AXELLIO

Software Based Data Intelligence Platform

Steve Mazzuca, Vice President, Federal
May 2025

AXELLIO

AGENDA

Axellio Update

Xpress Platform

- PacketXpress
  - Army DCO
  - USCC JCHK
  - IC Collection
- PacketXpress AI
  - DoD Dev Funding
- SensorXpress
  - RF/EW Collection

Corporate Overview

Axellio is a small, innovative, U.S. owned, non-traditional defense business based in Colorado Springs, CO. We develop cyber security and intelligence software for the Department of Defense, the Intelligence Community, and global security operations.

- **Contract Vehicles**
  - GWAC - NASA SEWP V – Category B –Group C (NNG15SD70B)
  - GWAC - NIH CIO-CS HHSN316201500025W
  - GSA MAS IT contract GS-35F-0511T
  - EWAAC Multi-Award IDIQ

- **Certifications**
  - ISO 9001:2015 Certified
  - Authority to Operate for three solutions
    - Army Authority to Operate across NIPR & SIPR

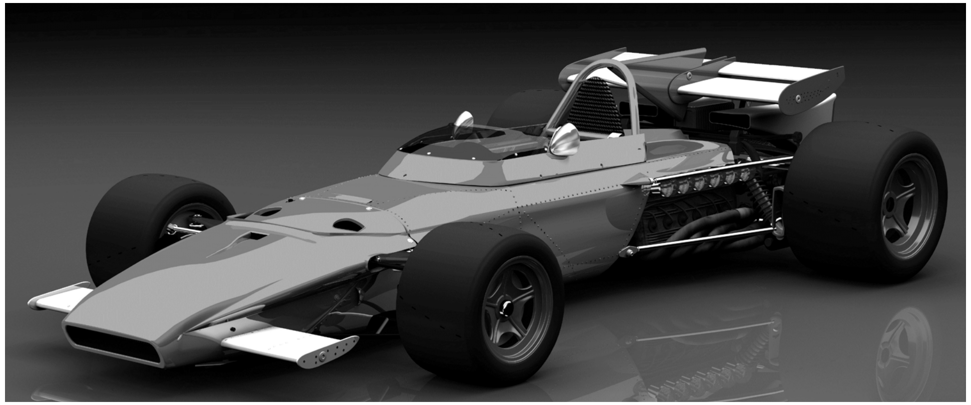
- **Prime Contracts**
  - US Army Defensive Cyber Operations (PM DCO) since 2020
    - Garrison Cyber Defensive Operations Platform (GDP)
      - OTA COBRA – CO-PLA-0025 (GDPv3 Prototype)
      - OTA COBRA – CO-PLA-0035 (GDPv3 Production)
      - OTA COBRA – CO-PLA-0037 (GDPv4 Prototype)
      - OTA COBRA – CO-PLA-0042 (GDPv4 Production)

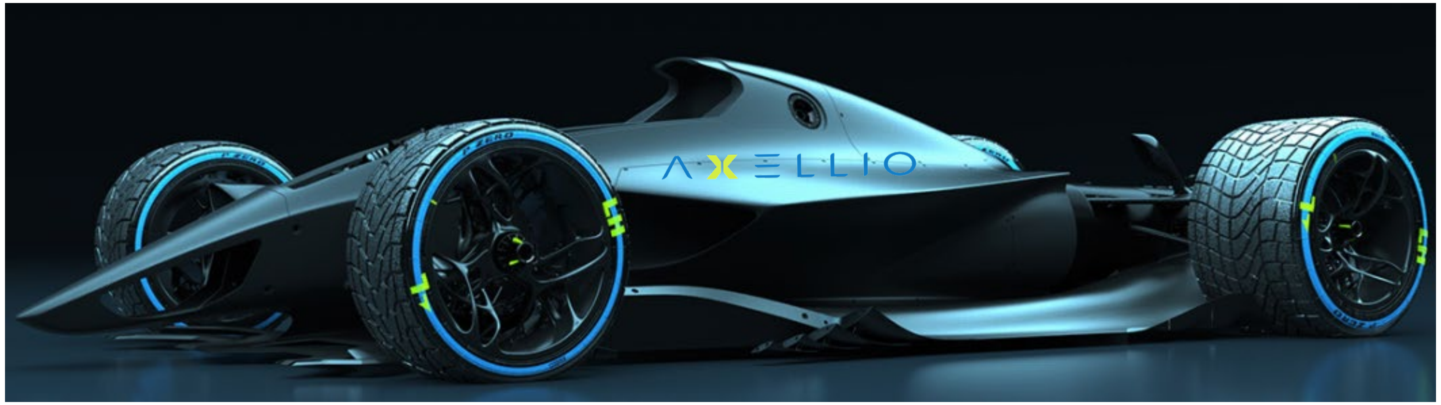
Multiple Award Schedule (MAS) Contract Holder

"Axellio provides us with the visibility needed to accelerate our response."

Lt. Col. Michael Lind Army's Defensive Cyber Operations

Empowering Extreme High-Speed Collection, Storage, and Analysis of Data at Scale





Traditional Storage

No Longer Adequate:

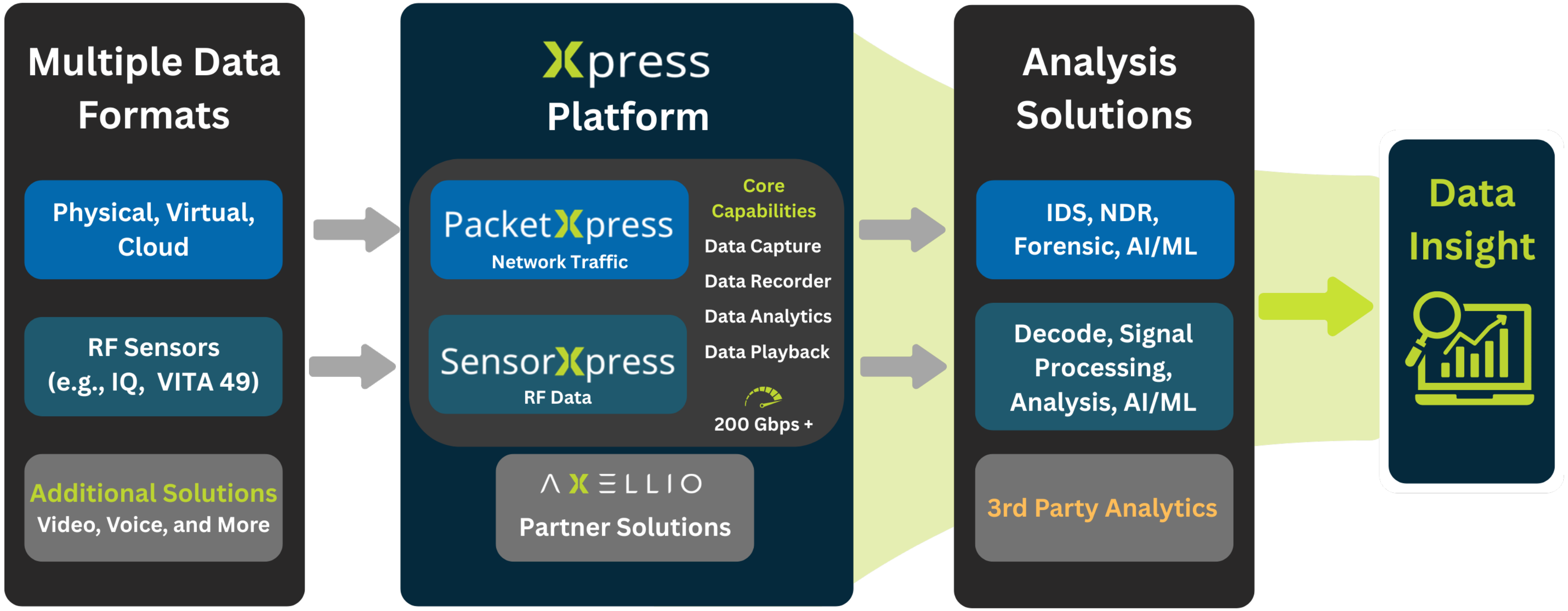
Slow, bulky, limiting, and unreliable

AXELLIO

Storage Innovation to Redefine Collection & Analysis

Simultaneous read and write performance to capture and distribute any time-series data at extremely high-speed, reliable, and at the lowest SWaP

Axellio’s Xpress Platform



Multiple Data Formats

Physical, Virtual, Cloud

RF Sensors (e.g., IQ, VITA 49)

Additional Solutions
Video, Voice, and More

Xpress Platform

PacketXpress
Network Traffic

SensorXpress
RF Data

Core Capabilities
- Data Capture
- Data Recorder
- Data Analytics
- Data Playback

200 Gbps +

AXELLIO Partner Solutions

Analysis Solutions

IDS, NDR, Forensic, AI/ML

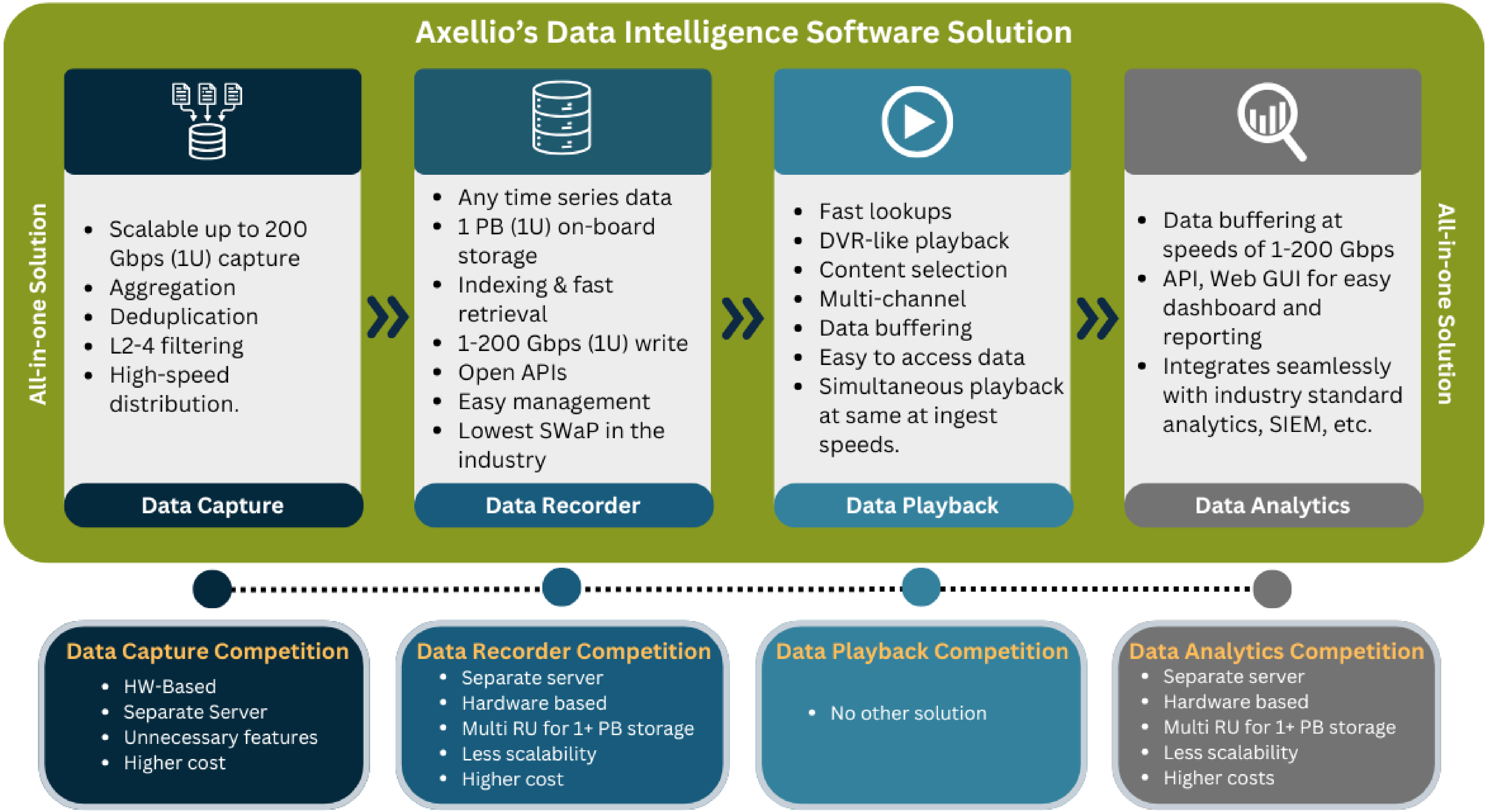
Decode, Signal Processing, Analysis, AI/ML

3rd Party Analytics

Data Insight

© Axellio Inc 2024

Why the Axellio All-in-One Data Intelligence Solution Outperforms the Competition



Axellio's Data Intelligence Software Solution

All-in-one Solution

Data Capture

- Scalable up to 200 Gbps (1U) capture
- Aggregation
- Deduplication
- L2-4 filtering
- High-speed distribution.

Data Recorder

- Any time series data
- 1 PB (1U) on-board storage
- Indexing & fast retrieval
- 1-200 Gbps (1U) write
- Open APIs
- Easy management
- Lowest SWaP in the industry

Data Playback

- Fast lookups
- DVR-like playback
- Content selection
- Multi-channel
- Data buffering
- Easy to access data
- Simultaneous playback at same at ingest speeds.

Data Analytics

- Data buffering at speeds of 1-200 Gbps
- API, Web GUI for easy dashboard and reporting
- Integrates seamlessly with industry standard analytics, SIEM, etc.

All-in-one Solution

Data Capture Competition

- HW-Based
- Separate Server
- Unnecessary features
- Higher cost

Data Recorder Competition

- Separate server
- Hardware based
- Multi RU for 1+ PB storage
- Less scalability
- Higher cost

Data Playback Competition

- No other solution

Data Analytics Competition

- Separate server
- Hardware based
- Multi RU for 1+ PB storage
- Less scalability
- Higher costs

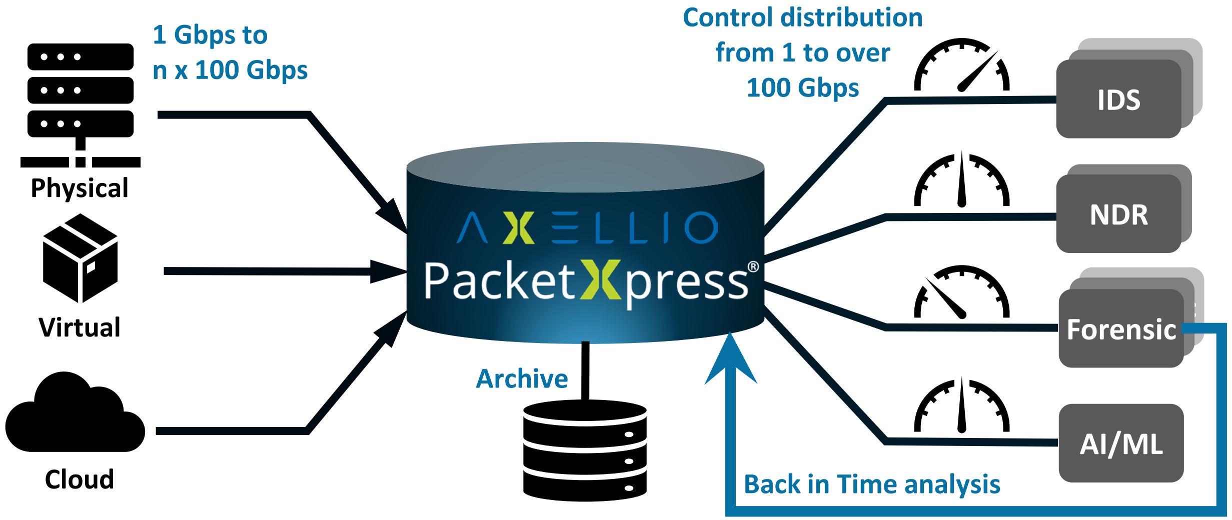
AXELLIO

PacketXpress

TRL 9 system in operation globally

Patented, ATOs on NIPR & SIPR

PacketXpress – Network Intelligence Platform



- **Collect anywhere**
  - Collect traffic from the physical ingress-egress, the internal network, to virtual, and cloud
  - No loss capture – from 1 Gbps to well over 200 Gbps sustained simultaneous data ingest, recording, and distribution
- **Adaptive traffic distribution**
  - Rewind, replay, re-analyze – for repeated in-depth analysis, mitigation validation, and training
  - Multiple data extraction streams can be individually configured for speed and content
- **Universal platform for any application**
  - Flexible form factor – from mobile to multi-rack data center configurations delivered on COTS hardware
  - Expandable storage – from hours to months – local or external
- **Patented**

Benchmark Example

(100Gbps aggregate data, 250 TB Storage, Analytics Framework, 3-year TCO)

Industry Standard

- Packet Broker/ Aggregator – 4U
  - $200k + Annual Main
- PCAP Store / Data Recorder – 14U
  - $300k + Annual Main
- Analytics – 3U
  - $120k + Annual Main
- Total TCO - $775k / Total HW – 21U

Axellio PacketXpress

- PacketXpress – SW + 2U COTS HW
  - $250k + Annual Main
  - SW Packet Broker included
  - SW PCAP Store included – 250TB
  - Industrial DVR included (Playback, Multi-system distribution)
  - On-board open-source analytics included
- Total TCO - $375k / Total HW – 2U

Massive SWaP-C savings, Efficiency in loss-less solution
Axellio direct to storage & buffering capabilities allow for a 60% reduction of analytics cost related to HW at any speed

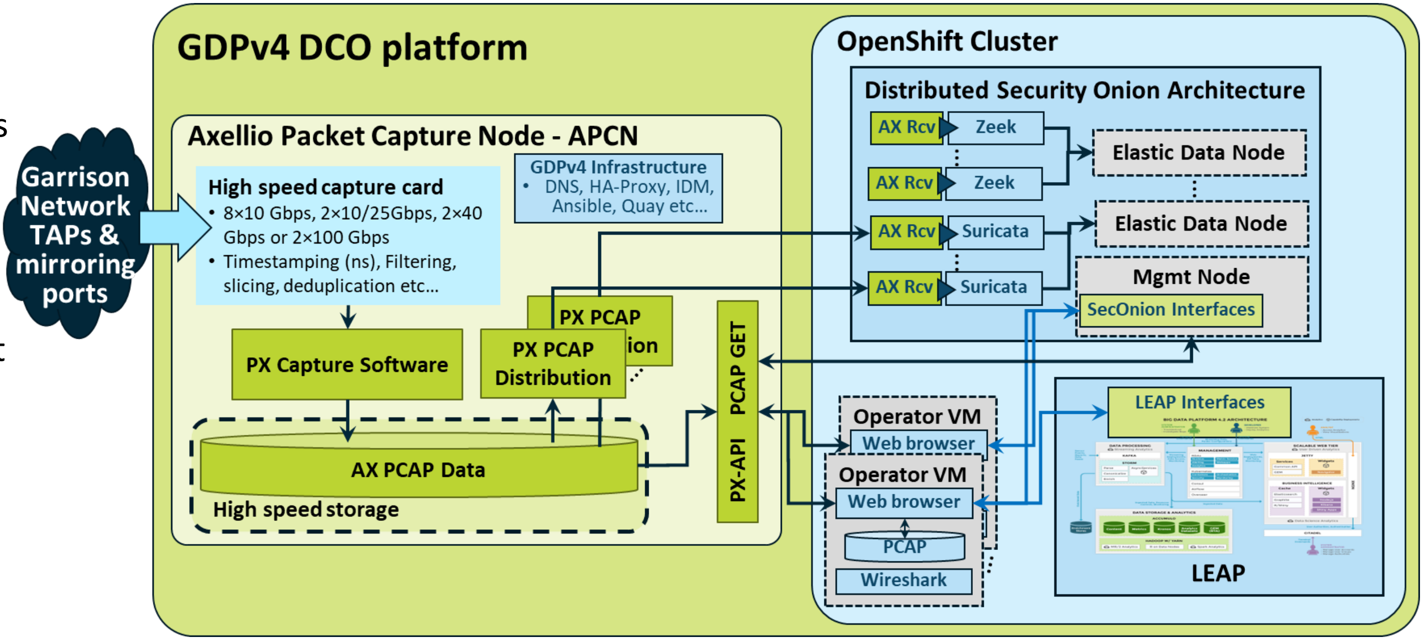
Axellio Solution - Army PM DCO
Garrison Defensive Cyber Operations Platform GDPv4

Statement of Objectives: The GDP/ Global Enterprise Fabric (GEF) convergence will enable cyber defenders to perform DCO expansion across various locations. The two current solutions require additional capability to outmaneuver the adversary to avoid detection based on new intelligence and/or new avenues of approach, due to the physical size of the GDPv2 and the reliance and tie to GEF locations for the GDPv3.

Challenge: Inability to clearly monitor and analyze the large amounts of data within Army networks and properly allocate defensive resources to detect, deter, deny or disrupt malicious activity.

Primary Requirements

- ✓ 40 Gbps+ packet capture and indexing to disk
  - ✓ Upgradeable to 100 Gbps+
- ✓ Lossless packet capture with filtering
- ✓ High speed PCAP distribution to virtual sensors
- ✓ Scalable software defined distribution architecture for flexible analytics
- ✓ Ad-hoc integrated PCAP retrieval for incident response workflow
- ✓ Self-contained operational capabilities without external dependencies for battle resilience
- ✓ Stand alone ATO
- ✓ Commercial airline checkable for rapid deployment in small footprint
- ✓ Automated, remote install, deployment &mgt
- ✓ Scalable, powerful and flexible architecture to support future toolsets as they evolve



6 Rack Units
- Firewall
- APCN
- Switches
- 3 node OpenShift cluster

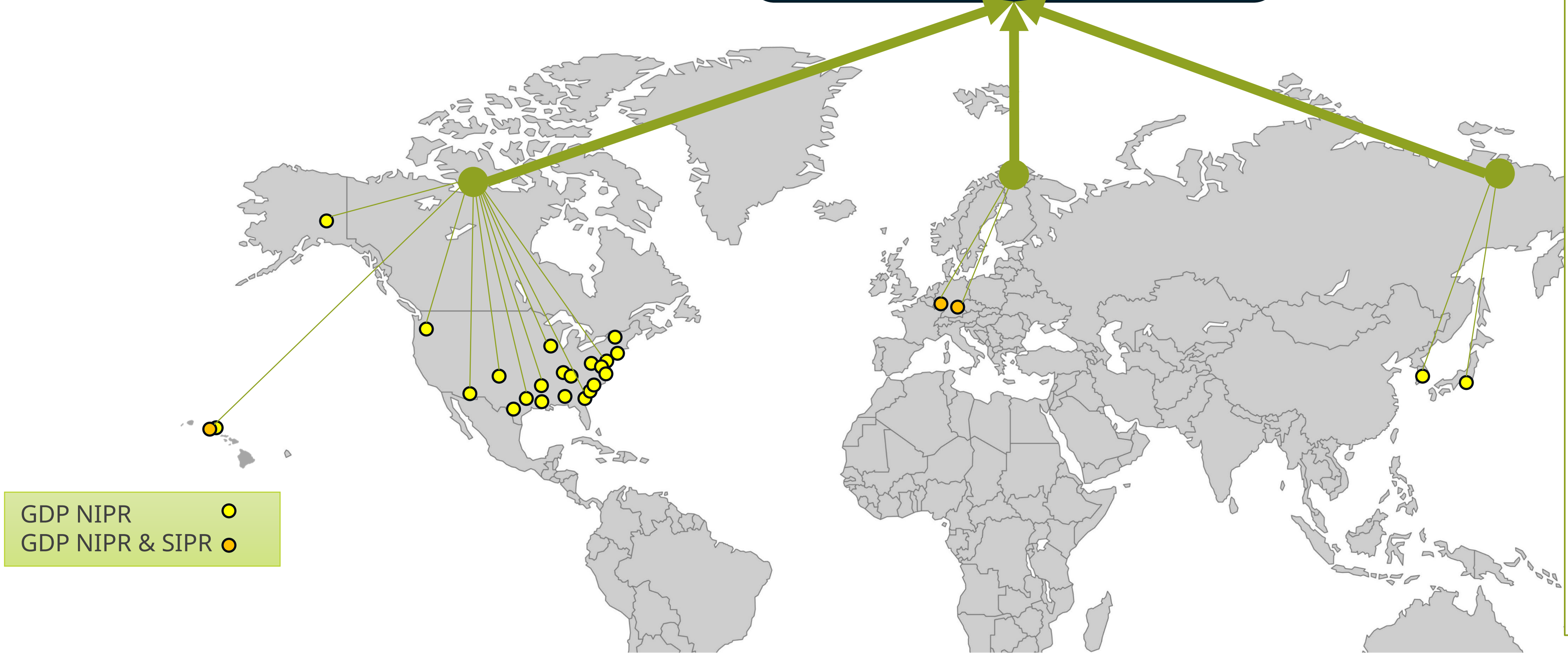
- Commercial airline checkable

US Army GDP Platform Integration with Gabriel Nimbus (BDP)

Garrison level
Network visibility for immediate threat detection and response

Gabriel Nimbus
Big Data Platform (BDP)

Global
threat visibility & analysis for broader site protection



CONOS:

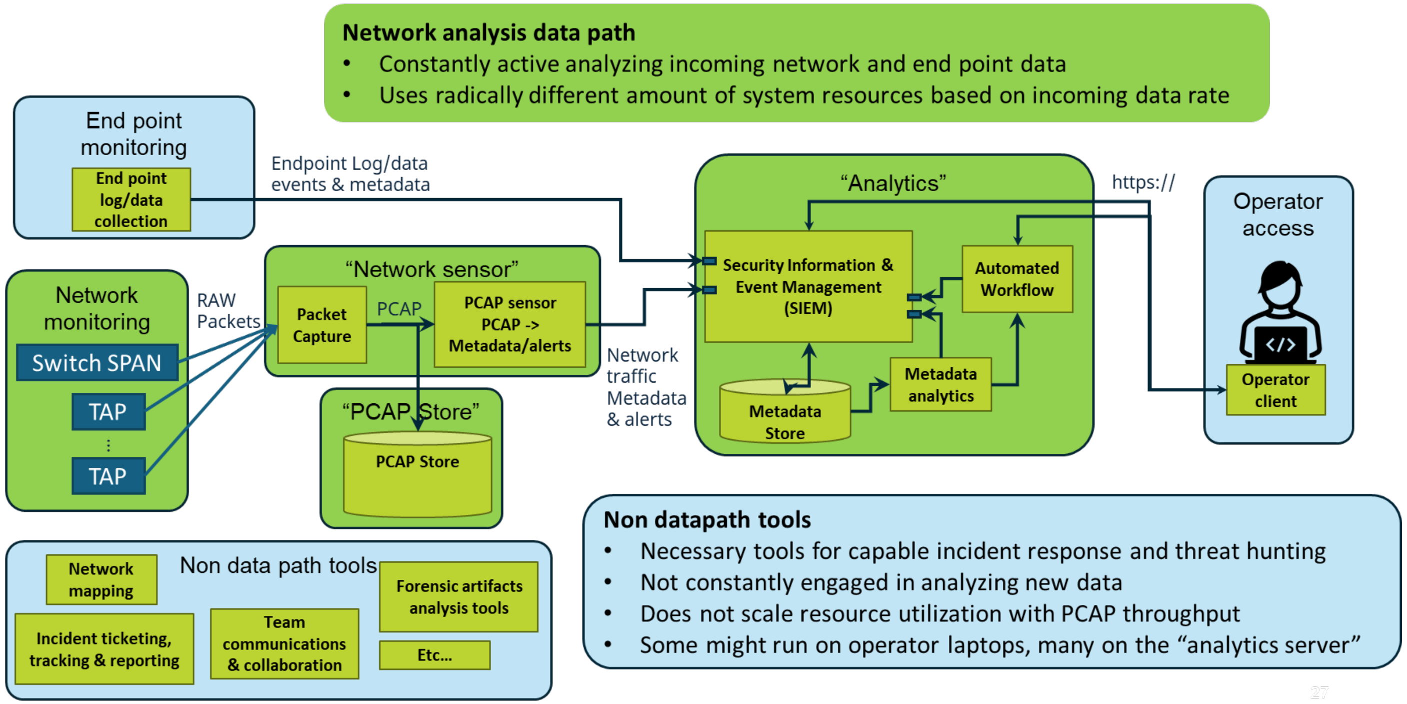
- Fort Cavazos, FT Cavazos, TX
- Fort Carson, Colorado Springs, CO
- Fort Stewart, FT Stewart, GA
- JBLM, Tacoma, WA
- Fort Eisenhower, Augusta, GA
- Redstone Arsenal, Huntsville, AL
- Fort Huachuca, FT Huachuca, AZ
- JBSA, San Antonio, TX
- Fort Liberty, Fayetteville, NC
- Fort Knox, Fort Know, KY
- Rock Island, Rock Island, IL
- Fort Johnson, Fort Johnson, LA
- Aberdeen Proving Ground, Aberdeen, MD
- Fort Belvoir, Alexandria, VA
- Fort Riley, Fort Riley, KS
- Fort Drum, Fort Drum, NY
- West Point Academy, West Point, NY
- Fort Campbell, Fort Campbell, KY
- Fort Gregg-Adams, Fort Gregg-Adams, VA
- Tobyhanna, Tobyhanna, PA

OCONOS:

- Kaiserslautern, Germany
- Grafenwöhr, Germany
- Camp Zama, Japan
- Camp Walker, Daegu, South Korea
- Fort Wainwright, Fairbanks, AK
- Schofield Barracks, Schofield Barracks, HI
- Fort Shafter, Honolulu HI

WWT/Axellio – US CYBERCOM Joint Cyber Hunt Kit

DCO System Architecture - Functional decomposition



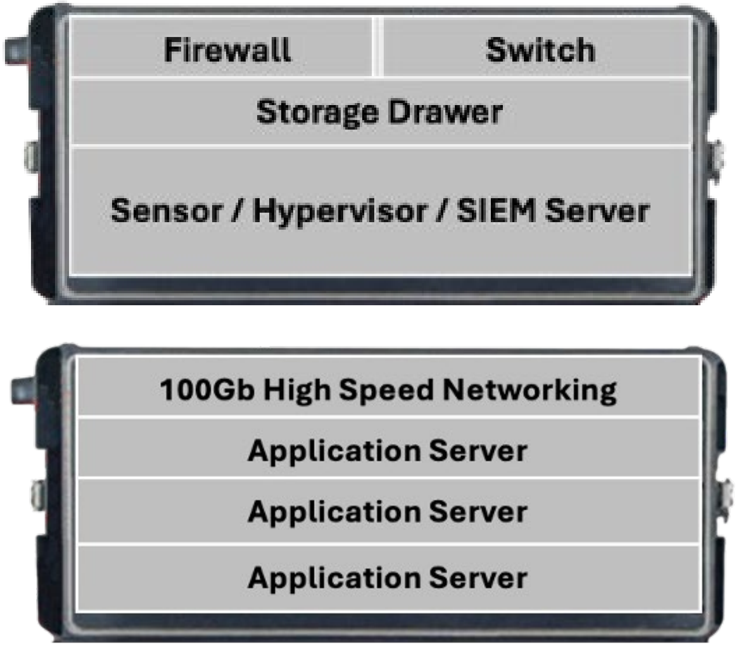
Network analysis data path

- Constantly active analyzing incoming network and end point data
- Uses radically different amount of system resources based on incoming data rate

Non datapath tools

- Necessary tools for capable incident response and threat hunting
- Not constantly engaged in analyzing new data
- Does not scale resource utilization with PCAP throughput
- Some might run on operator laptops, many on the “analytics server”

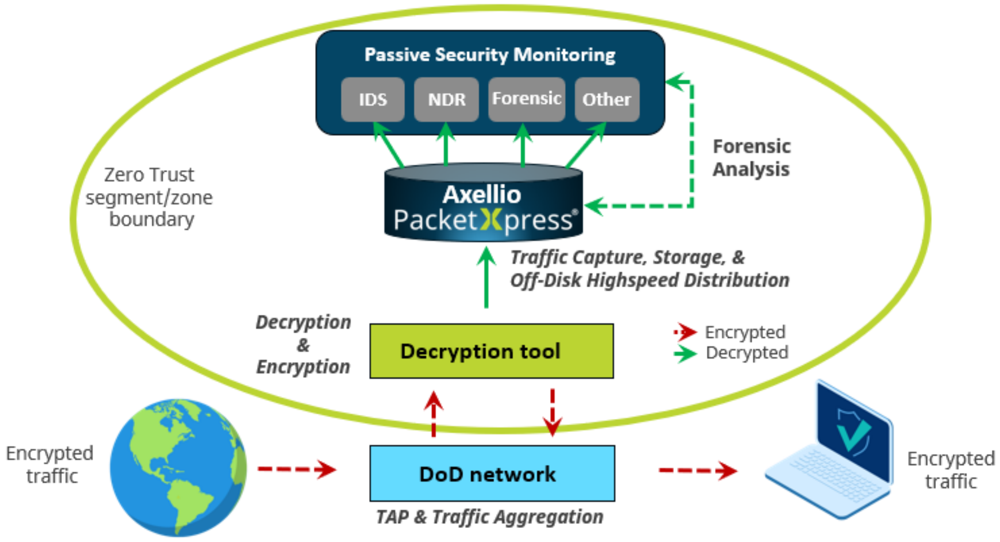
End point monitoring
End point log/data collection
Endpoint Log/data events & metadata
Network monitoring
Switch SPAN
TAP
TAP
RAW Packets
“Network sensor”
Packet Capture
PCAP
PCAP sensor PCAP -> Metadata/alerts
“PCAP Store”
PCAP Store
Network traffic Metadata & alerts
“Analytics”
Security Information & Event Management (SIEM)
Automated Workflow
Metadata analytics
Metadata Store
https://
Operator access
Operator client
Non data path tools
Network mapping
Forensic artifacts analysis tools
Incident ticketing, tracking & reporting
Team communications & collaboration
Etc…



Firewall
Switch
Storage Drawer
Sensor / Hypervisor / SIEM Server
100Gb High Speed Networking
Application Server
Application Server
Application Server

Gaining Visibility into Encrypted Traffic

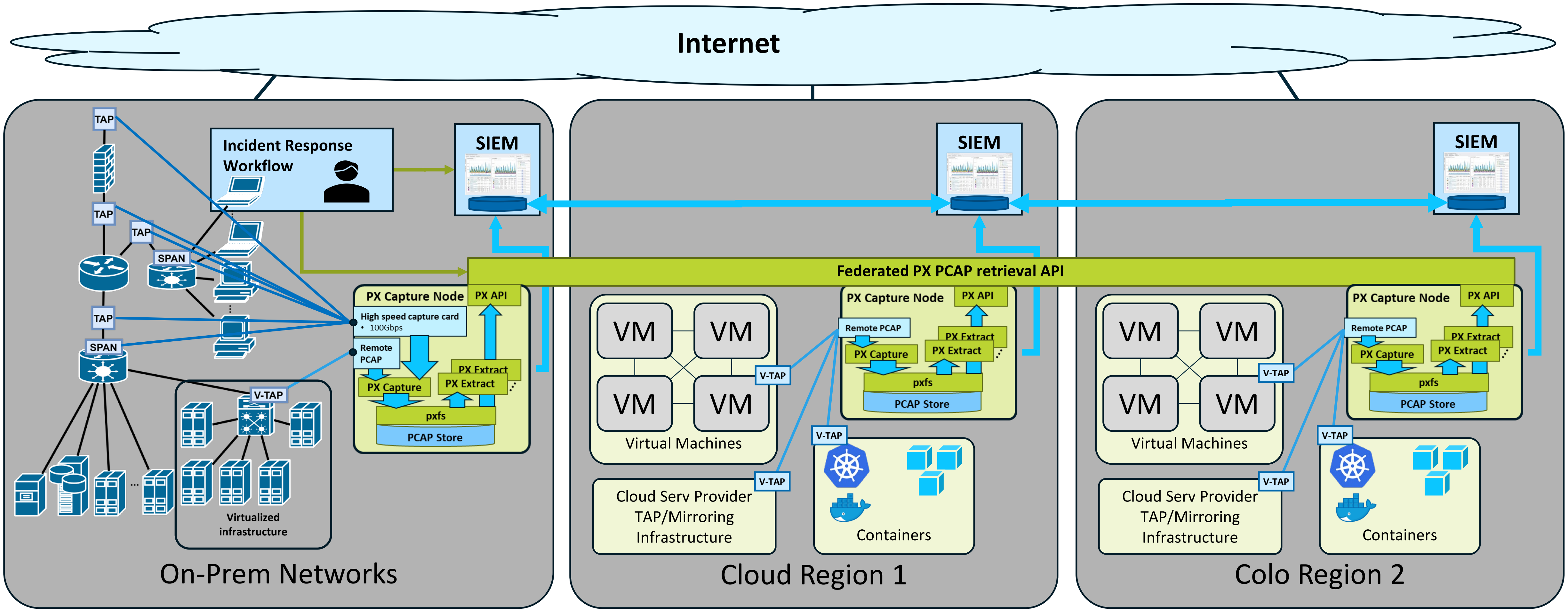
Axellio Decryption Solution



Key Components:

- **Decryption tool -** decryption & re-encryption for TLS 1.2, TLS 1.3, etc.
- **PacketXpress -**
  - **Packet data processing functions** – High speed data aggregation, filtering, de-duplication, buffering & distribution to security tools.
  - **Data storage** – on-board, high speed, high volume secure data storage repository with fast retrieval capability for NDR tools.
- **Security analysis/ threat analysis tools -** (IDS/NDR/DPI)

Unified PCAP Access - Distributed Hybrid Data Centers



PacketXpress Use Cases & Deployments

Defensive Cyber Operations	**US Army Garrison Defensive Cyberspace Operations Platform (GDP) POR** • Operationally deployed, 45 Systems across CONUS/OCONUS on NIPR/SIPR • Ingesting all network data, storing PCAP, and distributing to various cyber analytical tools including BDP (LTAC, LEAP, Gabriel Nimbus)
Cyber Hunt Kits	**Cyber Hunt Kits** • Lossless capture > 25Gbps, store and process PCAP in one system, 480TB storage • Single system with many TAPs, integrated SW aggregator • Ruggedized airline carry-on, Flexible, Scalable
Large Scale Cyber Collection	**High-Volume Network Collection** • Low SWaP-C – 200Gbps collection, storage, distribution on 1U • Filtering, Traffic Analysis, Parsing
Enabling the DoD Zero Trust Capabilities	**DoD ZT Visibility and Analytics** • End-to-end network visibility across physical, virtual, and cloud infrastructure • Real-time analysis for threat detection and in-depth retrospective analysis
Testing & Validation	**Large System Integrator** • Deployed for system test and validation, replaying traffic at 100 Gbps
Cloud PCAP & Storage	**AWS** • Deployed to optimize PCAP and direct storage to S3 buckets • Drives significant cost savings versus storage to Elastic Block Storage

AXELLIO

PacketXpress Axellio Insight (AI)

TRL 4

Prototype foundation built – working on DoD investment on UML Behavior Modules

Why Are We Still Losing the Cyber Battle?

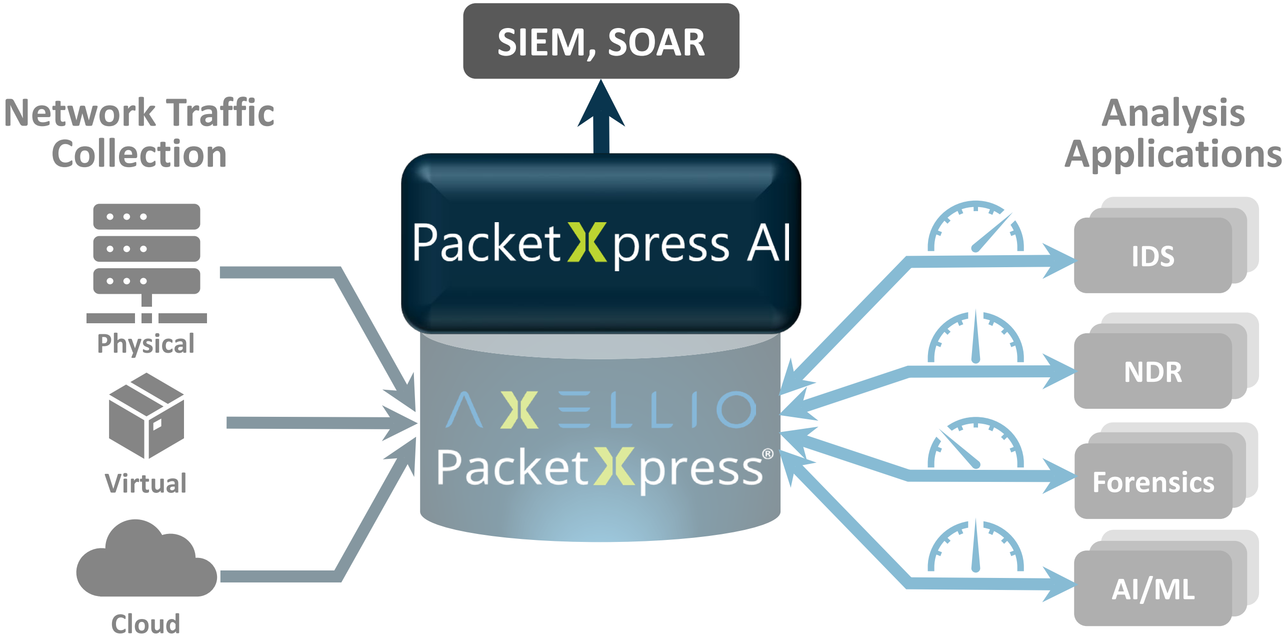
Known: Hostile cyber attacks are designed to evade rule-based detection systems by employing previously unknown network exploits

No Defensive Cyber technology product exists that…

- Detects both known and <u>unknown</u> threats
- Automatically learns normal traffic patterns in diverse network environments
- Autonomously configures itself based on Machine Learning without subject matter expertise
- Detects attacks at the <u>packet level</u>
- Runs at standard LAN speeds all the way up to 100 Gbps+ line rates
- Can be deployed in the field on lightweight hardware with no GPU or cloud support

PacketXpress® Axellio Insight (AI)

Cybersecurity Analysis At-Scale with AI/ML at 100 Gbps



- **Reliable:** Detects both known and unknown threats by analyzing traffic rather than metadata/logs that threat actors can manipulate
- **Fast & efficient – Working Prototype:**
  - ~1000x faster ML clustering than standard k-means
  - Anomalous vectors in 178 GB / 197M packets of network traffic were analyzed & detected in ~23 sec
  - Runs at 70 Gbps on a 16 Core, 64 GB RAM laptop
- **Unsupervised ML:** Trains in real time on production traffic
- **Regression & forensic analysis:** Rewind & Replay traffic
- **Compact:** Operates without cloud or GPU support - even on small (laptop) processors

Operationalizing AI/ML at 100 Gbps Through Patented Storage Architecture

AXELLIO

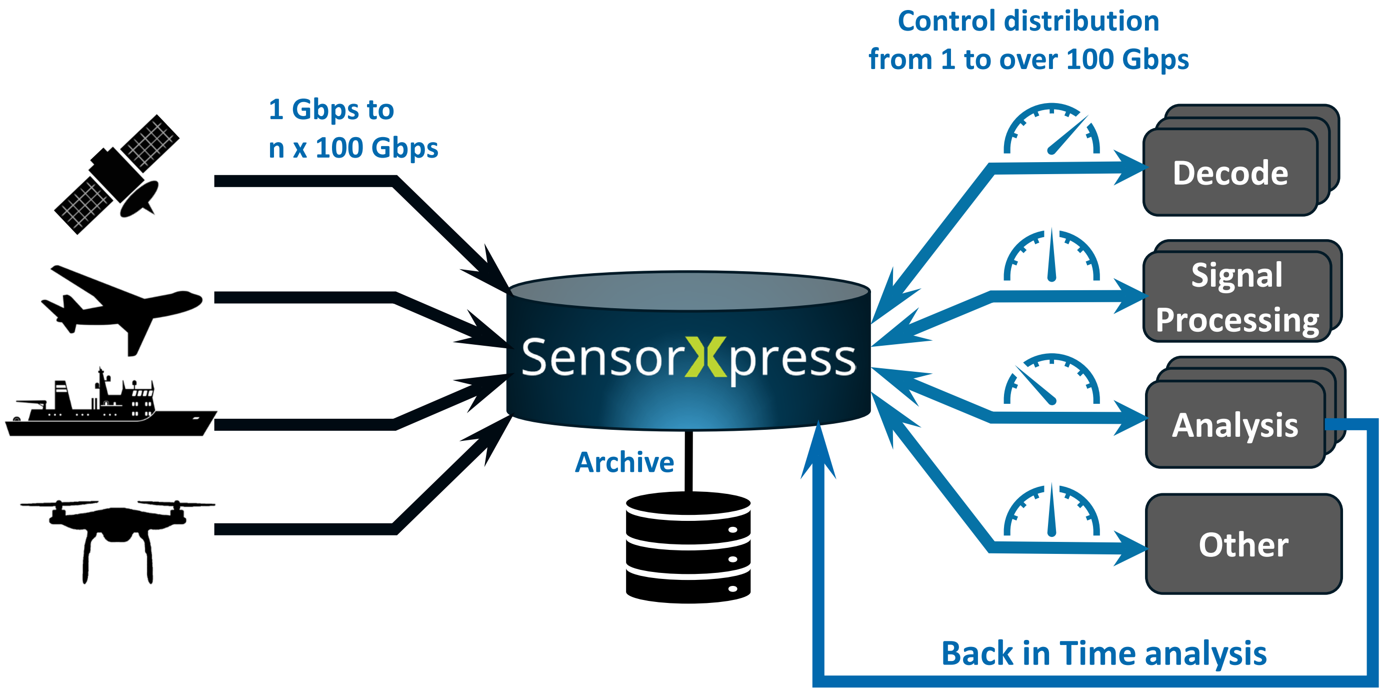
SensorXpress

RF Monitoring

TRL 7

SensorXpress™ for RF Monitoring

NextGen RF Ingestion, Storage, and Distribution



Extends time-on-target at the widest IBW possible:

- **Software solution**
- For **any time-series data** source (I/Q, VITA49)
- Freq, sensor, HW, and analysis application **agnostic**
- **No-loss capture** for high-quality results from multiple sensors at speeds greater than 100 Gbps
- **Scalable** from small custom HW solutions to data center solutions
- **Controlled and repeatable data distribution** to multiple analysis applications
- **Expandable, high-speed, and high-volume storage**, from hours to months

Maximize the capabilities and extend the useful life of your existing RF collection infrastructure:

- **Record longer at wider bandwidths from more devices**
- **Record and distribute simultaneously and continuously without looping**

SensorXpress™ Use Cases & Deployments

DoD Battlespace Awareness	Use cases include RF/EW/MASINT collection systems on Ships, Air Frames, Drones, Ground, etc.
SpectrumXport	Partnered with *CACI SystemWare* to build a real-time distributed display/analysis device that attaches to Spectrum Guard (wideband RF detection and monitoring system) • Actively streaming real-time IQ at 75MHz IBW (between 1KHz – 40GHz) to a small HW device with multi-TB U.2 drives • Allows for real-time capture of signals to go from seconds to days • Demo of system at Army CyberQuest 2024 and Navy Silent Swarm 2024
RAISER **(Rapid AI Signal Exploitation Regime)**	**Partnered with *DataShapes* (waveform AI/ML small business) to propose a flexible AI architecture for edge-based RF collection and analysis** • Solution will demonstrate superior exploitation of available signal data through enhanced ingestion capabilities, high-speed data storage, and operationalized AI-based analysis
IC Collection	Partnering with multiple FSIs on large scale IC collection programs. Both small tactical boxes and large data center systems.

AXELLIO

Thank you!

Steve Mazzuca, VP Federal
Steve.Mazzuca@axellio.com
(410) 591-8572

Contact us

🌐 www.axellio.com
@ contactus@axellio.com
☎ +1 (800) 463-0297
+1 (719) 309-3370