Radical Resilience on the Tactical Edge

Extend data security, recovery, and mobility for JADC2 success

The modernization of mission-critical data management technology and practices to meet JADC2 goals requires the integration of on-premises, virtual, and cloud-native workloads kept in highly distributed assets on the ground, at sea, and in air and space domains.

Integration is critical to providing superior real-time command, control, communication, computer, cyber, intelligence, surveillance, and reconnaissance (C5ISR). This includes threat responses in complex remote and contested operating environments. JADC2 requires assurance that actionable data is available across all domains and is instantly secure, immutable, recoverable, and portable 100% of the time.

Cloud and edge computing, DevSecOps automation, AI, and machine learning enable easier data fusion and management. This allows for better real-time situational awareness, collaboration, communication, and decision-making across U.S. and allied operational domains. Unfortunately, these technologies can be challenging to deploy.

Mission-Critical Assets

- Forward-operating or tactical edge data centers
- Airborne data centers
- Remote radar and sensor sites
- Cyber operations data centers
- Satellite ground stations
- Offline edge devices

Overcoming Cloud Native Deployment Challenges

Kubernetes, akin to virtual machines (VMs) for hardware, is becoming the middleware of the future. It is central to Infrastructure-as-Code and DevSecOps modernization and is fundamental to overcoming the cloud-native deployment challenges faced by the U.S. federal government and Department of Defense (DoD). Wherever Kubernetes and containers may be located across the tactical edge, they all must be fully and quickly recoverable in lethal risk and crisis environments to ensure mission continuity.

Kasten K10 delivers radical resilience on the tactical edge, whether teams are on the move or at pause (COTM/COTP) with military-grade encryption (FIPS 140-2/3). Bounce back with disaster recovery (DR) for any type of outage — including ransomware — and achieve application mobility even among the harshest of environments. Kasten K10 also aids application modernization via agile development processes that ensure all Kubernetes-based applications meet the most stringent security and availability standards required for U.S. governmental operations.

Some of the current challenges Kasten K10 can help your team overcome to meet JADC2 goals include:

- Application mobility and a seamless transition to new infrastructures
- Robust orchestrated backup, restoration, and DR capabilities
- Consolidation of Kubernetes environments to modernize and optimize costs

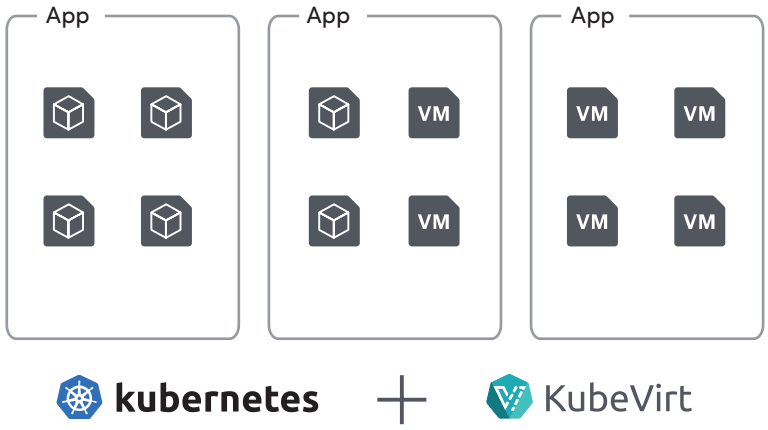
- Scalability that's in alignment with organizational growth and technical prowess
- Enhanced data protection that can withstand failures
- Simplified and automated container deployment and management

Why Kasten K10?

Edge deployments on unconnected devices have become vital to real-time tactical operations. This means they require robust and versatile data backup and recovery systems that can support a variety of mission-critical contexts.

It's more than just a safety net: It's an imperative for maintaining military readiness in a rapidly evolving digital battlefield. Veeam specializes in backup and DR for a variety of workloads, and is primed to meet the unique requirements of the U.S. government and defense industry with:

- A light and modular Kubernetes design
- Superior handling for all containerized applications
- Native support for both physical and virtualized hardware infrastructures
- Streamlined DevSecOps implementation
- Auto-scaling and resource-efficient operations
- KubeVirt for seamless VM integration into Kubernetes environments
- FIPS validation
- Dedicated U.S. support



Ask your Veeam representative for help in solving your backup and recovery challenges! This is why Kasten K10 has been rated #1 for Kubernetes Data Protection by analyst firm GigaOm for four years in a row.

About Veeam

Veeam®, the #1 global market leader in data protection and ransomware recovery, is on a mission to empower every organization to not just bounce back from a data outage or loss but bounce forward. With Veeam, organizations achieve radical resilience through data security, data recovery, and data freedom for their hybrid cloud. The Veeam Data Platform delivers a single solution for cloud, virtual, physical, SaaS, and Kubernetes environments that gives IT and security leaders peace of mind that their apps and data are protected and always available. Headquartered in Seattle, Washington, with offices in more than 30 countries, Veeam protects over 450,000 customers worldwide, including 73% of the Global 2000, who trust Veeam to keep their businesses running. Radical Resilience starts with Veeam. Learn more at www.veeam.com or follow Veeam on LinkedIn @veeam-software and X @veeam.