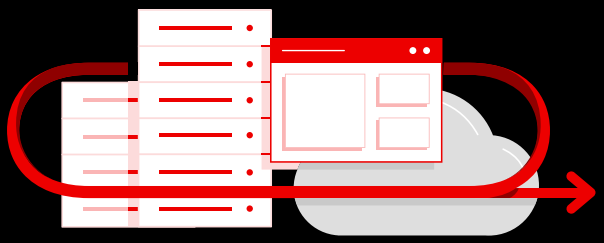
Red Hat | carahsoft

Mission-Ready Infrastructure

A Practical Path to IT Modernization with Red Hat OpenShift



Featuring:

William Ratican,
Solutions Architect,
Epoch Concepts

Matt Webster,
Chief Technology
Officer, Epoch Concepts

David Curry,
Director of Business Systems
& Data Modernization,
Epoch Concepts

Nicholas Gallo,
Senior Specialist, Solutions
Architect, Red Hat

Samuel Warren,
Associate Principal Solutions
Architect, Red Hat

For large, complex organizations like the United States Space Force, modernization is not a simple platform swap. It is a system-level transformation requiring planning, training and disciplined execution.

Mission requirements and burgeoning threats necessitate stronger security across the Federal government and especially within the military. A major step toward meeting this moment is transitioning programs to containerized, Zero Trust architectures. This is a journey that moves through four critical phases.

Phase 1: Legacy Virtualization

Traditional environments run virtual machines (VMs) with perimeter-based security models, where trust is assumed once inside the network. Systems are treated as unique, requiring manual intervention and limiting scalability. While historically effective, this provides little protection if an adversary gains access.

At this stage, agencies must conduct deep infrastructure assessments of their workload, storage and networking. Not every system will be compatible across platforms. Determine what can be retained versus what should be retired. The goal is greater than technological change. It is an operational change.

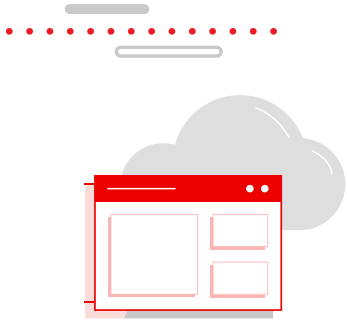
Phase 2: Transition to Containerization

VMs are migrated to platforms like OpenShift, enabling standardization, automation and API-driven infrastructure without full container adoption.

This phase is foundational. It introduces infrastructure-as-code, improved manageability and sets conditions for containerization. Even without full modernization, organizations gain resilience and operational consistency.

Migration tools can move VMs while validating workloads as infrastructure shifts from manual operations to automation. It is important not to rush this process. Allocate 12 to 18 months for the transition.

"If you've ever moved houses, you know it takes longer than expected and there's a lot more to do than you'd think. The same concept applies with migration."
– Nicholas Gallo, Senior Specialist, Solutions Architect, Red Hat



Mission-Ready Infrastructure
A Practical Path to IT Modernization with Red Hat OpenShift

Watch the Full Webinar

Phase 3: Containerization

Applications are deployed in containers, enabling portability, scalability and improved isolation. This action shifts mindsets from managing individual systems to managing services within a system.

Containerization provides insight into system performance and bottlenecks. Observability tools can help monitor performance and dependencies as processes adapt. At this stage, workloads are designed to be dynamic and replaceable and role-based access controls can be implemented.

Phase 4: Micro-Segmentation (Zero Trust)

Micro-segmentation enforces security at the workload level, limiting lateral movement and reducing the impact of breaches. This works in conjunction with a Zero Trust architecture, where every user and connection is continuously authenticated and authorized.

This model is critical for Space Force operations, especially in DDIL (denied, degraded, intermittent, limited) environments. It begins with asset identification, defining what data is critical and implementing least-privileged access controls. Skipping phases 2 and 3 leads to architectures that are hard to manage and hard to secure.

"Zero Trust doesn't make things harder or easier, it makes things explicit. Attribution is the same."
- Matt Webster, Chief Technology Officer, Epoch Concepts

Key Takeaways

Modernization is a phased journey, not a one-time migration. Skipping steps creates risks that can compromise your systems and sensitive data. While the tools and processes are important, success also depends on people:

- Invest in **training and in-house expertise**
- Allow adequate **time for planning and execution**
- Bring in **partners who have done this before**

Modernization takes time, but even partial progress delivers immediate value. Ultimately, A mission-ready, resilient infrastructure requires disciplined execution, realistic planning and an understanding that Zero Trust is an ongoing process, not an end state.

For more guidance on moving from legacy virtualization to a Zero Trust architecture, explore Epoch Concept's Advanced Zero Trust Enterprise Capability (AZTEC) methodology.

Contact Us:

Red Hat Solutions for Government

Toll-Free: (877)-RHAT-GOV
Main: (703)-871-8570
Fax: (703)-871-8505
Email: RedHat@carahsoft.com
www.carahsoft.com/red-hat