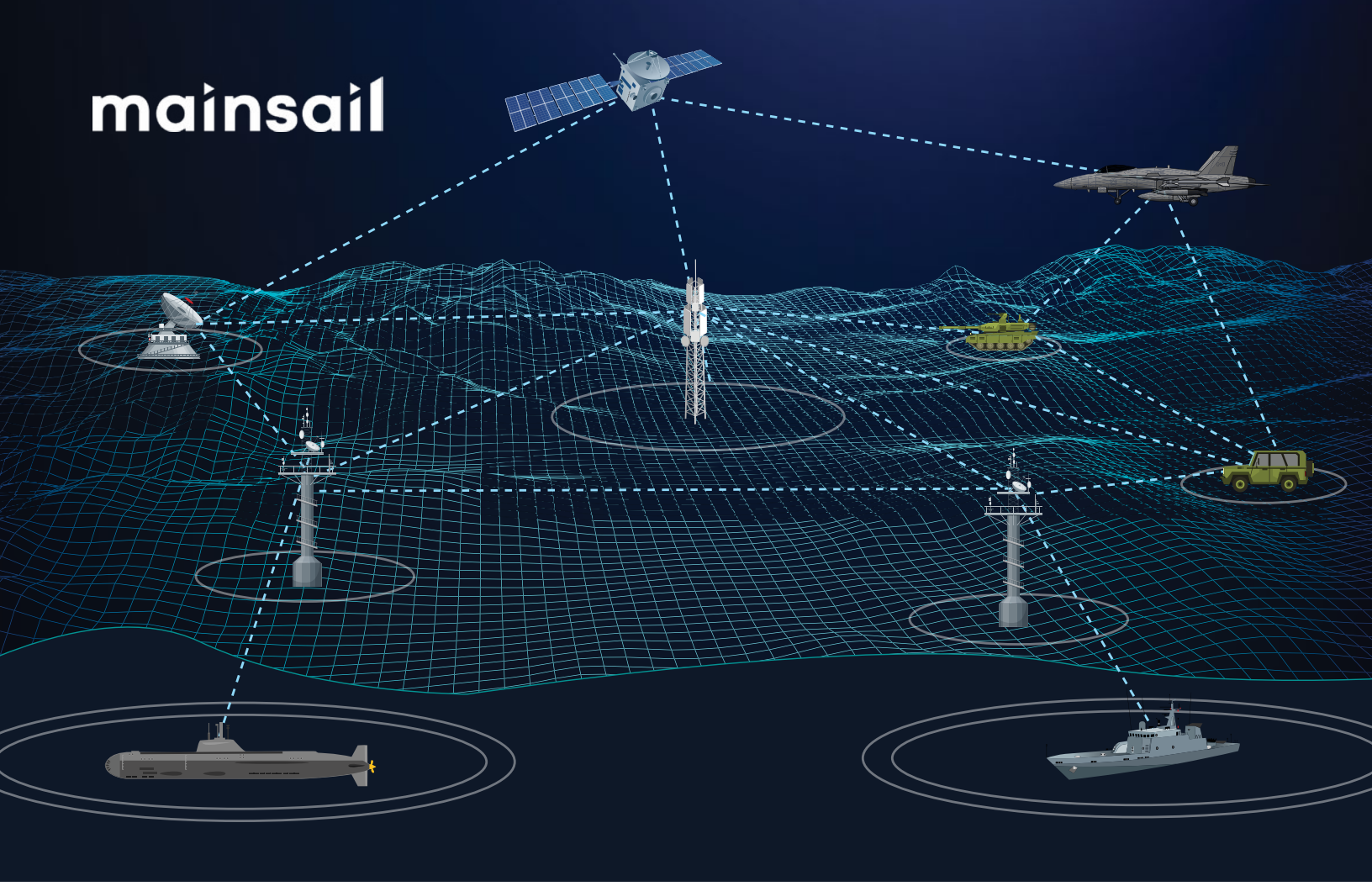


Simplify, Automate, and Secure Multi-DomainCommunications: Falcon Tactical Edge

Coordinating and managing resources, people, and assets on an information age battlefield requires adaptable secure communication networks that are automated for rapid, error-free deployment, and combine multiple available public or private transmission technologies for reliable connection from core applications in private/public clouds to the tactical edge.

Mainsail Falcon Tactical Edge (FTE) delivers the most secure and fastest edge platform for running mission-critical workloads. This platform integrates edge computing and communications into a single secured, multi-workload platform. Mainsail FTE is based on commercial-off-the-shelf technologies from Mainsail, IBM, and Turnium.

Real-time communications and decisions

Commanders in-theater need to be able to make decisions from information at the speed of relevance. Depending on enterprise clouds to process data and deliver decision-quality information can cause unacceptable latency and, in some cases, may not be an option due to intermittent, degraded, or denied conditions.

Overcoming these battlefield communications constraints, requires organizations to have the capability to deploy robust AI/ML processing for multi-domain analysis, understanding, and communications at the tactical edge and deliver answers to commanders supporting real-time decisions, ensuring that teams on the move are self-sustaining and not reliant on distant enterprise clouds.

Falcon Tactical Edge: Powered by proven COTS technologies

Mainsail FTE is based on proven, commercial off-the-shelf technologies from Mainsail, IBM, and Turnium. Together these technologies deliver:

- Zero Trust from the Silicon Up: Trust is built early on at the lowest levels to ensure confidentiality and integrity, extending your zero-trust architecture from the network down to the silicon to deliver a secure edge.
- Deployed and managed mission-critical applications at-scale with robust security and attribute-based access controls across containers, VMs, or bare metal.
- Radically simple containerized SDWAN with full AES 256 encryption and network link aggregation for maximum bandwidth utilization.

FTE extends zero trust architectures to the secure tactical edge, brings workload & data security, as well as secure communications as one integrated solution.

Falcon Tactical Edge: Secure Edge Platform

Mainsail Falcon Tactical Edge (FTE) is based on Metalvisor, which is a new type of platform where security begins in the silicon and implements a trusted foundation to build and run mission-critical applications. Trust is built early on at the lowest levels to ensure confidentiality and integrity. This ensures that edge platforms are not trusted until they are cryptographically verified to be in a known trusted state, thus extending your zero trust architecture from the network down to the silicon at the secure edge.

Zero Trust from the Silicon Up:

- Hardware-based Root-of-Trust derived from the CPU for workload signing and platform attestation
- End-to-end/full-stack approach to data security

Hardware-based Isolation of Workloads:

- Protection/Immunity against Side-Channel attacks by design (Spectre / Meltdown)

Confidential Compute:

- Triad of Data Protection: Encrypted At-Rest, In-Flight, In-Use
- No Application refactoring or additional software needed

Metalvisor utilizes hardware acceleration and dedicates hardware to workloads giving them the highest computing performance available for the edge. This ensures workloads get guaranteed quality of service, delivers maximum utilization of system resources, and delivers hardware-based acceleration for encryption/cryptographic workloads.

Process and Store Data Faster:

- Increased throughput and reduced latency

Highest Quality of Service QoS:

- Run Deterministic and Real-Time workloads

Isolation against Competing Workloads:

- 100% Protection from Noisy Neighbors and resource contention

Falcon Tactical Edge: Application Delivery at the Edge

Within Falcon Tactical Edge, workloads are securely deployed according to policy and secured with continuous monitoring and remediation. FTE uses IBM's Edge Application Manager (IEAM) (based on the LF Edge's Open Horizon project) to secure and automate the process of deploying workloads at the edge. This becomes especially important for edge workloads like AI/ML where deployment and management of data models need to be updated and protected.

IEAM is a hybrid solution that delivers embedded security and eliminates the need for additional edge security software. It provides a secure, authenticated method of distributing workloads at scale, supporting 30,000 edge endpoints, providing encrypted and signed messages, container tampering prevention, and update verification. It provides consistent visibility, control, and automation for managing and scaling workloads, even when disconnected.

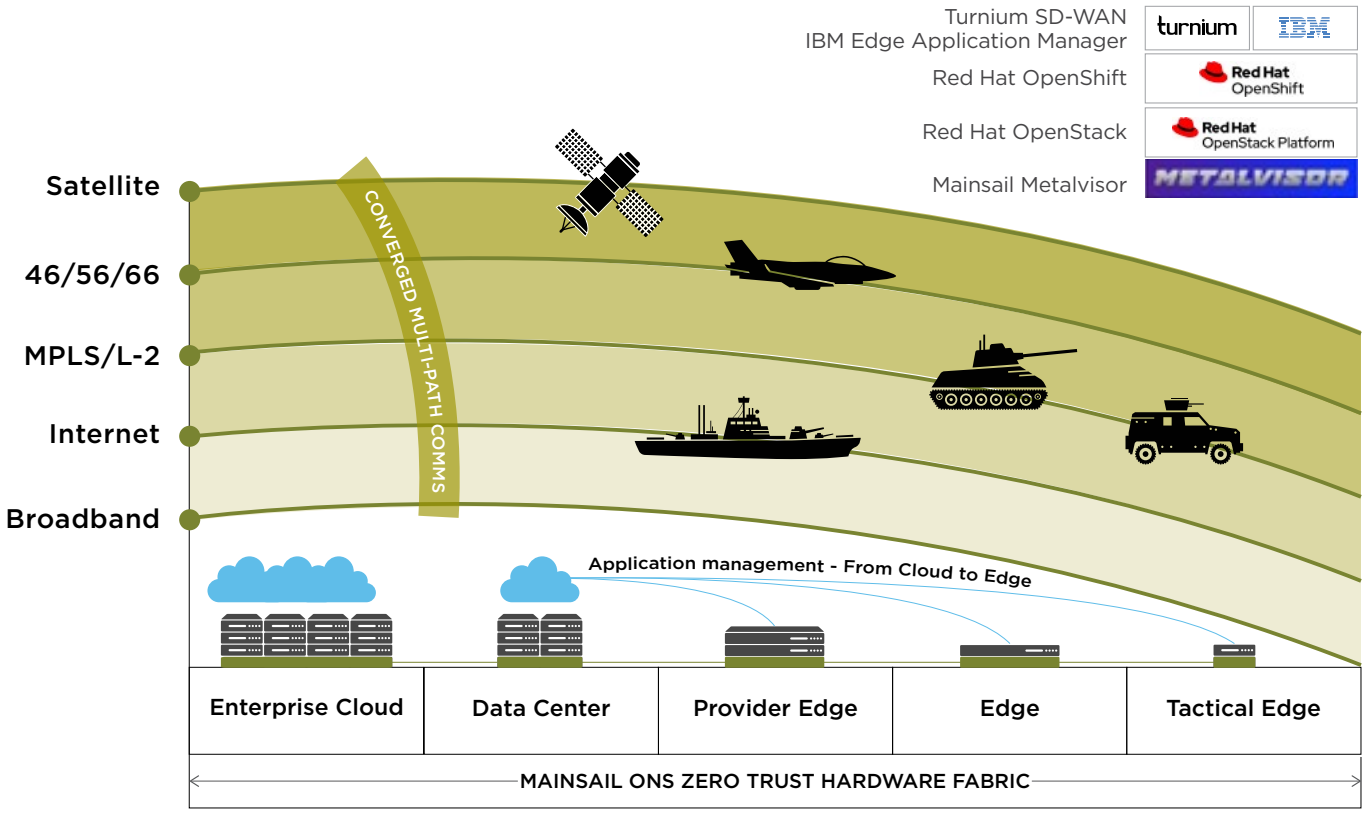
IEAM working with Metalvisor creates a secure platform to deploy mission-critical workloads and be confident that these workloads are deployed in accordance with organizational policies and are secure from the silicon up.

Falcon Tactical Edge: Secure Edge Communications

Mainsail FTE includes a software-defined wide-area networking (SD-WAN) environment from Turnium. This networking solution enables edge devices to be network and transport agnostic and enables edge devices to move freely while maintaining network connectivity across multiple private or public networks. As a device moves out of range of one network, connectivity transitions seamlessly to the next available, configured network while maintaining an AES 256 encrypted secure session.

Edge-to-core communications can use multiple paths at the same time, distributing packets across multiple circuits to obfuscate already encrypted data. This renders man-in-the-middle intercepts less likely to succeed. Network circuit failure or degradation is solved automatically, with data shifting gracefully to other available circuits. Secure sessions are maintained by using the same network operator/owner IP address on every circuit used at each edge node.

Within Mainsail FTE, the Turnium platform enables network connectivity to be delivered as containerized software that can ingest any available data links & networks extending connectivity from edge to cloud.



Summary

The Mainsail FTE provides a unified solution for deploying workloads securely to the edge while housing a zero trust hardware fabric to ensure the platform is verified from the silicon up, that workloads are managed according to policy with autonomous security monitoring, and container based SDWAN with AES 256 encryption for secure communications from edge to cloud. Low-level security details and configurations are predefined to be enabled and work transparently to the end-user, making the platform user-friendly and secure by default.

Contact

For more information, please contact Mainsail at info@mainsailindustries.com.

*The appearance of U.S. Department of Defense (DoD) visual information does not imply or constitute DoD endorsement.

mainsail