



TRUSTED TO SAFEGUARD THE WORLD'S
MOST SENSITIVE INFORMATION

March 2026 Quarterly Report

Q3 FY26



Daniel Lai
Managing Director
& CEO



Kurt Mueffelmann
Global COO
& US President

Disclaimer

No Warranties

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.

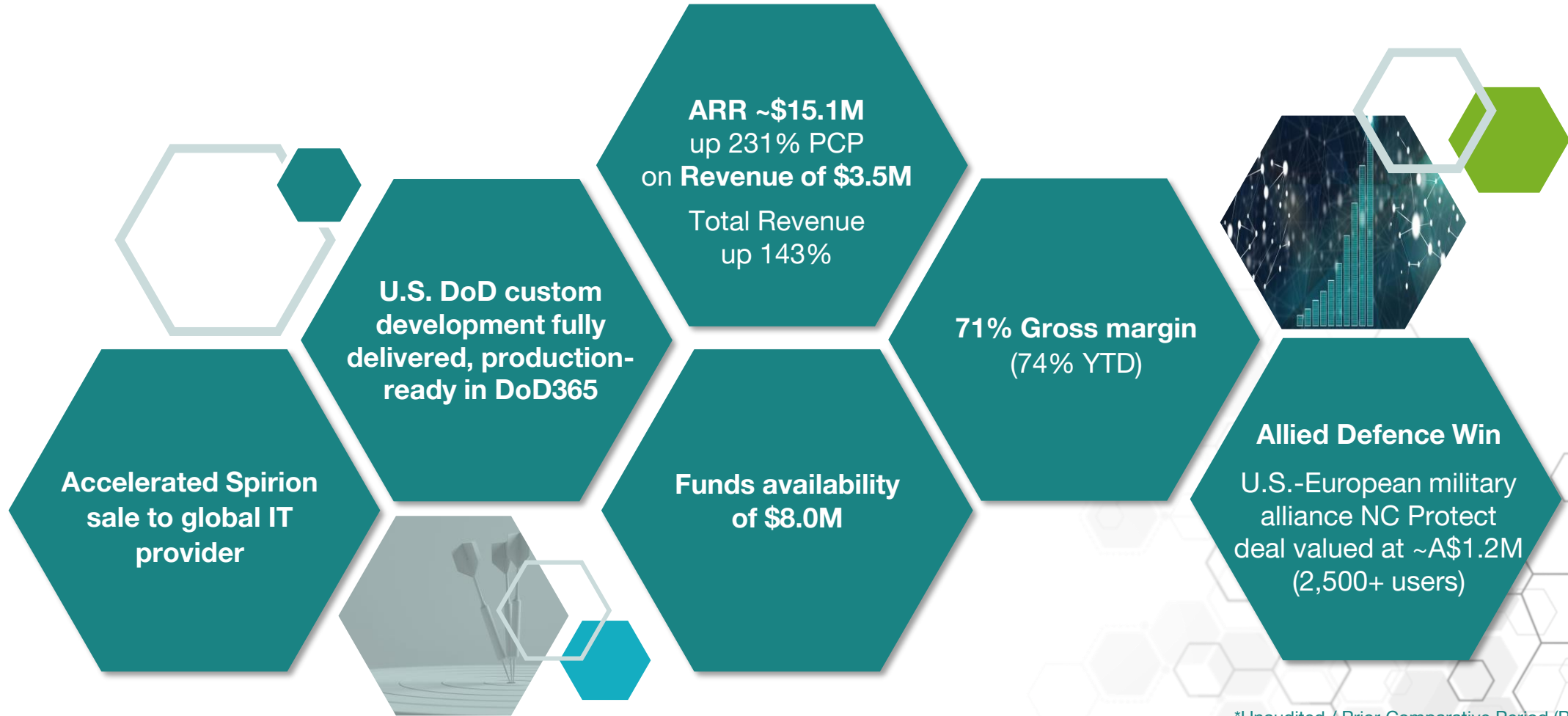
This presentation is not financial product or investment advice. It does not take into account the investment objectives, financial situation and particular needs of any investor. Before making an investment in the Company, an investor or prospective investor should consider whether such an investment 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.

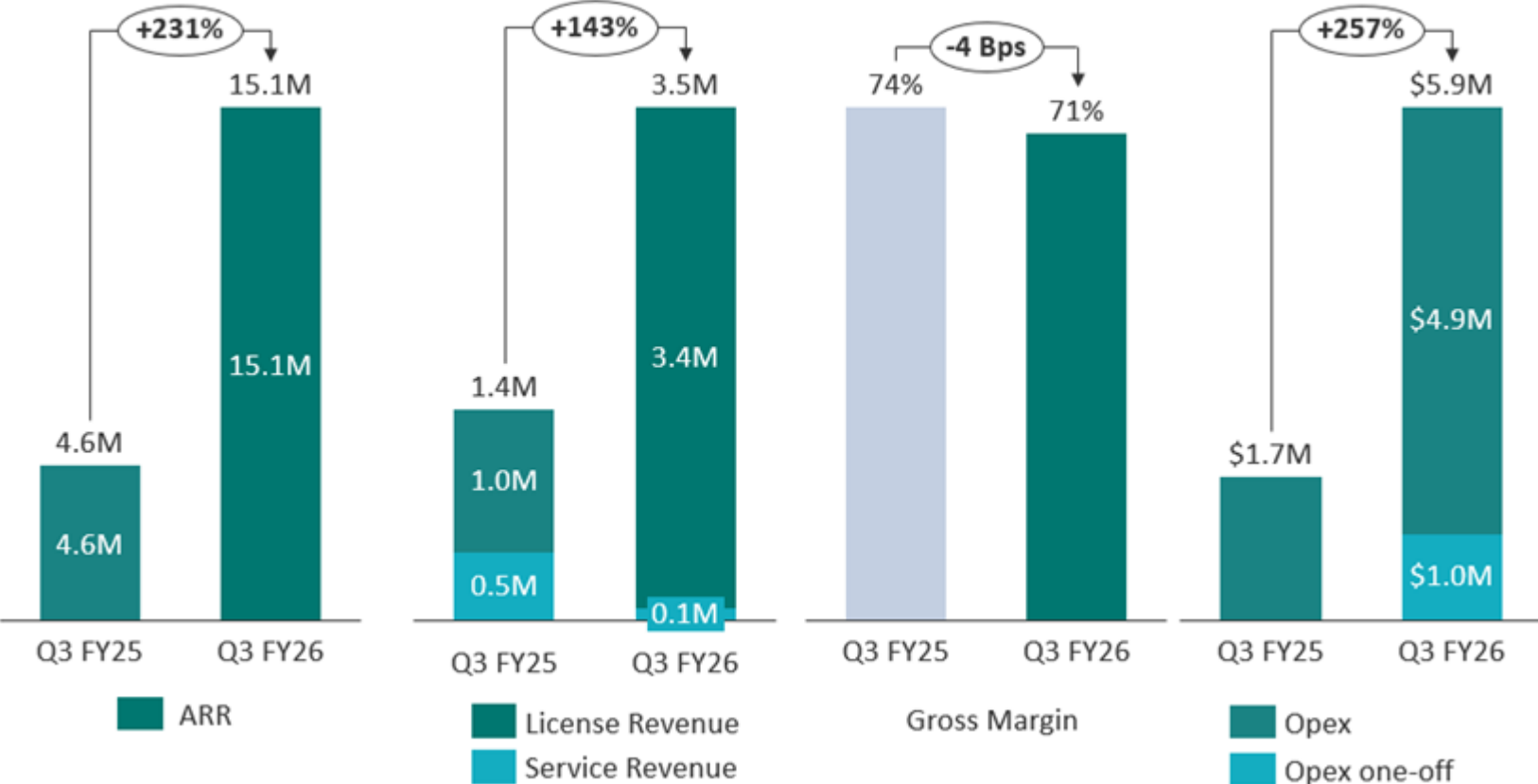
Q3 FY26 Quarterly Highlights

U.S. DoD Project Delivered, 231% ARR Growth, Allied Defence Wins



*Unaudited / Prior Comparative Period (PCP)

Q3 FY26 Financial Overview



Q3 FY26

ARR **\$15.1M**

Revenue **\$3.5M**
(+143% PCP)

Gross Margin **71% (74% YTD)**

Operating Expense **\$4.9M**
(excl. \$1M one-off costs)

Operating Cashflow **(\$3.7M)**

Cash & Equivalents **\$8.0M**

**Unaudited results*

Supporting Global Scalability and Growth



>> U.S. DoD & Allied Defence Momentum

- U.S. DoD custom software development project fully delivered and production-ready in DoD365 with technical road map alignment
- Engagement and technical validation advancing; procurement timelines extended by heightened military activity, with backlog conversion expected as funding normalises
- U.S.-European military alliance NC Protect contract win - 2,500+ users, ~A\$1.22M total contract value with two-year extension options

>> New Cross-Product Development, Wins & Renewals



- NC Protect AI integration for a **global manufacturing customer**. This integration will enable real-time, attribute-based access controls to be enforced directly within AI-powered search and knowledge discovery workflows
- New Spirion customer win (~\$145K) closed on a 60-day sales cycle with a global IT provider (US/UK)
- UK division for global aerospace and defence

Market Validation: Why Now Is the Right Time

Microsoft Just Defined the Gap

- Microsoft launched ZT4AI at RSA 2026 — 700 controls, a new AI pillar, and expanded Zero Trust framework. The framework is complementary, not competitive.
- Fine-grained, real-time ABAC across multi-cloud, classified, and sovereign environments is the gap they left for partners. That is archTIS.

Data Security Posture Management (DSPM) Is the #1 Fastest-Growing Security Category

- \$2.05B market today → \$10.4B by 2030. 38% CAGR (MarketsandMarkets).
- CISOs consolidating to trusted platforms, not best-of-breed point solutions.
- archTIS is uniquely positioned: Microsoft-native, deterministic ABAC, defence-cleared, and the only vendor combining discovery + enforcement + orchestration in the customer's own tenant.

RSA 2026 Confirmed the Data Security Policy Orchestration (DSPO) Category Is Forming

- *"Orchestration layer is the new center of gravity."* - William Blair
- CrowdStrike, Palo Alto, Netskope, and Check Point all entered AI governance in 2025–26.
- The category is forming in real time. The 12-18-month window to establish DSPO as a recognized category is open now.

3 Horizons for Growth

HORIZON

01 >>

Defend and Extend the Base

—
Sell existing products in Defence and Regulated Industries while expanding our strategic accounts

HORIZON

02 >>

Platform Solution & Policy Orchestration

—
Market expansion
Selling an integrated product platform

HORIZON

03 >>

Data Security Policy Orchestration (DSPO) & Innovation

—
Our products are all built on a single platform within module structures, increasing TAM and margins to drive shareholder value.

Overlapping Horizons Across 0-18 month Timeframe

U.S.-DoD
NATO
Microsoft co-sell
Spirion cross-sell

U.S.-DoD expansion
NEC
UK-MOD
DIB Supply Chain
Regulated industries

Repeatability that commercialises and scales the platform control plane while leveraging AI

Microsoft Validates Our Market

*"Agents that are overprivileged, manipulated, or misaligned can act like **double agents**, working against the very outcomes they were built to support."*

— Microsoft Security Blog, March 19, 2026

Microsoft Principle



Verify Explicitly

Evaluate identity and behavior of AI agents



Least Privilege

Restrict access to models, prompts, data



Assume Breach

Design for prompt injection, data poisoning

archTIS / DSPO Answer



NC Protect

ABAC evaluates user + agent + data attributes in real time



DSPO

Dynamic policy orchestration enforces least privilege across environments



Circuit Breaker

Real-time enforcement stops compromised agents mid-action

DSPO Vision and Strategy

archTIS must provide the **policy enforcement layer for Zero Trust data**, turning data discovery, classification, and risk into **real-time, enforceable access decisions across any platform.**

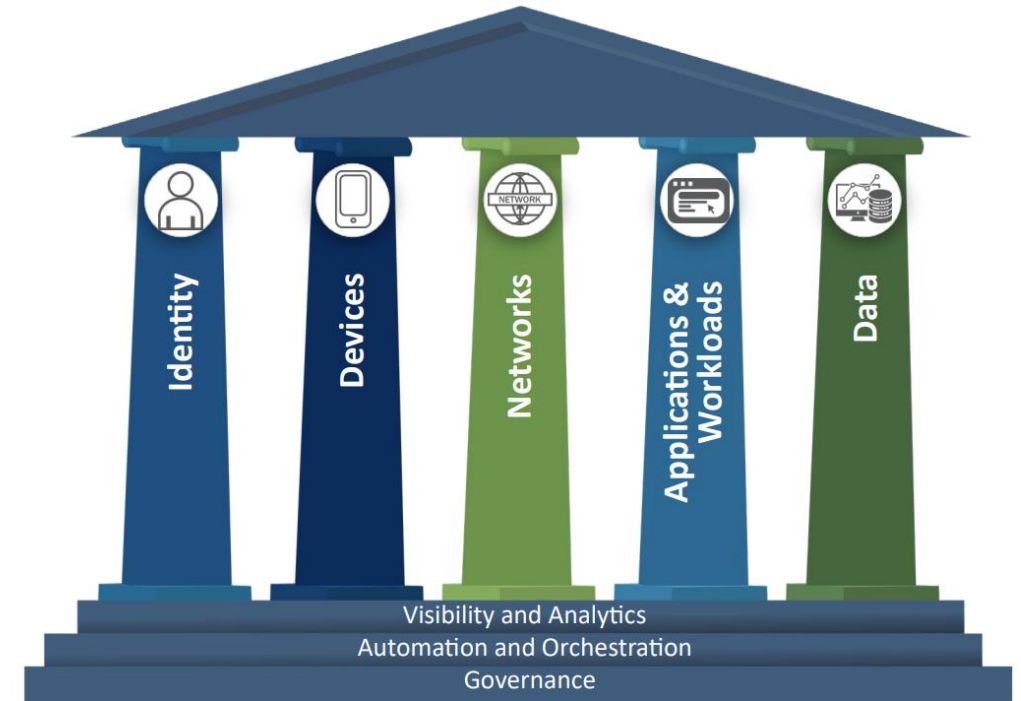
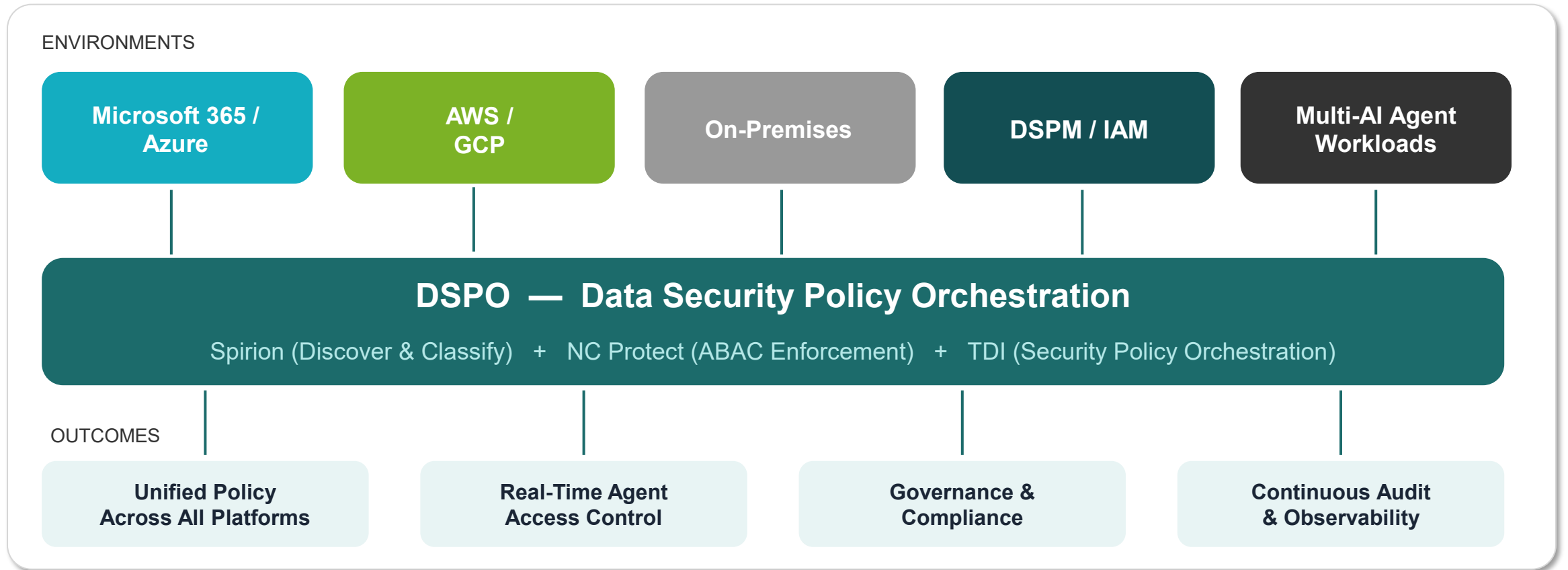


Figure 1: Zero Trust Maturity Model Pillars⁸

CISA's ZTMM is one of many paths to support the transition to zero trust.

Cross-Platform Control Plane

Position DSPO as the policy orchestration control plane that works across every platform — not just Microsoft's.



Where the Revenue Sits

The money is in what regulated customers need.



Cross-Platform DSPO

Gov customers on Azure + AWS + on-prem classified need one policy engine across all. Microsoft will never build this.

Large — recurring, sticky



ABAC for AI Agent Governance / Guardrails

Microsoft's agent controls are identity-centric (Entra) and network-centric (Defender). Real-time data-level access control for agents = NC Protect.

High growth — greenfield



Sovereign Compliance & Audit

Five Eyes / defense / intel communities need Kojensi + NC Protect credibility that Microsoft can reference but can't replicate.

Premium — high margin

60-day Priorities

- **Progress and convert U.S. DoD engagements** while advancing key strategic pipeline opportunities across defense, government, and priority enterprise accounts
- **Drive continued cost efficiencies** through operational optimisation, improved resource alignment, and disciplined expense management across the business
- **Expand U.S. operational focus**, strengthening market presence, deepening customer engagement, and broadening access across government, defense, and regulated commercial sectors
- **Advance delivery of core product capabilities and AI-driven features** to the market



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