Colvin Run Networks

Mission-Driven Analytics

Colvin Run

www.colvinrun.com

DAFITC 2025 Breakout Session

Securing Data-in-Use at the Tactical Edge:
Enforcing Zero Trust with SHIELD-C in DDIL Environments

August 2025

Heidi Slocum, Manager Partnerships and Strategic Growth
Bruce Olson, VP of Growth and Operations

Opening Scenario: Air Force Mission in a D-DIL Fight

Classified mission.

Subtle course change.
No alarms. No warnings.

Hours later, the world sees it intact.
In **enemy** hands.

Opening Scenario: Air Force Mission in a D-DIL Fight

COMPUTERS

Iran–U.S. RQ-170 incident has defense industry saying 'never again' to unmanned vehicle hacking

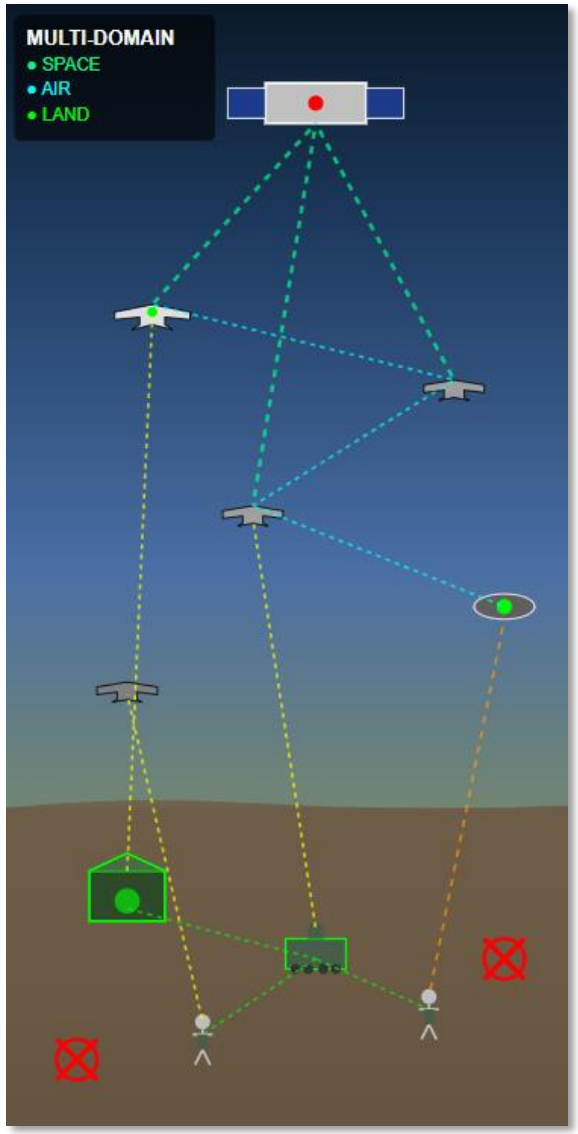
THE MIL & AERO COMMENTARY, 3 May 2016. If there's anything that continues to haunt U.S. military unmanned vehicle development, it's the December 2011 Iran–U.S. RQ-170 incident in which Iranian military cyber warfare experts commandeered a U.S. Lockheed Martin RQ-170 Sentinel stealth drone operating near the Iranian city of city of Kashmar.

May 3, 2016

https://www.militaryaerospace.com/computers/article/16715072/iranus-rq-170-incident-has-defense-industry-saying-never-again-to-unmanned-vehicle-hacking

https://en.wikipedia.org/wiki/Lockheed_Martin_RQ-170_Sentinel#/media/File:USAF_RQ-170_photograph.webp

The Challenge at the Tactical Edge



- Mission data travels across contested, coalition, and untrusted networks
- Current systems protect platforms, not the data itself
- Adversaries exploit gaps in authentication, encryption, and access
- Zero Trust concepts rarely extend to DDIL environments
- Every link, from sensor to C2, is a potential point of compromise

Colvin Run Networks: Company Overview

Expertise & Innovation

- ✓ **Top Secret FCL, CMMC Level 2.0**, GSA MAS Contract Holder, $7.5M Credit Line
- ✓ Seaport-NxG Prime Contract Holder
- ✓ Applied data science experts leveraging cloud analytics, AI/ML, distributed ledger, and market-leading technologies
- ✓ 2020 Virginia SBIR Success Story
- ✓ Recognized as Top 10 Startup serving the United States Air Force and MassChallenge
- ✓ Highlighted as the September **2024 Navy SBIR Success Story** by Navy SBIR Transition Program
- ✓ ACG National Capital 2025 Corporate Growth Awards Finalist

Our Platforms

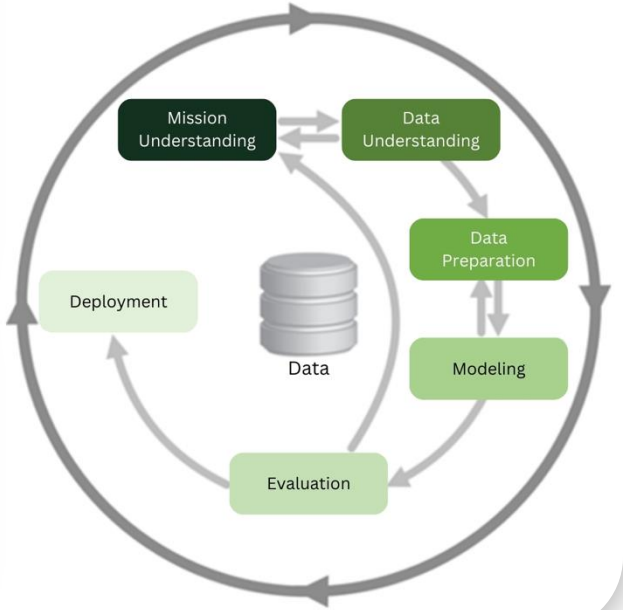
Afforma

Mission-Driven Analytics

Copia

Mission-Driven Hardware Trust & Assurance

User-Centered Design



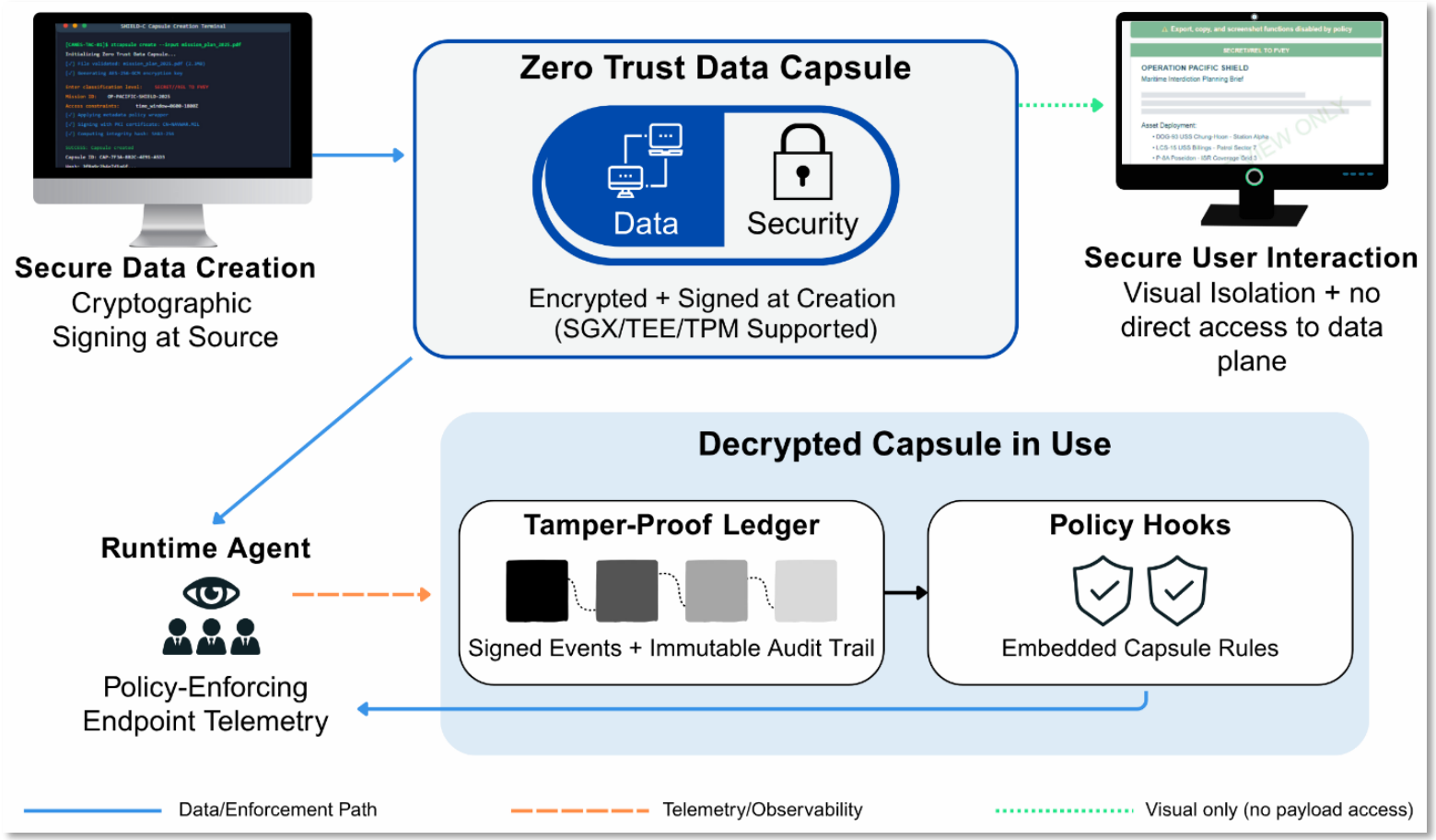
Mission-Critical Customers

World-Class Technology Partners

 | info@colvinrun.com | (571) 207-7487

SHIELD-C: Security That Travels With the Data

- Encrypts and tags data at the moment of creation.
- Operates in connected, contested, and disconnected environments.
- Policy stays with the data, anywhere it goes.
- Enforcement at the data layer, not just the network.



| info@colvinrun.com | (571) 207-7487

Core Innovations of SHIELD-C

Zero Trust Data Capsule

Sensitive Data
AES-256-GCM

Policy Metadata
- Clearance Level
- Usage Constraints
- Device Requirements

Key Features:
✓ Cryptographically signed metadata
✓ Integrity hash verification
✓ Policy travels with data
✓ Autonomous security agent

TEE-Backed Middleware

Hardware TEE
Graphene-SGX / AMD SEV

Software Feedback
OS-level Controls

Secure Operations

Key Features:
✓ Sub-millisecond encryption
✓ Isolated policy validation
✓ Tamper-resistant logging
✓ Modular TEE backend

Runtime Enforcement Engine

System Monitor

Clipboard | Screen Cap | File Ops

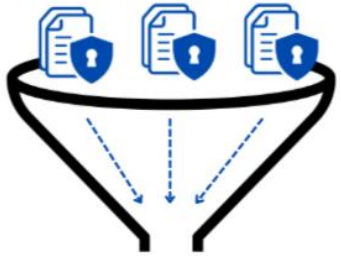
Policy Evaluation

✓ Allow ⊘ Block ⚠ Alert

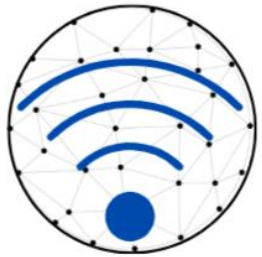
Key Features:
✓ Real-time policy enforcement
✓ Pattern-based threat detection
✓ Multi-threaded background service
✓ Delayed sync for D-DIL

From Perimeter-Only to Data-Centric Security

Transport-Based Controls



CDS Bottlenecks



Network Dependence

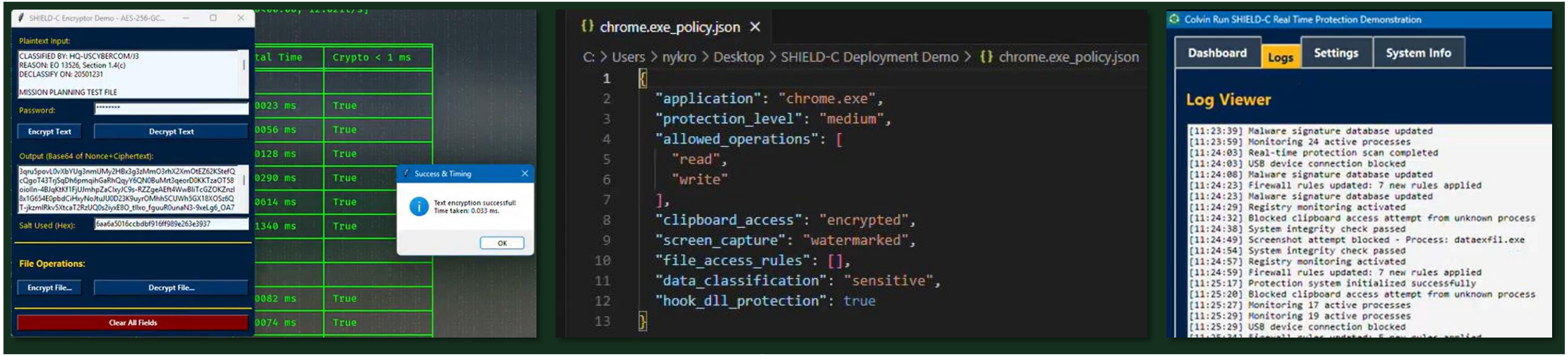
Self-Protecting Capsules

Instant Cross-Domain Readiness

Offline Enforcement

Reduced Complexity
Faster Access
Preserved Fidelity

Proven in Phase I, Poised for Phase II Impact



Phase I Results

- Sub-millisecond AES-256 encryption at data creation
- Runtime enforcement without kernel/hardware dependencies
- 78% threat detection rate in disconnected red team test
- Tamper-evident audit trails aligned with Navy CSSP schemas

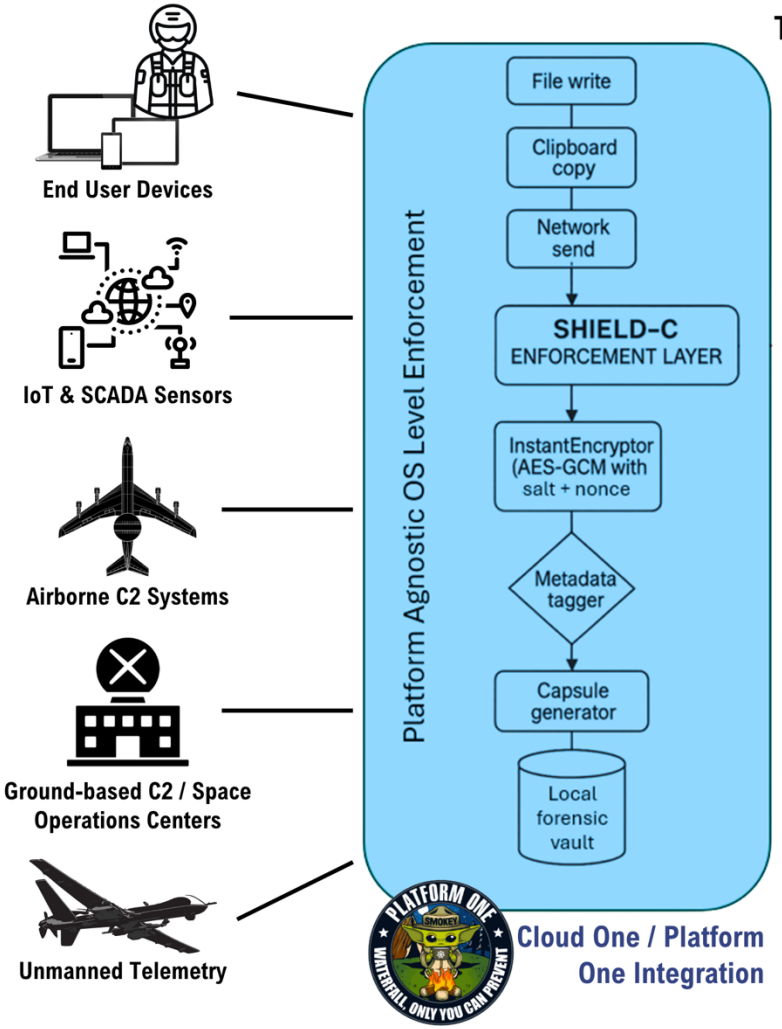
Phase II Expansion

- Cross-platform agent: Windows, Linux, Android, embedded
- IL6 containerized deployment for tactical & ISR platforms
- Advanced policy features: geo-fencing, temporal access, legal holds
- CSSP SIEM integration (Splunk, ArcSight, Elastic)
- Field testing in DDIL environments

| info@colvinrun.com | (571) 207-7487

Air Force Integration

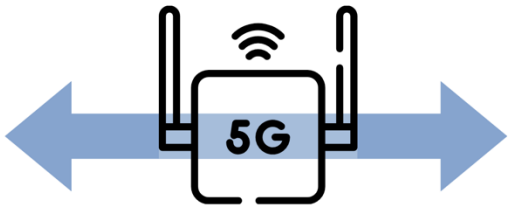
Enforcing Zero Trust where it matters: protecting data at the edge, in flight, and across joint/coalition operations.



Transport Agnostic Secure Data Channels

Tactical Mesh Networks
Link-16 / MADL / TTNT

SATCOM
AEHF / WGS / Star Link



Private 5G/Line of Sight Relays
flight line & deployed operations

Assured Delivery to Air Force Data Endpoints & Consumers

Cloud One

Unified Platform Analytics / DAF PEO C3BM

SIPRNet / JWICS / AFNET

AFRL AI/ML Models

Air Operations Centers / Distributed Common Ground System (DCGS)

BMS / C2IMERA / Theater Battle Management Core System (TBMCS)

LOGMOD / GCSS-AF / DEAMS / LIMS-EV

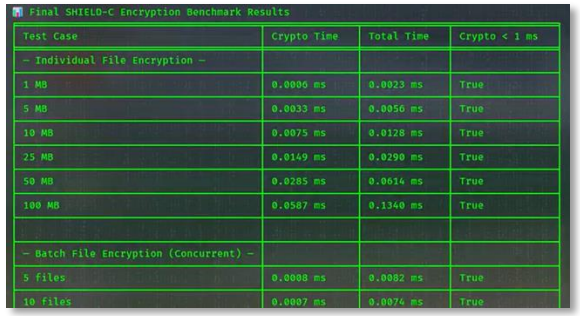
Mission Impact

AF Mission Context	SHIELD-C Impact
Mission Data Packages	Keeps ISR and C2 mission data **tamper-proof in contested comms** with no rework, no leaks, mission-ready in any environment.
Cross-Domain Ops	Enables **instant, secure CDS transfers** so multi-domain targeting and intel flow without delay.
Dispersed Ops / ACE	Maintains security in ACE and DDIL conditions **without relying on network availability** - ideal for forward-deployed units.
Flight Test and R&D	Protects hypersonic, ISR sensor, and weapons test telemetry from creation to analysis, ensuring **chain-of-custody from lab to range**.
Coalition / Joint Ops	Enforces **AF-tailored data policies** while enabling allied access for joint targeting, planning, and combined ops.
Cyber Range & Lab Trials	**Ready now** for AF cyber range evaluation under live threat scenarios- no integration lag.

Discussion & Next Steps

Where would self-protecting data give you the most impact?

Self-Protecting Data



Live Use Controls

Trusted Audit Trail

Trusted Execution Optionality

Heidi Slocum
Manager, Partnerships and Strategic Growth
heidi.slocum@colvinrun.com
(202) 515-6023

Bruce Olson
VP, Growth and Operations
bruce@colvinrun.com
(360) 551-0552

Nikhil Shenoy, CEO
nikhil@colvinrun.com
(703) 967-1967

SHIELD-C Phase I Demo

SHIELD-C is **procurable via pre-competed SBIR Phase III** (Navy SBIR Contract N6833525C0199)