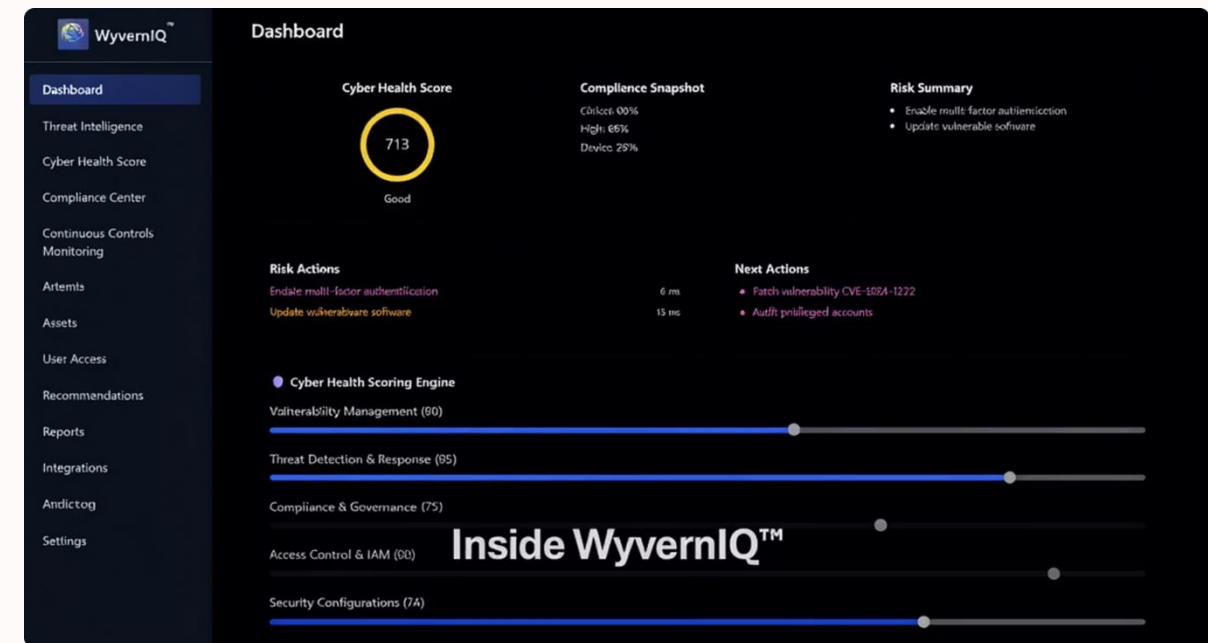# WyvernIQ™

AI Platform for Risk Scoring & LLM-Powered Compliance Intelligence

Intelligent Cybersecurity for a Secure Future

Problem

The Defense Information Systems Agency (DISA) faces the challenge of rapidly onboarding commercial software while ensuring strict compliance with DoD RMF, IL5/IL6 overlays, and the internal ATO process. Traditional methods rely on spreadsheets, static documentation, and fragmented toolsets, which can drag the ATO process out for up to two years. Vendors often struggle to clearly separate inherited controls (provided by DISA services like VDSS, Olympus, CI/CD pipelines, DLP, and network segmentation) from those they must implement themselves. This creates costly delays, redundant work, and incomplete packages—slowing DISA's ability to deliver secure, modern capabilities to the warfighter.

Solution: WyvernIQ™

WyvernIQ™ is an AI-powered cybersecurity and compliance platform that dramatically reduces the ATO timeline. Purpose-built for internal DoD systems and vendors operating in DISA-managed environments, WyvernIQ unifies:

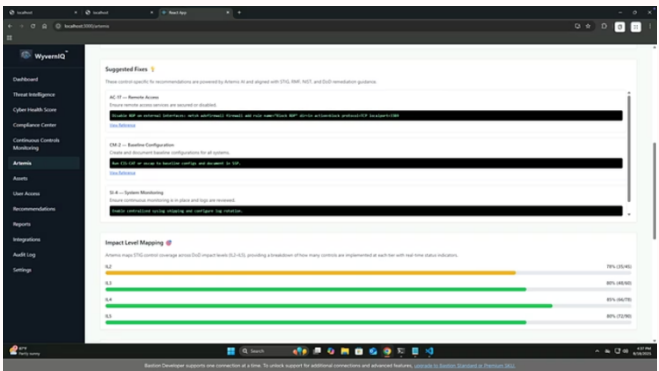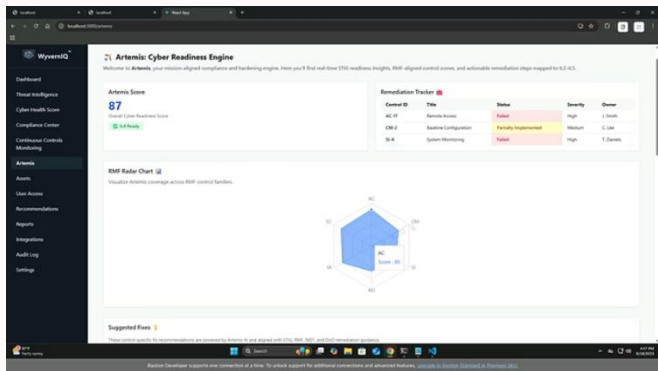|		
AI-driven RMF automation	**Continuous controls monitoring**	**A real-time Cyber Health Score**

Instead of reconciling disconnected spreadsheets and static artifacts, WyvernIQ automatically maps inherited vs. implemented controls, tracks compliance progress, and generates SSPs and POA&Ms more efficiently.

Artemis: The Core Engine

At its core is **Artemis**, WyvernIQ's remediation engine. Artemis delivers STIG-aligned recommendations, drafts compliant narratives, and provides automated fixes—reducing remediation cycles from months to days. Combined with continuous monitoring, leadership gains a FICO-style Cyber Health Score, offering a transparent, real-time view of readiness and risk.

APL Readiness

Configuration Alignment

Aligns configurations to APL requirements

Control Validation

Validates inherited vs. implemented controls

STIG Compliance

Ensures STIG/DISA baseline compliance

Automated Readiness

Automates readiness checks for APL listing

WyvernIQ, within Artemis, also provides a structured pathway to navigate the **DoD Approved Products List (APL)** process—something rarely offered in the market. The platform aligns configurations, control mappings, and evidence to APL requirements, validates inherited vs. implemented controls, ensures STIG/DISA baseline compliance, and automates readiness checks. This reduces cost, time, and uncertainty for APL listing, while creating a repeatable, low-risk approval pathway for future products.

Why WyvernIQ Stands Out

Unique Cyber Health Score

For real-time posture measurement, like a FICO score for cyber.

AI + LLM-powered automation

For RMF, SSP, POA&M, and evidence generation.

Control inheritance mapping

Tailored to DISA-managed services.

Artemis remediation engine

For automated STIG-aligned fixes and compliance narratives.

Continuous Controls Monitoring

To support continuous ATO (cATO).

Flexible deployment

As SaaS or fully self-hosted for IL5/IL6 and air-gapped environments.

DoD APL readiness automation

Cutting months off traditional validation.

ⓘ Vetted and backed by Carahsoft, Microsoft for Startups, NVIDIA Inception, and Google Cloud for Startups—reducing procurement and delivery risk.

How WyvernIQ's AI Platform Works

AI Scoring Engine: Real-time Cyber Health Score powered by Bayesian & time-series models.

CLI & PaaS Automation: API-first interface for both SaaS and Self Hosted deployments; enables automation, CI/CD integration and secure remote ops.

Continuous Monitoring: Tracks score drift, failed controls and remediation over time.

LLM Decision Layer: Executive summaries, fix prioritization and cost-of-inaction estimates.

Control Mapping via NLP: Maps ISO, HIPAA, PCI, STIG, NIST and SOC 2 frameworks to real-time cloud posture.

Model Context Protocol (MCP): Manages ML lifecycle context: inference, retraining and optimization.

Inside WyvernIQ™

- **Smart Risk Detection**

  Our AI analyzes data across your, systems finding hidden patterns and connections.

- **Total Security Score**

  Get a clear, unbiased score of your security health, bringing together threat information and compliance into one easy metric.

- **Automated Compliance**

  Automatically align your security with standards like CMMC, HIPAA, PCI, and SOC2, making audits less work.
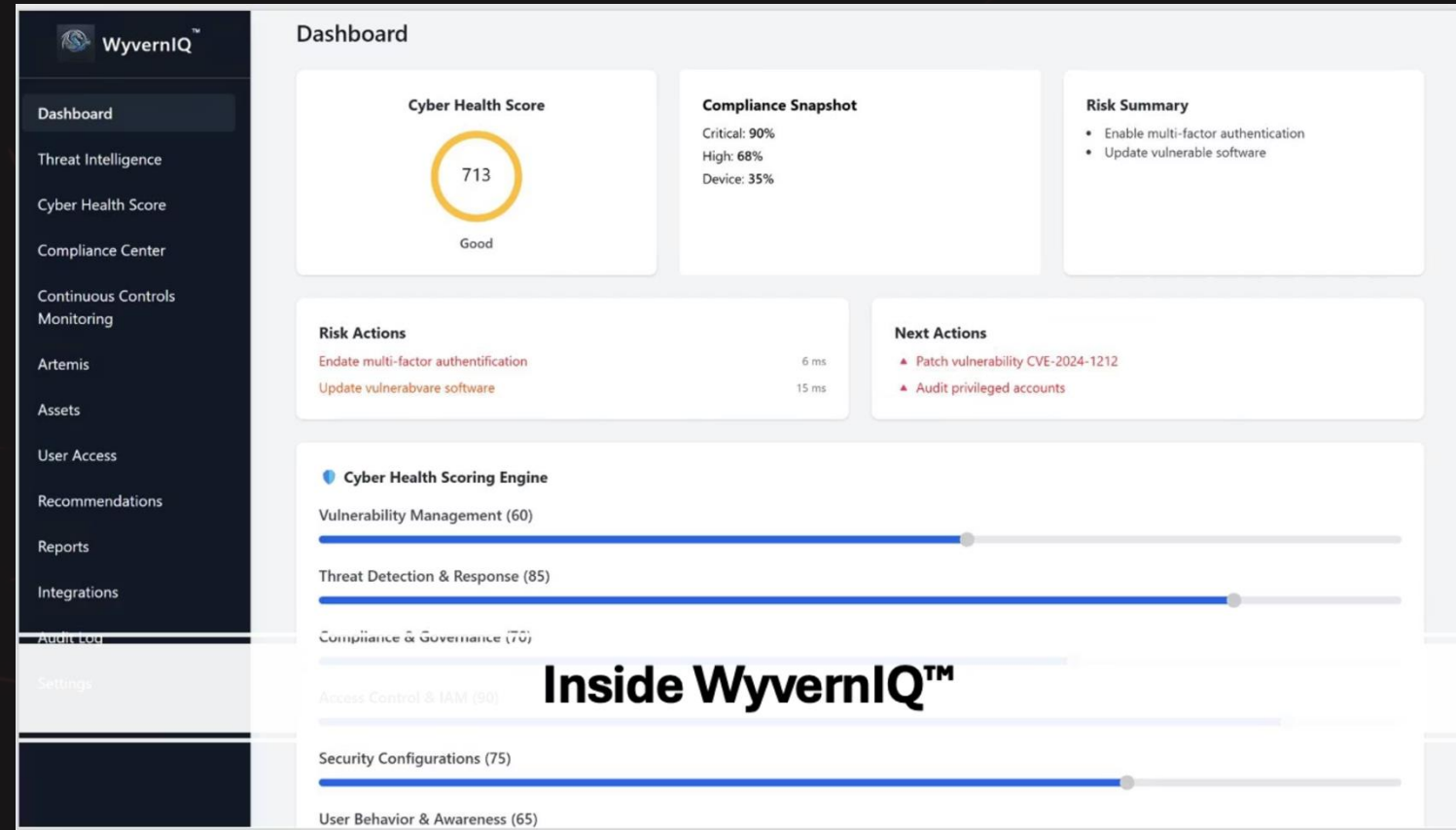
- **Easy Setup**

  Integrate quickly with your cloud and security tools using simple connections, no extra software needed.
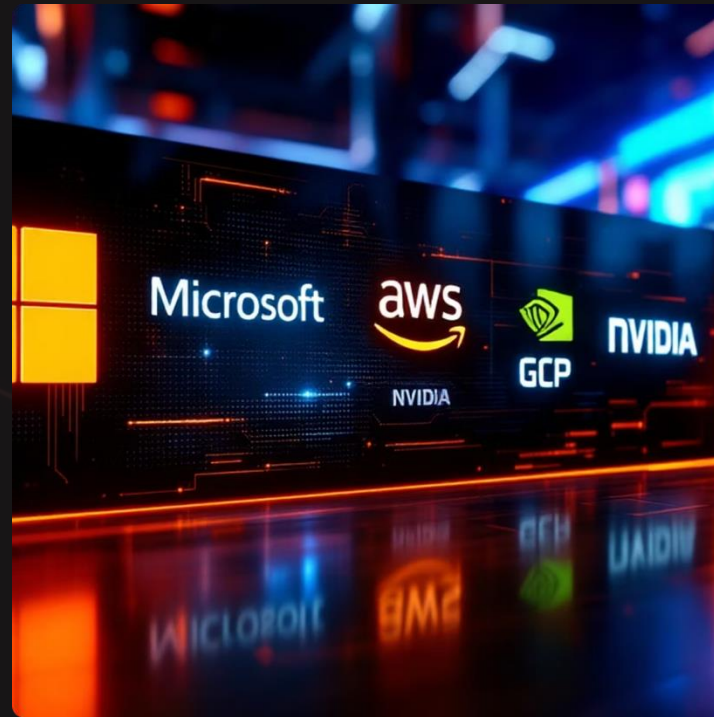
- **Prioritized Solutions**

  Focus on the most important actions with AI-powered advice, ranked by how much they reduce risk and fit your business needs.

- **Leadership Reports**

  Turns complex security information into clear, business-focused insights for better decision-making.

Dashboard

WyvernIQ™

- Dashboard
- Threat Intelligence
- Cyber Health Score
- Compliance Center
- Continuous Controls Monitoring
- Artemis
- Assets
- User Access
- Recommendations
- Reports
- Integrations
- Audit Log
- Settings

Cyber Health Score

713

Good

Compliance Snapshot

Critical: 90%
High: 68%
Device: 35%

Risk Summary

- Enable multi-factor authentication
- Update vulnerable software

Risk Actions

Endate multi-factor authentification — 6 ms
Update vulnerabvare software — 15 ms

Next Actions

- Patch vulnerability CVE-2024-1212
- Audit privileged accounts

Cyber Health Scoring Engine

Vulnerability Management (60)

Threat Detection & Response (85)

Compliance & Governance (70)

Inside WyvernIQ™

Access Control & IAM (90)

Security Configurations (75)
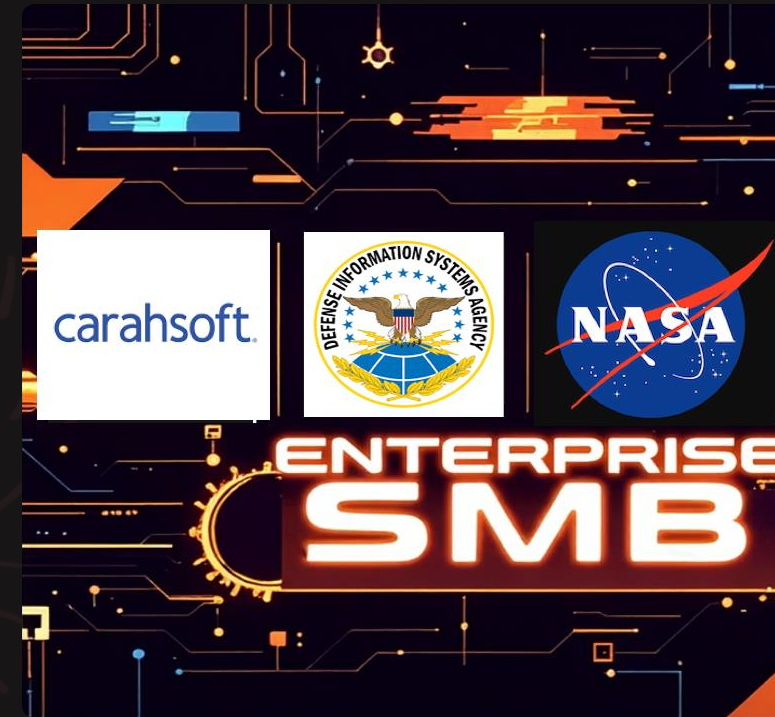
User Behavior & Awareness (65)

Early Validation & Momentum

Technical Validation

Integrated with Azure, AWS, and GCP APIs

Backed by Microsoft for Startups Founders Hub

NVIDIA Inception program member

Google Cloud for Startups participant

MVP completed and undergoing internal penetration testing

Market Validation

Aggregator agreement with Carahsoft for SLED

3 Early Partners (MSSPs & Compliance Advisors)

Pipeline: 3 SMB Prospects + 2 MSSPs in pilot discussions

Cost Savings & Headcount Reduction

Automates compliance & security triage

WyvernIQ™ replaces the manual, repetitive work of sorting through thousands of alerts, compliance checklists, and audit prep tasks. What once required dozens of analyst hours daily is now handled automatically by our AI-powered engine.

Reduces headcount requirements by up to 40%:

Security and compliance teams typically allocate 30–50% of staff time to low-value reporting and documentation. WyvernIQ™ eliminates this bottleneck, allowing organizations to operate leaner while reallocating talent toward higher-value risk strategy and innovation.

Millions in annual admin-to-dollar savings

For a mid-sized enterprise with a 10-person GRC/security team, WyvernIQ™ can offset the workload of 3–4 FTEs, equating to $400K–$600K+ in direct salary savings annually. For larger enterprises and federal agencies, savings scale into the multi-million range per year when factoring reduced audit costs, faster ATO cycles, and avoided regulatory penalties.

Board-level visibility on ROI: By quantifying cyber risk through the Cyber Health Score and tying it to headcount and financial metrics, WyvernIQ™ makes cost savings **transparent to CFOs and Boards**—not just security teams.

How WyvernIQ™ Stands Apart

As the comparison table illustrates, WyvernIQ provides a unique combination of capabilities not found in existing market solutions. Our platform goes beyond mere detection and asset management, offering proactive, prioritized remediation and business-centric insights that directly empower leadership to make informed cybersecurity decisions.

Feature / Capability	WyvernIQ	Wiz	Drata	Axonius
Cyber Health Score	✅	❌	❌	❌
Compliance + Threat Integration	✅	❌	✅	❌
DoD & APL Readiness	✅	❌	❌	❌
Agentless API-Based	✅	✅	❌	✅
AI-Powered Remediation Guidance	✅	❌	❌	❌
Cost-of-Inaction Estimates	✅	❌	❌	❌
Continuous Control Monitoring	✅	❌	❌	❌
Executive-Level Reporting	✅	❌	❌	❌

"While others address parts of the puzzle, WyvernIQ delivers a complete, accessible solution."

The WyvernIQ™ Impact

BEFORE WYVERNIQ

- ⬆ 24+ Months ATO
- ⬆ Redundant Manual Processes
- ⬆ Control Mapping Complexity
- ⬆ Static Documentation

WYVERNIQ

AFTER WYVERNIQ

- ✔ Months to Internal ATO
- ✔ AI/LM+Monitoring Automation
- ✔ Automapping for Inherited Controls
- ✔ Automated + Dynamic Evidence

By replacing manual, static compliance methods with WyvernIQ, agencies and vendors like Adobe can reduce ATO timelines from **years to months**, lower compliance costs, and gain a transparent, data-driven measure of security posture. WyvernIQ ensures compliance is not a bottleneck but a measurable strength that accelerates mission success.

24+
Months Saved

Reducing ATO process from years to months

100%
Visibility

Real-time compliance monitoring
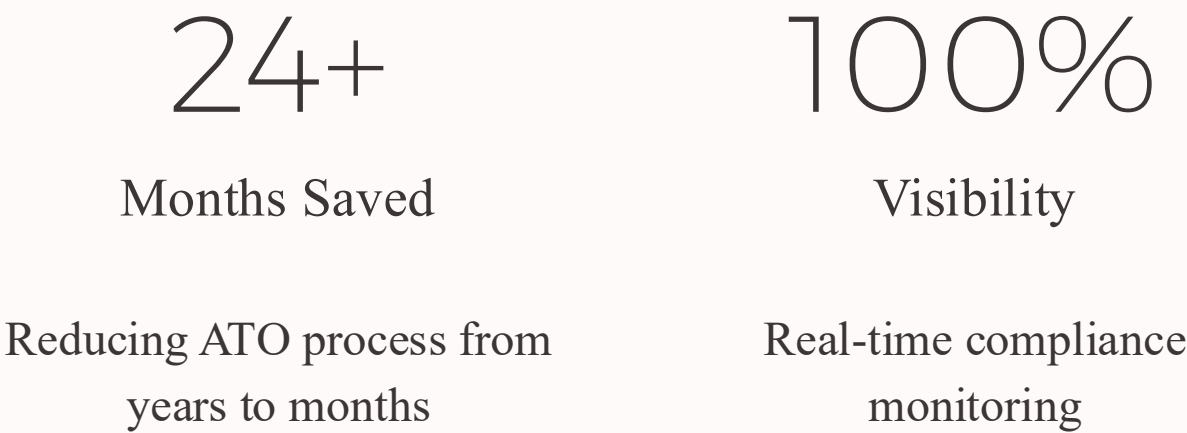
Contact Us

Why Engage With Us

- Real-time Cyber Health Score – Clear, FICO-style scoring for mission cyber readiness.
- AI/LLM-Powered Compliance – Automates RMF, FedRAMP, CMMC, and STIG mapping.
- Continuous Monitoring & Remediation – IL5/IL6-ready Artemis engine for secure hardening.
- Live Threat Intelligence Heatmap – Global, geolocated threat visibility enriched with IP reputation.
- Push Notifications & Alerts – Real-time notifications of active threats, anomalies, or posture drift.
- Multi-Cloud Scalability – Built for AWS, Azure, and GCP defense operations.
- Unified Data Fabric – Integrates telemetry, compliance, and remediation into one pane of glass.

Contact:
Dr. Suggs | Founder, WyvernIQ
Email: Chanel@wyverniq.com
Phone: 407-674-9700