Strengthen defense with a unified platform

Core benefits:

- No resilience gap from the strategic core to the tactical edge
- Consistent platform for mission-critical applications in disconnected environments
- Unified approach to autonomy and security

Closing the resilience gap from the strategic core to the tactical edge

Government defense organizations face a pivotal challenge: maintaining reliable operations across their entire spectrum, from the strategic core to the tactical edge. By the critical need for agility, robust security, and strategic autonomy, the defense sector is rapidly evolving. It is moving beyond traditional, centralized datacenters to highly distributed, mission-ready architectures. Profound transformation is essential for achieving decision dominance-the ability for all commanders to sense, understand, decide, and act swifter than any adversary across all domains.

The imperative for end-to-end operational resilience

Modern missions operate across a sprawling hybrid cloud continuum, encompassing private air-gapped clouds, deployed mini-datacenters, and ruggedized tactical devices such as drones and soldier-worn systems. The architecture is fundamental to executing multi-domain operations (MDO), which demands complex integration and coordination of assets across air, land, sea, space, cyber, and electromagnetic spectrum domains.

However, domain expansion also creates critical vulnerabilities and significantly magnifies technical complexity. Isolated technologies and disparate environments can fracture operational continuity, while cybersecurity threats multiply across a vast attack surface. A reliance on constant connectivity is a critical failure point. In contested environments, edge devices must function autonomously, synchronizing data only when trustworthy, intermittent links are available. The core challenge is achieving true resilience across the entire spectrum. Sovereignty in a central datacenter is not enough if the tactical edge cannot operate independently.

Key challenges in defense digital transformation

While the hybrid infrastructure offers undeniable flexibility, defense organizations encounter several critical hurdles in their digital transformation journey:

- **Cyber attacks:** Defense organizations are most concerned about the growing threat of sophisticated supply chain and cyber attacks. For instance, malicious code injected into open source libraries can compromise entire fleets of drones or vehicles. Similarly, man-in-the-middle (MitM) attacks can alter firmware updates in transit to tactical devices, potentially sabotaging critical missions.
- **Isolated technology structures:** Different environments–core, cloud, and edge–often use incompatible technology stacks. This incompatibility forces organizations to rebuild solutions for each deployment, leading to fragmentation. Consequently, soldiers and engineers must learn multiple platforms, from Amazon Web Service (AWS) and Microsoft Azure to specialized tactical operating systems, significantly slowing mission readiness.
- **Complexity:** Relying on manual processes inherently creates more complexity. For example, moving data between the core to edge location and back again requires custom workflows, which increases deployment times. At the same time, traditional security models struggle to adapt to distributed architectures, leaving critical gaps that adversaries can exploit.

Taking a unified approach

Defense organizations urgently need a unified, open framework that strengthens autonomy and security everywhere. The goal is a consistent platform for running critical applications in a private cloud, processing AI workloads at the edge, and providing real-time decisions on an edge device in the field. True modern resilience is the ability to function with unwavering integrity from the core to the front line.

How Red Hat helps

Facing a fragmented digital battlespace, defense organizations require a unified foundation and trusted advisor to ensure resilience from the strategic core to the tactical edge. Red Hat provides this essential, consistent platform. With a "deploy once, run anywhere" practice, Red Hat accelerates mission readiness, allowing personnel to use familiar tools across environments. In addition to the consistent experience, Red Hat solutions are built on open standards, and the platform prevents vendor dependence, allowing better integrations with a scalable and flexible solution.

Military-grade security: Red Hat embeds military-grade security by ensuring its core platforms, such as Red Hat® OpenShift®, adhere to rigorous compliance standards. Security is continuously enforced through Red Hat Trusted Software Supply Chain, providing a holistic and continued approach to security. This approach integrates DevSecOps practices to strengthen the chain-of-custody and verify that software meets agency standards for security, compliance, privacy, and transparency.

Assurance sovereignty: Cryptographic attestation verifies firmware and critical updates are untouched, supporting a broader goal of assurance sovereignty. This process verifies the integrity and reliability of digital systems, and is a core part of Red Hat's platform strategy to validate the software supply chain and mitigate the risk of malicious code injection.

Disconnected automation: Disconnected automation allows patching of field devices, integrating with any specific process the customer already has, without requiring any internet connection. Red Hat helps deliver dependable autonomous operations needed for a modern defense using Red Hat Ansible® Automation Platform. The platform helps manage devices in Denied, Disrupted, Intermittent, and Limited (DDIL) conditions without reliance on vulnerable external connectivity. This autonomy protects the massive, long-term investment in deployed software assets, minimizes security risks associated with malicious code injection, and guarantees continuous mission-critical operation when external support is impossible.

In the strategic core, reliable solutions like Red Hat OpenShift deliver scalable, sovereign infrastructure. At the deployed edge, compact OpenShift clusters process critical intelligence and AI workloads. On the tactical front line, the lightweight Red Hat Device Edge provides ultra-portable, disconnected operations on ruggedized systems.

Proven defense industry use cases

Several defense organizations have successfully implemented Red Hat solutions to overcome critical operational challenges and achieve significant advancements:

Optimized field operations for a European air force: A European air force confronted persistent mission disruptions caused by network outages in field operations. By implementing Red Hat OpenShift on portable edge datacenters, the air force IT department adopted local AI

processing capabilities that maintained continuous operations regardless of connectivity status, while significantly reducing bandwidth requirements.

In-flight software updates for unmanned aerial systems: In another demonstration of leading capabilities, a major defense contractor showcased the ability to perform in-flight software updates on unmanned aerial systems. Using Red Hat Device Edge, the contracting firm successfully deployed AI model upgrades to drones during active missions, enhancing real-time target recognition capabilities without requiring mission interruption or system downtime.

Accelerated infrastructure and deployment for a national defense organization: A national defense organization achieved remarkable efficiency gains by automating its Platform-as-a-Service (PaaS) processes with Ansible Automation Platform and Red Hat OpenShift. The organization's infrastructure deployment times were reduced from several weeks to just 24 hours, making them ready for combat operations. Simultaneously, its developer capacity expanded nearly 4 times within a single year, while maintaining strict security protocols.

To get started

Contact a Red Hatter to learn how to protect your defense operations from core to edge.

About Red Hat

Red Hat helps customers standardize across environments, develop cloud-native applications, and integrate, automate, secure, and manage complex environments with award-winning support, training, and consulting services.

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

North America
1 888 REDHAT1
www.redhat.com

Europe, Middle East, and Africa
00800 7334 2835
europe@redhat.com

Asia Pacific
+65 6490 4200
apac@redhat.com

Latin America
+54 11 4329 7300
info-latam@redhat.com

redhat.com
#3134353_1225