PRIVATE & CONFIDENTIAL
CONTACT: JIM BURKE
JIM.BURKE@KINNAMI.COM

RESILIENT HYBRID DATA FABRIC FOR THE TACTICAL EDGE

KINNAMI
Resilient Data Everywhere

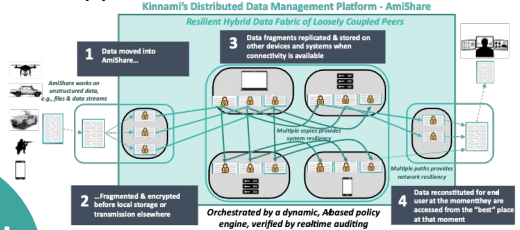
Problem

- Edge devices (sensors/IoT, drones, satellites, wearables, etc.) now have increased computing capabilities
- Data needs to be securely stored on these devices for real-time processing & autonomous operations
- Data needs to be securely transmitted from one edge device to other edge devices or back to datacenters/cloud
- Millions of such devices deployed in physically unsecure locations, where networks may be degraded or under-attack
- Traditional IT solutions for protecting centralized data not sufficient to secure data in edge environments
- Secure, resilient data management is crucial to missions

Resilient Distributed Data Security & Management

Solution

- Distributed peer-to-peer data management & security software
- Data security, protection, availability on any device & network
- Protects data at rest, in-transit, from edge device to cloud
- Supports data movement between devices



- Data replicated, sharded & encrypted at source
- Multiple copies stored in multiple places
- Real-time auditing
- Works across unreliable or air-gapped networks

DoD Success

- 22.1 AFWERX SBIR Phase 2: Biometric Sensor and Tactical Assault Kit (ATAK) integration for CSAR
- 21.2 AFWERX SBIR Phase 2: MLS for Compass Call data
- Agility Prime Phase 2 STTR: Enabling accurate localization using UAVs in GPS degraded environs for CSAR
- USACE ERDC: 5-yr project to secure sensor-based data collection from critical infrastructure (bridges, etc.)
- Air Force DTO SBIR Phase 2 : Securing movement of large engineering ASOT datasets for Digital Engineering
- Air Force ABMS: IDIQ contract for Secure Processing & MLS
- NGA: Part of the NGA's first ever accelerator program

Benefits

- Data security everywhere (even on non-DoD devices)
- Dynamic data closer to the user optimized for low bandwidth
- Back-up and disaster recovery while ensuring data integrity
- Automated policy-based admin transparent to the end-user

Dual Use

- Resilient data for complex environments—edge to cloud—autonomous devices, connected cars, smart cities, IoT devices
- Ensure regulatory compliance (GDPR, CCPA, etc.)
- Ransomware detection & rapid recovery
- Secure data sharing (customers, partners, suppliers, etc.)