Property of Sub Rosa Ventures

VigilantShield

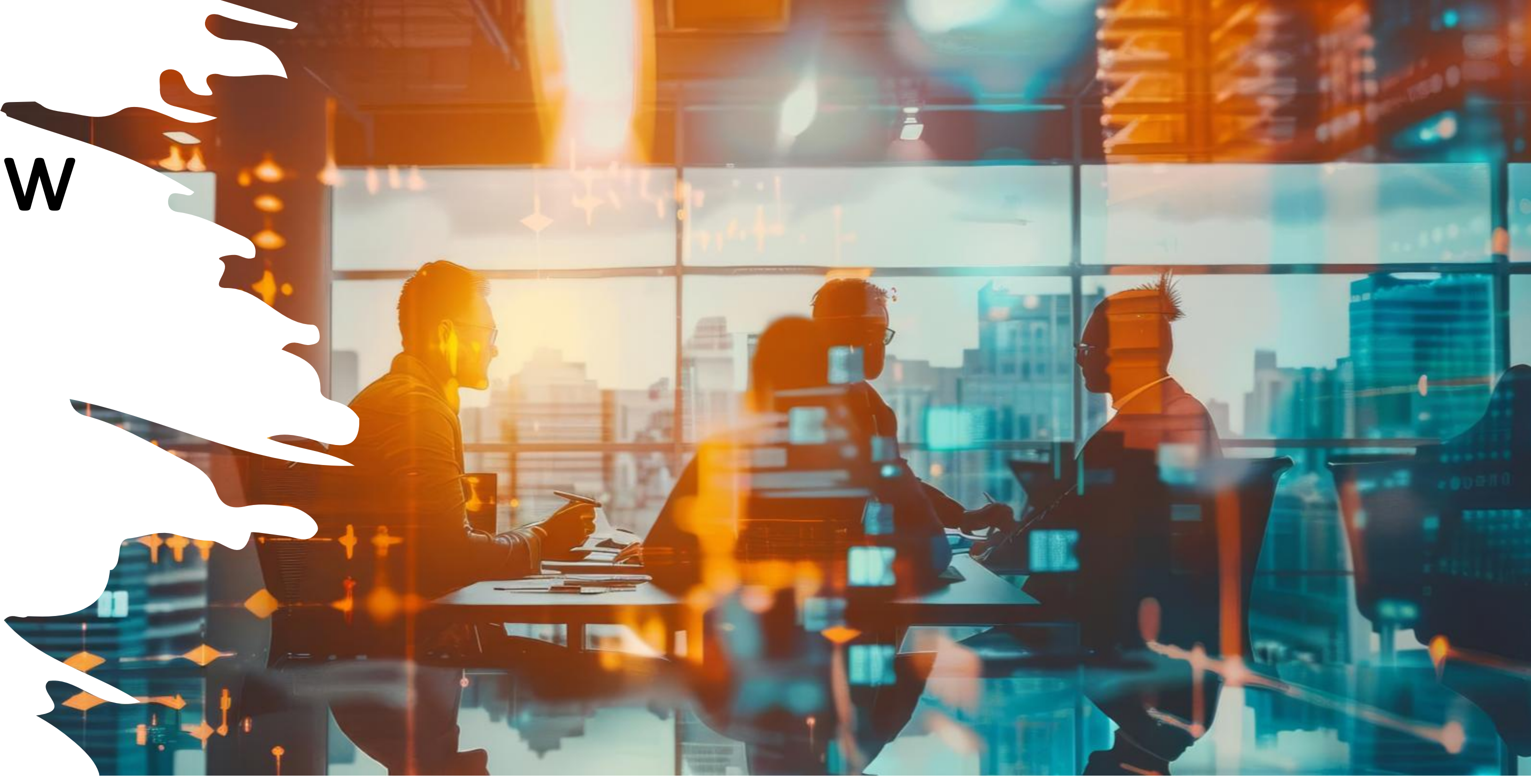
Engineered for Cyber Resilience.

Optimized for Tactical Edge

SUBROSA VENTURES

Detecting, analyzing, and mitigating anomalous network packets to protect systems from known and unknown (zero-day attacks). Whether internal or external.

SRV Company Overview



Full Spectrum Security Solution Company

- Emerging Technologies
  - Deep Packet Cyber IT/OT Protection
- Critical Infrastructure Sensors
- Insider Threat
  - Social Engineering
  - End to End Security Systems
- Consulting Services
  - Full-Service Security Layout

Property of Sub Rosa Ventures

Qualifications & Experience

Alan Seymour, PhD, is a seasoned CEO with over 25 years of leadership experience spanning business and information technology. He has driven transformative growth across corporate, non-profit, and academic sectors. His first strategic acquisition—an IT firm—achieved a fivefold expansion within five years before its successful sale. He then pivoted to the temperature & security sensing industry, where he led the company from $36 million to $50 million in revenue over the same timeframe.

Our team includes seasoned business development professionals with over 50 years of combined experience serving both commercial and government sectors. We're supported by engineers who were instrumental in the original product's development, as well as a diverse advisory group comprising engineers, domain specialists, and IT experts in augmented and virtual reality—providing strategic guidance as we build this next-generation solution.

VigilantShield Alignment with DISA Next Strategy (2025–2029)

Property of Sub Rosa Ventures

DISA Strategic Priority	VigilantShield Capability Alignment
Mission Partner Environment & Interoperability	Air-gapped, on-premises architecture supports secure, joint, and coalition operations.
Zero Trust Architecture & Cyber Defense	Real-time Deep Packet Inspection with Ensemble AI/ML fortifies layered, adaptive defense strategies.
Tactical Edge and Survivability	Sub-millisecond latency, low power (<15W), and no cloud reliance enable resilience in denied terrain.
Advanced Analytics & Operationalized Data	Combines supervised and unsupervised ML for proactive threat detection, even against zero-day attacks.
Integrated Infrastructure & AI Modernization	Ensemble Method architecture enhances precision and reliability while supporting continuous learning.
Cloud Smart Principles (Disconnected Ops)	Operates fully independent of cloud services, ideal for contested or low-connectivity environments.
Identity, Credentialing, Access Management (ICAM)	Packet-level anomaly detection reinforces behavioral consistency and identity assurance.

VigilantShield Utilizes FPGA Chips

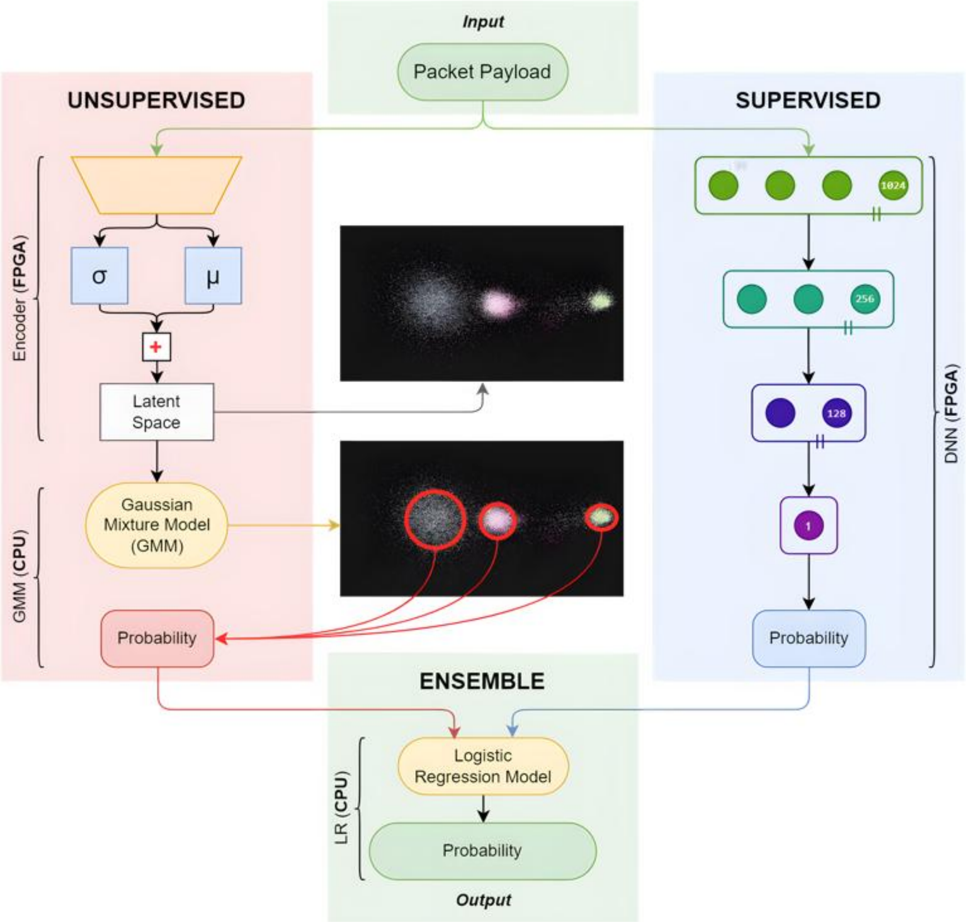
- Eliminates GPU-related latency and power overhead—no batch processing delays.
- Operates at <15 watts, making it ideal for low-SWaP, mobile, and forward-operating environments.
- Implements FPGA-based Ensemble AI, combining supervised and unsupervised learning models to detect evolving threat behaviors.
- Enables real-time inline threat analysis at the network level—no endpoint dependency or cloud reliance.
- Built to sustain continuous cyber defense under austere and denied conditions.

Built for continuous defense in today's rapidly evolving threat landscape.

Deep Packet Inspection: Ensemble Method

Machine Learning Approaches:

- Supervised methods are good at detecting known attack anomalies but can be vulnerable to unknown attacks. Has issues with false positives.
- Unsupervised methods will spot unknown threats but can struggle with accuracy and reliability. Has issues with false negatives.
- VigilantShield utilizes the best of both models by creating the Ensemble Method, which suppresses both false positives and false negatives.
- This method leverages the predictions of both supervised and unsupervised methods and creates a new prediction, giving a much higher accuracy to anomaly detection.



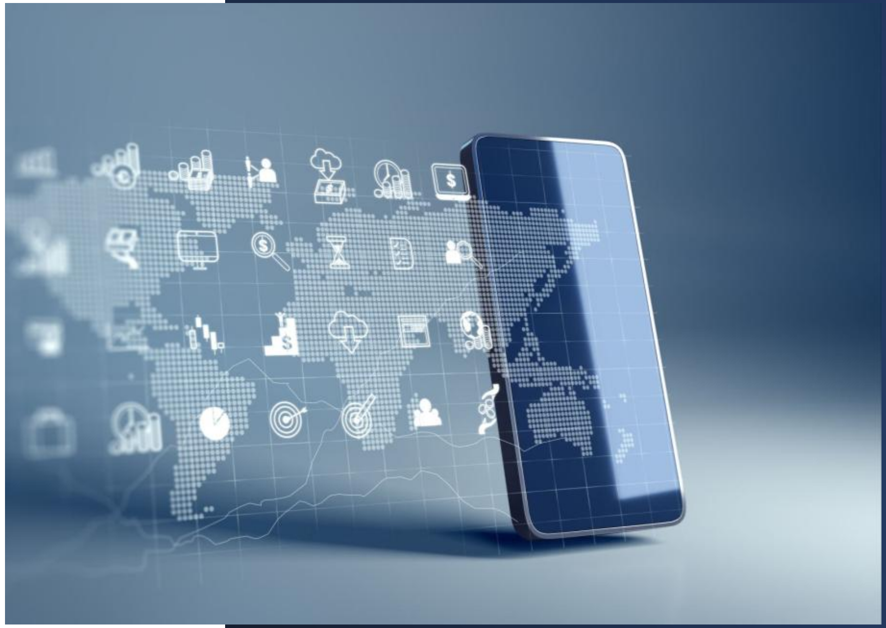
Conger et al. "Low-Power Deep Packet Inspection: A Programmable Logic Approach", Submitted to the Journal of Network and Computer Applications, 2025.

System Validation

- **Diverse Training Ecosystem:**
  - Employed a broad spectrum of network activity data—including IoT devices, smartphones, mobile platforms, and adversarial behaviors—to train and test supervised machine learning models

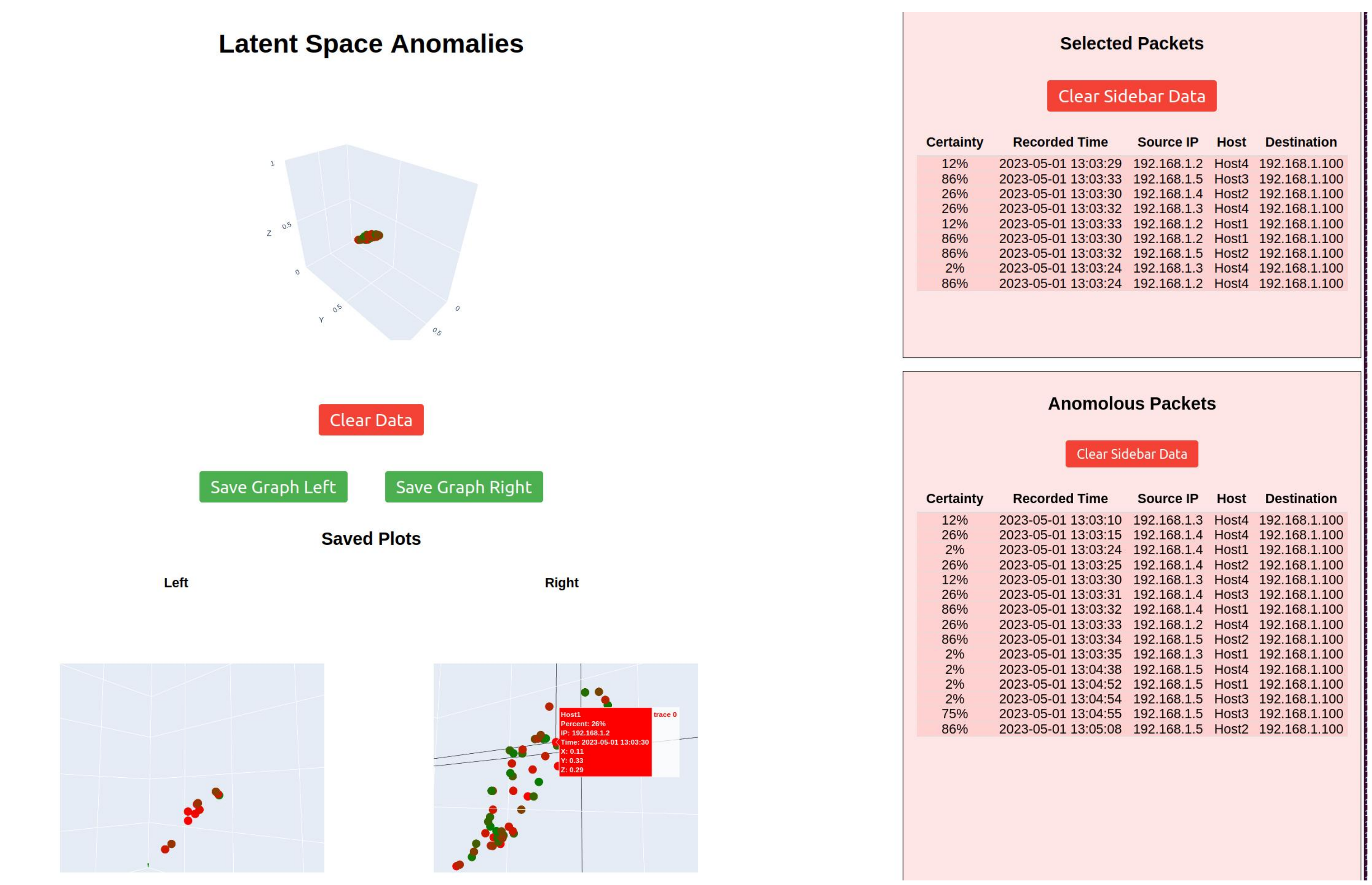
- **Mission-Informed Model Engineering:**
  - Algorithms were designed to detect anomalous activity across a range of operational environments, reinforcing cybersecurity posture in hybrid and tactical edge contexts.

- **BreakPoint-Based Model Validation:**
  - Leveraged the BreakPoint platform to rigorously evaluate model performance against novel, zero-day threat vectors—demonstrating adaptive defense capabilities in high-risk scenarios.



The Software API

- **Security Analysts:** Fast Identification of threats with full IP visibility.
- **Network Admins:** Visual Diagnostics to resolve bottlenecks & misroutes.
- **General Users:** Simple, Intuitive feedback for network health monitoring.
- **Training/Education:** Safe simulated environments for learning packet analysis.



Host1
Percent: 26%
IP: 192.168.1.2
Time: 2023-05-01 13:03:30
X: 0.11
Y: 0.33
Z: 0.29

Selected Packets

Certainty	Recorded Time	Source IP	Host	Destination
12%	2023-05-01 13:03:29	192.168.1.2	Host4	192.168.1.100
86%	2023-05-01 13:03:33	192.168.1.5	Host3	192.168.1.100
26%	2023-05-01 13:03:30	192.168.1.4	Host2	192.168.1.100
26%	2023-05-01 13:03:32	192.168.1.3	Host4	192.168.1.100
12%	2023-05-01 13:03:33	192.168.1.2	Host1	192.168.1.100
86%	2023-05-01 13:03:30	192.168.1.2	Host1	192.168.1.100
86%	2023-05-01 13:03:32	192.168.1.5	Host2	192.168.1.100
2%	2023-05-01 13:03:24	192.168.1.3	Host4	192.168.1.100
86%	2023-05-01 13:03:24	192.168.1.2	Host4	192.168.1.100

Anomolous Packets

Certainty	Recorded Time	Source IP	Host	Destination
12%	2023-05-01 13:03:10	192.168.1.3	Host4	192.168.1.100
26%	2023-05-01 13:03:15	192.168.1.4	Host4	192.168.1.100
2%	2023-05-01 13:03:24	192.168.1.4	Host1	192.168.1.100
26%	2023-05-01 13:03:25	192.168.1.4	Host2	192.168.1.100
12%	2023-05-01 13:03:30	192.168.1.3	Host4	192.168.1.100
26%	2023-05-01 13:03:31	192.168.1.4	Host3	192.168.1.100
86%	2023-05-01 13:03:32	192.168.1.4	Host1	192.168.1.100
26%	2023-05-01 13:03:33	192.168.1.2	Host4	192.168.1.100
86%	2023-05-01 13:03:34	192.168.1.5	Host2	192.168.1.100
2%	2023-05-01 13:03:35	192.168.1.3	Host1	192.168.1.100
2%	2023-05-01 13:04:38	192.168.1.5	Host4	192.168.1.100
2%	2023-05-01 13:04:52	192.168.1.5	Host1	192.168.1.100
2%	2023-05-01 13:04:54	192.168.1.5	Host3	192.168.1.100
75%	2023-05-01 13:04:55	192.168.1.5	Host3	192.168.1.100
86%	2023-05-01 13:05:08	192.168.1.5	Host2	192.168.1.100

Human-Investigation Integration

Automated Origin Detection

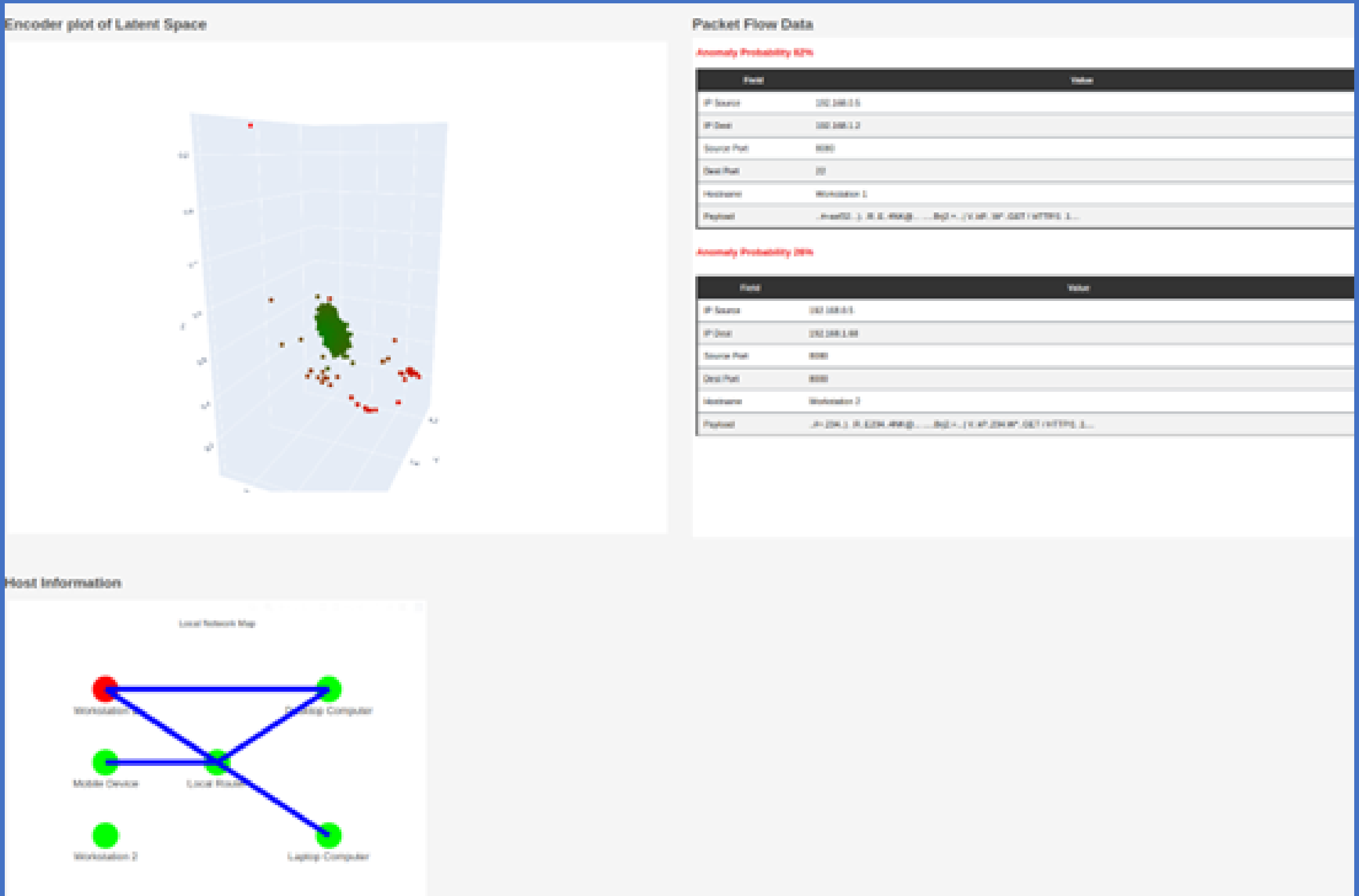
- The system utilizes intelligent network mapping to identify the source of anomalous packet activity within the network.

Threat Trajectory Visualization

- Anomalous packets are traced across their transmission path—highlighting destination endpoints and potential lateral movement toward critical assets or attack vectors.

Operational Support for Analysts

- This component enhances human investigation by surfacing key indicators, streamlining forensic analysis, and accelerating response workflows



Packet Flow Data

Anomaly Probability 82%

Field	Value
IP Source	192.168.1.5
IP Dest	192.168.1.2
Source Port	8080
Dest Port	22
Hostname	Workstation 1
Payload	[illegible] GET / HTTP/1.1...

Anomaly Probability 28%

Field	Value
IP Source	192.168.0.5
IP Dest	192.168.1.68
Source Port	8080
Dest Port	8080
Hostname	Workstation 2
Payload	[illegible] GET / HTTP/1.1...

SRV’s VigilantShield Key Differentiators

FPGA-Powered, Processor-Free Architecture

- Delivers ultra-fast packet inspection without conventional CPUs, leveraging field-programmable gate arrays for edge-optimized performance.

Hardware-Based Deep Packet Inspection (DPI)

- Conducts DPI natively at the hardware level for uncompromised throughput, inspecting every packet in real time with zero latency.

Cloudless, Air-Gapped Operation

- Fully self-contained—requires no cloud connectivity, making it ideal for austere, tactical, or disconnected environments.

Zero-Impact Deployment

- No software installation on client networks—preserves system integrity and avoids network slowdowns.

Payload-Level Analysis

- Goes beyond metadata to inspect full packet payloads, enabling detection of deeply embedded threats.

Autonomous Network Topology Mapping

- Visualizes attack paths and identifies origin points of anomalous packets across the entire topology.

On-Prem 5G-Capable Intrusion Detection

- Embedded 5G capabilities ensure compatibility with next-generation network operations, enhancing mobile defense posture.

Low-SWAP, Mission-Hardened Design

- Small form factor, <15W power draw, and RAD hardened for survivability in extreme conditions and contested environments.

Contact Information to Partner with Us

Alan Seymour
Owner/CEO
alans@subrosa.ventures
216.469.3044

Debbie Matzek
Business Development & Strategic Partnering Consultant
debbiem@subrosa.ventures
619.884.0980