ADVANTECH

Enabling an Intelligent Planet

Whitepaper

5G Communications, Computing and Control for the Warfighter

Author: Ryan Wang

Sr. Product Sales Manager

Kevin Lytle

Field Application Engineer

John Reis

Key Account manager

The Tactical Edge Cloud is Transforming!

The Edge is transforming! Enabling cloud capability on the edge in a tactical environment is an emerging trend. It refers to a paradigm shift which is migrating the computation and storage of the data closer to where the data is generated or needed, instead of getting the data from remote locations in the cloud. The appropriate computing and storage power, optimized and balanced, is needed at or near the edge to reduce latency of critical information while reducing the waste of space and energy in traditional centralized systems. The goal is to provide the computing power and data aggregation as close to the warfighter as possible. IoT devices at the edge need to be able to convey the needed information quickly and clearly and in as near real time as possible. To do this IoT devices need to be smarter, faster, smaller and able to communicate over any available communications system while being able to utilize self-forming and self-healing network topologies and techniques. One of the fundamental capabilities of this new model is to provide the needed information on the Tactical Edge while relying on low bandwidth networks when that is all that is available.

In such a new paradigm, the response time can be improved massively and more services can be enabled at the tactical edge to enrich and satisfy the application needs of today's and tomorrow's military. New technologies that are in the early stages of development will surely increase the amount of data that is generated as new applications come on-line. To serve the needs of these new data hungry applications, new networking and AI technologies need to be leveraged This includes the new 5G communication standard that speeds up network bandwidth with lower latencies. The Internet of Things (IoT) finds a perfect growth partner in 5G, which provides support for the increasing number of connected devices.

It is now becoming clear that the edge cloud aspect can indeed play a significant role in reducing latency in battlefield 5G networks.

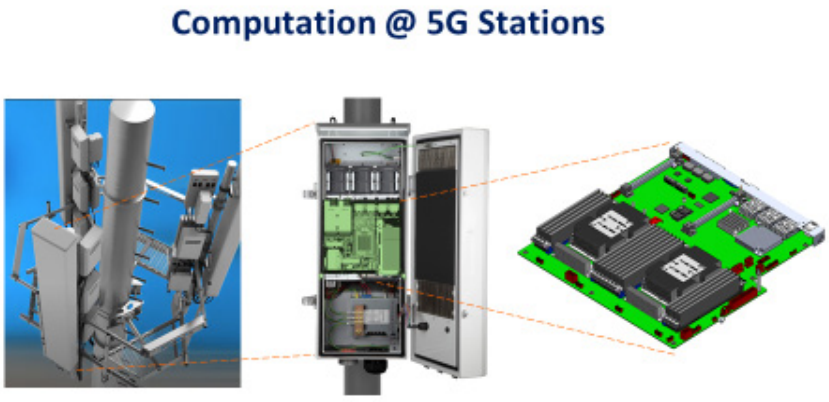
MEC or Multi-Access Edge Computing formerly known as Mobile Edge Computing provides the flexibility and capacity to meet the needs of the modern military. For a long time, most applications have handled their online computation and content storage on remote servers, which are typically located too far away from the end user. The promise and premise of the tactical edge cloud, or MEC in one of its fashions, is to bring these processes closer to the user by allowing them to be integrated into local base stations. Two organizations, 5G Future Forum and European Telecommunications

Standards Institute (ETSI) are going to detail these with their key specification in 5G Experience Management and Deployment and that in ETSI MEC GS028 to meet requirements of enterprises, while also including 802.11 WLAN as one of networking technologies for the implementation. A military private 5G network can be setup on the battlefield to ascertain high speed data and information to allow for more confident real time decision making in critical situations.

The edge cloud can deploy intelligent services to enrich and satisfy the local application needs in various fields while offloading inappropriate tasks to the cloud. Some, like, smart surveillance or intelligent security applied for search and rescue, detection missions, object recognition, or path planning, etc. are computation-intensive and latency-sensitive [2]. Relying on the cloud to process information from the tactical edge and then deliver decisions to the tactical edge cannot meet many of the modern warfighters needs! Hyper intelligent tactical edge devices that can be packaged for man-pack, drones, and autonomous scouts, IFVs or other vehicles, can perform the needed decision making with advance AI based engines without the latency of traditional cloud based systems.

Some of the systems that will reside on the Tactical Edge of the network are driving the need for improved network performance and availability, with lower latency while also requiring higher processing power than currently available systems. These next-gen solutions will utilize augmented or virtual reality, real-time visualization of the battlefield, optimized route planning, target identification and targeting, ad-hoc survivable mesh networks using data from many sources that needs to be timely and accurate.

In preparation for these new needs, edge cloud architecture models are being researched by many organizations. The corresponding architecture is approaching readiness for sophisticated implementations [3].



Virtualization and Containerization Benefit Mission Focused Communications!

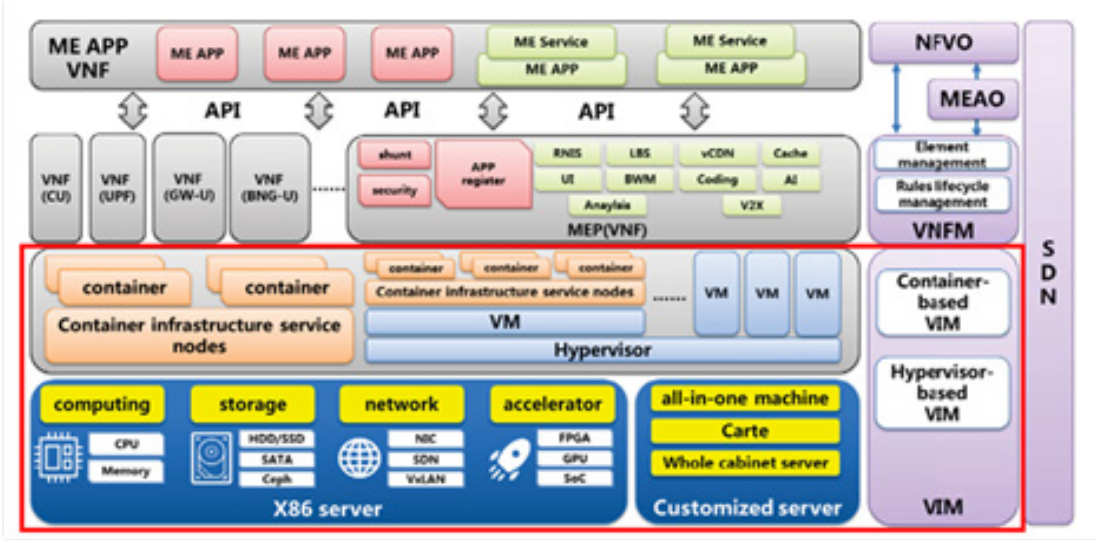
Benefitting from recent virtualization technology along with the advancement of the corresponding software stacks, physical hardware resources are used efficiently through virtualization and containerization as a resource pool and they can be leveraged or dismissed per the incoming tasks or end of the missions. The tasks or missions can be accomplished by utilizing hardware based acceleration running on discrete accelerators from Intel, Nvidia and others or in GPU or FPGA based systems.

The orchestration management scheme is deployed east-west bound for ensuring the entire edge cloud operates as expected and is flexible enough to adjust to virtually any given mission.

1. In the architecture shown below for a private cloud deployment, east and west bound, means each hierarchy in the architecture, or the functional blocks, or feature variants, etc. in a hierarchy, or a layer. So the orchestration management is going to manage all layers and all functions/features east to west (horizontally).

2. As above, north and south bound means vertical operation. Including the hardware resource layer, hypervisor layer, VNF layer, and ME App layer are needed to perform required operations in a cloud framework. In the figure below, the blocks are sitting in the north and south direction in the architecture map such as following.

3. The 5G mesh application case mentioned below, where users are sharing the same network involves both north-south operation, e.g. networking communication through vertical layers so packets can be delivered within the orchestration or outside of the orchestration, as well as east-west collaborations such as virtual networking, firewall, security, etc.



Ref: 5G Edge Cloud Networking and Case Analysis, IEEE ICCT, 2020

We Understand the Need for Securing the Information That Our Warfighters Depend On!

Having an optimized edge-to-cloud software platform for IoT at the Tactical Edge. The security features and user defined access pathways are enabled to ensure the privacy of data processed for applications. The software stack is named W-STACK Private Cloud solution [4] which has been evaluated in IoT environments. The advantage of using W-STACK Private Cloud is that applications can operate under an integrated infrastructure as a service, IaaS, which is highly available, provides for elastic expansion, and advanced security capabilities that support discrete hardware, FPGA or GPU based acceleration.

Additional security such as load balancing and firewalls are important for promoting the security of operations.

Trusted Services and Applications Cannot Be Built on Top of an Untrusted Platform

Cyber resilience is about business continuity in a continuously compromised environment.

No system or network is ever going to be impenetrable or absolutely trustworthy. The weakness in multi-layer defense is the “hard edge soft core” strategy. Providing resilience at the core with tamper-resistance and runtime integrity builds trust.

- Risk model-based metrics (Devices Risk /Intelligence
- Attested Platform and system measurements
- Monitoring with device and platform level event notifications of suspicious activities
- Protected Boot Sequence
- Device identification with immutable identity from any secure element as the root of trust
- Device onboarding with transfer of ownership from manufacturer to vendor to owner
- Node Locked with device fingerprint to prevent cloning and tampering
- Remote Device Recovery – Recover devices to a known good state securely and remotely
- OS and Processor agnostic
- Designed to achieve compliance readiness (FIPS 140-2 Level 1, NIST 800-53, ISA 62443 (SL 2-4), NERC/FERC (CIP), NIST 800-63-3, DO-178, GDPR)

Trust begins with immutable identity for hardware, software or firmware components. This serves as the root of trust. Persistence of trust requires verification of bootloaders and images, key protection, rotation and certificate renewal, which enables a capability to remotely and securely recover platforms into a known-good state.

Security requires: Device identification and authentication, Dynamic key exchange, assurance of data integrity, Data privacy, Secure enrolment and updates, software PuF, and minimal or no coding needed to perform the above once the system is deployed leveraging off-the-shelf client binary agents like the Mocana TrustPoint agents.

This solution must have the ability to add new or re-enroll, recovering platforms to a known-good state, network users such as sensors, voice, video and data agents to the trusted network once they have been enrolled into the trust database service. Continuous monitoring of any exceptions or potential threats must be alerted and streamed into a SIEM/SOAR engine, in real-time!

The cybersecurity system, including as many of the components that make up this system as possible, must be identified with a fingerprint that prevents tampering before it reaches the field. Providing for the prevention of tampering or cloning, etc., of hardware, BIOS, and applications before it leaves the producer, allows for a very solid level of trust.

The cybersecurity system must also enable remote and secure onboarding at scale of these trusted platforms in the field with minimal disruption of operations.

The system must also enable a bridge between requisite IT cybersecurity controls, e.g., PKI, Certificate Authorities, Active Directory and/or LDAP. Additionally, these trusted agents should generate a stream of device security specific data illuminating indications of compromise which can feed into a data analytics engine AI/ML, SIEM/SAM or other threat data analytics or SOAR systems for remediation.

Protection of a Trusted System is required for a Perpetual Trust

Preserving the trustworthiness of devices from manufacturer to end of life begins at the factory and must persist through the life cycle of firmware, software and configuration updates. This requires a tamper resistant content delivery platform and a trusted supply chain of providers and publishers. Further Operational Technology devices require a perimeter-less network defense, efficient and effective key and certificate management, and remote device recovery.

Some of the key features that should be considered are:

- Cyber protection “as a service” architecture for devices and cloud at the edge
- Hardware or software-based cryptographic enclaves across a wide spectrum of classes/sectors
- Secure trust store and key rotation integrated with enterprise and commercial certificate authorities
- Extends secure element protection to containerized applications with process isolation
- Ability to “data diode” the device (no inbound network connectivity) and lock-down network access
- Securely enroll, register and update wired, wireless and air gapped devices
- Tamper-resistant delivery with supply chain provenance
    - (Developer, provider, upstream publisher, downstream publisher)

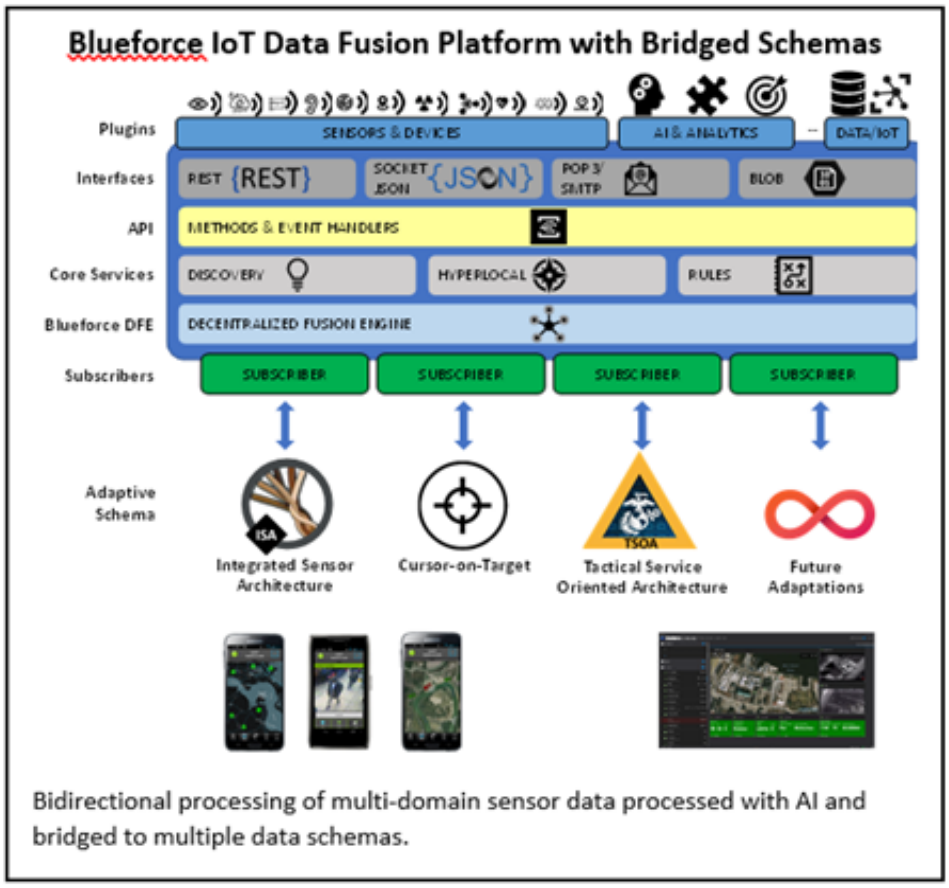
Having Needed Components is Good…. Solutions That Are Complete And Comprehensive Are Better!

Without having the glue that holds this all in together there will not be a significant benefit from the tactical edge. Having a middleware with open source plugins will be necessary for the seamless communication and ability of the smart sensors to perform cohesively in concert.

blueforce DEVELOPMENT

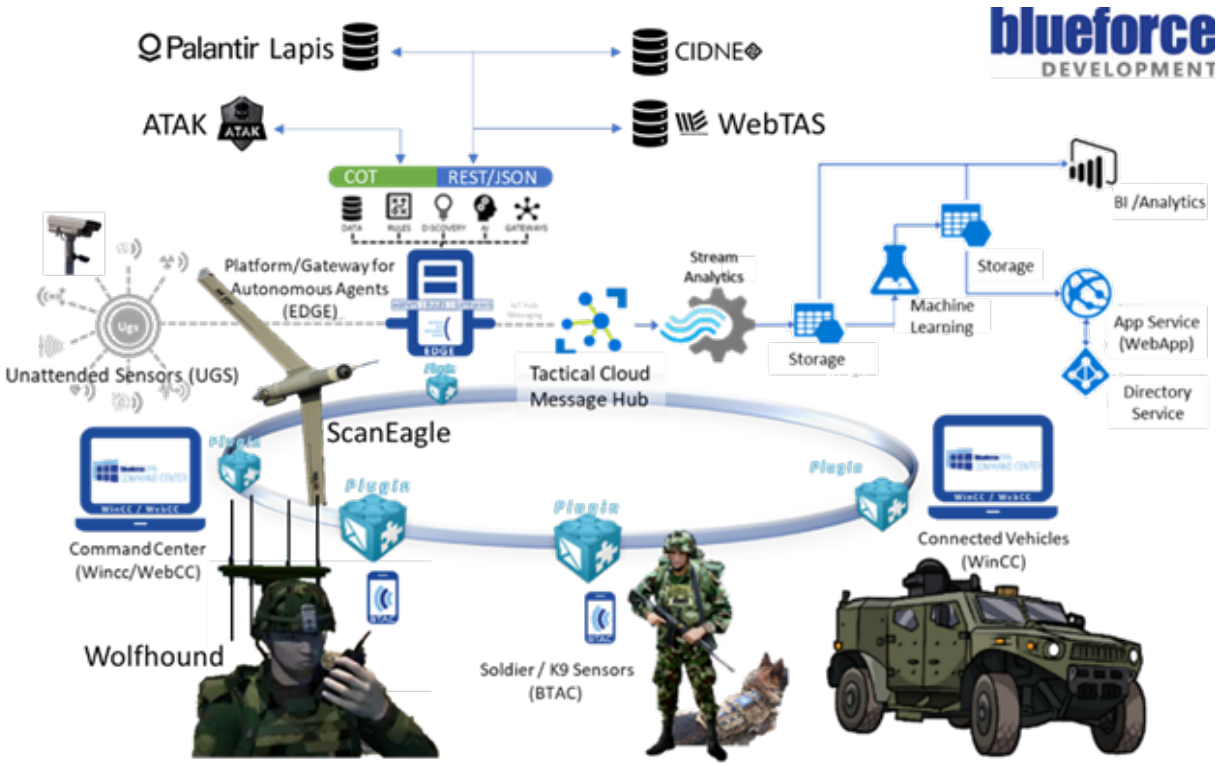
IoT Data Fusion

Blueforce is an IoT data fusion software platform for forward sensor fusion with edge-based processing to accelerate recognitional decision-making at the edge of the network. The Blueforce Decentralized Fusion Engine (DFE) and services oriented architecture (SOA) allow serial or parallel processing with artificial intelligence (AI) at edge of the network, which decreases the need for upstream processing, shortens decision cycles with less network traffic and a smaller electromagnetic signature.



Bidirectional processing of multi-domain sensor data processed with AI and bridged to multiple data schemas.

The operationally-proven (TRL 9) Blueforce core provides universal addressability, discoverability, and subscription to sensor data from any point on the network and is interoperable with Integrated Sensor Architecture (ISA), the adopted sensor networking standard of the Sensor Common Environment. The Blueforce distributed plugin framework provides a centrally manageable mechanism to control the distribution and updating of software and services on the tactical network stack.



Through its integration with ISA, Blueforce achieves transparency with the Sensor CE and compatibility with the Common Operating Environment, providing bi-directional discovery, publishing, and subscription of sensors, among multiple Blueforce and ISA realms.

Blueforce Development has three product offerings:
BlueforceTACTICAL (for Android and iOS)
BlueforceCOMMAND (for Windows and platform-independent HTML5)
BlueforceEDGE (server-based and/or cloud-hosted).

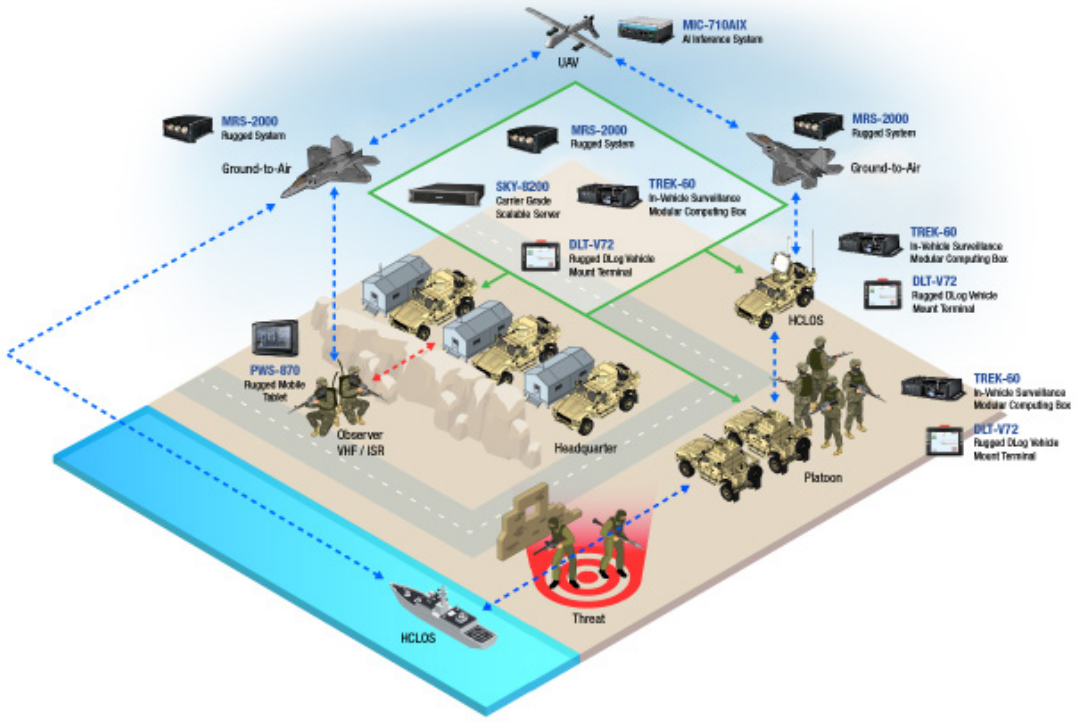
Operator-centric Data-fusion Kits (ODK)
Kits of edge compute and smart IoT devices to simplify the acquisition, processing, and analysis of sensor data from diverse types of sensors.

EDGE-Box™, built on the Cubic M3 Lite, is a powerful, ruggedized, small form-factor edge compute device that integrates IoT data fusion, autonomous AI agents, and interoperability bridges across C4ISR systems to support high-throughput processing of machine-to-machine messages for airborne and ground mission networking without a network back haul.

BTAC-Hub™ is a low-SWAP smart hub that integrates, transmits, and receives diverse sensor data, while managing the network connectivity, power, and operation of all devices and sensors for the operator.

Blueforce provides a services-oriented architecture for forward sensor fusion with edge-based processing.

Internet of Warfare – Bringing the Warfighter and the New Emerging Tactical Edge Systems Together for Greater Awareness and Increased Survivability!



Before the Internet of Things (IoT), electronic warfare was riddled with proprietary solutions that made it difficult or impossible for systems to communicate with one another and the sharing of accurate data between groups was very poor. This was in large part due to the military directly partnering with specific manufacturers that would create heavily engineered solutions specific to its needs, which resulted in minimal competition, due to having a non-reoccurring cost that outweighed the benefits of changing manufacturers over time.

Today, IoT has brought this full circle with open solutions to provide warfighters a seamless stream of information in an open systems environment. The ecosystem for these types of technology are now vast and far more competitive; however, having an open system solution is not without its drawbacks. With technology wars now being fought over the internet as well as on the battlefield, we are faced with cyber hackers who are trying to disrupt the stream of information to the warfighter. As such, cybersecurity and artificial intelligence will become mainstream paired alongside IoT devices.

The Internet of Warfare or IoW is an area where Advantech, with our hardware and software partners, can and will play a key role in bringing Commercial-Off-The-Shelf systems to the IoW that provide the following capabilities:

- Multi-User Multi-network self-building, self-healing Mesh and Adhoc networks.
- Subscribe and publish model bringing to the warfighter, on one cohesive network, many of or all of the diverse sensor inputs, UAVs, Autonomous Scouts, and other accessible systems needed.
- COTS based AI, Data Storage, 5G and Mesh Network Servers designed for use in the IoW.
- COTS based mini and Small Form Factor fanless computing units that support significant IO capabilities with on-board AI accelerators that are built for rugged mobile use.

Advantech has the depth of product to provide solutions in the data aggregation, machine vision, AI based visualization, and rugged fan less small form factor systems to address the needs of the IoW!

Why Advantech?

Advantech specializes in the design, manufacturing, integration, and fulfillment of a wide range of COTS mission critical hardware for embedded and ruggedized applications. Hardware such as, Com Express Carrier boards, Jetson NX carrier board platforms, COM-HPC Servers, high performance servers, appliances, motherboards, embedded modules, tablets, and displays. In addition, Advantech's DTOS or Design to Order Services team can develop tailor-made systems or boards to meet specific application requirements by leveraging off our innovative and world leading technologies. With Advantech, there is no limit to the applications and innovations our products make possible.

References

1. Edging Towards a 5G Future: Mobile Edge Computing
2. Distributed Fog Computing for Latency and Reliability Guaranteed Swarm of Drones
3. 5G Edge Cloud Networking and Case Analysis
4. https://www.advantech.com/srp/wise-stack-private-cloud

Authors

Ryan Wang
Ryan.Wang@advantech.com
Ryan Wang specializes in Servers for the Infrastructure of Edge, 5G, and ruggedized applications.

Kevin Lytle
Kevin.lytle@advantech.com
Kevin Lytle is a Technical Project Manager with over 20 years in the IoT and Intelligent Logistics markets.

John Reis
john.reis@advantech.com
John Reis is a Key Account Manager with 30 years' experience in the embedded military computing market