LMNTRIX

BE THE HUNTER | NOT THE PREY

CYBERSECURITY WITHOUT VENTURE CAPITAL

Funding Models, Hidden Costs, and the Future of Trustworthy Security Vendors

WHITEPAPER

LMNTRIX USA
19800 MacArthur Blvd,
Suite 850
Irvine, CA 92612
sales@lmntrix.com
888-388-1879

LMNTRIX UK
Kemp House, 152–160
City Road, London,
EC1V 2NX
sales@lmntrix.com
+44.808.164.9442

LMNTRIX INDIA
VR Bengaluru, Level 5, ITPL Main
Rd, Devasandra Industrial Estate,
Bengaluru, Karnataka 560048, India
sales@lmntrix.com
+91-22-49712788

LMNTRIX AUSTRALIA
Level 25, 100 Mount Street,
North Sydney 2060
sales@lmntrix.com
+61.288.805.198

LMNTRIX SINGAPORE
60 Kaki Bukit Place, #05-19,
Eunos TechPark
sales@lmntrix.com
+65-3129-2639

EXECUTIVE SUMMARY

Venture capital (VC) has played a decisive role in accelerating innovation across the cybersecurity industry, enabling rapid commercialisation of new ideas and helping startups challenge entrenched incumbents. However, as cybersecurity tools have become embedded in mission-critical infrastructure, the traditional VC growth model is increasingly misaligned with the expectations placed on security vendors.

Pressure to scale quickly, capture market share, and pursue near-term exits has contributed to product instability, security and technical debt, workforce disruption, and erosion of customer trust. High-profile outages, repeated layoffs, and stalled roadmaps have underscored the operational risks that emerge when investor timelines take precedence over long-term resilience and reliability.

These challenges have prompted buyers, CISOs, and procurement teams to reassess how vendor risk is evaluated. Product features and market positioning are no longer sufficient indicators of vendor quality. Customers are now scrutinising ownership structures, funding models, governance practices, and transparency into internal security controls. In this environment, VC backing is no longer a proxy for stability; in some cases, it has become a signal of dependency on external capital cycles and potential disruption through acquisition or restructuring.

Against this backdrop, alternative funding models — bootstrapping, customer-funded growth, cooperative ownership, angel investment, and community-driven structures — are gaining renewed attention. These approaches offer greater strategic independence, align incentives more closely with customers, and support governance models that emphasise transparency and long-term product integrity. This paper examines the structural forces at play and provides a framework for buyers and founders to navigate this evolving landscape.

> **Key Finding:** VC backing is no longer a reliable proxy for vendor stability. Buyers must evaluate ownership structures, funding sustainability, and governance transparency alongside product capabilities.

CONTENTS

INTRODUCTION

Venture capital has long played a central role in shaping the cybersecurity industry. For decades, VC funding accelerated innovation by enabling startups to commercialise new defensive techniques faster than large incumbents could. This model rewarded rapid growth, aggressive customer acquisition, and the promise of technological differentiation — often through point solutions aimed at emerging threats. In return, enterprises accepted a degree of risk, trusting that VC-backed vendors would mature quickly, scale reliably, and eventually consolidate into stable platforms.

That relationship is now under strain. As cybersecurity spending has become a board-level concern and security tools have moved into mission-critical infrastructure, buyers are less tolerant of instability. The traditional VC playbook — optimise for growth first, operational rigour later — conflicts with the expectations placed on vendors protecting core business operations, sensitive data, and regulated environments.

Outages, Layoffs, Product Stagnation, and Trust Erosion

Recent years have exposed structural weaknesses in many VC-backed security vendors. High-profile outages have highlighted brittle architectures and overextended engineering teams. Waves of layoffs — often following funding slowdowns or failed exits — have reduced support quality, slowed vulnerability remediation, and undermined customer confidence.

At the same time, product roadmaps have stagnated as companies prioritise cost-cutting or short-term revenue over long-term innovation. These are not isolated incidents; they represent a systemic pattern inherent to the VC growth model when applied to a domain where reliability is non-negotiable.

The Traditional Vendor Risk Model Questioned

Procurement and security leaders are increasingly sceptical of assessing vendor risk primarily through financial backing, brand recognition, or market hype. VC sponsorship no longer signals resilience or longevity; in some cases, it signals dependency on continuous funding rounds or an eventual acquisition that may disrupt products and contracts.

Buyers are instead scrutinising operational maturity, staffing stability, architectural resilience, and the ability to sustain development without external capital infusions. In cybersecurity, vendor failure is not a theoretical risk — it is an operational and business risk that directly transfers to the customer.

The VC Growth Model vs. Cybersecurity Stability Needs

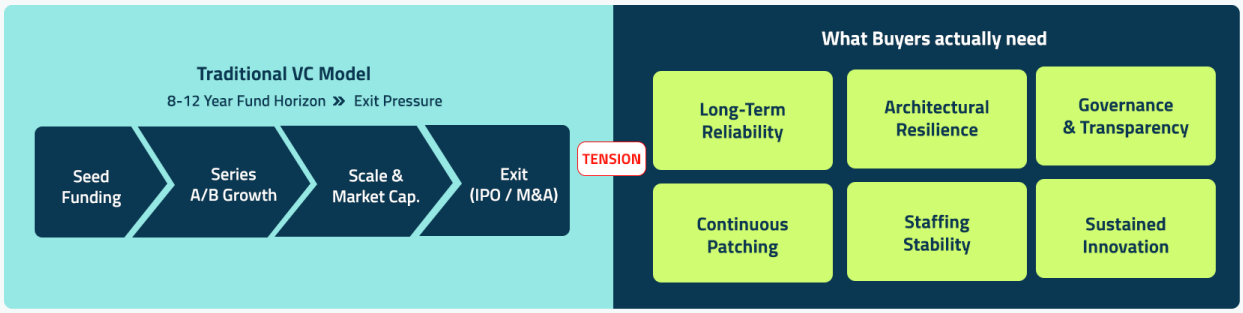

Figure 1: The fundamental tension between VC growth expectations and the stability requirements of cybersecurity buyers.

OVERVIEW OF VC'S ROLE IN TECH AND CYBERSECURITY

Venture capital has historically been a cornerstone of innovation in technology, acting as a critical conduit between early-stage ideas and scalable commercial solutions.[1] In the broader tech sector, VC firms inject growth capital into promising startups, helping them build teams, develop products, and expand into markets that traditional lenders might consider too risky.[2] This dynamic is equally relevant in cybersecurity, where rapidly evolving threats require equally rapid innovation.

VCs validate high-risk, high-potential security technologies by providing both funding and strategic guidance that enables startups to bring novel defences — such as AI-enhanced threat detection or cloud-native zero-trust architectures — to market faster than would otherwise be possible. In cybersecurity specifically, VC investment helps diversify the innovation landscape and address emerging vulnerabilities that legacy incumbents may not prioritise.

Typical Incentives and Expectations of VC Investors

Venture capital is structured around a distinct set of incentives that heavily influence how technology startups grow. VCs typically operate funds with a finite lifespan (often 8–12 years) and have fiduciary obligations to their limited partners to deliver large returns, often 10x the initial investment or more on successful deals.[3] These expectations reward companies that can scale fast, capture market share, and demonstrate clear differentiation in crowded spaces.

VCs also expect founders to aggressively pursue product development milestones and user growth, securing subsequent funding rounds at progressively higher valuations. While this can drive innovation velocity, it embeds pressure to align product roadmaps with investor expectations around performance metrics, growth pace, and monetisation strategies — priorities that may not always align with customer needs.

How VC Influence Shapes Product Roadmaps

VC influence manifests strongly in how cybersecurity startups define their product roadmaps. Capital influx allows rapid iteration but also conditions founders to chase trends that attract further investment. This incentive structure can shape priorities in ways that diverge from customer needs:

- **Trend-Driven Development:** Startups may pivot toward hot domains (AI, cloud security) to remain attractive to investors, even when customer needs are broader or more foundational.
- **Short-Term Feature Pushes:** Pressure to demonstrate product traction may lead teams to prioritise surface-level features that generate quick adoption over deep architectural robustness.
- **Platformisation and Consolidation:** Well-funded startups often pursue ambitious platform visions to justify higher valuations — stretching engineering resources and potentially delaying core defensive innovation.

The result is an ecosystem where many products reflect the priorities and timelines set by venture capital as much as the needs of the customers they serve.

THE HIDDEN COSTS OF VC-DRIVEN ROADMAPS

In the specific context of VC-driven cybersecurity vendors, the hidden costs embedded in product roadmaps are driven by short-term performance expectations. These costs grow over time and become increasingly material to buyers' bottom lines, even when they are invisible at the point of procurement.

Short-Term Performance Pressure vs. Long-Term Product Quality

VC expectations for fast iteration and rapid customer acquisition can inadvertently encourage teams to compromise on internal quality. Research across sectors demonstrates that venture-backed firms guided to hasten their development cycles often truncate key engineering processes, leading to "shortened key processes and reduced technological content," which correlates with product quality problems later in the lifecycle.[5]

These trade-offs manifest in rushed releases that skip thorough testing, automated validation, or proper code reviews — steps critical for assuring secure, scalable systems. What looks like progress on the quarterly scoreboard can create fragile systems where outages, security gaps, and regressions become more likely over time.

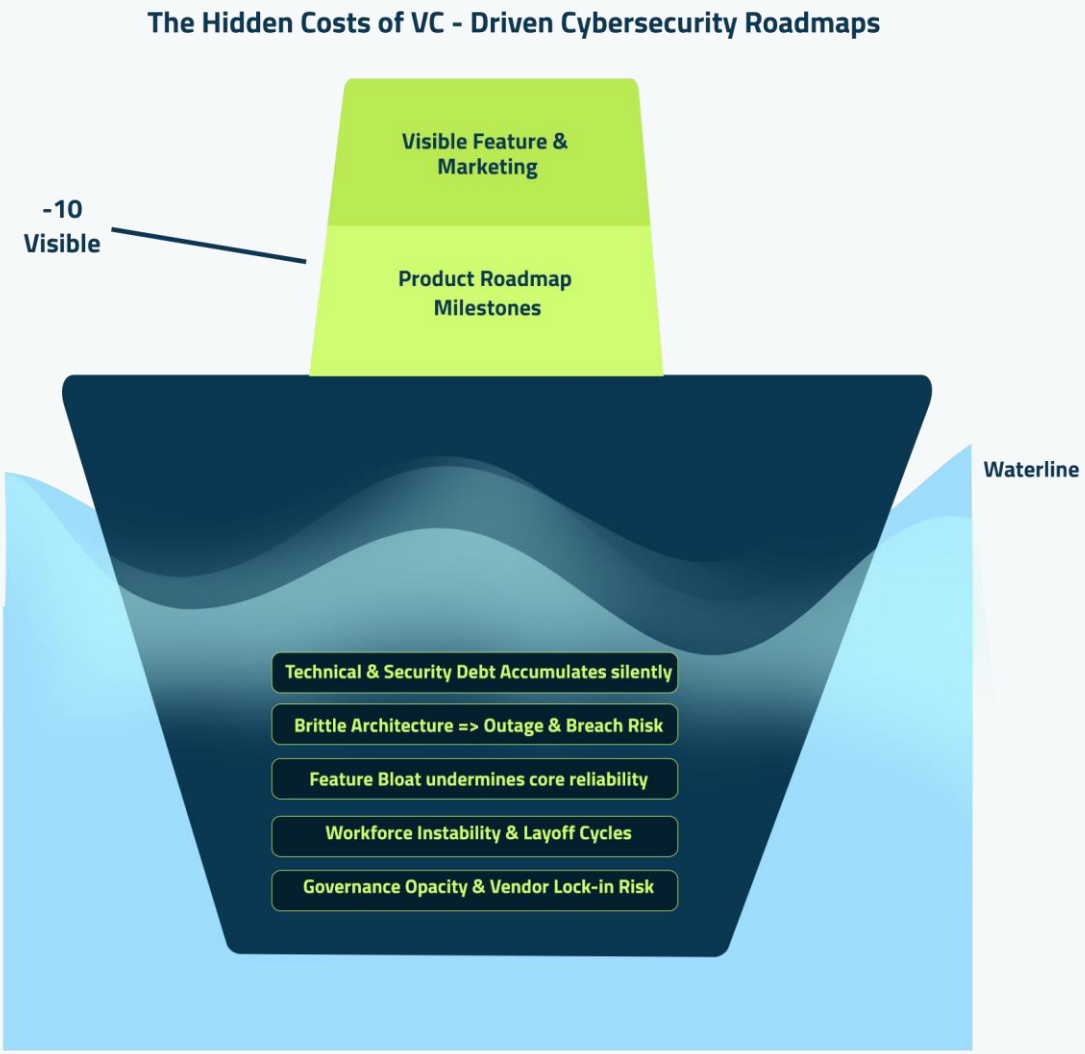

Figure 2: The Hidden Costs Iceberg — the visible features of VC-backed products conceal far greater structural risks below the surface.

Security Debt and Trade-Offs in High-Growth Startups

Technical debt — the code and architectural shortcuts taken under time pressure that incur compounding "interest payments" over time — is central to understanding the hidden costs in VC-backed security products.[4] Technical debt emerges when teams defer refactoring, robust security controls, or comprehensive documentation.

Over time, this debt erodes velocity and increases operational risk: developers spend disproportionate effort on incremental changes, security issues proliferate, and performance becomes brittle. In environments where the vendor's own platform becomes a vector for vulnerabilities, outages, or compliance gaps, the irony is acute — and the cost transfers directly to the customer.

Feature Bloat vs. Core Security Reliability

VC-driven roadmaps can also encourage feature bloat — the accumulation of surface-level capabilities designed to impress investors and broaden market appeal, rather than disciplined refinement of core security functionality.[6] An overcrowded roadmap may look impressive on pitch decks but ultimately spreads engineering effort thin, leading to increased complexity and reduced reliability.

Meanwhile, foundational parts of the product suffer as teams reactively patch problems instead of building resilient architecture. Delivery slows, bug rates climb, and the platform's ability to defend against real threats weakens. These are precisely the liabilities that enterprise buyers are now factoring into vendor risk assessments.

> **Risk Signal:** When evaluating VC-backed vendors, ask not just about the roadmap — ask about what has been deferred. Accumulated technical and security debt is rarely disclosed proactively.

WHAT INDEPENDENCE FROM VC CAPITAL LOOKS LIKE

As the cybersecurity market grapples with the limitations and hidden costs of VC-driven roadmaps, founders and buyers are exploring alternative funding pathways that support sustainable growth, customer-centric value, and deeper operational transparency.[7] Traditional venture capital is not the only way to fund innovation, and in a domain where reliability and trust are paramount, other models can yield stronger alignment between product quality and customer needs.

Alternative Funding Pathways

The most prominent alternatives to traditional VC funding include:

- **Customer-Funded Growth or Bootstrapping:** Early revenue, pre-orders, and paid pilots fund development rather than outside capital. Bootstrapped firms retain full autonomy over strategic choices, prioritise product-market fit over rapid scale, and avoid valuation pressures that can push premature feature expansions. Internal funds remain the first choice in the pecking order of financing for many founders, due to lower information asymmetry and mission alignment.
- **Cooperative or Platform-Cooperative Structures:** Ownership and governance accrue to users or workers rather than outside investors. Platform cooperatives are democratically governed and thus less susceptible to VC time horizons, enabling strategic choices that reflect stakeholder interests and long-term product reliability.
- **Decentralised Autonomous Organisations (DAOs) and Community Collectives:** Communities pool capital and decide collectively which projects to back. Founders engaging with DAOs receive funding alongside an engaged user base that helps shape strategy — blurring the line between funders and customers in ways traditional VC rarely does.[8]
- **Angel Investment:** Individual investors providing personal capital early can offer mentorship and smaller, less controlling funding rounds that avoid some of the institutional pressures of VC growth expectations.

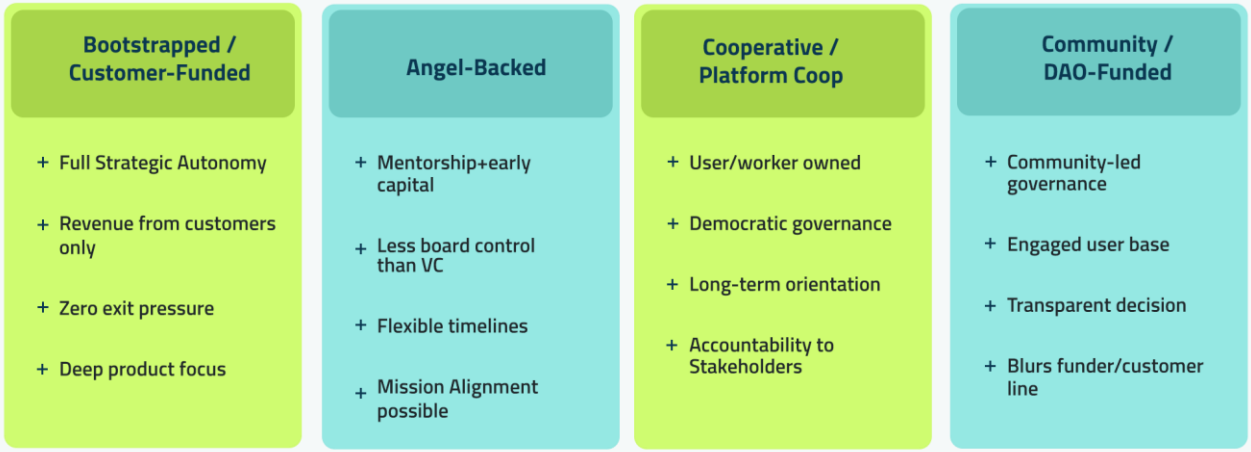

Figure 3: Alternative funding models and their distinctive governance, alignment, and strategic characteristics.

How Funding Source Influences Governance, Transparency, and Trust

The source of funding has significant downstream effects on governance, strategic focus, and stakeholder trust. VC funding often comes with governance structures — board seats, performance milestones, exit timelines — that can drive companies toward prioritising scale and exit value over product endurance or customer-centric reliability.

In contrast, alternative models tend to align governance with those closest to the product and its mission. Cooperatives and DAOs embed frameworks that increase accountability to users rather than distant investors, encouraging greater transparency in decision-making and product priorities. Academic research reinforces that clarity about how decisions are made reduces information asymmetry and fosters confidence among contributors and customers alike.[9]

VC's Structural Limits and Innovation Biases

Academia offers useful insights into why alternative funding routes matter. Studies of startup finance find that not all capital sources encourage the same innovation behaviours: VC tends to drive rapid scaling and strong signalling effects, but other forms of financing can support deeper, sustained innovation without the same growth imperatives.

As VCs often rely on internal heuristics, networking cues, and external validation signals (growth metrics, media buzz), they may systematically favour certain types of innovation while overlooking others that are less immediately quantifiable — such as architectural resilience and security hardening. This reinforces the case for a more pluralistic funding ecosystem that aligns incentives with reliability, transparency, and long-term stakeholder value.

BUYER DUE DILIGENCE AND NEW PROCUREMENT QUESTIONS

When procurement and security teams assess cybersecurity vendors today, they are asking far deeper questions than feature checkboxes and product claims. With concerns about outages, roadmap uncertainty, and VC-linked risks in the background, buyers need clear insight into vendor ownership, sustainability, security practices, and risk governance.

Questions Buyers Should Ask Beyond Product Features

A robust vendor due diligence process must expand beyond standard security questionnaires to cover the underlying business fundamentals:

- **Who owns the codebase?** Is it fully owned by the vendor, or are there third-party or open-source dependencies that could complicate licensing, support, or security patching? Knowing the ownership helps assess future risk, especially if part of the codebase is externally maintained or vulnerable to upstream changes.
- **What is the vendor's funding model?** Ask how future development is funded — customer revenue, VC injections, debt instruments, or otherwise — and how that influences roadmap stability. A clear articulation of the funding model reveals whether strategic decisions are profit-driven, growth-driven, or customer-aligned.
- **What transparency exists into security practices?** Insist on evidence of security maturity, not just claims. Ask for documented policies, audit reports (SOC 2, ISO 27001), penetration test results, and evidence of ongoing security governance and training programmes.

Procurement Checklist and Risk Indicators

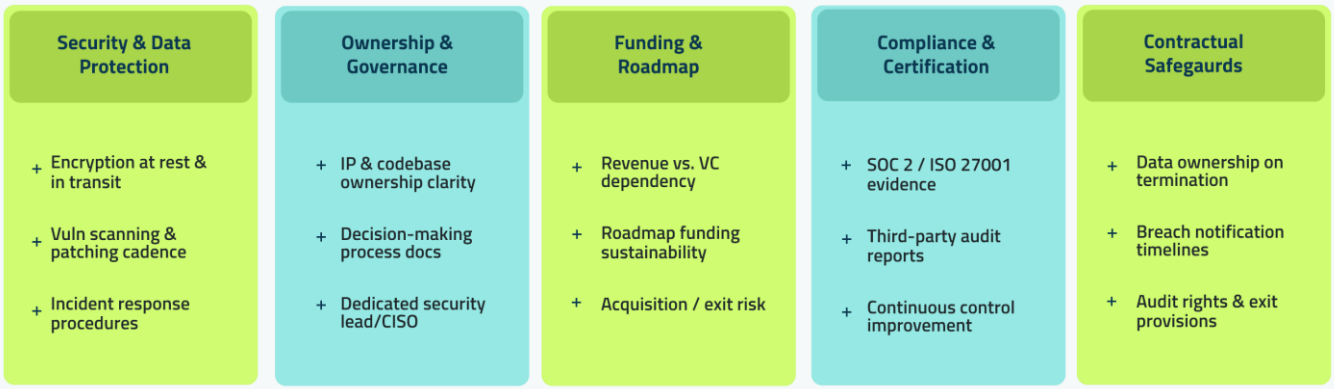

Figure 4: A structured due diligence framework across five key domains of vendor risk assessment.

A comprehensive vendor procurement checklist should address five core domains:

- Security & Data Protection: Encryption standards, vulnerability scanning cadence, patching procedures, and documented incident response and recovery plans.
- Ownership & Governance: IP ownership documentation, decision-making processes for product development, and the existence of a dedicated security leadership function (e.g., CISO or equivalent).
- Funding & Roadmap Sustainability: Financial indicators of cash runway or profitability, clarity on whether growth is VC-dependent or customer-revenue-driven, and any known acquisition discussions.
- Compliance & Certifications: Proof of third-party certifications, audit history, and evidence of continuous improvement in security controls.
- Contractual Safeguards: Clauses covering data ownership on termination, breach notification timelines, audit rights, and exit provisions that protect the buyer if the vendor is acquired or restructures.[10]

Tiering vendors by risk level — critical, high, or medium — based on data sensitivity and system access allows procurement teams to allocate their due diligence effort proportionally and avoid checkbox fatigue on lower-risk suppliers.

> **Practical Tip:** Self-reported answers to security questionnaires must be backed by verifiable artefacts. Treat unsubstantiated claims as a red flag equivalent to a negative finding.

CONCLUSION

The cybersecurity industry is reaching an inflection point where the limitations of VC-driven growth are becoming increasingly visible to buyers and practitioners alike. While venture capital has enabled remarkable technological progress, its emphasis on rapid scaling, exit timelines, and valuation growth can conflict with the core purpose of cybersecurity: protecting systems, data, and operations over the long term.

The hidden costs — security debt, feature bloat, governance opacity, and organisational instability — are no longer abstract risks but tangible concerns shaping procurement decisions at the board and executive level. Buyers who do not account for vendor funding model and governance structures in their risk assessments are leaving a significant blind spot in their overall security posture.

Alternative funding models demonstrate that innovation does not require sacrificing independence or trust. Customer-funded and bootstrapped companies can prioritise reliability and depth over hype; cooperatives and community-based models embed accountability directly into governance; and angel-backed ventures can grow without the same structural pressure to pursue premature exits.

For founders and investors, this shift highlights the opportunity to rethink how cybersecurity innovation is financed and governed. For buyers, it reinforces the importance of deeper due diligence and more sophisticated procurement questions. Ultimately, a more resilient and trustworthy cybersecurity ecosystem will emerge not from a single funding model, but from a deliberate alignment of capital, incentives, and responsibility with the long-term security needs of customers and society.

REFERENCES

[1] World Economic Forum. "This is venture capital's key role in driving global cyber resilience." September 2024. https://www.weforum.org/stories/2024/09/venture-capital-role-cyber-resilience-cybersecurity/

[2] Kato, A.I. "Venture Capital as a Catalyst for Innovation and Economic Growth in Emerging Economies." Adm. Sci. 2025, 15, 405. https://doi.org/10.3390/admsci15110405

[3] FinmodelsLabs. "The Role of Venture Capital in Innovation." December 2025. https://financialmodelslab.com/blogs/blog/role-venture-capital-innovation

[4] Faddom. "What Is Technical Debt? Causes, Consequences, and Best Practices." December 2025. https://faddom.com/what-is-technical-debt-causes-consequences-and-best-practices/

[5] Shin, M., Bae, J., Ozmel, U. "Effect of venture capital investment horizon on new product development." Journal of Business Venturing, Vol. 40, Issue 1, 2025.

[6] Faster Capital. "The Impact of Product Roadmaps on VC Investments." April 2025. https://www.fastercapital.com/content/The-Impact-of-Product-Roadmaps-on-VC-Investments.html

[7] Manso Laso J., Moya-Clemente I., Ribes Giner G. "Accessing Alternative Finance in Europe." Journal of Risk and Financial Management 2025. https://doi.org/10.3390/jrfm18090496

[8] Mrad, R. "Beyond Venture Capital: Alternative Funding Models for Startups in 2025." Equisy, 2025. https://equisy.io/beyond-venture-capital-alternative-funding-models-for-startups-in-2025/

[9] Ed-Dafali, S., Bouzahir, B. "Trust as a governance mechanism of the relationship between venture capitalists and managers." June 2022.

[10] Yegin, N. "Vendor Security Questionnaire Best Practices and Risk-Based Due Diligence." Value Governance, 2026. https://valuegovernance.com/2025/12/10/vendor-security-questionnaire-best-practices-and-risk-based-due-diligence/