Mission-edge platform for global forces

Preserve sovereignty and strategic autonomy with enterprise open source

Components of a mission-edge platform

Red Hat Device Edge includes:

- Red Hat Enterprise Linux
- MicroShift (a lighter Kubernetes runtime built to be similar to Red Hat OpenShift)
- Ansible Automation Platform
- Edge Manager

Enhance operational resilience with sovereign support

Red Hat Confirmed Sovereign Support[1] is a dedicated support service staffed by citizens of the European Union (EU) and delivered entirely within EU borders.

Overcoming barriers to tactical edge computing

Information dominance and algorithmic warfare across kinetic and inactive domains require strategic autonomy, coalition interoperability, and rapid operational tempo. Achieving these imperatives is especially challenging in multidomain operations (MDO), where forward-deployed forces often operate in highly contested, denied, degraded, intermittent, and limited (DDIL) environments. When connectivity to headquarters is unavailable, tactical edge forces lose access to intelligence, AI-enabled decision support, autonomous capabilities, and command and control (C2). Mission risks include degraded decision advantage and reduced overmatch and survivability.

Global military forces can avoid reliance on a network connection by fielding an autonomous edge platform. Key platform requirements include:

- Digital sovereignty and strategic autonomy. This allows full visibility into the source code and the ability to add or adapt capabilities without relying on a third party.
- Operation on diverse hardware. Small-form-factor (SFF) devices are included.
- Low training requirements.
- Operational resilience. The ability to rapidly reestablish destroyed capabilities on new hardware.

Meeting the requirements with Red Hat edge solutions

Red Hat provides open source platforms and tools to build and run sovereign software across hybrid cloud environments. Red Hat® Device Edge serves as an open source digital backbone that extends command capabilities from the strategic core to the tactical edge of the network. Military planners can rapidly push containerized AI models and C2 applications onto diverse, ruggedized tactical assets. This write once, deploy everywhere architecture supports digital sovereignty by avoiding vendor lock-in. Forward-deployed units retain autonomous operational capabilities even when connectivity is unavailable, supporting mission continuity and a persistent decision advantage in the battlespace.

Maintain digital sovereignty and strategic autonomy

Mission requirement: To confirm that there are no backdoors or malware, military organizations need full visibility into the source code running on edge servers. In addition, IT teams should be able to update security features and capabilities without reliance on a specific vendor.

1 Red Hat press release. "Red Hat Introduces Confirmed Sovereign Support for European Union," 6 Nov. 2025.

Optimize AI performance on any available processor

Not all edge devices have graphics processing units (GPUs). Red Hat AI Inference uses vLLM, an engine that is optimized for throughput and memory efficiency and can run on a central processing unit (CPU)-based infrastructure if GPUs are not available.

Red Hat advantage: When military organizations use open source software, they, not a vendor, control the entire software platform. IT specialists have full access to the source code to confirm there are no backdoors or hidden behaviors.

Red Hat makes open source enterprise-ready by adding the stability, built-in security focus, and support required by military forces. Unlike community open source, Red Hat technologies meet stringent military-grade security requirements, such as Federal Information Processing Standard Publication 140-3 (FIPS 140-3), validated crypto, and Common Criteria certified platforms, including post-quantum cryptography. The curated images and application libraries included with Red Hat software have been signed and verified with provenance checks through Red Hat Trusted Software Supply Chain.[2]

Write once, deploy everywhere

Mission requirement: Edge applications are often deployed on small, resource-limited hardware, including trucks, tanks, ships, and manned and unmanned aircraft. Forces need the flexibility to move software quickly to another platform without modifying the code.

Red Hat advantage: Red Hat platforms and tools are certified to run on a wide variety of hardware systems, including those used in classified-mission environments and in harsh conditions. Virtual machines (VMs) and containerized applications running on Red Hat OpenShift® or Red Hat build of MicroShift can be readily moved to new hardware with little or no modification. Applications can be deployed on small edge devices with space and power constraints. Therefore, military teams can host containerized applications on MicroShift, Red Hat build of Podman Desktop[3], or Red Hat Enterprise Linux®, depending on their hardware resources.

Operate in DDIL environments

Mission requirement: Applications and models must be able to operate when connectivity is unavailable.

Transfer skills knowledge

Red Hat Services provides training on the skills needed to sustain edge solutions. The goal is to prepare global forces to manage the solution internally.

Red Hat advantage: Red Hat edge solutions operate in DDIL environments. Updates are optimized for low bandwidth and intermittent connectivity. Failed updates automatically revert to the last known good state, and updates interrupted by a dropped connection restart where they left off rather than starting over.

Minimize skills requirements for deployment and sustainment

Mission requirement: IT specialists who learn skills in one environment should be able to transfer those skills to another environment without retraining.

Red Hat advantage: Red Hat skills learned in a datacenter, military base, or at the mission edge are portable across echelons and environments. IT specialists can manage the fleet of devices more efficiently with Red Hat Edge Manager, a component of Red Hat Device Edge.

Red Hat Device Edge provides device resource monitoring and security-focused communication using mutual transport layer security (mTLS) protocol.

2 Red Hat brief. "Red Hat Trusted Software Supply Chain," 22 Jan. 2024.

3 Red Hat blog. "Introducing Red Hat build of Podman Desktop," 17 Jan. 2026.

Build operational resilience

Mission requirement: To continue operating at the speed of relevance when capabilities are destroyed, forces need the ability to restore those capabilities on any available hardware. Rapid restoration is essential. A requirement to rehydrate and repopulate a lost database is unacceptable (e.g., because it requires specialized knowledge and can take hours under battlefield conditions).

Red Hat advantage: Personnel can quickly reproduce the decision-support environment on other hardware if a tactical edge deployment is unavailable. Red Hat Edge Manager provides rapid deployment of workloads or models onto new hardware by sending them as a single image, eliminating the need for complex orchestration of multiple images.

Lockheed Martin accesses targets on unmanned aerial systems

Lockheed Martin used Red Hat Device Edge on an unmanned aerial system (UAS) to identify and assess military targets with AI. When the UAS detected a simulated target, engineers updated the UAS software mid-flight to locate the new target, increasing situational awareness.

"With Red Hat Device Edge, Lockheed Martin is leading the infusion of cutting-edge commercial technology into military capabilities that deliver advanced solutions to our customers. Unlocking these AI technologies can help national security decision-makers stay ahead of adversaries, enabling a safer and more secure world."[4]

Justin Taylor
Vice President
of Artificial Intelligence,
Lockheed Martin

Choose Red Hat for mission-ready open source

Red Hat has been a trusted partner to the defense sector for more than 3 decades. Our perpetual subscription model and commitment to open standards provide confidence that government agencies are never coupled to a vendor in perpetuity. Agencies retain the right to use and maintain their software indefinitely, protecting their long-term investment against shifting vendor roadmaps or geopolitical restrictions.

Sample edge use cases for defense

Train an AI model in a cloud or datacenter, deliver to the battlespace

Update decision-maker tools at the speed of relevance and deliver them to the field. An example is identifying airborne targets to classify the threat level.

Build and train the model on high-performance computing (HPC) servers in the core, then use Edge Manager to distribute a compact, containerized model to edge devices. The model is sent as a single image, typically within seconds. Depending on the resources required, edge devices can run models on MicroShift, the Red Hat Podman Desktop, or Red Hat Enterprise Linux AI.

Sensors in the field collect and process contact-related data. The AI model flags objects for operator review. No network connection is necessary for inference. As new target signatures are recognized, the model is updated in the datacenter, and then Edge Manager distributes the updated model to edge devices when connectivity is available.

Field a mini tactical datacenter

Equip forces with a ruggedized, portable computer that can run command-and-control applications without a connection to the datacenter.

A European military organization fields SFF devices that fit in a backpack and run the same tools and containerized applications available at headquarters. The tactical datacenter operates offline:

- Forward troops power on the device.
- Establish a brief connection to download orders.
- Close the connection.

4 Lockheed Martin. "Lockheed Martin, Red Hat Collaborate to Advance Artificial Intelligence for Military Missions." Accessed 7 May 2026.

The user experience is the same as it is on the larger devices used in military bases and datacenters, avoiding the need for specialized training.

Operate a shipboard datacenter on a single-board computer

Provide decision support aboard naval vessels.

Navantia,[5] a Spanish public company providing naval and defense systems, built a shipboard datacenter using Red Hat Device Edge on single-board computers, supporting VMs and containers. Naval personnel manage system and security updates remotely using Red Hat Satellite.

Update system configuration and patch operating systems in flight

Automate patching and operating system (OS) updates to stay abreast of new security advisories released daily.

Manual patching and updating are time-consuming, and systems remain vulnerable to cyberattacks until the patch is downloaded and applied. With Red Hat Device Edge and Red Hat Ansible® Automation Platform, defense IT teams can automatically apply patches and updates to all connected devices at once. This way updates are applied or are not applied.

If the update does not perform as expected, the system can quickly be reverted to the last known good state. Automated patching strengthens the network edge security posture, saving time for IT specialists and avoiding unwanted human error.

Build a sovereign platform for the mission edge

Red Hat meets public sector organizations at any point of their modernization journey.

Whether that step is modernizing the OS, adopting containers, or deploying capabilities in an open hybrid cloud to the mission edge, Red Hat can help your organization advance to the next level.

Read more about how global public sector organizations are accomplishing their missions with Red Hat.

5 Red Hat press release. "Navantia Builds the Future of Naval Systems with Red Hat," 20 Jan. 2026.

North America	Europe, Middle East, and Africa	Asia Pacific	Latin America
1 888 REDHAT1 www.redhat.com	00800 7334 2835 europe@redhat.com	+65 6490 4200 apac@redhat.com	+54 11 4329 7300 info-latam@redhat.com

facebook.com/redhat
x.com/RedHat
linkedin.com/company/red-hat

redhat.com
#4059454_0526