

Colvin Run Networks

Mission-Driven Analytics

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



www.colvinrun.com



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.

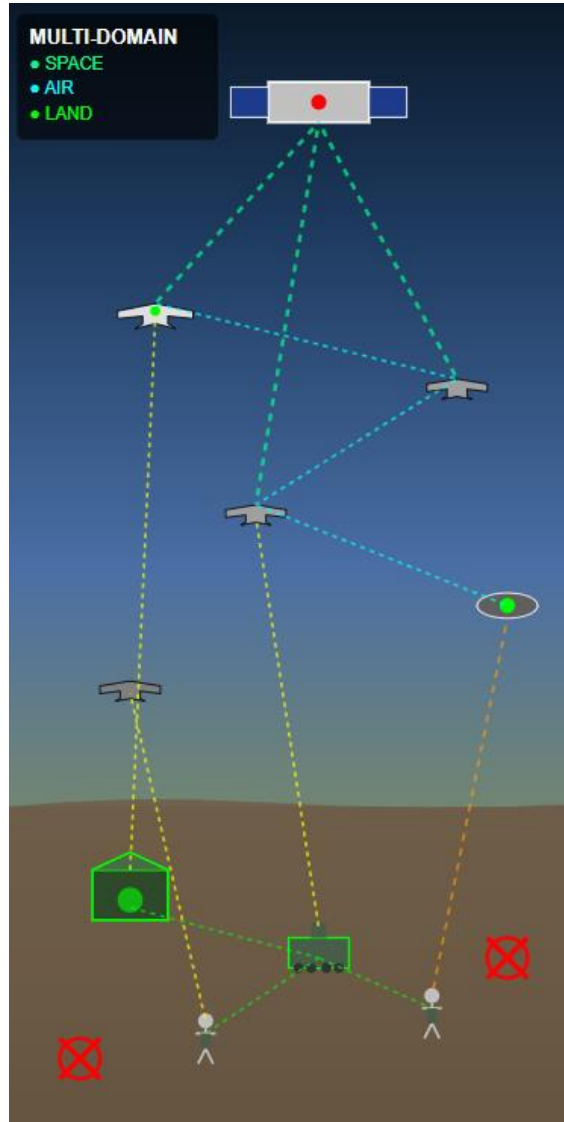
May 3, 2016 



<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



Affirma

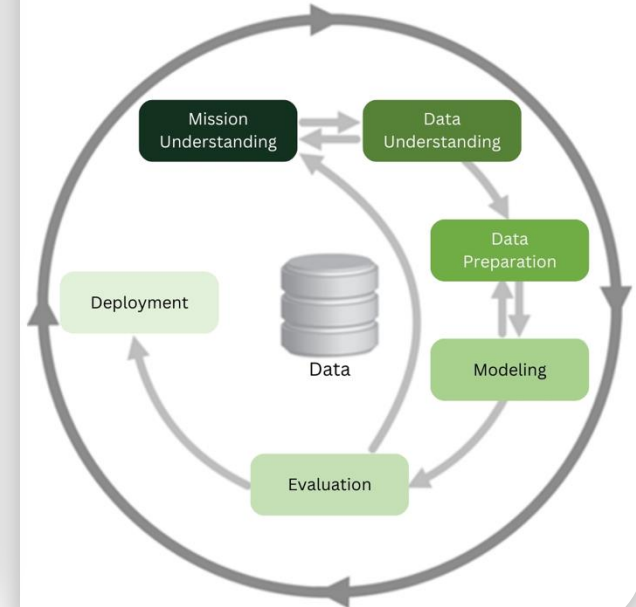
Mission-Driven Analytics



Copia

Mission-Driven Hardware Trust & Assurance

User-Centered Design



Mission-Critical Customers

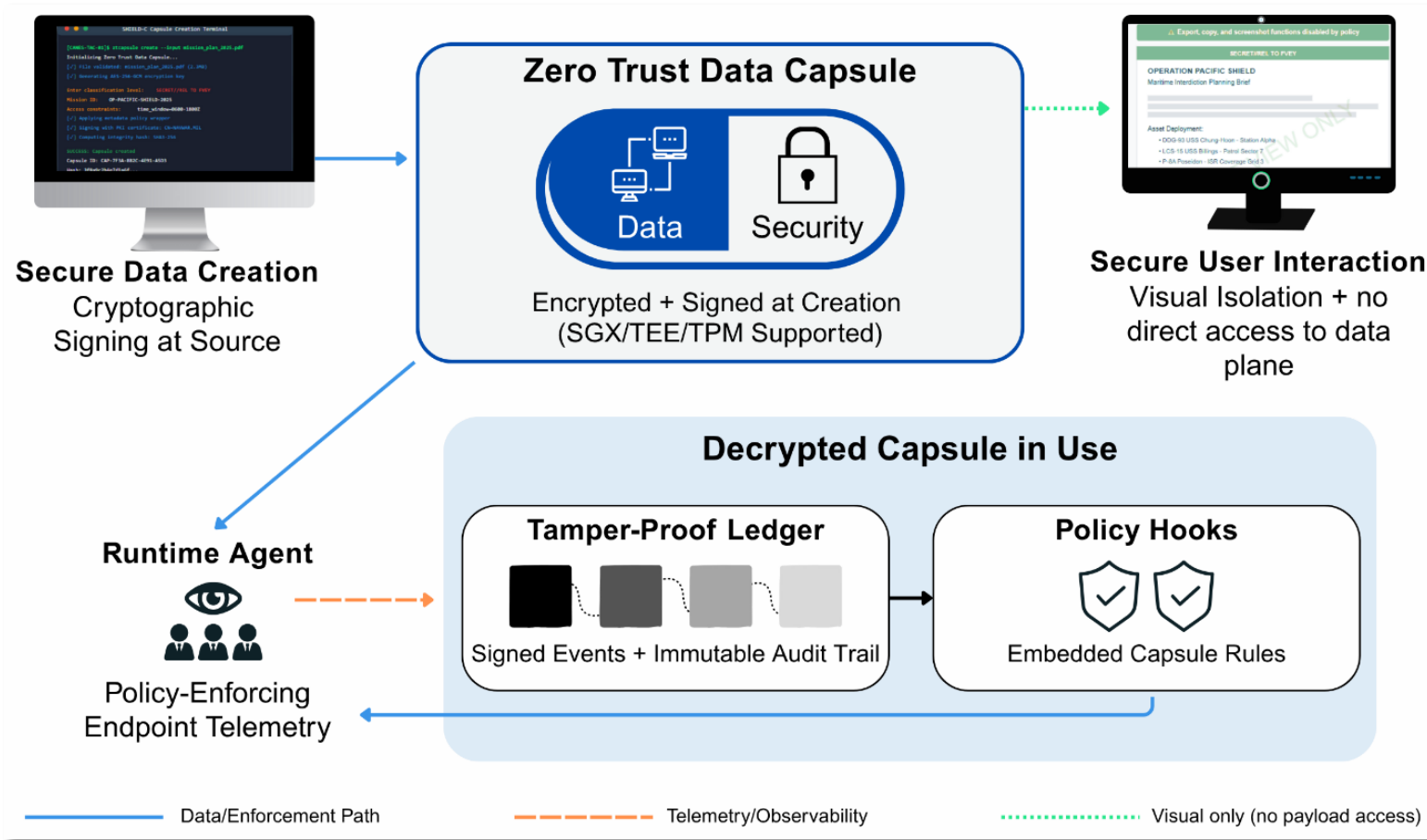


World-Class Technology Partners



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.



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

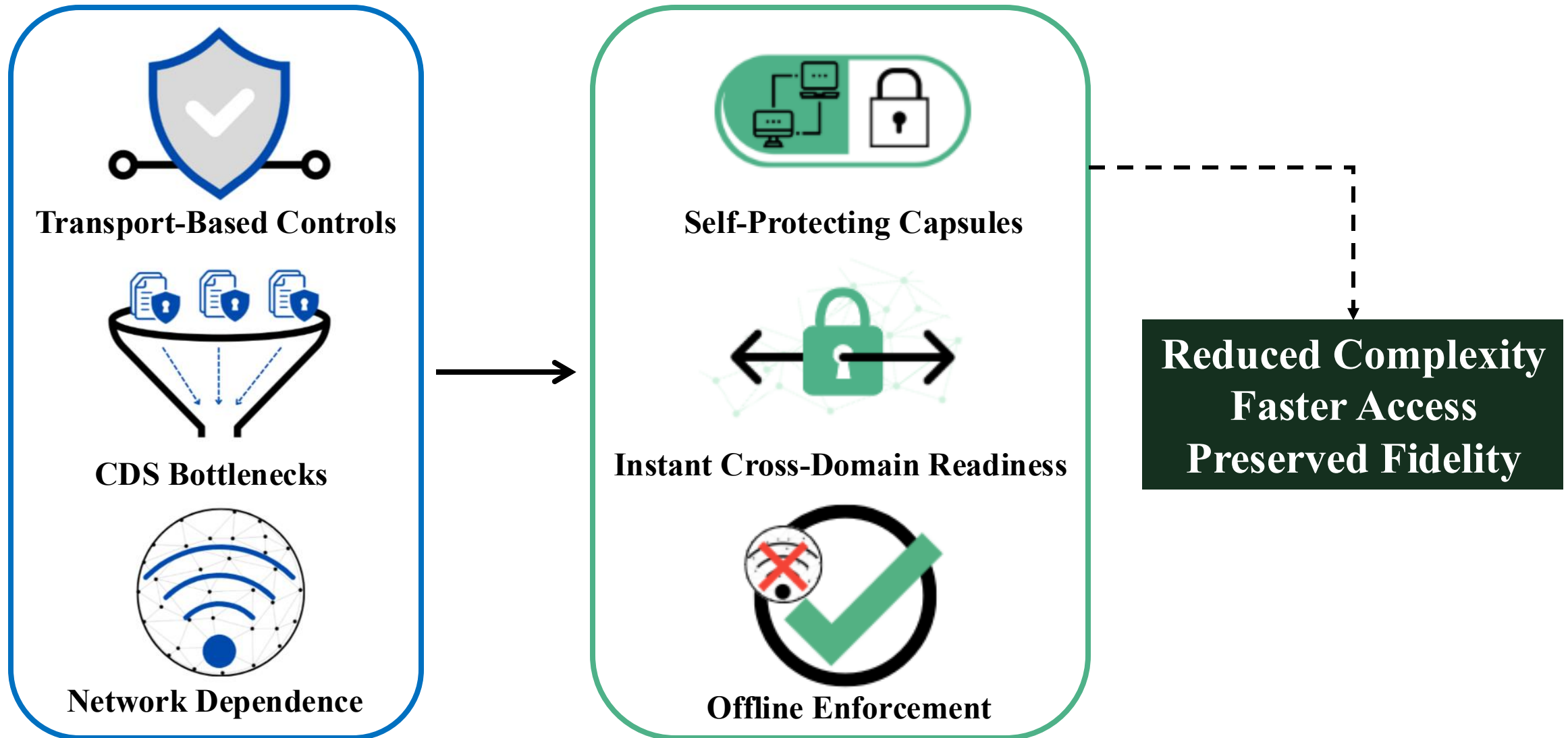
Policy Evaluation

✓ 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



Proven in Phase I, Poised for Phase II Impact

SHIELD-C Encryptor Demo - AES-256-GCM

Plaintext Input:
CLASSIFIED BY: HQ-USCYBERCOM/J3
REASON: EO 13526, Section 1.4(c)
DECLASSIFY ON: 20501231

MISSION PLANNING TEST FILE

Password: [REDACTED]

Encrypt Text Decrypt Text

Output (Base64 of Nonce+Ciphertext):
3qrn5povL0vXbYUg3nmUMy2HB3g3zMM03rhX2xm0tEZ62KStfQ
cQgoT43Tq5qDh6pmqihGaRhQqyV6QN08uMt3qeerD0KKTzaOT58
oiolin-4B1qKtK1FjUJmhpZaClyj/C9s-RZZgeAEft4WwBltCgZOKZnl
8x1G654E0pbdCihyNoItuJ00D23K9uayrOMhSUCUWhSGX18XOSz6Q
T-jkzmiRky5XtcaT2RzUQ0s2yx8EO_tlxo_fgauR0unaN3-9xLg6_OA7

Salt Used (Hex): 6aa6e5016ccbbf916ff909e263e3937

File Operations:
Encrypt File... Decrypt File...

Clear All Fields

Time	Crypto
0023 ms	True
0056 ms	True
0128 ms	True
0290 ms	True
0614 ms	True
1340 ms	True
0082 ms	True
0074 ms	True

Success & Timing
Text encryption successful
Time taken: 0.033 ms

chrome.exe_policy.json

```
{
  "application": "chrome.exe",
  "protection_level": "medium",
  "allowed_operations": [
    "read",
    "write"
  ],
  "clipboard_access": "encrypted",
  "screen_capture": "watermarked",
  "file_access_rules": [],
  "data_classification": "sensitive",
  "hook_dll_protection": true
}
```

Colvin Run SHIELD-C Real Time Protection Demonstration

Dashboard Logs Settings System Info

Log Viewer

[11:23:39] Malware signature database updated
[11:23:59] Monitoring 24 active processes
[11:24:03] Real-time protection scan completed
[11:24:03] USB device connection blocked
[11:24:08] Malware signature database updated
[11:24:23] Firewall rules updated: 7 new rules applied
[11:24:23] Malware signature database updated
[11:24:29] Registry monitoring activated
[11:24:32] Blocked clipboard access attempt from unknown process
[11:24:38] System integrity check passed
[11:24:49] Screenshot attempt blocked - Process: dataexfil.exe
[11:24:54] System integrity check passed
[11:24:57] Registry monitoring activated
[11:24:59] Firewall rules updated: 7 new rules applied
[11:25:17] Protection system initialized successfully
[11:25:20] Blocked clipboard access attempt from unknown process
[11:25:27] Monitoring 17 active processes
[11:25:29] Monitoring 19 active processes
[11:25:29] USB device connection blocked

Phase I Results

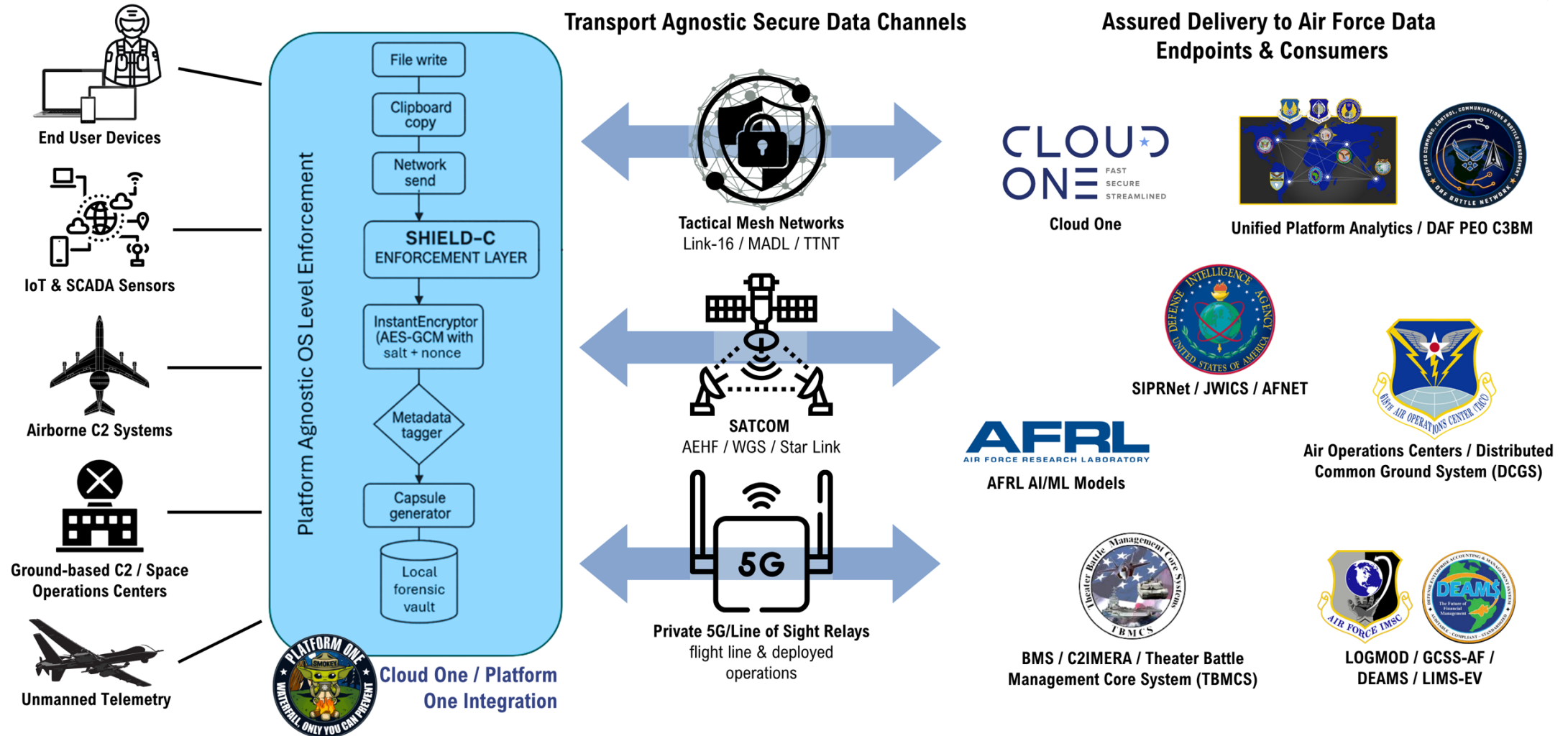
- Sub-millisecond AES-256 encryption at data creation
- Runtime enforcement without kernel/hardware dependencies
- 78% threat detection rate in disconnected red team test
- Tamper-evident audit trails aligned with Navy CSSP schemas

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

Air Force Integration

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



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

Final SHIELD-C Encryption Benchmark Results			
Test Case	Crypto Time	Total Time	Crypto < 1 ms
Individual File Encryption			
1 MB	0.0000 ms	0.0023 ms	True
5 MB	0.0033 ms	0.0050 ms	True
10 MB	0.0075 ms	0.0128 ms	True
25 MB	0.0149 ms	0.0290 ms	True
50 MB	0.0285 ms	0.0614 ms	True
100 MB	0.0587 ms	0.1340 ms	True
Batch File Encryption (Concurrent)			
5 files	0.0008 ms	0.0082 ms	True
10 files	0.0007 ms	0.0074 ms	True

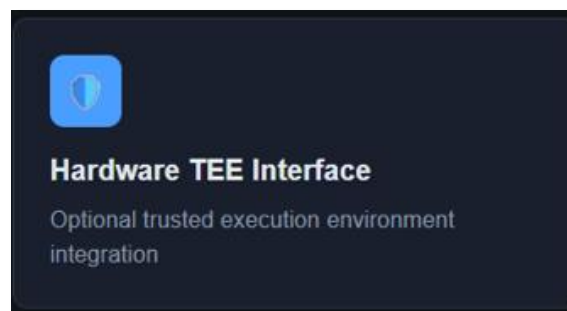
Live Use Controls

```
chrome.exe_policy.json
C:\Users\nykro\Desktop>SHIELD-C Deployment Demo> chrome.exe_policy.json
1
2
3 "application": "chrome.exe",
4 "protection_level": "medium",
5 "allowed_operations": [
6   "read",
7   "write"
8 ],
9 "clipboard_access": "encrypted",
10 "screen_capture": "watermarked",
11 "file_access_rules": [],
12 "data_classification": "sensitive",
13 "hook_dll_protection": true
```

Trusted Audit Trail

```
Log Viewer
[11:23:39] Malware signature database updated
[11:23:59] Monitoring 24 active processes
[11:24:03] Real-time protection scan completed
[11:24:03] USB device connection blocked
[11:24:08] Malware signature database updated
[11:24:23] Firewall rules updated: 7 new rules applied
[11:24:23] Malware signature database updated
[11:24:29] Registry monitoring activated
[11:24:32] Blocked clipboard access attempt from unknown process
[11:24:38] System integrity check passed
[11:24:49] Screenshot attempt blocked - Process: dataexfil.exe
[11:24:54] System integrity check passed
[11:24:57] Registry monitoring activated
[11:24:59] Firewall rules updated: 7 new rules applied
[11:25:17] Protection system initialized successfully
```

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)