ArxNimbus

ThrivacaCORE™

PRODUCT SUMMARY

WHAT IS ThrivacaCORE™?

ArxNimbus ThrivacaCORE is the only NIST-aligned actuarial platform that quantifies cyber exposure in financial terms—delivering a defensible baseline of EBITDA at risk.

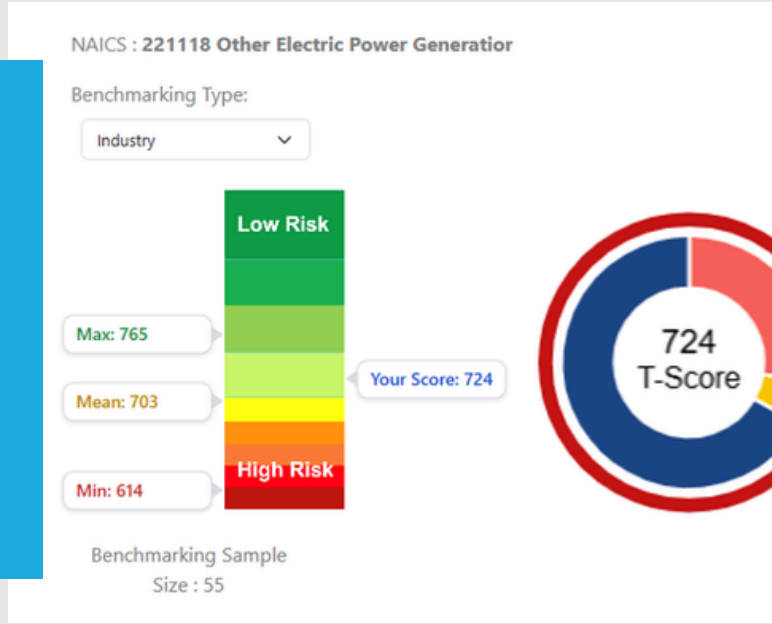
Powered by the patented Thrivaca actuarial AI engine, **CORE** combines external threat intelligence with enterprise data to produce a complete financial exposure profile—*within hours, not months.*

T-Score™: Your Exposure, Benchmarked, as a Point-in-Time Measurement

T-Score™ (0–1000 actuarial risk positioning) provides a standardized benchmark of your organization's exposure relative to peers.

Think of it as a credit score for cyber exposure—but grounded in actuarial modeling and financial impact, not subjective scoring.

- Benchmark exposure across industry and peer groups
- Understand relative risk positioning instantly
- Track improvement as exposure is reduced



CORE establishes your starting point—quantifying exposure today so it can be continuously managed and reduced over time.

Machine-to-Machine Normalization:

Integrates external scans, threat intelligence, and enterprise data into a unified actuarial exposure model—eliminating fragmented tools and inconsistent inputs.

Trusted by Insurers Underwriting 35% of the S&P 500

Machine-to-Human Financial Translation:

Converts technical exposure into quantified financial impact—expressed as EBITDA at risk and defensible exposure metrics executives, boards, and insurers can act on.

1.

ArxNimbus

ThrivacaCORE™

Defensible Financial Outcomes.
Not Subjective Scoring.
Your Financial Exposure Baseline.
In Dollars. Within Days.

Powered by the Thrivaca Actuarial Engine

Two Numbers Boards Trust:

- → Current EBITDA at Risk
1. → Projected Exposure After Mitigation
2. Every decision measured against financial impact
3.
4.

Actuarial Financial Truth:

Built on real-world loss data and insurance-grade modeling—not assumptions—delivering exposure grounded in probability and financial impact.

MOST ORGANIZATIONS CAN'T MEASURE FINANCIAL EXPOSURE.

CORE CHANGES THAT.

Cyber exposure isn't a visibility problem. It's a measurement problem. Yet most organizations cannot answer the boardroom's most fundamental question: ***"How much financial exposure does our business face?"***

PROBLEM:	CORE SOLVES:
The Illusion of Security: Organizations deploy 50+ sophisticated security tools but lack unified visibility into actual financial exposure. Spending millions creates a false sense of protection without a common language to measure what's working.	ThrivacaCORE establishes a single actuarial-grade risk metric across all tools—breaking through the illusion with defensible financial truth.
The Communication Gap: A documented 12–30 percentage point gap exists between what CISOs report and what boards understand. Heat maps and traffic-light scoring lack the precision for fiduciary decision-making.	Dual translation converts technical complexity into two numbers boards trust: current EBITDA at risk and projected exposure after controls.

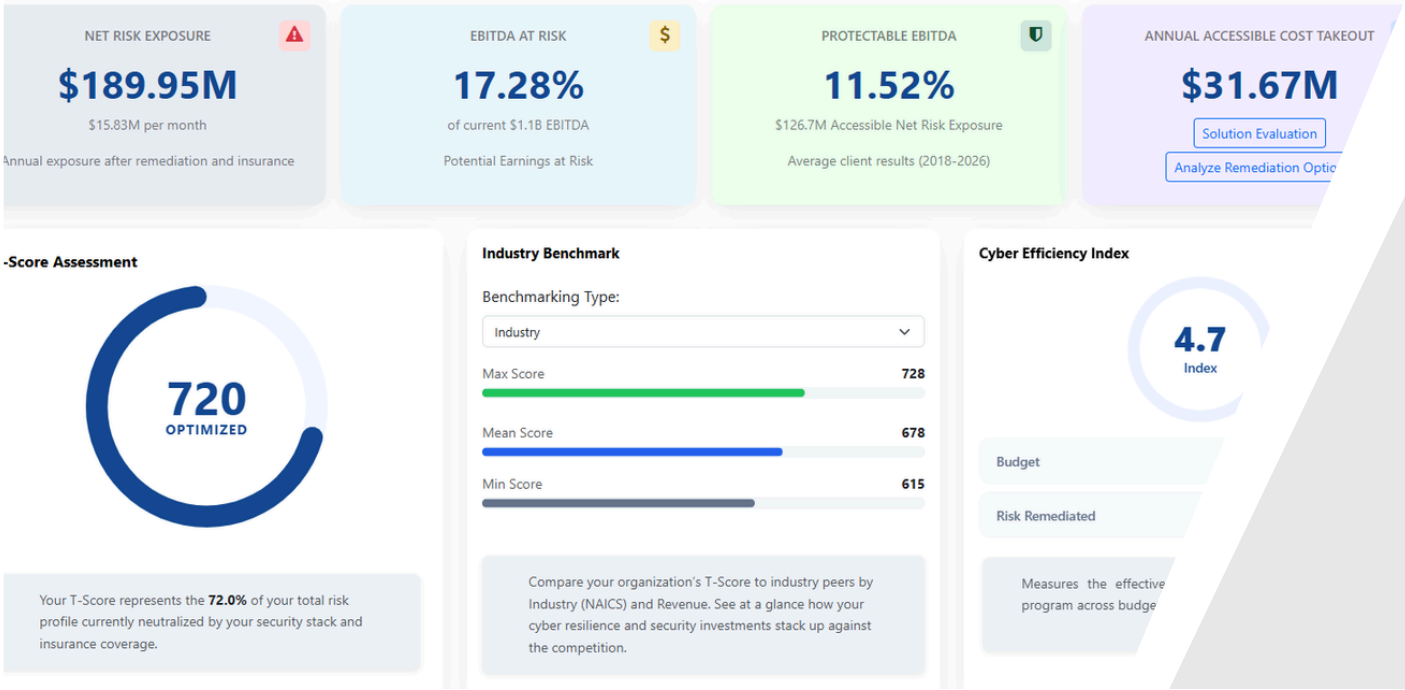
BOARDS FACE FUDICIARY EXPOSURE WITHOUT FINANCIAL TRUTH

MOST ORGANIZATIONS CAN'T MEASURE FINANCIAL EXPOSURE.

CORE CHANGES THAT.

PROBLEM	CORE SOLVES
Subjective Risk Models: Legacy CRQ approaches (FAIR, Monte Carlo, VaR) depend on professional opinion and expert judgment, introducing bias and producing estimates that fail under legal and audit scrutiny.	Actuarial methodology validated by insurers, NIST, and academic institutions delivers audit-defensible, repeatable results—not opinions.
Hidden Exposure: Organizations consistently underestimate true digital risk by 89–400%. Unfunded liabilities, insurance gaps, and unquantified exposures remain invisible until a breach reveals them.	CORE quantifies actual financial exposure in days—often revealing risk exceeding 25% of EBITDA.

Without actuarial quantification, cyber exposure remains opaque, unmanaged, and indefensible.



CORE ENGINE CAPABILITIES→

HOW EXPOSURE IS MEASURED.

- EXPOSURE QUANTIFICATION: impact valuation, probability engine, financial translation
- BENCHMARKING & POSITIONING: T-score, peer comparison, efficiency index
- CONTROL & FRAMEWORK MAPPING: NIST, MITRE, compliance
- SCENARIO & DECISION MODELING: digital twin, ROI modeling, integrations

ACTUARIAL CYBER RISK QUANTIFICATION (ACRQ)

How CORE Calculates Financial Exposure. It's not magic. It's math.

FUNCTION	WHAT IT DOES	WHY IT MATTERS
Impact Valuation	Calculates potential financial impact across eight risk types (hacktivism, denial of service, ransomware, digital fraud, insider threat, data breach, IP theft, business interruption) using economist-defined formulas developed with the University of Chicago.	Produces Near Worst Case Scenario (NWCS) exposure values calibrated at 85% of worst case—providing conservative yet realistic loss estimates that boards and insurers trust.
Probability Engine	Applies actuarial loss distributions validated by insurance industry data to quantify the likelihood of each risk type materializing, based on 300+ years of actuarial science.	Eliminates subjective scoring. Produces audit-defensible, repeatable risk estimates with 85% demonstrated predictive accuracy (validated in the UnitedHealthcare breach: $7.4B projected vs. $6.3B actual).
Financial Translation	Converts actuarial risk output into dollarized exposure metrics: EBITDA at Risk, Net Risk Exposure, Remediated Risk value, annualized expected loss by control family, and ROI per remediation dollar.	Translates cyber risk into the same financial language used for all other business decisions—enabling direct comparison to revenue, margins, and capital allocation.
Threat-Vulnerability Mapping	Maps 47,000+ threat-vulnerability pairings across dual threat taxonomies (FFIEC 23 high-level threats + MITRE ATT&CK ~1,200 attack techniques) to specific financial exposure.	Precisely attributes financial risk to specific technical vulnerabilities. One healthcare provider used this precision to eliminate 97% of cybersecurity risk by targeting the issues creating the most business exposure.

BENCHMARKING & INTELLIGENCE

How CORE Positions Your Risk Against the Market

FUNCTION	WHAT IT DOES	WHY IT MATTERS
T-Score™ Risk Measurement	Standardized 0–1000 scale quantifying organizational risk posture relative to industry peers, updated quarterly against a database of 3,500+ companies across 580 industries.	Provides clear, comparable risk positioning—like a credit score for cybersecurity. Enables boards to ask "Where do we rank?" and get a defensible answer.
Cyber Efficiency Index	Calculates return on cybersecurity investment: dollars of risk reduced per dollar of security spend. Benchmarks organizational efficiency against industry peers.	Leading organizations achieve $144 in risk reduction per $1 spent. The Index reveals whether security budgets are producing measurable results or creating diminishing returns.
Competitive Intelligence Database	Largest commercial risk profile library tracking every U.S. publicly traded company (NASDAQ, NYSE, S&P 500, Russell 2000)—providing continuous performance comparison.	Enables data-driven conversations about competitive positioning, M&A due diligence, and insurance optimization with peer-validated benchmarks.

FRAMEWORK & COMPLIANCE ANALYTICS

How CORE Maps Exposure to Controls and Compliance

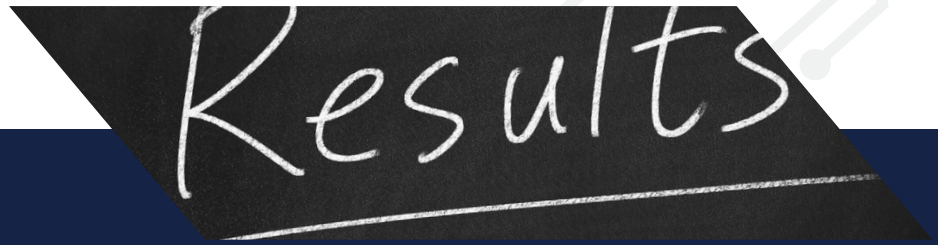
FUNCTION	WHAT IT DOES	WHY IT MATTERS
NIST CSF Analysis	Evaluates organizational capability and expected loss across all six NIST CSF functions (Identify, Protect, Detect, Respond, Recover, Govern) with specific control-level attribution.	Shows exactly where capability gaps create the highest financial exposure—enabling targeted investment that maximizes risk reduction per dollar.
MITRE ATT&CK Analysis	Ranks Top 200 attack techniques by expected loss value, mapping organizational vulnerability to the specific techniques most likely to cause financial harm.	Prioritizes remediation by business impact, not just technical severity. Identifies which attack techniques represent the greatest EBITDA threat.
Multi-Framework Reporting	Generates compliance analytics across NIST 800-53, ISO 27001, CMMC, HIPAA, and sector-specific frameworks with 650+ NIST-approved remediation playbooks.	Supports regulatory readiness and audit preparation with quantified, control-level evidence rather than checkbox compliance.

ADVANCED CAPABILITIES

How CORE Supports Strategic Decision-Making

FUNCTION	WHAT IT DOES	WHY IT MATTERS
Digital Twin Technology	Creates virtual replicas of organizational security environments for "what-if" scenario modeling—evaluating potential improvements, M&A impacts, technology deployments, and strategic alternatives before implementation.	One healthcare organization evaluated seven potential improvement scenarios before committing resources—from M&A analysis to telehealth expansion—reducing decision risk and accelerating outcomes.
Arx+ Enhancement Modules	Extends core capabilities with specialized solutions: ProActive Defense (DoD-grade AI threat detection with 9 months earlier breach identification), Enterprise Security (unified endpoint/email/cloud protection), Asset Management (graph-based discovery), and Data Security (automated SBOM/RBOM generation).	Modular architecture lets organizations deploy capabilities in phases based on priorities and budget—each module feeds automated data back to the actuarial engine, continuously improving model precision.
Integration-First Design	RESTful APIs connect to existing SIEM, vulnerability management, endpoint, cloud security, and asset management platforms. Behind-the-firewall data aggregation for internal network analysis. Built-in integration with Security Scorecard, Risk Recon, NESSUS, Panorays, and Alien Vault OTX.	Works with your existing tools—no replacement required. Makes prior security investments more valuable by translating their outputs into a common financial risk language.

KEY OUTCOMES WITH ThrivacaCORE



- **Unified Financial Truth for Cyber Exposure**
  Defensible, dollarized exposure metrics trusted by insurers, auditors, and enterprise leaders—Not dashboards or subjective scoring.
- **Board-Ready Clarity**
  Cyber exposure communicated in EBITDA terms that executives can govern, measure, and act upon—closing the 12–30% CISO-to-board communication gap.
- **Measurable ROI on Security Spend**
  Every remediation dollar tracked against financial risk reduction, with leading organizations demonstrating real-world $10–$144 in risk reduction per $1 invested.
- **Regulatory & Insurance Confidence**
  Auditable, NIST-approved actuarial methodology supporting compliance evidence, SEC disclosure, and insurance underwriting optimization.
- **Compliance Intelligence**
  Clear positioning against 3,500+ peer organizations, revealing optimization opportunities and validating strategic cybersecurity investments.

KEY OUTCOMES WITH CORE:

Validated Outcomes Across Real-World Deployments

METRIC	RESULT
Cyber Risk Eliminated (Healthcare)	**97% of total exposure over 5 years**
EBITDA at Risk Reduced (Healthcare)	**From 18.60% to 4.98% (−73%)**
Annual Earnings Protected (Healthcare)	**~$7M per year**
Return on Investment (Healthcare)	**$145 exposure reduction per $1 spent**
T-Score Achievement (Healthcare)	**965 (elite performance, 0–1000 scale)**
Hidden Risk Discovered (Financial Services)	**$381M actual vs. $75M estimated (408% variance)**
Cost Recovery Year 1 (Financial Services)	**$25M in previously unrecognized costs**
Risk Carrying Cost Reduction (Financial Services)	**8.2% reduction in first year**
Predictive Accuracy (UnitedHealthcare)	**$7.4B projected vs. $6.3B actual (85% accuracy)**
Assessment Variance Uncovered (Bio-Pharma)	**89% underestimation of data breach risk; 98% miscalculation of ransomware losses**

ThrivacaCORE

When You Need a Defensible Baseline—Fast.

- **CISOs**: Translate technical exposure into measurable financial impact—establishing a baseline for prioritization and board communication.
- **CFOs:** Quantify cyber exposure in EBITDA terms—enabling capital allocation, risk transfer decisions, and financial accountability.
- **CROs:** Benchmark enterprise exposure against peers—grounded in actuarial modeling, not subjective scoring.
- **Boards & C-Suite:** Replace fragmented reporting with a single, defensible financial view of exposure—before approving investments or strategy.
- **Legal & Compliance:** Establish an auditable, NIST-aligned record of exposure—supporting regulatory disclosure and litigation defensibility.
- **Insurance & Risk:** Quantify exposure to optimize coverage strategy, underwriting alignment, and premium negotiations.

CORE answers the first question every stakeholder shares: "Where do we stand today—in financial terms?"

Where CORE Creates Immediate Financial Clarity

APPLICATION	DELIVERABLE
Board & C-Suite Communication	Delivers board-ready financial metrics aligned with NACD governance principles and SEC disclosure requirements. Two defensible numbers—current EBITDA at risk and projected exposure after controls—replace subjective heat maps. Includes PowerPoint board presentation template with SEC and NACD guidelines. Enables up to 30-minute quarterly board cyber risk reviews with strategic value demonstration.
Cybersecurity Program Optimization	Identifies the highest-impact areas for risk reduction based on financial exposure, not just technical severity. Within the first week, quantifies the cost-benefit of all cybersecurity challenges. Over 90–120 days, pinpoints targeted risk reduction priorities aligned to budget, risk appetite, and organizational goals. The Cyber Efficiency Index reveals whether security spending is producing measurable ROI or diminishing returns.
Merger & Acquisitions	Generates independent Risk Profiles for both acquiring and target companies, enabling direct comparison of digital risk postures. Identifies unfunded cybersecurity liabilities that affect deal valuation—some M&A deals have lost up to $100M from undetected cyber exposure. Thrivaca ROI analysis identifies the most valuable remediation strategies to include in integration planning.
Benchmarking	Compares organizational cybersecurity posture against 3,500+ peer companies across 580 industries using T-Score™ and Cyber Efficiency Index. Identifies best-in-class practices, competitive gaps, and optimization opportunities. Tracks progression over time from “Unaware” to “Optimized” on the Digital Risk Journey maturity model.

Where CORE Creates Immediate Financial Clarity

APPLICATION	DELIVERABLE
Cyber Insurance Planning	Quantifies actual financial exposure to determine appropriate coverage levels, deductibles, and policy structures. Identifies areas where self-remediation is more cost-effective than insurance transfer. Prevents underinsurance disasters—as demonstrated when UnitedHealthcare held only $100M in coverage against $6.3B in actual breach losses.
Regulatory Compliance & Audit Support	Maps risk quantification to NIST, ISO 27001, CMMC, HIPAA, PCI DSS, and sector-specific frameworks with 650+ remediation playbooks. Provides data-driven, auditable evidence of cybersecurity posture—replacing checkbox compliance with quantified control-level risk attribution. Supports SEC cyber disclosure requirements with defensible financial metrics.
Litigation Support	Documents cybersecurity due diligence with actuarial-grade evidence that withstands legal scrutiny. Tracks organizational risk progression over time, demonstrating systematic improvement. Provides quantified loss estimates aligned to NIST controls that support both defense and insurance recovery arguments.
Remediation Solution Selection	Prioritizes remediation investments based on financial return—showing which vulnerabilities create the most EBITDA exposure and which controls deliver the greatest risk reduction per dollar. Eliminates the “fix everything equally” approach that wastes resources on low-impact issues while critical exposures persist.

ThrivacaCORE DEPLOYMENT SNAPSHOT

DELIVERY	SaaS platform with optional on-premise integration
SETUP TIME	Days, not months. Initial Risk Profile within 48 hours or up to 5 days (if integrating).
DATA SOURCES	External scans (automated), customer financial data, security documentation, risk registers, audit reports, penetration testing results, SME attestation, and optional direct SIEM/vulnerability management integration via RESTful API.
INITIAL ANALYSIS	Week 1: Complete Risk Profile with cost-benefit quantification of all cybersecurity challenges. Days 90–120: Targeted risk reduction plan aligned to budget and risk appetite.
COMPLIANCE ALIGNMENT	NIST CSF, NIST 800-53, MITRE ATT&CK, ISO 27001, CMMC, HIPAA, PCI DSS, FFIEC, and sector-specific frameworks. 650+ NIST-approved remediation playbooks.
SCALE	Enterprise-grade: validated to 600,000+ endpoints, 5,300+ applications. Benchmarking database covers 3,500+ companies across 580 industries.
ENHANCEMENT OPTIONS	Arx+ modules: ProActive Defense, Enterprise Basic/Full, Data Security (SBOM/RBOM), and AI Operational Assurance (AIBOM)—each feeding automated data back to the actuarial engine.

Organizations often uncover unquantified exposure exceeding 25% of EBITDA.

Clients typically achieve 1–3% EBITDA improvement through risk reduction.

Recognized: Chicago Innovation Awards Finalist | Gartner Cool Vendor | Momentum Cyber CyberScape | Cyber Insurance Insider 2025 | Pepperdine Most Fundable | Chicago Booth NVC Finalist | WIPO PCT International Patent

ArxNimbus

ArxNimbus replaces the illusion of security with financial truth.

Thrivaca™ combines AI and actuarial modeling to do what traditional approaches can't: normalize fragmented security data at scale and convert it into defensible financial exposure.

This isn't scoring. It's measurement—grounded in real-world loss data, expressed in EBITDA, and trusted by boards, insurers, and regulators.

AI to normalize.
Actuarial science to quantify.
Financial truth to govern.

It's not magic. It's math.

888-422-6584
info@arxnimbus.com
arxnimbus.com/CORE