ESTABLISHING THE COMMON LANGUAGE OF CYBER RISK

POSITION PAPER

EXECUTIVE SUMMARY

Enterprises today face a foundational challenge in managing cyber risk. Despite billions spent on increasingly sophisticated defenses, the arms race between attackers and defenders has left most organizations no better protected in the mid-2020s than they were 10 or even 20 years ago.

How can responsible leaders break this cycle?
What must change beyond the current mix of tools, frameworks, and jargon?

The modern cybersecurity ecosystem has become a **Tower of Babel.** The average enterprise now runs more than 50 security solutions—*from endpoint protection and identity management to threat intelligence and next-gen firewalls*—each speaking a different language of data, metrics, and risk scores. Vulnerability feeds, CVEs, and event logs arrive in incompatible formats, with no common taxonomy or scale.

Even with this costly stack, the simplest boardroom question—**"How well protected are we?"**—remains unanswerable. This lack of normalization cripples observability, wastes scarce security resources, and undermines confidence in the data long before it reaches decision-makers.

Existing solutions fall short.

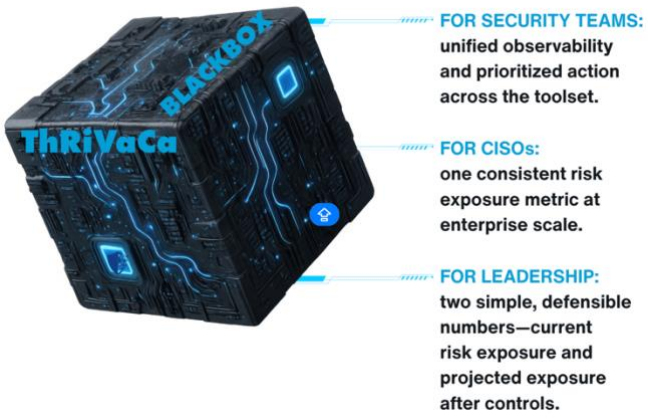
- SIEMs aggregate events but fail to normalize risk.
- Legacy models like FAIR and VaR attempt to quantify it—but depend on clean, consistent data that rarely exists and on human judgment that introduces bias.

The result is predictable: conflicting reports, incomplete visibility, and leaders unable to trust the numbers driving critical decisions.

FROM FRAGMENTATION TO FINANCIAL CLARITY

THE INDUSTRY DOESN'T NEED MORE DASHBOARDS— IT NEEDS TRANSLATION.

Cyber risk has two audiences that rarely speak the same language: machines and humans. Until those worlds align, cybersecurity will remain reactive, fragmented, and financially opaque.



ArxNimbus Thrivaca™ BlackBox solves this dual-language problem at its root. Acting as a universal translator, it first performs machine-to-machine translation—normalizing fragmented outputs across platforms into one actuarial-grade risk model. It then delivers machine-to-human translation, converting those normalized outputs into financial metrics that executives, boards, and regulators can trust.

The outcome is a single common language of cyber risk:

- For security teams: unified observability and prioritized action across the toolset.
- For CISOs: one consistent risk exposure metric at enterprise scale.
- For leadership: two simple, defensible numbers—current risk exposure and projected exposure after controls.

ArxNimbus Thrivaca BlackBox™ is not another reporting overlay. It is the foundation layer of modern cyber risk management—aligning security, finance, and governance around quantified, defensible, and actionable intelligence.

CONVERGING MARKET FORCES

THE LACK OF A COMMON LANGUAGE ACROSS TOOLS

The need for this unified foundation couldn't be more urgent. Market forces are converging to demand the very clarity ArxNimbus delivers—clarity that regulators, investors, and insurers now expect as standard practice.

Enterprises are drowning in complexity.

The average organization runs **53 security tools**, with one in five managing more than 75. **But more tools do not mean more clarity**. Instead, CISOs find themselves reconciling a flood of fragmented, inconsistent outputs while regulatory pressure and stakeholder expectations rise.

The SEC's 2023 cyber disclosure rules, Europe's DORA framework, and the upcoming Cyber Resilience Act all increase the demand for standardized, defensible risk reporting. At the same time, insurers and investors are pushing enterprises to demonstrate financial-grade cyber resilience. The MITRE ATT&CK framework has gained wide adoption as a common reference point for threats, yet it only partially addresses the deeper issue: **the lack of a common language across tools.**

THE PROBLEM: THE BABEL OF TOOLS

NO SINGLE, CONSISTENT VIEW OF ENTERPRISE EXPOSURE

Enterprises depend on dozens of platforms—Qualys, Wiz, Armis, Snyk, Tenable, Rapid7, CrowdStrike, and many others—to identify vulnerabilities and manage assets. Each tool applies its own taxonomy, format, and scoring system. A vulnerability critical in one system may not even register in another. **Asset inventories and CVE reporting are siloed, fragmented, and irreconcilable.**

The result is a **babel of tools** where CISOs and their teams lack the ability to form a single, consistent view of enterprise exposure. Even before reaching the board, the absence of normalized data cripples observability, limits actionability, and erodes confidence in decision-making.

Layering SIEMs on top has not fixed the problem. SIEMs centralize logs but do not normalize risk data. Legacy CRQ models assume consistent inputs that enterprises simply do not have. The outcome: fragmented reporting, misaligned priorities, and boards left with incomprehensible or incomplete metrics.

ESCAPE FROM THE BABEL OF TOOLS

A SINGLE TRUSTED VIEW OF RISK

The solution isn't another dashboard—it's translation. To escape the Babel of tools, enterprises need a foundation layer that normalizes every data source into a single, trusted view of risk.

That's precisely what ArxNimbus Thrivaca BlackBox™ was built to do.

Designed in collaboration with US Strategic Command, MITRE Corp and the University of Chicago, ArxNimbus Thrivaca BlackBox addresses this dual-language problem at its root by functioning as a **universal translator** across both machines and humans.

Technical Integration (Machine-to-Machine Translation)

- **Normalize Fragmented Data**: Consolidates CVEs, asset records, and vulnerability outputs from multiple platforms into a single actuarial-grade standard.
- **Unified Metric Across Tools**: Delivers one consistent risk exposure metric regardless of vendor or source.
- **Enterprise Scale**: Processes 600,000+ endpoints and 5,300+ applications without bottlenecks.

Business Translation (Machine-to-Human Translation)

- **Financial Clarity**: Converts normalized technical outputs into actuarial, dollarized metrics aligned with NIST, MITRE, and actuarial science.
- **Two Defensible Numbers**: Provides board-ready clarity with current financial risk exposure and projected exposure after controls.
- **ROI Justification**: Enables CISOs to show the impact of every control dollar by unit, application, and initiative.

***THE RESULT:* ArxNimbus becomes both the foundation layer of technical observability and the common language of financial cyber risk.**

BENEFITS FOR CISOs & THE ENTERPRISE

1. **Unified Observability Across the Toolset**	ArxNimbus Thrivaca BlackBox eliminates the inefficiency and risk caused by tool sprawl. By normalizing vulnerability, CVE, and asset data across dozens of platforms, it provides CISOs with a single, coherent view of enterprise exposure.
2. **Actionable Risk Prioritization**	With one actuarial-grade exposure metric, security leaders can prioritize remediation based on financial impact, not conflicting alerts.
3. **Enterprise Scalability**	Thrivaca BlackBox reliably processes risk across hundreds of thousands of endpoints and thousands of applications, ensuring consistent visibility across business units and geographies.
4. **Boardroom and Executive Clarity**	Once normalized, outputs are translated into actuarial, dollarized risk metrics. Boards receive two clear numbers—current exposure and projected exposure after controls—allowing for defensible decisions on budget and strategy.
5. **ROI-Driven Decision Making**	Security spend is no longer a black box. ArxNimbus demonstrates the return on every dollar invested in controls and initiatives.
6. **Talent Enablement and Futureproofing**	New hires and security teams work from a unified, standardized framework rather than fragmented reports, accelerating onboarding and preventing reversion to legacy practices

SUMMARY: FROM FRAGMENTED TOOLS TO UNIFIED INTELLIGENCE

SECURE THE BUSINESS, NOT JUST THE TECHNOLOGY

The evidence is clear: technology sprawl isn't delivering better protection. The next leap in cybersecurity maturity comes from integration, normalization, and financial translation—not more point solutions.

While massive investment has gone into increasingly sophisticated and costly point solutions, the payoff from continuing this path is now clearly diminishing. The real answer lies in solving the overall problem and gaining a complete view of the security landscape—not deploying more and more isolated tools. Forward-thinking management teams are recognizing these limitations and moving to secure the business, not just the technology.

Early results demonstrate measurable ROI through reduced risk exposure, optimized cyber insurance programs, and enhanced litigation preparedness—all supported by complete traceability and adherence to recognized standards.

Boards and management teams now have clear answers to three critical questions:

1. ***How much cyber risk does the organization face?***
2. ***Where does it originate?***
3. ***What is the financial impact?***

ABOUT THE AUTHORS

R. David Moon, CEO and co-founder of ArxNimbus, is a quant-focused cybersecurity risk specialist, Fortune 500 CIO, CISO, Big Four consulting partner, CISSP, software industry product manager and senior officer. A four-year US Air Force veteran with Secret clearance, David is an expert information security and executive-level technology professional with a 20+ year portfolio of some of the most ground-breaking and high-value project results in information security, technology, privacy, asset management, IT risk management and infrastructure. For more than a decade he has been privileged to serve and consult to some of the world's most respected organizations in the United States, Latin America, and Europe. His writing includes examining the measurable value of technology-based capability and its role in risk mitigation in the 2011 book “Webify” (https://www.amazon.com/Webify-Interconnections-Strategy-Capability-Volatility-ebook/dp/B006RX4PXM). He has served on the board of a public investment trust and as a member of the senior executive committee of a $5bn Nasdaq company.

Andrew Patterson, COO of ArxNimbus, leads the delivery and optimization of advanced cyber and AI risk management solutions. His distinctive background bridges public service and private sector expertise in global risk management. Prior to joining ArxNimbus, Andrew held several high-level positions in government, including Deputy Chief of Staff and Global Risk Advisor at the U.S. Department of Energy and liaison to the National Security Council. In these roles, he shaped critical risk management strategies at the highest levels of government decision-making. Andrew's private sector experience encompasses strategic positions with PwC's Research and Insights team, where he analyzed emerging global risks and trends. His background also includes significant work with leading hedge funds and commodity traders, helping these organizations anticipate and navigate complex operational and portfolio risks. In his decades of risk management experience, Andrew has pioneered a unique methodology that integrates advanced analytics with hands-on implementation expertise, empowering organizations to proactively identify and address emerging cyber threats.

ABOUT ARXNIMBUS | CYBERSECURITY FOR BUSINESS

ArxNimbus transforms how organizations see, measure, and manage cyber risk. Built on actuarial science and advanced analytics, our Thrivaca™ data engine converts fragmented technical data into financially defensible intelligence. Originally commissioned by U.S. Strategic Command and co-developed with MITRE Corp and the University of Chicago, Thrivaca™ delivers the industry’s first NIST-aligned, actuarial-grade model for quantifying cyber exposure. Today, ArxNimbus equips enterprises, insurers, and investors with the clarity to make confident, risk-adjusted decisions—and build true cyber resilience in an age of AI-driven complexity.

Contact: info@arxnimbus.com | 888-422-6584 | ArxNimbus.com/thrivaca-blackbox
Follow us on LinkedIn for the latest cyber risk insights.