

12 October 2026

QUIXXI ACQUISITION COMPLETE: HOW QUIXXI EXTENDS WHITEHAWK INTO AI GOVERNANCE AND AI CYBER SECURITY

Highlights

- Shareholders have strongly endorsed the Quixxi acquisition, with all resolutions passed by poll at the Extraordinary General Meeting held on 8 October 2026 and each receiving more than 95% of votes cast in favour by non-associated shareholders.
- Five illustrative stories show how the combined WhiteHawk and Quixxi portfolio is now positioned to address AI governance, AI security and mobile app risks across financial services, banking and fintech, defence and government supply chains, professional services and education, including industry sectors new to WhiteHawk.
- Quixxi's Clarity AI, PromptGuard, Scan, Shield and Supervise products extend WhiteHawk's existing platform, adding new markets alongside Cyber Resilience: AI Governance and AI Cyber Security.
- On 1 October 2026 it was announced that Quixxi's Clarity AI platform was selected for a four-year binding contract with a major Italian industrial group worth A\$635,237.96 from 1 November 2026. DoxAI Australia led the customer engagement and will provide its automation solutions. Quixxi will provide Clarity AI.

Sydney, NSW and Virginia, USA - WhiteHawk Limited (ASX: WHK) ("WhiteHawk" or "the Company") is pleased to advise that the acquisition of Quixxi Pty Ltd ("Quixxi") is now complete, having met the completion requirements of the share sale agreement as announced on 13 April 2026.

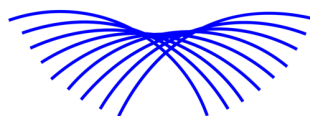
Adrian Vallino, Group CEO, said:

"I thank shareholders for their support of the Quixxi acquisition. With that approval, our focus moves from the case for the transaction to delivering on it."

The opportunity is straightforward. Organisations are adopting AI faster than they can govern or secure it, while Boards and regulators are increasingly demanding greater visibility, accountability and evidence. WhiteHawk already works with the risk, compliance and executive buyers responsible for these decisions. Quixxi adds complementary products, an international customer base and new opportunities across multiple sectors and use cases beyond our existing cyber resilience business. The five illustrative (fictional) stories in this announcement show how these combined capabilities can be applied in practice."

New Markets, Expanding Capabilities

On 13 April 2026, WhiteHawk announced its agreement to acquire Quixxi Pty Ltd, extending the Company into two new markets: AI Governance and AI Cyber Security. Shareholders approved the transaction at the Extraordinary General Meeting on 8 October 2026, as set out in the results of meeting announcement released to ASX on 8 October 2026. The terms of the transaction are set out in the Notice of Meeting and the Independent Expert's Report.



Quixxi's capabilities complement and extend WhiteHawk's existing Cyber Risk Program, Cyber Risk Radar and Cyber Analyst Platform as a Service via their established international customer base spanning central banks, commercial banks, insurers, fintechs, telecommunications providers and government entities; approximately A\$575,000 in FY25 revenue; a platform built on SOC 2 Type II foundations.

Quixxi capability	What it does	How it extends WhiteHawk
Clarity AI	AI inventory including AI risk and maturity assessment, governance workflows, AI framework alignment, and Board and regulator reporting	Adds AI risk to the Cyber Risk Program and Cyber Risk Radar
PromptGuard	Safeguards how staff use generative AI, keeping sensitive data out of prompts	Extends protection to everyday AI use, mitigating risk and reputational damage
Quixxi Scan	Static, dynamic and API vulnerability testing of applications; its dynamic application security testing (DAST) technology is the subject of one of Quixxi's two U.S. patent applications	Complements Cyber Analyst Platform as a Service
Quixxi Shield	Runtime protection against app cloning and tampering	New mobile security product line
Quixxi Supervise	Continuous monitoring of live threats against apps in the field	Extends continuous monitoring to mobile apps

Why the Acquisition Strengthens WhiteHawk

- **It builds on relationships we already have.** AI governance is typically procured by the same risk, compliance and executive buyers who use WhiteHawk's Cyber Risk Program and Cyber Risk Radar, so AI risk can be added to existing relationships rather than built from a standing start.
- **It opens new sectors and use cases.** Mobile application security and AI governance extend WhiteHawk into banking and fintech apps, professional services, and enable existing defence and government customers new ways to manage supplier risk.
- **It supports recurring and international revenue.** Quixxi's products suit subscription and partner-led delivery, and its international customer base and intellectual property support WhiteHawk's growth beyond Australia.

Five Illustrative Scenarios: The Quixxi and WhiteHawk Opportunity

(1) The Question Boards are now asking | *Financial Services*

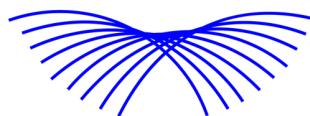
The challenge: At a superannuation fund's strategy day, a director asks three questions: where are we using AI, which systems make decisions about our members, and who owns the risk? Management cannot answer for each division, let alone for the whole organisation. AI sits inside vendor software, the contact centre, claims and fraud tools, marketing platforms, and the public chatbots and LLMs staff use every day.

Today: WhiteHawk's Cyber Risk Program gives executives a clear view of cyber posture, but AI can still sit outside that view.

With Quixxi: Clarity AI discovers the AI in use, builds the AI register and delivers a Board report mapped to APRA's CPS 230 and CPS 234 expectations. PromptGuard keeps member data out of the prompts staff send to AI tools.

What improves: The Board gets answers, evidence and an ongoing record, not a point-in-time snapshot.

For WhiteHawk: the same executives who already receive our cyber risk reporting can now receive a combined, company-wide view of cyber and AI risk, with the opportunity to turn a one-off assessment into a recurring governance subscription.

**(2) The AI you cannot see | Defence primes and government supply chains**

The challenge: A defence prime on a major sovereign program must show that hundreds of subcontractors protect controlled technical data. Suppliers are now adopting AI tools, and the prime's compliance lead cannot see which ones.

Today: Cyber Risk Radar already monitors the cyber posture of the prime's supply chain.

With Quixxi: Clarity AI governance signals are added to Radar, giving each supplier an AI risk profile beside its cyber score, while Quixxi Scan tests the apps and APIs suppliers use to exchange data with the prime.

What improves: One supply chain view across cyber, AI and application risk, with evidence aligned to defence industry security requirements and a faster path for suppliers to remediate.

For WhiteHawk: a direct extension of an existing product into a fast-growing compliance need, sold to primes and agencies that already trust the platform, with each prime bringing its supplier base into scope.

(3) The banking app under attack | Banking and fintech

The challenge: A regional bank finds cloned copies of its mobile app circulating, and customers reporting credentials stolen by malware that sits over the genuine app. Scam losses quickly become a Board and reputational issue.

Today: Traditional controls protect the bank's network and servers; the app on a customer's phone sits largely outside that perimeter.

With Quixxi: Quixxi Shield hardens the app against cloning and tampering without a rebuild, Quixxi Scan tests every release before it reaches customers, and Quixxi Supervise monitors live threats against the app in the field.

What improves: Protection extends from the bank's perimeter to the customer's pocket, supporting the bank's obligations under Australia's Scams Prevention Framework.

For WhiteHawk: a new mobile security product line, backed by Quixxi's intellectual property and international banking references, that opens fintech, telecommunications and government service apps.

(4) Shadow AI in the mid-market | Professional services

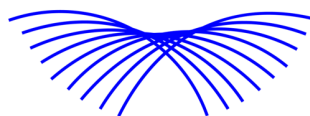
The challenge: A 400-person accounting firm discovers staff pasting client files into public AI tools. It has no AI policy, no register and no way to prove to clients that their data is safe.

Today: A traditional cyber assessment would find the firm's systems in reasonable shape and still miss the risk of client data leaving the building in AI prompts.

With Quixxi: Delivered through a channel partner as a monthly subscription, Clarity AI finds the AI tools in use and applies policy, PromptGuard protects client data at the point of use, and the firm receives evidence it can show clients and auditors.

What improves: Staff keep the productivity gains of AI while the firm is better placed to meet its confidentiality and Privacy Act obligations.

For WhiteHawk: a repeatable, partner-led offer for mid-sized legal, accounting and consulting firms, designed for recurring revenue.

**(5) AI in the classroom | Education**

The challenge: A state school system is rolling out generative AI for teaching and administration. Students and teachers also use their own AI tools, and families access services through a school app holding personal records.

Today: Security teams protect networks and student systems but have no single view of which AI tools are in use or how student data flows into them.

With Quixxi: Clarity AI registers and assesses AI tools against the Australian Framework for Generative AI in Schools, PromptGuard protects student and staff data in prompts, and Quixxi Shield and Scan secure the school app.

What improves: The system can adopt AI with confidence and give parents, students and regulators clear answers.

For WhiteHawk: entry into education, a large sector of school systems, universities and training providers where demand for AI guidance is growing.

The common thread. In every story, WhiteHawk starts from a capability customers already trust, then adds AI governance or mobile security to solve a problem they could not solve before. The result is more value for customers and a larger addressable market for WhiteHawk.

Why AI Governance is now a Board issue

AI oversight is increasingly a Board responsibility. Directors' duties extend to material business risks, while regulators are raising expectations around AI governance, controls and accountability.

- **ASIC** found in its October 2024 review of 23 financial services and credit licensees that AI adoption was accelerating faster than governance arrangements, highlighting gaps in areas including consumer risk, bias and third-party AI oversight.
- **APRA**, in its letter of 30 April 2026, called for a step-change in AI risk management and expects Boards of regulated entities to have sufficient AI literacy, oversee AI strategy against risk appetite and receive effective monitoring and reporting. CPS 230 also requires effective controls, monitoring, testing and management of operational and third-party risks.
- **Regulation and frameworks** including the Privacy Act reforms, NIST AI Risk Management Framework, ISO/IEC 42001 and the EU AI Act create clearer expectations for AI governance, transparency, accountability and control.

WhiteHawk provides Boards with a practical, evidence-based view of cyber risk, resilience and governance, helping them understand their exposure, prioritise risk, monitor controls and demonstrate appropriate governance. The combination with Quixxi extends this capability across AI risk, governance and compliance, supporting organisations as AI adoption accelerates.

Position for what comes next

Each of the risks below is already emerging and is addressed by capabilities WhiteHawk and Quixxi deliver now. The roadmap reflects the integration priorities announced in April 2026.

Emerging risk	How WhiteHawk and Quixxi respond today	Roadmap
Shadow AI and data leakage. Staff paste client and personal data into public AI tools.	Clarity AI discovers the AI in use and applies policy; PromptGuard keeps sensitive data out of prompts.	Clarity AI brought into the WhiteHawk platform alongside the Cyber Risk Program.
Ungoverned AI decisions. AI shapes decisions with no register, owner or evidence.	Clarity AI registers and risk-rates AI systems and produces Board and regulator reporting.	A unified dashboard across cyber, data and AI risk for executives and Boards.



Hidden AI in the supply chain. Suppliers adopt AI tools the organisation cannot see.	Cyber Risk Radar monitors supplier cyber posture; Clarity AI assesses AI risk.	An AI risk profile for each supplier within Cyber Risk Radar.
AI-accelerated app and mobile attacks. Faster discovery of app and API weaknesses, cloned apps and overlay malware.	Quixxi Scan tests apps and APIs, complementing the Cyber Analyst Platform as a Service; Shield hardens apps; Supervise monitors live threats.	The combined offer distributed internationally through aligned partner channels.

Forward Looking Statement

This announcement contains forward-looking statements, including in relation to the Company's funding position, Quixxi and its pathway to self-sustainability. These statements reflect the Company's current expectations and are based on assumptions that are subject to risks and uncertainties, many of which are outside the Company's control. Actual results may differ materially. The Company does not undertake to update any forward-looking statement except as required by law or the ASX Listing Rules.

This announcement has been authorised for release by the Board of Directors.

ENDS

For more information:

Media inquiries (USA)

WhiteHawk

COO

Soo Kim

publicrelations@whitehawk.com

Investor inquiries (Australia)

WhiteHawk

Company Secretary

Louisa Ho

investors@whitehawk.com

+61 2 9713 9495

About WhiteHawk

WhiteHawk Limited (ASX: WHK) provides AI-enabled cyber risk management solutions that help organizations identify, assess, prioritize and mitigate cyber risk across their operations, supply chains and third-party ecosystems. Through its automated Cyber Risk Radar and Cyber Risk Program offerings, WhiteHawk enables government, critical infrastructure, education and commercial organizations to continuously monitor cyber risk, strengthen resilience and support compliance requirements at scale.

WhiteHawk's cloud-based platform combines cyber risk assessments, monitoring, prioritization and mitigation capabilities with access to a broad ecosystem of cybersecurity solutions and services. For more information, visit www.whitehawk.com.