Zero trust platform for the tactical edge

Trust starts at the silicon

mainsail

DoD edge workloads

- Real-time & low latency
- 5G & open radio access network (ORAN)
- AI/ML inference & models
- High-performance computing (HPC)
- Multilevel security (MLS)
- Critical supervisory control and data acquisition (SCADA)
- Containers & virtual machines (VMs)

Edge computing is part of JADC2 and JWCC

The JWCC, JADC2 framework ties sensors to shooters across all domains, commands, and services using AI/ML and analytics. Processing at the edge avoids the delays of transmitting data from local sensors to distant clouds for processing.

Decision-making moves to the tactical edge

The U.S. Department of Defense (DoD) is pursuing a new direction in providing capabilities to the warfighters across the joint force, accelerating timelines for contracting.[1] To support swift decision-making, the DoD is moving analytics from datacenters to the tactical edge—ships, aircraft, vehicles, and forward deployed bases. Artificial intelligence and machine learning (AI/ML) models running on edge devices can ingest sensor data more efficiently and more accurately to produce information commanders use for faster decision-making. Processing sensor data closer to where it is produced avoids the latency incurred from a round trip to a cloud that might be thousands of miles away.

DoD edge computing use cases help with decision advantage in the following ways:

- Image detection and classification.
- Geospatial image analysis and integration.
- Automated data analysis, enrichment, and flows.
- Connected standalone data to make real-time decisions.
- Cyber threat visibility, coordination, and response.
- Autonomous logistics and support systems.
- Signals detection, classification, and deconfliction.
- Enrichment of augmented reality and virtual reality (AR/VR) with real-time all-domain battlespace data.

Edge computing is a pillar of the Joint Warfighter Cloud Capability (JWCC), Joint All-Domain Command and Control (JADC2) framework to connect sensors across all military branches.[2]

What are common threats at the edge?

Devices at the cloud edge are outside the physical controls of the enterprise datacenter and attacks are getting more sophisticated by infiltrating the application stack (bootkits and rootkits). Attackers are finding it increasingly difficult to exploit and maintain access to the application and operating system (OS) levels due to better software controls and third party security products. Therefore, attackers are looking to exploit things like external supply chains and are moving their strikes lower in the stack—e.g., firmware and basic input/output systems (BIOS)—to avoid detection. Mainsail is protecting against these threats at the lowest point (the silicon) and delivering Zero Trust at the central processing unit (CPU) level using cryptographic verification of hardware.

facebook.com/redhatinc
@RedHat
linkedin.com/company/red-hat

1 *Lopez, C. Todd. "DOD aims for new enterprise-wide cloud by 2022." U.S. Department of Defense, July 7, 2021.*

2 *Hoehn, John R. "Joint All-Domain Command and Control." Congressional Research Service, report IF11493, 21 Jan. 2022.*

"The JWCC will... be a bridge to our longer term approach, allowing us to leverage cloud technology from headquarters to the tactical edge."

John Sherman
Acting CIO, Department of Defense[2]

Red Hat associated technologies with Metalvisor

Red Hat Enterprise Linux

Red Hat OpenShift container platform

Edge workload consolidation

Edge workloads consist of critical, latency-sensitive applications that do not perform well on multicore chips. This situation results in stand-alone deployments, which causes growth in size, weight, required power (SWaP) and high latency. Metalvisor, powered by Red Hat Enterprise Linux, consolidates real-time and latency-sensitive workloads, freeing mission space for additional capabilities, while ensuring mission requirements for speed.

METALVISOR

Hardware-based Zero Trust model from Mainsail and Red Hat

Mainsail's Metalvisor is a security platform built on Red Hat® Enterprise Linux® that protects edge workloads outside of the enterprise datacenter or cloud environment. The platform protects edge workloads from sophisticated cyberattacks by using separation—enforced by security functions built into the hardware. These features protect data in all forms: at rest, in transit, and in use.

Metalvisor uses a custom separation kernel at the unified extensible firmware interface (UEFI) layer to provide a security-hardened environment at the OS core. By implementing security at this level, it is able to restrict threats and adversaries that could otherwise bypass traditional security measures; thus, offering robust protection against sophisticated cyberattacks.

The collaboration between Red Hat and Mainsail promises to bring powerful and security-focused processing capabilities to the edge. A technology originally developed and used by the U.S. DoD, Metalvisor is now commercially available and uses RHEL as the foundation for orchestration.

Metalvisor meets and exceeds National Institute of Standards and Technology (NIST) 800-207 Zero Trust and Metalvisor enhances the mission capabilities of Red Hat OpenShift® Container Platform.

Mission benefits

- **Zero trust.** Zero Trust principles are built into the design by "trusting nothing, and always verifying" starting with the Intel processor, where cryptographic verification of hardware leads to a secure hardware-based root of trust. This is where higher-level software and application chains of trust are built. Metalvisor provides advanced security measures that meet and exceed the guidelines set forth by NIST 800-207 for Zero Trust.
- **Stronger security.** Until now, encrypting data in-use required additional software or application refactoring. Both are time-consuming and costly. Metalvisor transparently encrypts data in-use by default. Red Hat OpenShift protects sensitive container data, like platform secrets and application configurations, with Federal Information Processing Standards (FIPS) 140-2 Level 1-compliant encryption controls.
- **High performance.** Red Hat OpenShift can have the same profile as bare-metal with dedicated server resources, while still using the benefits of virtualization. Applications don't have to compete for resources with other containers deployed on the same server. Critical applications also perform if they are deployed on bare-metal servers. The Metalvisor TypeZero hypervisor provides hardware-level virtualization and improved performance and resource management, allowing system resource efficiency and better workload performance.
- **Simple deployment.** Workloads are cryptographically signed and deployed via Cockpit or Red Hat Ansible® Automation Platform. Metalvisor is integrated with Cockpit, a familiar web interface for managing Red Hat Enterprise Linux. Metalvisor has certified platform support with Red Hat Enterprise Linux.
- **Lower SWaP requirements.** Latency-sensitive and real-time applications run on the same platform, consolidating multiple containerized or virtualized applications onto one multicore server frees space for additional mission capabilities.

- **Autonomous threat protection.** The entire system is constantly verifying workload runtimes, enforcing security policy, and protecting against advanced attacks. Metalvisor has built-in active response capabilities (ARC) to detect, respond to, and prevent cyber threats, including zero-day exploits.

Mainsail Metalvisor enhancing security and performance at the edge

Red Hat OpenShift for safeguarding edge workloads

Red Hat OpenShift is a Kubernetes container based application platform that includes an enterprise-grade Linux operating system, container runtime, networking, monitoring, registry, and authentication and authorization solutions. Mainsail's Metalvisor brings hardware-based isolation to Red Hat OpenShift, ensuring separation between workloads and high-quality service.

This helps to run demanding edge workloads that require high determinism and quality of service, like 5G and AI/ML workloads. Metalvisor also transparently encrypts memory so workloads can benefit from confidential compute and protect data in use.

Metalvisor removes the virtualization overhead and allows you to use Red Hat OpenShift to build workloads without worrying about degraded performance experienced with traditional virtualization. Red Hat OpenShift workloads run with the same profile as a bare-metal machine with the benefits of virtualization and Red Hat Enterprise Linux compatibility.

Find out more

To schedule a demonstration of Mainsail Metalvisor, email info@mainsailindustries.com.

Thank you for downloading this Red Hat brief! Carahsoft is the Master GSA and SLSA Dealer and Distributor for Red Hat Enterprise Open Source solutions available via GSA, SLSA, ITES-SW2, The Quilt and other contract vehicles.

To learn how to take the next step toward acquiring Red Hat's solutions, please check out the following resources and information:

For additional resources:
carah.io/RedHatResources

For upcoming events:
carah.io/RedHatEvents

For additional Red Hat solutions:
carah.io/RedHatPortfolio

For additional Open Source solutions:
carah.io/OpenSourceSolutions

To set up a meeting:
redhat@carahsoft.com
877-RHAT-GOV

To purchase, check out the contract vehicles available for procurement:
carah.io/RedHatContracts