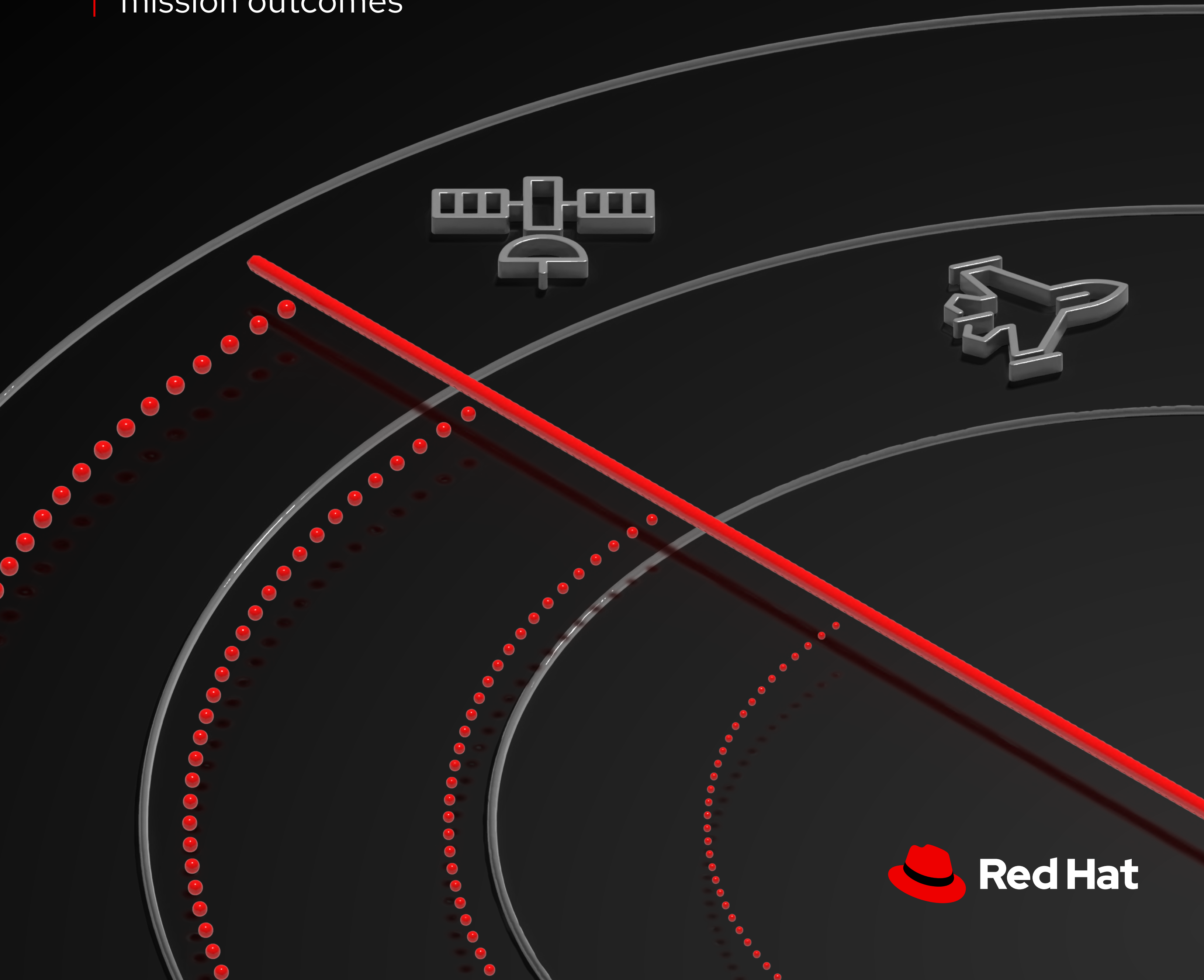
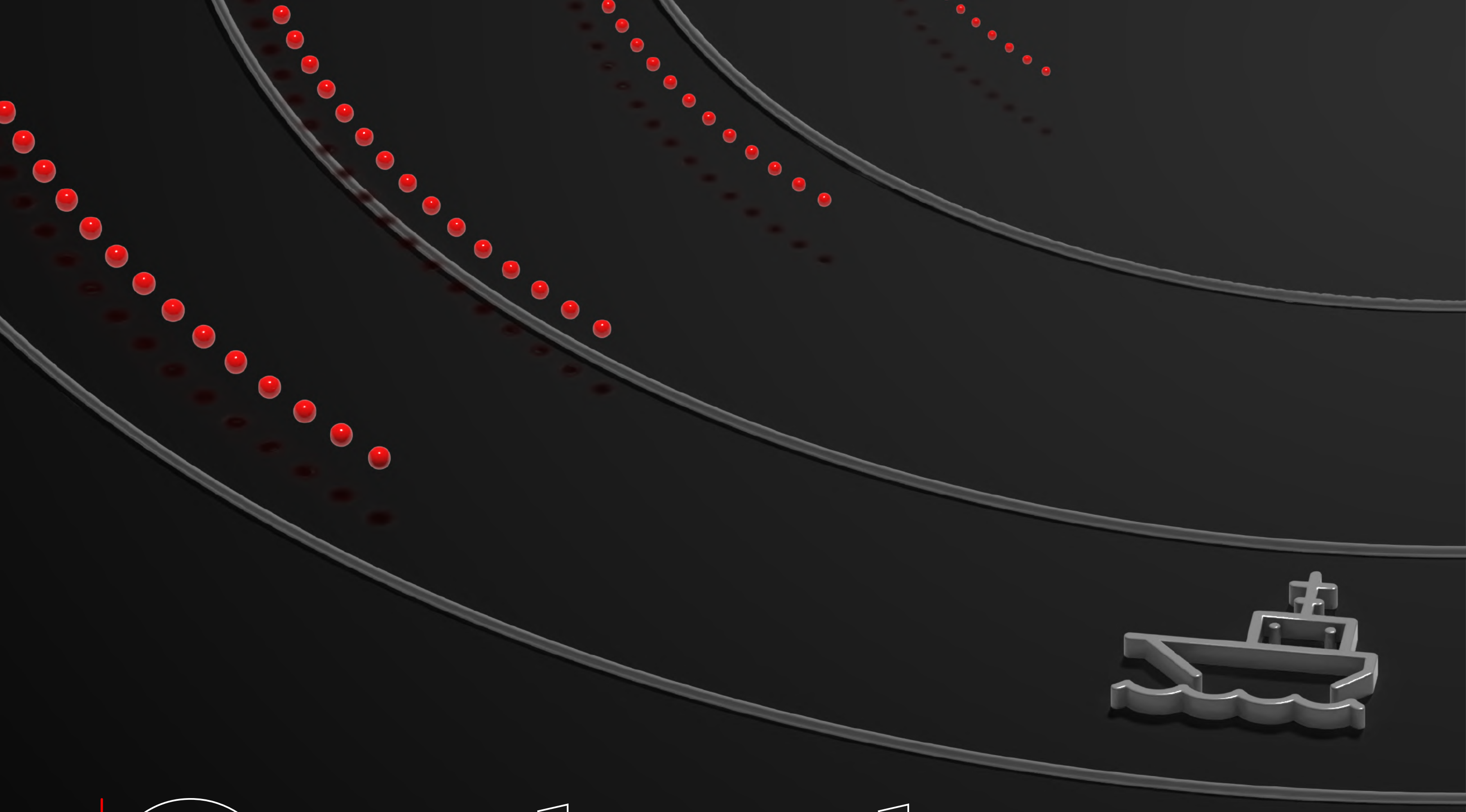
Mission edge

How Red Hat can help the DoD achieve and accelerate mission outcomes





Contents

Introduction
A fundamental shift in IT approach

Chapter 1
Decision dominance is the new weapon dominance

Chapter 2
A path to resilient operations

Chapter 3
Interconnectedness is mission critical

Chapter 4
Data sharing: From intelligence to insights

Chapter 5
Red Hat's approach to mission edge

Learn more

Introduction

A fundamental shift in IT approach

Across the United States Department of Defense (DoD), branches and agencies are using operational and user-generated data to make critical decisions, solve challenges, and maintain dominance in the modern battlespace. But the way data is collected, shared, and used is changing for the modern warfighter.

To integrate and coordinate command and control simultaneously across land, air, maritime, space, and cyber, digital capabilities need to extend beyond the traditional datacenter or cloud environments to the people, machinery, and technology that need them–at the edge of the network.

The DoD faces new and emerging peer adversaries despite the tyrannies of distance, water, time and scale-all present in the pacing theater, United States Indo-Pacific Command (US INDOPACOM). To overcome these challenges and peer adversaries in any theater, the DoD needs solutions that can:

Innovate with agility.

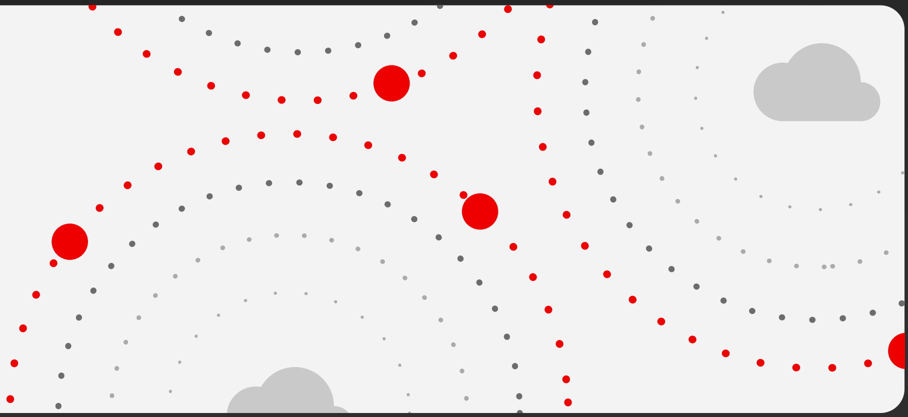
Maintain a high security posture.

Standardize interoperability across all branches and agencies.

Operationalize data.

Ensure cyber operational readiness.

The ultimate goal is to move faster with less risk. Mission edge is an approach that can help achieve this goal to advance mission objectives across the DoD. Mission edge can be defined as a dynamic, decentralized computing architecture consisting of heterogeneous hardware and workloads that connects data producers and data consumers.



A new IT approach for the modern battlespace

Traditional systems used to plan for warfighting have produced unique monolithic domain-specific systems with a history of dominance in classical warfighting battlespaces. However, as technology continues to progress, so have the capabilities and sophistication of the United States' near-peer adversaries. The new challenge is finding ways to achieve the complex integration of the systems needed to coordinate, maintain, and increase operations security across all domains and more specifically, at the edge.

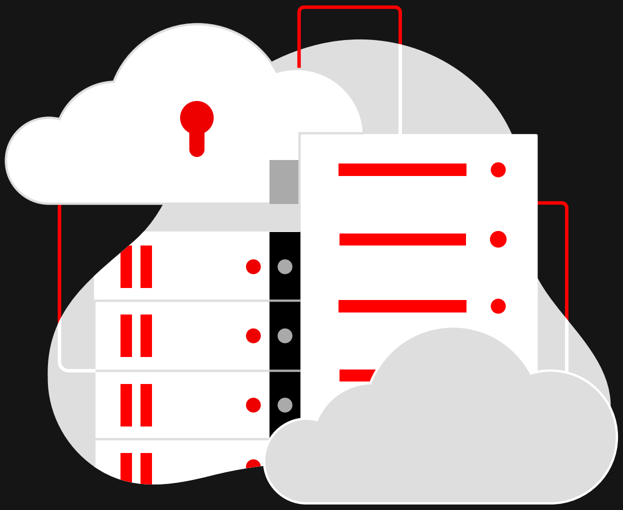
Every modernization strategy should consider the following edge computing environments:

Enterprise edge. Any enterprise capabilities delivered to the consumer via modernized networking and application environments that are standardized and secured. For example, service member and service personnel training for those who are tactically deployed.

Operations edge. Local networks of smart devices that interact with each other, providing key capabilities such as monitoring and control of processes, predictive analytics, and supply chain optimization. For example, in the manufacturing of an F-35 fighter jet, each component is equipped with a radio-frequency identification device (RFID) tag that gets scanned before it is put on the jet during production to ensure the highest level of quality control.

Provider edge. Bringing compute processing closer to the consumer so that extensive back and forth to datacenters such as Air Operations Center (AOC) and Distributed Common Ground System (DCGS) is limited or eliminated.

Engagement edge. Globally distributed compute systems that allow users to engage with applications. In a military operation, this can refer to soldiers in the field that need real-time data to make informed tactical decisions in the battlespace.



In the context of the warfighter, these definitions can help identify the edge requirements necessary for achieving mission objectives across the DoD.

Using a hybrid cloud approach and comprehensive solutions, Red Hat can not only jumpstart Day 1 modernization efforts, but also remain a partner with the DoD throughout the entire process to achieve mission capabilities. More specifically, Red Hat provides expertise and technology solutions to modernize decentralized decision making (DDM), increase operations resilience, extend interconnectedness, and improve data sharing.

Chapter 1

Decision dominance is the new weapon dominance

Mission success relies on decision-quality data to support the warfighter with trusted access to reliable and timely information. And, while data has been much of the focus across the defense landscape more recently, it is only part of the equation. Accelerating the transformation of data into actionable intelligence is a vital component to compete and win against near-peer adversaries. Decision dominance is supported by 3 foundational capabilities: data availability, distributed decision making, and interconnectedness.

As connected devices become more capable and reliance on them grows, adding complexity to the connected networks, decentralized decision making is the throughline to increase operations resilience, extend interconnectedness, and improve data sharing. But decentralized decision making is not without its challenges.

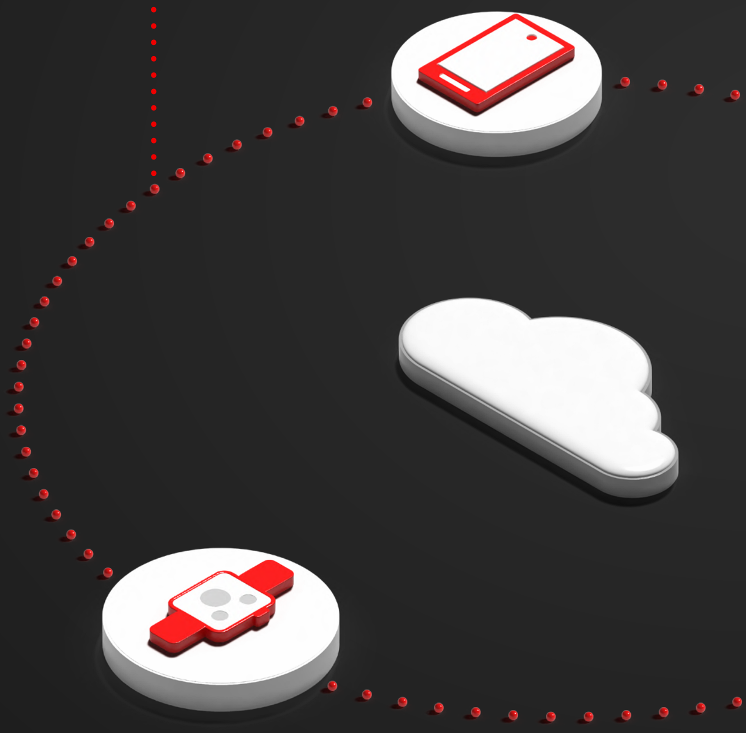
Key challenges of decentralized decision making:

- Edge systems are often difficult to access and have limited bandwidth.
- Shifting long-held perspectives toward adopting a software-first approach is not simple.
- Adhering to zero trust requirements because isolation is no longer a suitable security measure for protecting against outside and inside threats.
- Addressing these challenges, among others, involves implementing robust security hardening across the cyber terrain to ensure that every device and user on the network is continuously authenticated and verified, enhancing the DoD's overall cyber operational readiness.

Improve data availability, visibility, and impact

Multidomain operations (MDO) and technology initiatives such as Combined Joint All-Domain Command and Control (CJADC2) are methods already in use by the DoD to improve data availability and integration among and within service branch and coalition partner systems.

Building MDO capabilities on the foundation of an edge and hybrid cloud architecture offers the ability to effectively distribute and manage the high data volume workloads of a convergence event quickly, resiliently, and dynamically. An edge and hybrid cloud system infrastructure will be necessary to provide the elasticity and resilience needed to support the volume and velocity of data during a convergence event.



Key aspects to edge and hybrid cloud architecture

Open standards

Using open source standards maintains extensibility and interoperability between solutions and pushes collaboration and innovation.

Data management

Intelligence and insight relies on analysis and inference of data. The assets fielded and available vary from encounter to encounter, so the ability to manage and integrate systems must be flexible enough to adjust to the dynamic nature of available assets.

Tactical networks

MDO convergence opportunities rely on tactical networks such as sensors, the Internet of Military Things (IoMT), and 5G networks to facilitate the thousands of devices pushing and pulling data across the battlefield.

Artificial intelligence

AI is a vital advantage in achieving decision dominance, as machine-assisted decision making relieves a significant and growing burden on decision makers to classify, organize, and gain insight from the increasing torrent of data that the modern battlespace produces. Mission edge significantly reduces the burden of full software development life cycle management of AI and machine learning (ML) workloads.

Automation

Add and remove assets using automation to gain consistent repeatability to replicate adding and removing capacity and features to an area of service on demand and in a rapid fashion.

Decision dominance requirements

For Combined Joint Force C2 functions to achieve decision dominance in all-domain operations, implementation requires planning guidance, industry advancements, and modernized technologies that use and combine existing data and new data while adapting commercial solutions to military-specific requirements.

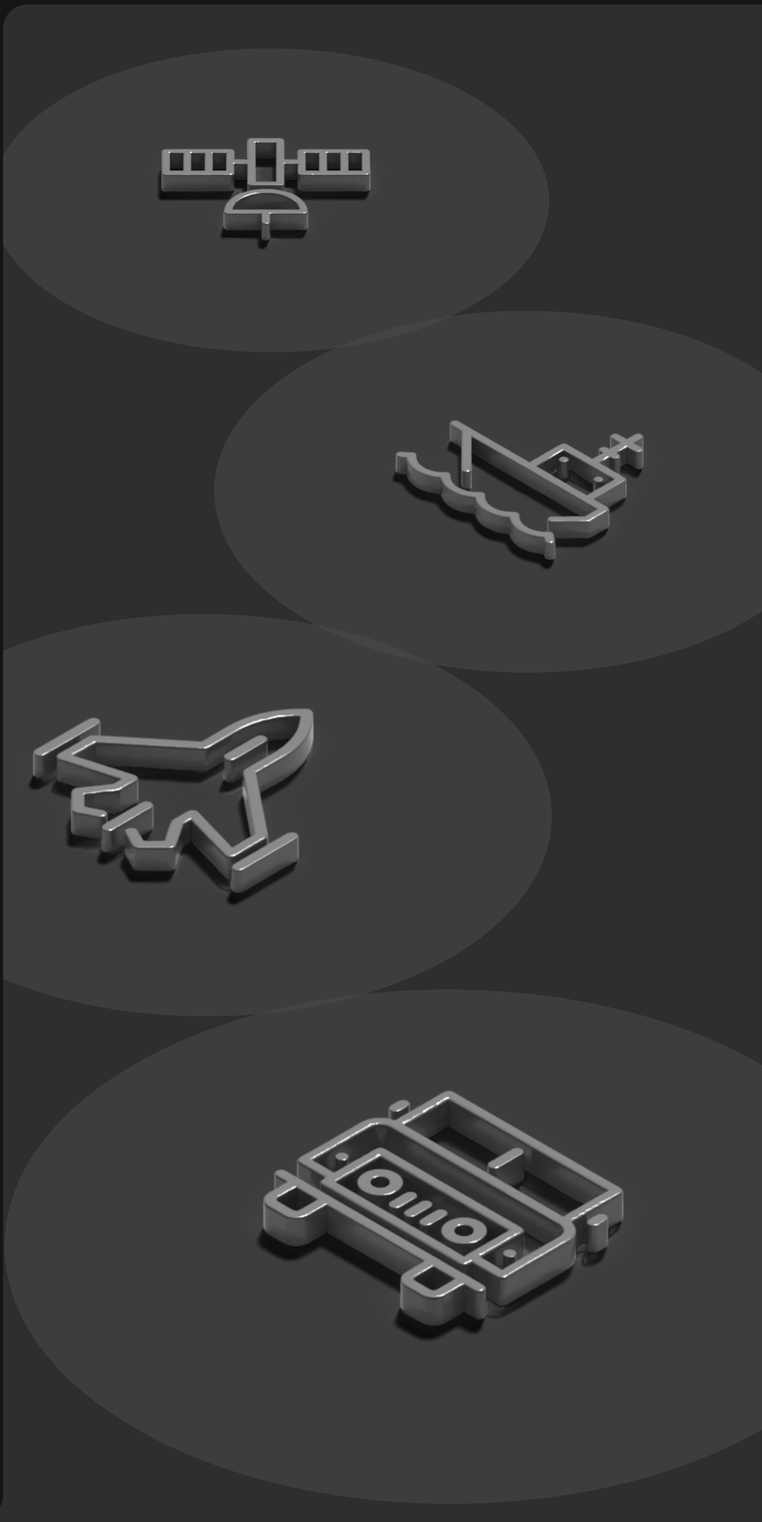
Agile integration

With the variety of data produced and consumed by MDO assets, agile integration allows data veracity and value to be brought to bear as intelligence through event-driven, micro service architectures to feed human and artificial intelligence (AI) decision making.

Chapter 2

A path to resilient operations

Multidomain operations aim to bring together various assets across land, air, maritime, space, and cyber domains simultaneously in a window of peak capability known as convergence to overwhelm an adversary's ability to respond. The characteristics of the heightened demand for data and workloads across multiple devices and assets can be described using the 5 Vs.



Volume

As more assets enter the battlefield, data volume increases as more producers and consumers of data are introduced.

Variety

These assets belong to the various domains and focus on different information, increasing the variety of data produced and consumed.

Velocity

As convergence is reached, the number of producers and consumers of data will peak, and the amount of data each asset will produce or consume will increase, increasing the velocity of the data flow.

Veracity

The veracity of the data will become more critical as convergence progresses. Data veracity is not just concerned with if the data is authentic, but also if it is timely and actionable.

Value

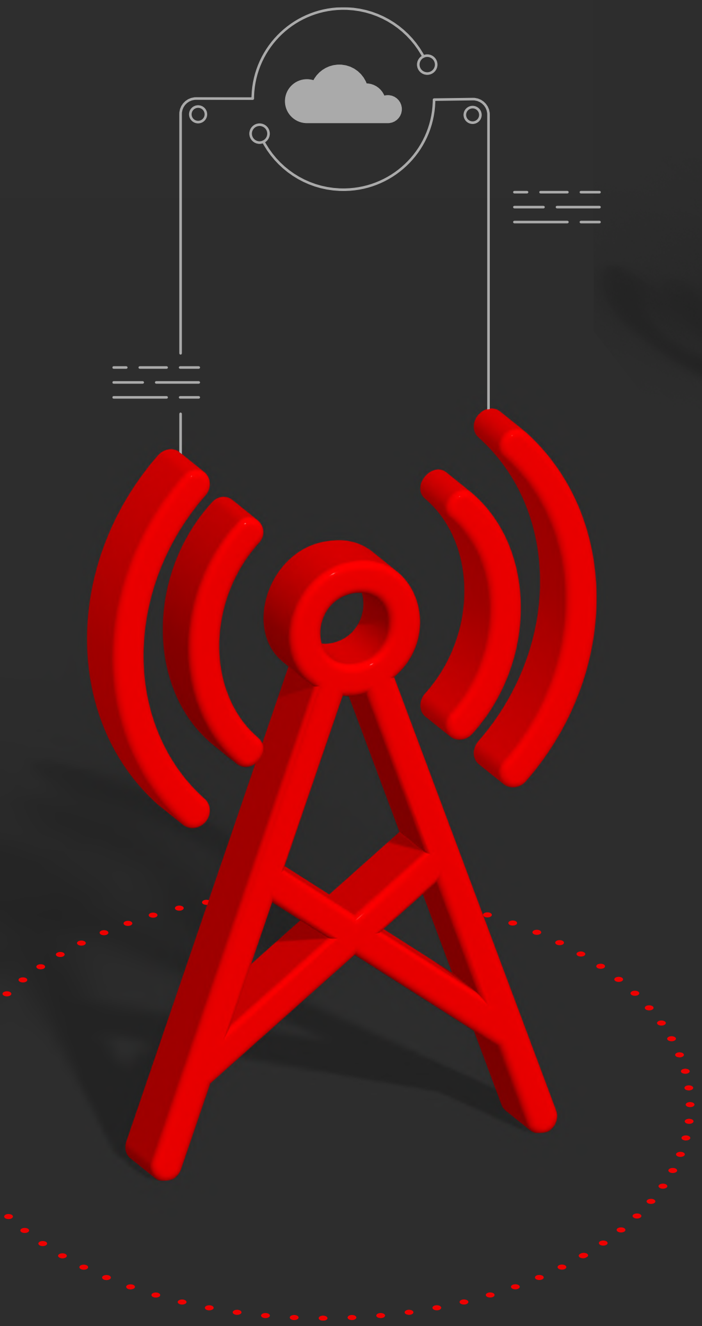
The value of data is affected by the veracity, volume, and velocity of the data at the point of decision making.

The MDO battlespace is dynamic. Each engagement is unique, with different assets being fielded from encounter to encounter. This means that the ability to manage and integrate systems must be flexible enough to adjust to the dynamic nature of available assets for each battle.

A convergence event within a theater might see thousands of assets producing and consuming data from in-vehicle sensor systems, satellite systems, and offensive and defensive cyber operations, among others. This rich sensor data can be a vital asset, giving combatant commanders the ability to sense, make sense, and act on that information. However, traditional field communication systems are not equipped to support the volume of data being transmitted to provide data-based mission selections.

MDO convergence demands will likely need to rely on fielding connected 5G spectrum communications to facilitate the thousands of devices pushing and pulling data across the battlefield.

By comparison, major sporting events that host tens of thousands of fans, such as the Super Bowl or World Cup, generate significant amounts of data in a concentrated area and time. Telecommunications companies prepare for these events ahead of time by bringing additional assets to manage increased traffic volume. They are able to scale on demand because they built an infrastructure on an extensible edge and hybrid cloud architecture. However, this architecture is only a single part of the equation. The ability to scale at the edge quickly and dynamically requires automation.



Automating at the mission edge

By using an automation-first approach, telecommunications companies can add and remove assets, with consistent repeatability and speed. Automation allows for simple and reproducible changes that increase flexibility and boost capacity. If manual intervention was needed for each of these instances, the capability could not scale fast enough, and the implementation of each intervention would be irregular and prone to errors.

By building MDO capabilities on an edge and hybrid cloud architecture, the DoD can gain the ability to distribute and manage the high data volume workloads of a convergence event efficiently, resiliently, and dynamically.

Enhance cyber readiness with automation

By integrating automation into cyber operational readiness strategies, the DoD can harden information systems, reduce attack surfaces, and strengthen defenses. Additionally, mission assurance can be underpinned with advanced capabilities of automation tools that can support continuous operational readiness and adaptability to new threats as they emerge. This helps to strengthen and maintain a robust security posture, which enhances decision making to support greater command and control.

Automation boosts cyber operational readiness by providing:

Improved efficiency in threat detection and response.
Automate real-time threat detection to responses and reduce the impact of attacks.

Consistency in secure operations.
Apply security protocols uniformly, minimizing human error and policy deviations.

Scalability of security operations.
Expand security capabilities efficiently as organizational needs grow.

Reduction in human error.
Decreases the likelihood of breaches caused by manual mistakes.

Improved compliance monitoring.
Systematically manage and document adherence to policies, cyber tasking orders, and readiness assessments.

Enhanced incident management.
Initiate swift incident response and gain detailed insights for quicker resolution.

Resource optimization.
Unburden skilled mission defense teams, cyber protection teams, and others to focus on strategic operational tasks and innovation.

Chapter 3

Interconnectedness is mission critical

The edge is not a singular place. It's a dynamic mesh of interconnected systems and devices that produce and consume data. The flow of that data is crucial for operational effectiveness. While it is essential to collect comprehensive information about the ever-changing conditions of a battlespace, the vast amount of data that needs to be processed and analyzed presents significant obstacles. This is especially true when military commanders face pressure to make critical decisions with urgency.

Addressing that challenge is the objective of CJADC2, which seeks to use ever-increasing, disparate data flows across all domains, uncover insight using automation and AI-enabled processes, and deliver the results to the warfighter at unprecedented speed. The overarching aim is to help the DoD sense, make sense, and act upon data to achieve advantage and decision dominance.

For example, space-based technologies provide important advantages in communication, reconnaissance, and navigation, which are essential for real-time global military operations. Whether referring to the deployment of satellites that inform secure communications, precise global positioning systems (GPS), or surveillance capabilities that can detect threats from great distances, interconnectedness is essential to mission assurance.

To achieve the speed, stability, and scale at the edge necessary for success requires:

An information advantage by accelerating informed decision making at the edge.
Transmitting data from the tactical edge up echelon for processing introduces too much lag. By the time actionable intelligence is sent back to the edge, decisions may be overcome by events. Information advantage requires decision making at the speed of action—at the edge.

Shortening the time to observe, orient, decide, and act.
Accelerating decision making allows warfighters to make better decisions faster, outpacing the adversary's ability to sense, make sense, and act. The idea is to move more quickly than the adversary, making better decisions faster. Warfighters can sense, make sense, and act faster with a Modular Open Systems Approach (MOSA) to edge computing and data science.

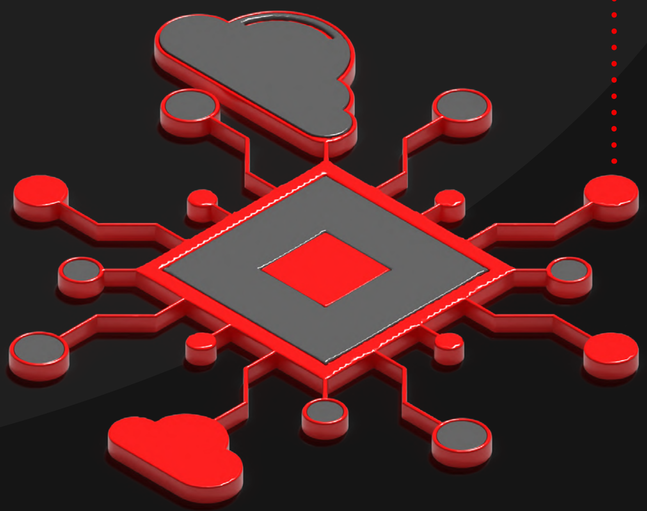
Uninterrupted data availability.
Many tactical computers are customized for a single purpose. If 1 of 2 computers on a tank is destroyed, for instance, the other cannot take over its functions. To maintain decision advantage, the joint forces need the ability to quickly recompose mission capabilities on any computer.

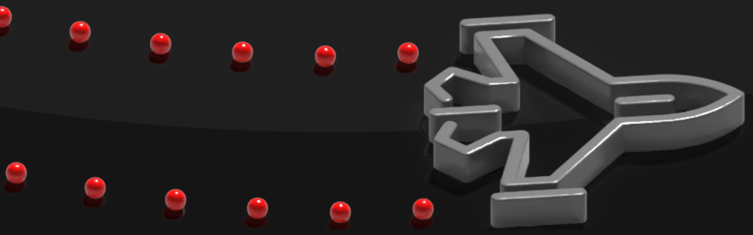
Sharing AI and ML capabilities across forces.
Today, each combat system and mission application program office develops bespoke software capabilities, leading to non-interoperable and duplicate applications. An interface for sharing capabilities like ML models and AI algorithms—without disclosing other intellectual property—will help the joint forces achieve decision advantage.

Extending innovation across domains using AI

AI and ML technologies are playing a transformative role in advancing unmanned vehicles and field tools, enhancing capabilities across all domains including air, land, maritime, and cyber.

Continued improvements at the hardware and software level have led to reduced size, weight, and power (SWAP), and a greater ability to do more while operating with agility at the edge. Future reliance on more unmanned and autonomous systems is becoming a pervasive edge technology consideration.





The potential for greater interconnectedness across the DoD may include:

Fleet management.
AI can optimize the deployment, maintenance, and routing of military fleets, including aircraft, naval vessels, and vehicle convoys, improving logistical efficiency and readiness.

Predictive maintenance.
Being able to predict equipment failures before they occur by analyzing data from sensors and usage logs will reduce downtime and extend the lifespan of military hardware.

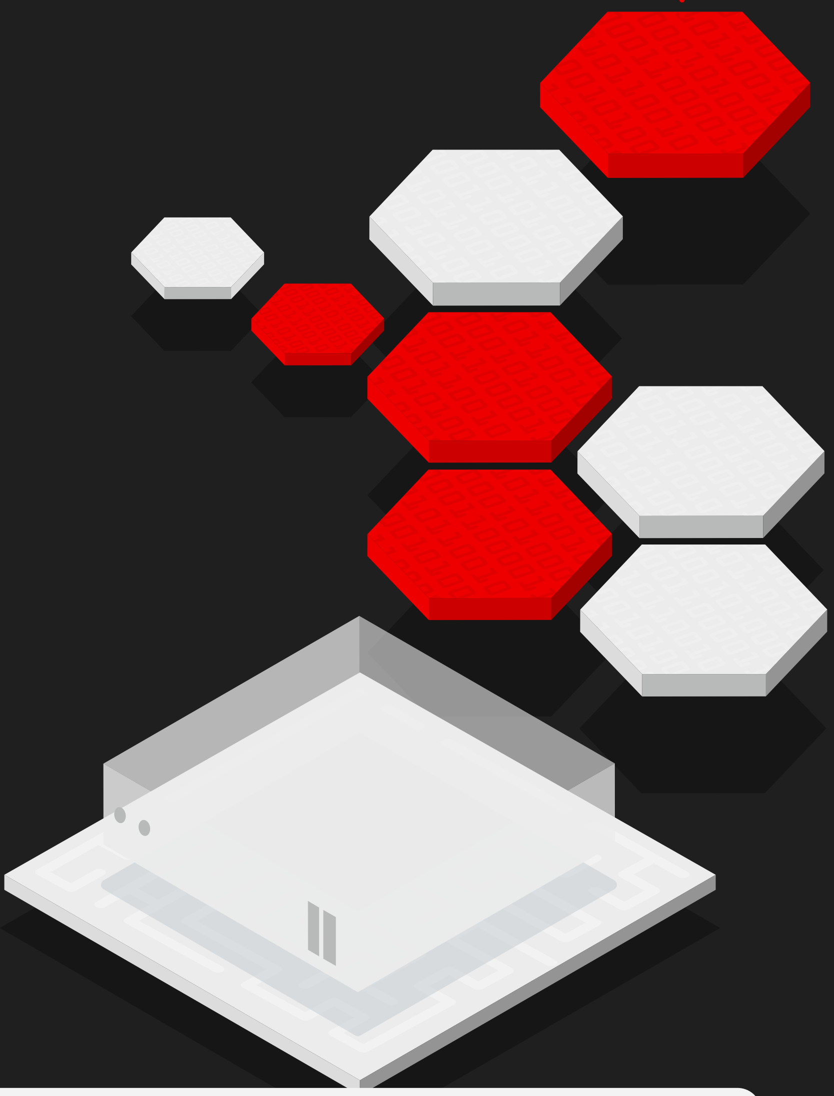
Surveillance and reconnaissance.
AI-enabled systems can autonomously monitor vast areas using unmanned vehicles such as drones and satellites, identifying changes and potential threats with greater accuracy and speed.

Cyber defense.
Using AI algorithms to monitor, detect, and respond to cyber threats in real time helps protect critical data and infrastructure from increasingly sophisticated attacks.

Training and simulation.
AI can create realistic training environments and simulations, helping soldiers prepare for a variety of scenarios without the risks associated with live training or training during deployment.

Chapter 4

Data sharing: From intelligence to insights



As data continues to shape the modern battlespace, it's important to note that more data is not an advantage itself. Data from sources such as HUMINT (human intelligence), AI, and ML must be processed and analyzed to create decision-quality information with actionable insights.

To provide the data flow and processing capabilities necessary to deliver the goals of a convergence scenario while maintaining the flexibility to adapt from 1 dynamic event to another, infrastructure operations, integrations and fusion, and data-in-motion processing must be built using open standards.

An open standards approach

Eliminating the barriers between digital infrastructure is essential for mission success. Critical data can too often get trapped in disconnected or isolated departments and agencies. Open standards ensure accessibility and interoperability between solutions to provide the characteristics necessary for actionable intelligence.

Eliminating barriers between digital infrastructures drives convergence

Collaboration
Battle lab with a multitenant, consistent, and standardized infrastructure.

Speed
Frictionless access to all-domain data, rapid prototyping, experimentation, and iteration.

Agility
Build recomposable capabilities and deploy anywhere with all-domain data integration and DevSecOps.

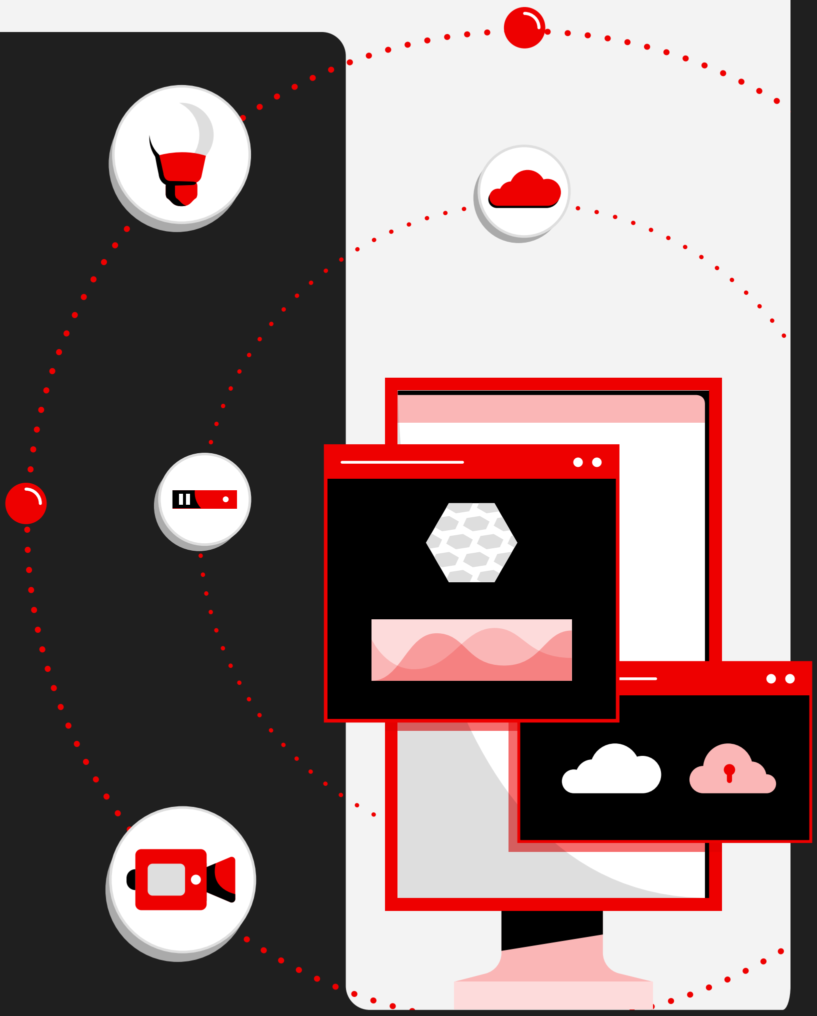
Flexibility
Open standards for data and infrastructure across lab and operational landscapes.

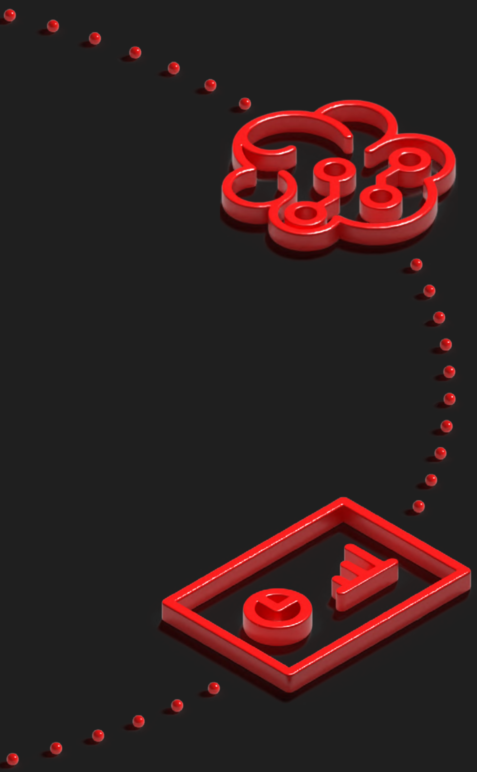
Figure 1. Characteristics necessary for actionable intelligence.

Build on a software-defined foundation

A software-defined network (SDN) architecture provides the backbone for a security-focused and converged joint all-domain digital infrastructure solution. Red Hat provides this foundation which includes data collection, integration, analysis, and syndication. The goal is to provide the warfighters and commanders with a single collaborative environment to access geospatial data combined with the latest analytic models and tools.

This foundation encompasses the key tenants for mission priorities of security, latency, and speed across all topologies, end-to-end. It's an approach that provides a rich transport, communication, and integration layer for mission success. The collaborative environment and analytic tools help the warfighter interact with data at any echelon, in a common relevant operational picture (CROP).





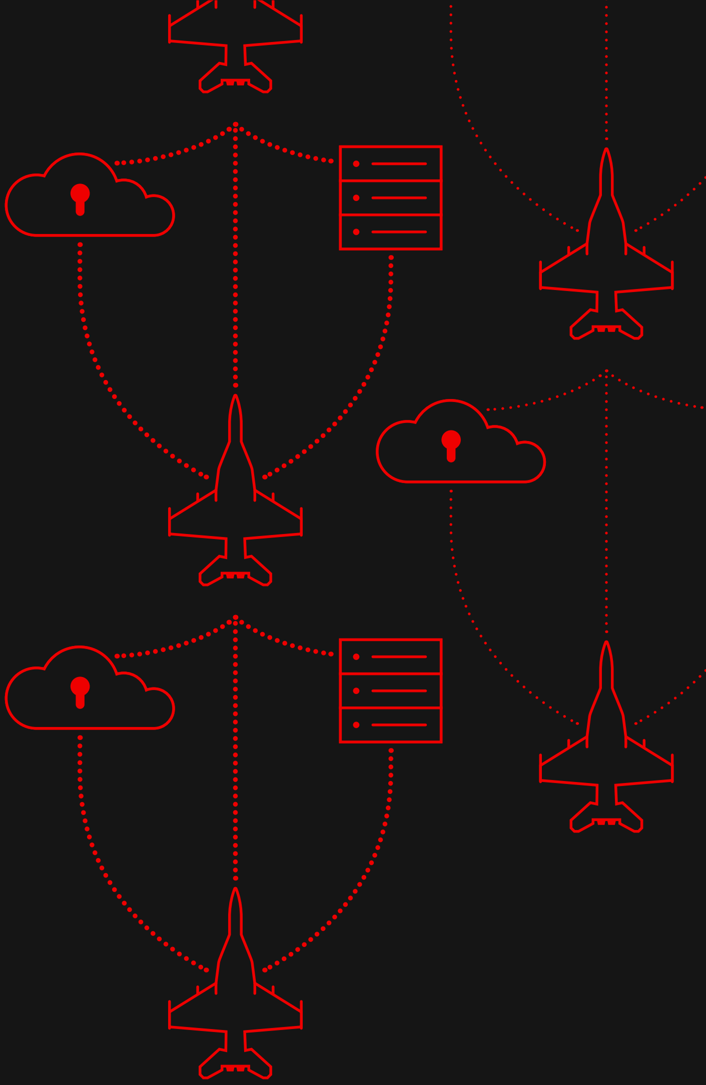
The importance of management

AI/ML are strategic tools, but today's AI/ML systems are far more dynamic and must be regularly updated, modified, and adjusted to maximize the accuracy and value of the insights they deliver. AI and ML tooling should be focused on portability, data management, and configurable deployments. Red Hat's portfolio provides the flexibility to deploy models with a focus on security to quickly build, scale, reproduce, and share AI/ML results consistently with a joint community of interest (COI).

A key differentiator of Red Hat® technology is flexible messaging architectures to achieve near-real-time situational awareness. A robust messaging infrastructure will allow a rich and performant data exchange among all nodes in the CJADC2 domains, creating the capability to process enormous volumes of data at speed. This helps teams bridge data between disparate systems with the ability to transform and enrich data at the edge of the network.

Chapter 5

Red Hat's approach to mission edge



Edge computing is a natural extension of Red Hat's open hybrid cloud strategy, which is to support any workload on any environment in any location. But no single vendor can provide it all–not even Red Hat.

Our approach to mission edge includes solutions and expertise supported by a vast hardware and software partner ecosystem to help achieve mission objectives. We provide an extensive catalog of certified hardware, software, and cloud partners that can help modernize widespread resources across the DoD while maintaining agility, a focus on security posture objectives, and standardizing interoperability across all branches and agencies.

With a modern, container-based application platform, the joint force can build applications once, deploy them at any edge location (e.g., forward operating base, vehicle, semiautonomous weapon system, etcetera.), and migrate workloads to other hardware when needed.

What does a container-based application platform provide?

Cost containment

Containers support the MDO and CJADC2 objectives to create an integrated warfighting capability by integrating existing systems. Hardware doesn't need to be ripped and replaced. Legacy applications don't need to be rewritten because they can be deployed and managed on the same platform as modern, microservices-based applications.

Mission agility

When AI and ML applications are built from microservices, DoD developers can adapt quickly to change by disintegrating and then recomposing microservices—for example, to ingest data from a new type of sensor.

Data interoperability

Using integration technologies, the DoD can push newly acquired information to other systems at the speed of action, without relying on manual entry. This helps the joint forces to quickly disseminate information up echelon—from deployed units to combatant commanders, all the way to the Pentagon—allowing a fused common operational picture (COP).

Mission resiliency and survivability

All computers on an edge asset such as a ship or tank form a MicroCloud. If 1 computer fails, the team can quickly recompose the mission capability on another.

Why Red Hat for mission edge?

Adopting edge computing for all-domain decision advantage requires the right technology along with the right techniques, tactics, and procedures (TTPs).

Build once, deploy anywhere

Red Hat OpenShift® Container Platform helps DoD forces build applications once and deploy them anywhere, for any echelon. Red Hat OpenShift focuses on security at every level of the container stack. Use Red Hat Integration technologies to adapt to inevitable changes in data formats and protocols, bringing together data from past, present, and future systems.

Automate for efficiency

Operational effectiveness at the edge also requires robust, scalable automation that allows rapid, consistent deployment and management of critical infrastructure and applications. Red Hat Ansible® Automation Platform can help the DoD automate routine tasks and configurations to reduce the need for manual intervention to minimize errors and downtime in remote and austere environments.

Ansible Automation Platform also enforces security policies and compliance requirements automatically, supporting a strong secure posture for edge devices and operations in diverse conditions.

Addressing challenges at the edge

Efficiency at the edge requires lightweight, flexible solutions tailored for edge computing environments. Red Hat Device Edge supports the deployment and management of containerized applications and services on edge devices, ensuring consistent and efficient operations even in remote and resource-constrained locations.

Red Hat Device Edge can help the DoD achieve real-time data processing and analytics at the edge, reducing latency and enhancing decision-making capabilities. The platform's robust security features boost the security focus for edge deployments to protect against cyber threats, while integrating with existing IT infrastructure to allow for streamlined updates and scalability. This empowers the DoD to maintain mission-critical operations with high reliability and agility, even in challenging and dynamic environments.

Red Hat is also uniquely positioned to guide DoD teams through this digital transformation as they adopt a hybrid cloud platform and new DevSecOps processes. We understand that cyber operational readiness is critical for national security. We provide the necessary technology expertise to support the DoD in protecting its networks, systems, and data from malicious cyber activities, and support overall military readiness and operational capabilities.

> Our open source roots bring together ideas from a community that's as complex and diverse as the DoD. Then we distill the best ideas from upstream communities into focused solutions to help our customers achieve their mission objectives.

See how Red Hat helps the U.S. Department of Defense [move faster, with less risk.]

Find out how to achieve and accelerate operational effectiveness. [Contact a Red Hat Department of Defense expert.]

About Red Hat
Red Hat is the world's leading provider of enterprise open source software solutions, using a community-powered approach to deliver reliable and high-performing Linux, hybrid cloud, container, and Kubernetes technologies. Red Hat helps customers integrate new and existing IT applications, develop cloud-native applications, standardize on our industry-leading operating system, and automate, secure, and manage complex environments. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500. As a strategic partner to cloud providers, system integrators, application vendors, customers, and open source communities, Red Hat can help organizations prepare for the digital future.