using new technologies to glean important information, such as big-data analytics, machine learning, and artificial intelligence. However, organizations must rely on outside technology vendors to deploy these technologies. These can all conspire to increase the risk of data leakage. According to Ponemon Institute’s “2020 Cost of Insider Threats Global Report,” 62% of data breaches involve employee or contractor negligence. Furthermore, the average cost of such a breach is estimated at US\$307,111 per incident for an average of US\$4.6M per year, per organization.

Gartner expects cloud spend to grow at a 5-year CAGR of 16.1% to reach US\$692.1M in 2025.

RSA survey shows 80% of people are concerned about their data and privacy.

62% of data breaches are employee or contractor negligence leading to an average cost per breach, per year, per organization of US\$4.6M.

Management Team

Daniel Lai
CEO & Managing Director

Mr. Lai is the CEO and Managing Director of archTIS. He has extensive industry experience in successfully delivering outcomes as part of a senior executive team to both government and commercial organizations. Most importantly, Mr. Lai has direct experience in implementing organizational change to address the real challenges business confront today in a rapidly evolving environment. Over his career, he has had many successes including leading the Security Enterprise Architecture for the Single Information Environment for the Department of Defense, leading enterprise change as the National Manager for Service Delivery for the Australian Customs and Border Protection service and restructuring and implementing enterprise ITIL services for the Australian Customs and Border Protection Service. Mr. Lai is a regular speaker at industry events and has been feature in the Financial Review and CIO magazine.

Kurt Mueffelmann
Global COO & US President

As Global COO and US President of archTIS and Nucleus Cyber, Mr. Mueffelmann brings over 25 years of technology leadership to the companies. He brings his passion for start-ups, and proven strategies for scaling go to market efforts and achieving hyper revenue growth to the role. Mr. Mueffelmann has overseen the growth and sale of four technology companies and earned two Deloitte Fast 500 company awards at previous companies. He has served as CEO of Cryptzone, HiSoftware (acquired by Cryptzone), Create!form International (acquired by Bottomline Technologies), and RealWord (acquired by Microsoft Great Plains). Mr. Mueffelmann was Vice President and General Manager of both the Document Output Solutions and Business Process Solutions divisions of Bottomline Technologies where he was responsible for over \$40 million in profitable revenue while broadening the product lines and expanding the distribution model. Mr. Mueffelmann has served on the advisory boards of numerous companies and professional organizations within the technology industry. He holds a BA degree in economics and political science from Fairfield University in Connecticut.

Kylie Sheather
Chief Financial Officer

Ms. Sheather is the Chief Financial Officer of archTIS. With extensive knowledge of software as a service companies, Ms. Sheather has held senior financial roles for medium and large listed companies. Ms. Sheather's strong project management, associated process re-engineering and change management skills support the Company's expansion goals. Ms. Sheather most recently served as TechnologyOne Director of Finance and Business Partnering. Her prior roles include Group Financial Controller at ASX-listed engineering services company LogiCamms and held a number of senior roles at Boom Logistics.

Leigh Rowland
Chief Engineer

As the Chief Engineer of archTIS and Nucleus Cyber, Mr. Rowland is responsible for driving the evolution of the company's technology to provide secure collaboration and seamless integration into supported platforms. Under his leadership, NC Protect has expanded from its core strength of protecting documents in SharePoint, to extend the same protection to cloud collaboration and storage repositories including SharePoint Online, Microsoft 365, Microsoft Teams, and Nutanix, as well as the protection of Exchange emails. He began his career at Xerox and has been involved in a series of successful startups as a consultant and development leader including Cyxtera, Cryptzone (acquire by Cyxtera), and Create!form International. He helped build and on-sell the businesses through a strong focus on innovative software solutions. His involvement with Security Sheriff began back in 2011 and he has continued to be involved in the design and development of the industry leading security solution. Mr. Rowland earned Bachelor of Science (Hons) in Mathematics from University of York.

Irena Mroz
Chief Marketing Officer

Ms. Mroz is CMO of archTIS and Nucleus Cyber. She is responsible for defining the company's branding, demand generation and public relations. An innovative strategist with impeccable attention to detail, Ms. Mroz leverages more than 20 years of B2B marketing expertise to direct the company's marketing strategy and communications programs. Ms. Mroz has built her successful career by empowering start-ups and public software companies to exceed growth objectives through successful demand generation programs, product positioning, high profile events and product evangelism. Most recently, Ms. Mroz was the VP of Marketing at Infocyte, a malware and threat hunting solution. She served as the SVP of Marketing for Cryptzone's network and application security solutions, and the VP of Marketing for HiSoftware, a provider of compliance and security solutions acquired by Cryptzone. She led the integration of the two global marketing organizations, while managing development of all strategic marketing programs and communications for the joint entity. Her previous roles include senior marketing positions at Bottomline Technologies and Create!form International. Ms. Mroz holds a Bachelor of Science in Mass Communications from Boston University's College of Communication.

Matthew Klukun
VP & General Manager Asia Pacific

Mr. Klukun has 27 years' experience in the Information and Communication Technologies Industry in Sales, Marketing, Technical and Customer Experience in Australian ICT and large multinational technology and advisory companies such as Gartner, NetApp, CA Technologies, and Oracle. As Vice President & General Manager Asia Pacific, Mr. Klukun's primary focus is building archTIS' presence with global Defense, Intelligence, Federal and State Governments and Defense Industry companies, as well as building and growing our partner eco-system supporting these markets, both within the Asia Pacific region.

Pete Smith
VP & General Manager EMEA

As Vice President & General Manager EMEA of archTIS and Nucleus Cyber, Mr. Smith brings over 30 years' experience in sales and management to the role, particularly with start-ups and emerging IT security brands. With a record of forging strong, long-term partnerships with customers and partners, Mr. Smith has successfully delivered dynamic growth across the EMEA region in a number of different market verticals at technology companies including OCR, Netwrix, Intalio, Cable & Wireless, and SonicWall amongst others. With a keen understanding of how best to harness cutting edge technology to its full advantage, Smith advises customers on how to anticipate changes, and stay one step ahead threats.

Competition

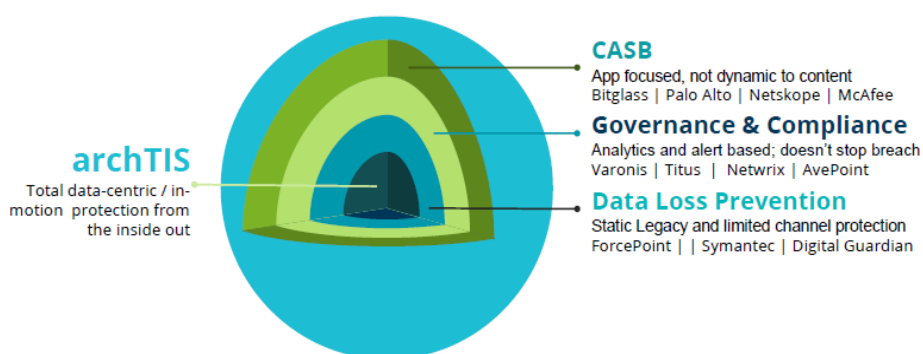
Highly differentiated solution by employing total data-centric, in-motion protection from the inside out.

We note that there are many cyber security firms which produce firewall, antivirus, anti-intrusion, or other anti-threat software solutions. But archTIS' solution is different because it protects an organization's information. Its policy enforcement or attribute-based access control allows the archTIS' software to present information in context of people's risk profile, and who, and where they are.

For example, if an employee logs onto her terminal using a public Wi-Fi network, the employee will only see unclassified information because the employer policy will say that the employee is logged into an untrusted pathway.

Exhibit 14: Competitive Differentiation

Proactive in-transit vs. Static after-the fact



Australian Department of Defense deployment shows technology validation

Importantly the company's products have some of the highest levels of accreditation, including from the US National Security Agency (NSA) and the Australian Signals Directorate. In fact, the Australian Department of Defense is using archTIS' Kojensi and NC Protect solutions. The FY21 contract is valued at AUD\$6.18M and is securing supply chain communications and securing and restricting access to highly sensitive files across multiple deployed SharePoint farms.

Competitor profiles are below:

Bitglass (Private) - Bitglass provides security solutions that automatically segments, tracks, and secures businesses' sensitive data across cloud and mobile without invading the employees' privacy. Its mobile security solutions offer alerts and insights into suspicious behavior, as well as warn clients of potential policy or security issues. The company's cloud solution enables users to track organization's sensitive data, including confidential files and corporate data through Internet, as well as alerts clients on policy violations, data leakage, and other security issues. Bitglass was founded in 2013 and is based in Campbell, California.

NextLabs, Inc. (Private) - NextLabs, Inc. provides information risk management software for large enterprises in financial services, aerospace and defense, design and manufacturing, high tech manufacturing, healthcare, and pharmaceuticals and life sciences industries. It offers NextLabs Enterprise Data Protection, an identity-aware endpoint software suite that discovers, classifies, monitors, protects, and manages sensitive data based on content, identity, and context; Compliant Enterprise, a content-aware entitlement management system that provides allows users to authorize, classify, enforce, and audit enterprise resources across Microsoft Sharepoint, File Servers, PLM, ERP applications, and custom applications; and NextLabs Control Center, a XACML-based policy management solution that offers versatile application development tools. The company also provides technology solutions, such as application and device

control, role-based access and document control, SharePoint information governance, endpoint data loss prevention, misdirected communications, hidden data removal, information barriers, file server entitlement management, unified communications control, intellectual property protection, file server access, audit and compliance, and information rights management. In addition, it offers professional services, and training and risk assessment services. The company was formerly known as Blue Jungle, Inc. NextLabs, Inc. was incorporated in 2003 and is based in San Mateo, California.

Netskope, Inc. (Private) – Netskope is a cloud application analytics and policy company. Its products and services safely and quickly connects users directly to the internet, any application, and their infrastructure from any device, on or off the network. With CASB, SWG, and ZTNA built natively in a single platform, the Netskope Security Cloud provides granular context, to enable conditional access and user awareness while enforcing zero trust principles across data protection and threat prevention everywhere. Netskope, Inc. was formerly known as Skope, Inc. and changed its name to Netskope, Inc. in November 2012. The company was founded in 2012 and is headquartered in Santa Clara, California.

Varonis Systems, Inc. (NASDAQ: VRNS) - Varonis Systems, Inc. provides software products and services that allow enterprises to manage, analyze, and secure enterprise data. Its software enables enterprises to protect data stored on premises and in the cloud, including sensitive files and emails; confidential personal data belonging to customers, and patients and employees' data; financial records; strategic and product plans; and other intellectual property. Varonis Systems was incorporated in 2004 and is headquartered in NY, New York.

TITUS, Inc. (a Help Systems Company; Private) - TITUS provides solutions that enable organizations to classify, protect, and confidently share information, and meet regulatory compliance requirements by identifying and securing unstructured data. It offers data identification, data loss prevention, intellectual property protection, insider threat prevention, privacy protection, mobile data security, cloud data security, encryption and rights management services, information lifecycle management, and SharePoint security solutions. The company also provides professional services and customer support and services. TITUS Inc. was formerly known as Titus Labs Inc. and changed its name to TITUS Inc. in 2010. The company was founded in 2005 and is based in Ottawa, Canada.

Netwrix Corporation (Private) - Netwrix develops IT auditing software. It operates the Netwrix Auditor Platform that focuses on audit data solutions for IT systems. The company provides security and compliance, content services, Information technology operations, and business continuity solutions. The company also provides data access, prepares reports for passing compliance audits, and increases the efficiency of IT operations. The company was founded in 2006 and is based in Irvine, California.

AvePoint, Inc. (NASDAQ: AVPT) – AvePoint provides Microsoft 365 data management solutions worldwide. It offers a suite of SaaS solutions to migrate, manage, and protect data. The company provides cloud solutions for Office 365, Salesforce, and Dynamics 365; and hybrid/on-prem products. It also offers advisory and implementation, maintenance and support, Microsoft Teams surge and advisory, migration as a service, and quick start services. The company was founded in 2001 and is headquartered in Jersey City, New Jersey

ForcePoint LLC (Private) - Forcepoint provides software solutions to protect users, data, and network against insider threats and outside attacks. It offers content security solutions that provides protection against multi-stage threats, data theft, and to reduce malware infections. The company provides insider threat data protection solutions. In addition, the company provides network security solutions to optimize and scale network security for distributed enterprises; and advanced analytics solutions,

Forcepoint LLC was formerly known as Raytheon|Websense and changed its name in January 2016. The company was founded in 2015 and is based in Austin, Texas.

Digital Guardian, Inc. (Private) - Digital Guardian designs and develops data security solutions to protect data from insider and outsider threats. It offers data loss prevention solution that automatically blocks and controls only those behaviors that pose a threat to organization based on the user, event, and data type. The company also provides professional services and training. The company was formerly known as Verdasys Inc. and changed its name to Digital Guardian, Inc. in August 2014. The company was founded in 2003 and is based in Waltham, Massachusetts.

Investment Risks

Technology risk

Technology markets are a continually evolving marketplace. To succeed, the company will need to research, develop, design, manufacture, assemble and bring to market new enhancements to its existing products as well as new products that are suitable for existing markets and new markets.

Sales and timing risks

The secure content and collaboration market is still evolving in response to market need. While market demand is growing, available secured sharing information solutions are limited, focused on solutions that use basic security but may not be accredited for higher levels of protections, which governments require. Additionally, government sales cycles can be lengthy.

Competition

The markets in which the company operates is particularly competitive. While the company will try to manage this risk with a targeted marketing strategy, competition may arise from several sources including companies with greater capital resources.

R&D and intellectual property risk

The company's products and its potential products are subject to continued R&D efforts. There is no guarantee that the company will be able to achieve its desired outcomes from its R&D. Furthermore, a substantial part of the company's commercial success will depend on its ability to maintain, establish, and protect its intellectual property, maintain trade secret protections, and operate without infringing the proprietary rights of third parties.

Reliance on third party sales channel

While the company has direct sales, it is also dependent on third party resellers, VARs, and system integrators. The company does not have direct control over these third-party entities and their sales efforts on behalf of the company.

Summary

archTIS designs, develops, and markets software solutions and services for secure information sharing and collaboration globally. The company's flagship solutions, Kojensi and NC Protect, enables organizations to share and collaborate on files in a secure space. Kojensi allows the sharing of sensitive and classified information securely, while NC Protect provides dynamic access and data protection for Microsoft 365 applications and file shares.

Large and expanding target market

Global data growth is exploding, with unstructured data at nearly 80% of total data, and growing at 25% to 50% per year. Compounding the growth in data volume and variety, has been the dispersion of this data across on-premises and cloud IT environments. This explosion in data, the need for enterprises to collaborate on files/data/projects, coupled with an upsurge in the global growth of a remote workforce, is creating large challenges to enterprises to protect its valuable data from security breaches.

As a result of the above, data-centric cyber security solutions are gaining in popularity as a comprehensive way to protect strategic data to meet compliance protocols and lock-guard the most critical/sensitive information. The data-centric security market is expected to grow at a 23.1% CAGR to US\$9.8B by 2026. Driving growth is an increasing number of high-cost data breaches, an increase in cloud-based data security needs, coupled with the need to better secure remote employees' work and access to information.

Unique technology underpins patented software platform and drives differentiation

archTIS differentiates itself from other security companies by employing a security method called Attribute Based Access Control (ABAC). ABAC is a security model that allows individuals to define rules to control who accesses information, and under what conditions. The ABAC enforces zero trust at the perimeter and at the data layer.

While there are many cyber security firms which produce firewall, antivirus, anti-intrusion, or other anti-threat software solutions, archTIS' solution is different because it protects an organization's information. Its policy enforcement or ABAC allows archTIS' software to present information in context of people's risk profile, and who, and where they are. Importantly, the security platform is patent protected.

Proven technology platforms poised to take market share

archTIS' software solutions are patented, data-centric cyber security software that enables secure information sharing and inter-organization collaboration anywhere and on any platform. Kojensi is a multi-government certified platform for the secure access, sharing and collaboration of sensitive and classified information. NC protect provides dynamic access and enhanced data protection for file access and sharing, messaging, and emailing sensitive and classified information/content across Microsoft 365 applications, Dropbox, Nutanix Files, and Windows file shares.

Importantly, archTIS' goal is to be the company that the world trusts with its most sensitive information. As such, the company is focused on unlocking the potential of an information-driven world by enabling trust. The company expects to achieve this mission by leading the world in developing and applying new security models and distributed security platforms that enable people, governments, and corporations to share and collaborate on their most valuable and sensitive information/content securely.

Global sales network and key strategic partnerships to drive growth

archTIS' distribution strategy is based on a solid foundation of direct sales, indirect sales through key channel partners, and strategic alliances. The company's direct regional presence is spread through Asia Pac, the America's and EMEA. The company's indirect channel includes various system/defense integrators, and value-added resellers that are Microsoft certified, focused on the security vertical, and has a trusted advisor relationship with its customers. Enhancing the company's channel partnerships includes key strategic alliances with Microsoft, that co-sells NC Protect, and Thales S.A., and Raytheon.

Solid FY21 performance drives cash flows and solid balance sheet

archTIS' business model is based on driving annual recurring revenue (ARR) from licensing its software solutions. Given the inherent nature of software sales, archTIS' should be able to deliver high gross margins. Furthermore, archTIS' is targeting low-churn rates through the inherent stickiness of its software that is designed to protect the world's most sensitive information.

archTIS' business model appears to be working as evidenced by its FY21 results, where the company saw record breaking financial results. Of note, the company saw FY21 y/y growth in revenue, ARR, and EBITDA of 743%, 681%, and 44%, respectively. Furthermore, the company saw cash receipts from customers increase 846% y/y. As a result, the company saw a healthy cash balance of AUD\$12.7M as of June 2021.

Income Statement

For the Fiscal Period Ending	Restated 12 months Jun-30-2018	12 months Jun-30-2019	12 months Jun-30-2020	12 months Jun-30-2021
Currency	AUD	AUD	AUD	AUD
Revenue	0.574	1.022	0.549	4.627
Other Revenue	-	-	-	-
Total Revenue	0.574	1.022	0.549	4.627
Cost Of Goods Sold	0.001	0.228	0.304	1.544
Gross Profit	0.572	0.795	0.245	3.083
Selling General & Admin Exp.	2.956	5.004	4.641	8.055
R & D Exp.	-	-	-	-
Depreciation & Amort.	-	-	-	-
Other Operating Expense/(Income)	-	-	-	-
Other Operating Exp., Total	2.956	5.004	4.641	8.055
Operating Income	(2.383)	(4.209)	(4.396)	(4.972)
Interest Expense	-	-	-	-
Interest and Invest. Income	0.008	0.079	0.007	0.003
Net Interest Exp.	0.008	0.079	0.007	0.003
Other Non-Operating Inc. (Exp.)	0.22	0.292	0.664	1.54
EBT Excl. Unusual Items	(2.155)	(3.839)	(3.725)	(3.429)
Impairment of Goodwill	-	-	-	-
Other Unusual Items	-	-	-	0.094
EBT Incl. Unusual Items	(2.155)	(3.839)	(3.725)	(3.334)
Income Tax Expense	(0.009)	0.093	-	(0.343)
Earnings from Cont. Ops.	(2.146)	(3.932)	(3.725)	(2.991)
Earnings of Discontinued Ops.	-	-	-	-
Extraord. Item & Account. Change	-	-	-	-
Net Income to Company	(2.146)	(3.932)	(3.725)	(2.991)
Minority Int. in Earnings	-	-	-	-
Net Income	(2.146)	(3.932)	(3.725)	(2.991)
Pref. Dividends and Other Adj.	-	-	-	-
NI to Common Incl Extra Items	(2.146)	(3.932)	(3.725)	(2.991)
NI to Common Excl. Extra Items	(2.146)	(3.932)	(3.725)	(2.991)
Per Share Items				
Basic EPS	(0.04)	(0.03)	(0.03)	(0.01)
Basic EPS Excl. Extra Items	(0.04)	(0.03)	(0.03)	(0.01)
Weighted Avg. Basic Shares Out.	55.228	119.993	126.673	201.344
Diluted EPS	(0.04)	(0.03)	(0.03)	(0.01)
Diluted EPS Excl. Extra Items	(0.04)	(0.03)	(0.03)	(0.01)
Weighted Avg. Diluted Shares Out.	55.228	119.993	126.673	201.344
Normalized Basic EPS	(0.02)	(0.02)	(0.02)	(0.01)
Normalized Diluted EPS	(0.02)	(0.02)	(0.02)	(0.01)

Balance Sheet

Balance Sheet as of:	Restated Jun-30-2018	Jun-30-2019	Jun-30-2020	Jun-30-2021
Currency	AUD	AUD	AUD	AUD
ASSETS				
Cash And Equivalents	1.639	3.255	2.429	12.739
Short Term Investments	0.057	-	-	-
Total Cash & ST Investments	1.696	3.255	2.429	12.739
Accounts Receivable	0.043	0.094	0.041	0.574
Other Receivables	0.976	1.562	0.091	0.001
Notes Receivable	-	-	-	-
Total Receivables	1.018	1.657	0.132	0.575
Prepaid Exp.	0.109	0.055	0.062	0.276
Other Current Assets	-	0.059	0.946	1.488
Total Current Assets	2.824	5.025	3.568	15.078
Gross Property, Plant & Equipment	0.429	0.449	2.282	1.623
Accumulated Depreciation	(0.275)	(0.342)	(1.19)	(0.423)
Net Property, Plant & Equipment	0.153	0.107	1.092	1.2
Goodwill	-	-	-	2.75
Other Intangibles	3.06	4.383	4.261	10.959
Deferred Tax Assets, LT	0.093	-	-	0.264
Deferred Charges, LT	-	-	-	-
Other Long-Term Assets	-	-	0.0	-
Total Assets	6.129	9.516	8.922	30.251
LIABILITIES				
Accounts Payable	0.173	0.193	0.118	0.634
Accrued Exp.	0.678	0.579	0.332	0.602
Short-term Borrowings	0.3	-	-	-
Current Portion of Leases	-	-	0.116	0.144
Unearned Revenue, Current	-	-	0.178	3.705
Other Current Liabilities	0.108	0.064	0.023	0.371
Total Current Liabilities	1.259	0.835	0.767	5.455
Long-Term Leases	-	-	1.241	0.936
Pension & Other Post-Retire. Benefits	0.038	0.019	0.028	0.058
Def. Tax Liability, Non-Curr.	-	-	-	1.663
Other Non-Current Liabilities	0.073	0.073	0.074	2.495
Total Liabilities	1.37	0.927	2.111	10.608
Common Stock	7.467	15.467	17.718	34.015
Additional Paid in Capital	-	-	-	-
Retained Earnings	(2.795)	(6.726)	(10.71)	(13.702)
Treasury Stock	-	-	-	-
Comprehensive Inc. and Other	0.088	(0.152)	(0.196)	(0.67)
Total Common Equity	4.759	8.589	6.811	19.643
Total Equity	4.759	8.589	6.811	19.643
Total Liabilities and Equity	6.129	9.516	8.922	30.251

Cash Flow

For the Fiscal Period Ending	Restated 12 months Jun-30-2018	12 months Jun-30-2019	12 months Jun-30-2020	12 months Jun-30-2021
Currency	AUD	AUD	AUD	AUD
Net Income	(2.146)	(3.932)	(3.725)	(2.991)
Depreciation & Amort.	0.061	0.068	0.209	0.2
Amort. of Goodwill and Intangibles	-	-	-	0.177
Depreciation & Amort., Total	0.061	0.068	0.209	0.377
Other Amortization	-	0.116	0.671	1.347
(Gain) Loss from Sale Of Assets	-	-	-	-
Asset Write-down & Restructuring Costs	0.157	0.784	-	-
Stock-Based Compensation	0.469	0.376	0.09	0.036
Other Operating Activities	0	0.001	-	(0.479)
Change in Acc. Receivable	0.202	0.066	(0.004)	(0.428)
Change In Inventories	-	-	-	-
Change in Acc. Payable	(0.638)	(0.024)	(0.274)	(0.288)
Change in Unearned Rev.	-	-	0.178	2.912
Change in Inc. Taxes	(0.303)	(0.521)	0.609	(0.343)
Change in Other Net Operating Assets	(1.441)	(2.482)	(0.593)	(0.669)
Cash from Ops.	(3.641)	(5.549)	(2.838)	(0.526)
Capital Expenditure	(0.044)	-	(0.004)	(0.104)
Sale of Property, Plant, and Equipment	-	0.024	-	-
Cash Acquisitions	-	-	-	-
Divestitures	-	-	-	-
Invest. in Marketable & Equity Securities	-	-	-	-
Net (Inc.) Dec. in Loans Originated/Sold	-	-	-	-
Other Investing Activities	-	-	-	-
Cash from Investing	(0.044)	0.024	(0.004)	(0.104)
Short Term Debt Issued	-	-	-	-
Long-Term Debt Issued	-	-	-	-
Total Debt Issued	-	-	-	-
Short Term Debt Repaid	-	(0.3)	-	-
Long-Term Debt Repaid	-	-	(0.102)	(0.077)
Total Debt Repaid	-	(0.3)	(0.102)	(0.077)
Issuance of Common Stock	6.225	8.826	2.117	11.199
Total Dividends Paid	-	-	-	-
Special Dividend Paid	-	-	-	-
Other Financing Activities	(0.691)	(1.442)	-	(0.497)
Cash from Financing	5.534	7.083	2.015	10.625
Foreign Exchange Rate Adj.	-	-	-	(0.016)
Misc. Cash Flow Adj.	-	-	-	0.331
Net Change in Cash	1.849	1.559	(0.827)	10.311

Ratios

For the Fiscal Period Ending	12 months Jun-30-2018	12 months Jun-30-2019	12 months Jun-30-2020	12 months Jun-30-2021
Profitability				
Return on Assets %	(32.7%)	(33.6%)	(29.8%)	(15.9%)
Return on Capital %	(44.8%)	(38.6%)	(32.8%)	(21.5%)
Return on Equity %	(75.8%)	(58.9%)	(48.4%)	(22.6%)
Return on Common Equity %	(75.8%)	(58.9%)	(48.4%)	(22.6%)
Margin Analysis				
Gross Margin %	99.7%	77.7%	44.6%	66.6%
SG&A Margin %	515.1%	489.5%	845.7%	174.1%
EBITDA Margin %	NM	NM	NM	(102.9%)
EBITA Margin %	NM	NM	NM	(103.6%)
EBIT Margin %	NM	NM	NM	(107.4%)
Earnings from Cont. Ops Margin %	NM	NM	NM	(64.7%)
Net Income Margin %	NM	NM	NM	(64.7%)
Net Income Avail. for Common Margin %	NM	NM	NM	(64.7%)
Normalized Net Income Margin %	(234.8%)	(234.7%)	NM	(46.3%)
Levered Free Cash Flow Margin %	(264.7%)	(278.8%)	(243.2%)	43.5%
Unlevered Free Cash Flow Margin %	(264.7%)	(278.8%)	(243.2%)	43.5%
Asset Turnover				
Total Asset Turnover	0.1x	0.1x	0.1x	0.2x
Fixed Asset Turnover	3.5x	7.9x	0.9x	4.0x
Accounts Receivable Turnover	4.8x	14.9x	8.1x	15.0x
Inventory Turnover	NA	NA	NA	NA
Short Term Liquidity				
Current Ratio	2.2x	6.0x	4.7x	2.8x
Quick Ratio	2.2x	5.9x	3.3x	2.4x
Cash from Ops. to Curr. Liab.	NM	NM	NM	NM
Avg. Days Sales Out.	76.1	24.5	45.3	24.3
Avg. Days Inventory Out.	NA	NA	NA	NA
Avg. Days Payable Out.	NM	293.1	186.8	88.8
Avg. Cash Conversion Cycle	NA	NA	NA	NA
Long Term Solvency				
Total Debt/Equity	6.3%	NA	19.9%	5.5%
Total Debt/Capital	5.9%	NA	16.6%	5.2%
LT Debt/Equity	NA	NA	18.2%	4.8%
LT Debt/Capital	NA	NA	15.2%	4.5%
Total Liabilities/Total Assets	22.3%	9.7%	23.7%	35.1%
EBIT / Interest Exp.	NA	NA	NA	NA
EBITDA / Interest Exp.	NA	NA	NA	NA
(EBITDA-CAPEX) / Interest Exp.	NA	NA	NA	NA
Total Debt/EBITDA	NM	NA	NM	NM
Net Debt/EBITDA	NM	NM	NM	NM
Total Debt/(EBITDA-CAPEX)	NM	NA	NM	NM
Net Debt/(EBITDA-CAPEX)	NM	NM	NM	NM
Altman Z Score	(1.52)	8.22	0.8	2.92

Disclaimer

This report has been prepared by Viriathus Holdings LLC, Viriathus Research, LLC Series (“Viriathus Research”) based upon information provided by the Company. Viriathus Research has not independently verified such information and cannot guarantee the total accuracy of the information in this report. This is not a research report under NASD Rule 2711 and has not been prepared by Viriathus Capital LLC Series. Viriathus Research has been compensated for the authoring of this report. This report is not directed to, or intended for distribution to or use by, any person or entity who is a citizen or resident of or located in any locality, state, country, or other jurisdiction where such distribution, publication, availability or use would be contrary to law or regulation or which would subject Viriathus Research, its subsidiaries, or its affiliates (“Viriathus”) to any registration or licensing requirement within such jurisdiction. Some of the information in this report relates to future events or future business and financial performance. Such statements constitute forward-looking information within the meaning of the Private Securities Litigation Act of 1995. This report is published solely for information purposes and is intended to provide investors and interested parties with a fundamental understanding of the company covered herein including the company’s technology, business model, financial condition, and business prospects. It is not intended as an offer or a solicitation with respect to the purchase or sale of a security, and it should not be interpreted as such. Past performance does not guarantee future performance. Viriathus will not treat recipients as its customers by virtue of their receiving this report. Affiliates of Viriathus Research do and seek to do business with companies covered in its informational reports. Viriathus Research and its clients, affiliates, and employees, may, from time to time, have long or short positions in, buy or sell, and provide investment advice with respect to, the securities and derivatives (including options) thereof, of companies mentioned in this report and may increase or decrease those positions or change such investment advice at any time. Viriathus Research is not registered as a securities broker-dealer or an investment adviser either with the U.S. Securities and Exchange Commission or with any state securities regulatory authority.

› VIRIATHUS is a registered mark of Viriathus Holdings LLC.

› Viriathus Research LLC, 2021. All rights reserved. Any unauthorized use, duplication or disclosure is prohibited by law and will result in prosecution.

Financial data provided by: 

Historical Equity Pricing Data supplied by: 