WITFOO, INC. · JULY 2026

The Cyber Security multiplier — and the channel already selling it

WitFoo's innovation — **empathetic processing**— transforms security telemetry into 100% deterministic, forensic-grade evidence for all Cyber Security applications, whilst simultaneously removing 90%+ of the traditional downstream processing and related Ai costs incurred by both vendors and customers.

The channel that takes it to market is signed, transacting and growing.

WitFoo, Inc. invites verified accredited investors to participate in a raise of up to US$2.5 million. The investment case rests on two assets working together: defensible intellectual property — empathetic processing, the innovation on top of which WitFoo's full Cyber Security reporting and analytics suite is built — and a contracted route to market that is growing, spanning seven transacting channel partners and the core software role in a major US Navy programme. This raise bridges those signed relationships to recurring annual revenue on a deliberately small cost base.

>90%
security telemetry reduced before AI or SIEM, with no evidence lost

7
channel partners signed and transacting, including WWT and Accenture Federal Services

US$789M
US Navy SHARKCAGE programme in which WitFoo is the core software component

~87%
gross margin, with EBITDA breakeven modelled in 2028

The offer at a glance

ISSUER	WitFoo, Inc. — Delaware C-corporation; holds all group intellectual property
AMOUNT	Up to US$2,500,000
INSTRUMENT	Investor's choice — common stock, or a convertible note
EQUITY TERMS	US$25,000,000 pre-money · US$2.50 per share · US$27,500,000 post-money fully subscribed · about 9.1% dilution (1,000,000 new shares)
CONVERTIBLE TERMS	US$30,000,000 conversion ceiling · 10% discount to the next qualified financing · 4–6% p.a. · 36–48 month maturity
MINIMUM SUBSCRIPTION	US$10,000
EXEMPTION	Regulation D, Rule 506(c) · Form D filed 26 June 2026 · verified accredited investors only
US SECURITIES COUNSEL	Kennyhertz Perry LLC

Terms are indicative and subject to the Private Placement Memorandum and definitive subscription documents. Cybersecurity for Collective Defense.

ASSETONE—FOUNDATIONALIP

Technology the whole market needs, owned outright

A structural cost problem the incumbents cannot solve for themselves or their customers

Cybercrime keeps compounding — projected at US$10.5 trillion a year (Cybersecurity Ventures 2025), with the average breach now costing US$4.44 million globally and a record US$10.22 million in the US (IBM 2025). The industry's default answer is to feed everything to AI, and the input costs of that answer are rising for both vendors and customers on every axis at once:

~US$7T
data-centre capital spend required to meet 2030 AI demand — McKinsey

~40%
of AI data centres forecast to be power-restricted by 2027 — Gartner

1.6%
record-low North American data-centre vacancy; largeblock rents up 19% in a year — CBRE 2025

US$25–75
per million output tokens for frontier-model reasoning — and no longer falling — Market snapshots, April 2026

Vendors cannot absorb costs of that scale, so they meter them onward: SIEMs bill per gigabyte ingested, AI SOC tools at published price points of roughly US$9 per investigation or US$0.27 per alert at enterprise scale. Every one of those meters runs against raw, six-to-tenfold-redundant security data — which is the layer WitFoo transforms. The pass-through economics are the size of WitFoo's opening. Ai is not the silver bullet.

WitFoo's answer: empathetic processing

WitFoo's core IP works out what each security event actually means before any expensive system touches it, simultaneously collapsing the six-to-tenfold redundancy typical of security data into a single enriched record. Volume falls by more than 90%; with 100% of evidence an investigation might ever need is preserved. The cheap, high-volume work is done with fast deterministic logic, so costly probabilistic AI reasoning is reserved for the small share of work that needs it. Lower cost, faster answers, a forensic-grade evidence trail, and a global Cyber Defence ecosystem that becomes sustainable.

What that is worth to one mid-sized end customer

US$3.28M
modelled annual cost of a typical SIEM-plusAI stack at 500 GB/day

US$595K
the same stack with WitFoo's Conductor in front

5.5×
first-year payback on the Conductor investment

Figures illustrative; actual savings vary by contract structure. In a US Navy benchmark, the same class of workload ran on 28 CPUs where a leading SIEM needed 1,700.

Why this position is defensible

- **ProtoGraph, Adaptive Parsing and Temporal Link Analysis** — the semantic engine that understands events, entities and relationships, with zero parser upkeep for the customer. (Transforming “Security Awareness” to “Security-Coherence”)
- **The Precinct 6 Cybersecurity Dataset** — 114 million labelled records built from real adversary behaviour, released with the University of Canterbury; to WitFoo's knowledge the largest of its kind, and part of what makes the semantic layer hard to replicate.
- **An economic moat in the architecture** — flat per-appliance pricing with unlimited data. There is no metering anywhere in the platform, so WitFoo's value to customers compounds as rivals' per-gigabyte bills grow.
- **A proprietary AI-assisted R&D system** — a written, versioned development methodology, maintained as a trade secret, in which AI executes every stage of specification, implementation, verification and release under human governance, with each stage independently re-verified. It is the engine that carried the platform through 341 verified work orders from research to general availability with a team of eight — and the reason WitFoo's research pivots have been funded by operating discipline rather than raised capital.
- **A patent program on file** — five U.S. provisional patent applications filed 13 July 2026 covering the platform's core mechanisms, with a counsel-directed United States and New Zealand prosecution strategy (see below).
- **Category position** — WitFoo is not another SIEM or AI SOC tool; it is the substrate underneath them. Incumbents are enablers and partners, not head-to-head competition.

ASSETONE—FOUNDATIONALIP,CONTINUED

Protected two ways: patents filed, trade secrets kept

On 13 July 2026 WitFoo filed five provisional patent applications with the United States Patent and Trademark Office — one for each core mechanism of the platform. Filings were prepared and code-verified through WitFoo's AI-assisted R&D system and reviewed by US patent counsel; each application preserves a United States and New Zealand prosecution path, with conversion to full applications due by July 2027.

64/110,132	Passive detection and graph representation of autonomous AI agents in network telemetry — visibility into the agentic-AI wave, filed before any public disclosure
64/110,134	Deterministic entity identity with monotonicity-preserving merge — the graph integrity backbone behind more than 90% telemetry reduction with no evidence lost
64/110,135	Detection-preserving pseudonymization of security telemetry — privacy redaction that keeps detection, correlation and deduplication working
64/110,138	Consent-gated cross-organization federation with revocation propagation — the CyberGrid protocol behind Cybersecurity for Collective Defense
64/110,139	Evidence-derived incident risk composition with outlier damping — triage scoring that gates automation and analyst attention

The methodology that produced them is deliberately protected the opposite way: the AI-assisted R&D system, the company's operating canon, and WitFoo's in-house AI platform work remain unpublished trade secrets, so the mechanisms they generate stay WitFoo's alone. Provisional applications establish priority dates; they are not issued patents, and no assurance can be given that any patent will be granted or will provide the scope of protection sought.

ASSETTWO—THESIGNEDCHANNEL

The route to market is already contracted

Great IP fails without distribution. WitFoo made the channel the strategy: rather than building a large direct sales force, the company signed the firms that already hold the customer relationships. Profound product-market fit acquired, the platform suite is fully productionised, fully commercialised. Version 1.0.0 reached general availability in Google and Azure marketplaces on 30 June 2026 — and seven partners are signed and transacting today:

WWT · Accenture Federal Services · Ardalyst · Kordia · SSS Cybersecurity · TD SYNNEX · Tech Data

A second wave is in documentation with MSSP's like DEFEND, in agreements executed with IBM and with Carson & SAINT (prerevenue), and negotiations under way with Cisco.

The anchor: SHARKCAGE

WitFoo is the core software component of SHARKCAGE, a US Navy modernisation programme delivered under a US$789 million, five-year contract (with a five-year option) on which Accenture Federal Services is the prime contractor. WitFoo's forecast contribution is about US$2.5 million a year at base run-rate — federal-scale validation, carried by a partner's balance sheet rather than WitFoo's.

ASSETTWO—CONTINUED

A cost base built for the channel model

Because partners carry distribution, WitFoo stays small. Gross margin runs near 87%. On the base-case plan the company reaches EBITDA breakeven in 2028 and about a 36% EBITDA margin by 2030, while headcount grows only from 8 to 14 people. Near-term revenue is anchored to named channel and federal catalysts rather than speculative pipeline. The same AI-assisted R&D system that carried the platform from research to general availability without raised capital holds that cost base flat as the roadmap expands. (Base-case model; forward-looking — see the disclaimer below.)

Use of proceeds — bridging signed partnerships to recurring revenue

Sales and channel enablement	**38% · US$950,000**
Product and engineering	**28% · US$700,000**
WFL commercial operations	**18% · US$450,000**
Working capital and contingency	**10% · US$250,000**
Offering, legal and compliance	**6% · US$150,000**

The raise deliberately does not fund AI-hardware capital expenditure, which is paced against realised revenue rather than paid for upfront.

THE OPPORTUNITY

Why now, and how to participate

Why now

The AI cost collision is already under way, and WitFoo sits on the right side of it: flat per-appliance pricing with no data-volume charges becomes more valuable as AI inference costs rise. The strategic thesis is set out in two companion whitepapers — *The AI Cost Collision in Cybersecurity* and *The CyberGrid Imperative* — currently in partner review. This raise is timed to the same window: the channel is signed, the platform is GA, and the funding converts those relationships into recurring revenue.

Structure and governance

Investors choose the instrument that suits them: common stock at the US$25 million pre-money, or a convertible note at a US$30 million ceiling with a 10% discount for those who prefer to let the next round settle valuation. WitFoo, Inc. retains 100% voting control; new common stock ranks equally with existing common stock; the round adds no investor board seat and authorises no preferred stock.

How to participate

1

NDA and data room — sign a mutual NDA and receive access to the investor data room (which now includes the five patent filings as investor briefs).

2

Verification — complete accreditedinvestor verification, as Rule 506(c) requires.

3

Subscription — elect the instrument and execute subscription documents. Full terms are in the Private Placement Memorandum.

Charles Herring — Chairman and co-Founder

charles@witfoo.com · +64 (0) 27 770 0365 · Christchurch, New Zealand & Dunwoody, Georgia

WitFoo

Disclaimer. *This document is for informational purposes only and is not an offer to sell or a solicitation of an offer to buy any security. Any offer is made solely through the Private Placement Memorandum and definitive subscription documents, to verified accredited investors, under Regulation D, Rule 506(c). The securities have not been registered under the U.S. Securities Act of 1933 or any state securities laws and may not be resold absent registration or an applicable exemption. Forward-looking statements — including projections, revenue trajectory, margins and use of proceeds — are based on assumptions described herein and elsewhere in the offering materials; actual results may differ materially. Statements regarding patent applications describe provisional filings only; provisional applications are not issued patents and confer no enforceable rights unless and until patents are granted. Third-party statistics are attributed to their sources (including IBM, Cybersecurity Ventures and others).*

Where WitFoo sits — and why it is a category of ONE

"AI" and "Cybersecurity" landscapes are crowded. WitFoo is not another SIEM, AI SOC, or data pipeline — empathetic processing is the 'Security-Coherent' layer that both powers WitFoo's platform suite AND that sits underneath them all — putting the industry's best-funded brands on WitFoo's side of the table.

	Generic ETL / observability	"Securityaware" pipelines[1]	XDR / SIEM analytics platforms	WitFoo — Empathetic Processing
WHAT IT WORKS ON	Bytes and streams	Security log fields	Alerts and detections, best on own-vendor data	Security events, entities and relationships — the actual meaning
HOW IT REDUCES	Filter and sample — drops data	Rule-based filtering — drops data	No upstream reduction — a data consumer	Security-coherent deduplication (ProtoGraph) — more than 90%, with zero evidence lost
UPKEEP AND PRICING	Hand-written rules · per GB/day	Hand-written rules · per GB/day	Per endpoint / per GB ingested	Zero parser upkeep · flat per appliance, unlimited data
POSITION IN THE STACK	Upstream plumbing	Upstream routing	Downstream analytics — consumes WitFoo output	The substrate — feeds and de-duplicates ahead of all of them, protected by ProtoGraph, Adaptive Parsing, the Precinct 6 dataset[2], five U.S. patent filings and an unpublished AI-assisted R&D system

Friend, not foe — how the incumbents relate to WitFoo

- **Enablers** — WitFoo makes them cheaper and better: SIEMs and data lakes (Splunk, Microsoft Sentinel, Google, Elastic) and AI SOC tools (Dropzone, D3, Security Copilot and peers). WitFoo cuts their input by more than 90% and feeds them clean, structured evidence.
- **Strategic and channel partners** — signed and transacting today: WWT · Accenture Federal Services · Ardalyst · Kordia · SSS Cybersecurity · TD SYNNEX · Tech Data Australasia — with WitFoo as the core software of the US Navy SHARKCAGE programme; further agreements executed (IBM, Carson & SAINT) or in negotiation (Cisco).
- **Natural acquirers[3]** — strategic or financial rationale: Strategic — SIEM and platform incumbents (e.g. Cisco/Splunk, Microsoft, Palo Alto, CrowdStrike) and pipeline players (e.g. Cribl): they need this layer and it is hard to build. Financial — software-focused private equity, drawn to high-margin recurring revenue at standard software multiples.

---

1 An emerging category of tools that filter and route security telemetry (for example Cribl and newer entrants); security-aware in routing, but they reduce by dropping data and build no evidence graph. Reduction claims for ETL and pipeline tools are directional, drawn from those vendors' own marketing. 2 Precinct 6 Cybersecurity Dataset — 114 million labelled records drawn from real adversary behaviour, released with the University of Canterbury (April 2026); to WitFoo's knowledge the largest dataset of its kind. Benchmark: in independent Navy-workload testing (Ardalyst / WWT ATC labs, Advisory-Board-reviewed), WitFoo processed on 28 CPUs a workload that required 1,700 CPUs on a leading SIEM. 3 Illustrative of market structure only — not a statement that any acquisition discussions exist or that any particular valuation would apply.