White Paper

Modernizing Virtual Desktop Infrastructure for Government and Defense Missions

RGS
Rancher Government Solutions

Kasm
TECHNOLOGIES

Table of Contents

Executive Summary

Legacy virtual desktop infrastructure (VDI) is holding government and defense agencies back by draining budgets, widening security gaps, and choking operational agility. Hypervisor-based solutions were built for yesterday's IT environment, not today's complex missions. To decisively meet modern demands, government agencies and military operations need a cloud-native workspace platform engineered with zero-trust security and powered by DevSecOps innovation and simplicity.

Kasm Technologies and Rancher Government Solutions (RGS) have partnered to provide a cloud-native, Kubernetes-powered workspace solution that integrates Kasm Workspaces with the RGS stack, including Harvester Government, a hyperconverged infrastructure (HCI) solution. This "Better Together" partnership provides government agencies with secure, scalable, and cost-effective virtual workspaces that operate seamlessly across on-premises, hybrid, and cloud environments.

Key Benefits

- **No Vendor Lock-In:** Move away from proprietary hypervisors like VMware and Nutanix.
- **Scale Anywhere:** Deploy across on-premises, hybrid, and multi-cloud environments (AWS, Azure, GCP, OCI).
- **Ironclad Security:** Built on zero-trust architecture, workload isolation, and classified network support.
- **Reduce Costs:** Lower total cost of ownership (TCO) by greatly reducing hypervisor licensing fees, improving efficiency on more hardware solutions, and leveraging repurposed hardware.

The Shortcomings of Traditional Virtual Desktop Infrastructure

Federal agencies are experiencing major shifts in technology priorities, driven by strict zero-trust mandates, growing concerns about vendor lock-in, and increasingly rigorous operational requirements. Traditional VDI solutions, such as VMware Horizon and Citrix, were initially designed for static data center deployments, making them unsuitable for today's highly mobile, cloud-native, and multi-cloud environments. In addition, recent budget cuts, reducing costs and overall TCO is a major driver for the DOD and civilian agencies to move towards a hyperconverged infrastructure solution for VDI workloads.

Infrastructure Limitations

These legacy solutions impose rigid infrastructure requirements and demand specific hardware configurations that limit deployment flexibility while raising costs of vendor-locked licensing and support. The heavy compute overhead per user reduces scalability, and inadequate GPU passthrough support severely restricts the use of advanced workloads like artificial intelligence (AI) and data visualization. As user profiles grow, storage costs balloon and create further inefficiencies. The inherent complexity of legacy network architectures also hampers remote access, an important requirement for modern operations.

Operations Limitations

Operationally, traditional VDI introduces unnecessary friction and is often very difficult to install and maintain. Installation and ongoing maintenance of VDI agents consume IT resources and expand the potential attack surface. Hot-desking becomes cumbersome as it requires administrative intervention for session reconfiguration. Classified network deployments face additional hurdles due to complex air-gapped setups and cross-domain networking rules. Manual patching across thousands of endpoints becomes a daunting, resource-intensive task. Managing user profiles at scale demands continuous synchronization and extensive storage, adding to the overall operational strain.

Security Vulnerabilities

Relying heavily on endpoint agents expands the potential attack surface. Hypervisor vulnerabilities pose systemic risks, allowing for a single exploit to jeopardize entire host systems. Techniques such as memory deduplication open the door to side-channel attacks, and shared hardware infrastructure elevates the risk of cross-VM exploits. These traditional solutions operate under the flawed assumption of trusted internal networks, an approach incompatible with today's zero-trust standards and threat landscape.

Given the demand for tactical operations, hybrid cloud strategies, and edge computing, organizations clinging to outdated VDI technology risk losing critical capabilities. Federal IT leaders, already burdened by vendor lock-in, rising operational costs, and the inherent limitations of hypervisor-based virtual desktops, urgently require a modern, cloud-native alternative that supports flexibility and ironclad security.

A Cloud-Native Alternative

Modern workspace delivery requires a fundamentally different approach, especially for government and military use-cases. With traditional VDI solutions that can compromise national security, relying on legacy technology is not an option.

Unlike these legacy hypervisors, a cloud-native, Kubernetes-based approach provides:

Web-Native Access

Browser-based workspaces eliminate endpoint dependencies while maintaining security. Hardware-level controls prevent unauthorized access through physical manipulation or remote exploits.

Resilient, Self-Healing Infrastructure

Government and military operations demand continuous availability. Container-native architectures provide inherent redundancy and rapid recovery capabilities.

Automated Scalability

Traditional VDI becomes unwieldy as deployments grow. Container orchestration powered by Kubernetes provides consistent, scalable operations across diverse environments.

Compliance Integration

Container-native platforms streamline regulatory compliance through built-in controls covering all system aspects, from hardware to application delivery.

A 'Better Together' Approach: Rancher Government Solutions + Kasm Technologies

The partnership between Rancher Government Solutions (RGS) and Kasm Technologies gives government agencies and defense operations the cloud-native alternative needed for continuous availability. The combination of Kasm Workspaces and the Rancher stack provides a powerful alternative to traditional VDI, giving agencies a secure, scalable, and cost-effective workspace solution.

No Proprietary Hardware Requirements

Supports x86, arm64, and repurposed hardware

Zero-Trust Security Model

Enforces strict workload isolation and granular access controls

Flexible Deployment Options

Operates in air-gapped, on-prem, and multi-cloud environments

Hyperconverged Simplicity with Harvester Government

RGS's Harvester Government provides a purpose-built hyperconverged infrastructure (HCI) solution that integrates computing, storage, and networking on a single platform to simplify deployment and management while reducing costs.

Unlike traditional hypervisors constrained by proprietary hardware dependencies, Harvester Government embraces an open approach. It fully supports both modern and legacy hardware architectures, including x86 and arm64, giving agencies flexibility to maximize existing hardware investments. This hardware-agnostic design maximizes cost efficiency, extends hardware lifecycles, and supports agencies as they adapt infrastructure to changing mission requirements.

From a security perspective, Harvester Government adopts a defense-grade approach rooted in zero-trust principles. It enforces strict workload isolation and granular, role-based access controls (RBAC) at every infrastructure layer to prevent lateral movement of threats and unauthorized data access. This level of security management maintains operational continuity and safeguards classified data to ensure compliance with federal security standards and mandates.

Harvester Government is designed to operate reliably in diverse deployment environments, including air-gapped networks, on-premises data centers, Edge, and hybrid or multi-cloud deployments. This flexibility supports operations across varied and austere environments without sacrificing performance or security.

Web-Native VDI with Kasm Workspaces

Kasm Workspaces eliminates reliance on endpoint-installed VDI agents or software clients Users securely access their personalized virtual desktops directly through a web browser, simplifying IT management while enhancing security. This browser-native approach simplifies endpoint deployment, reduces administrative overhead, and allows instant, secure access from virtually any device.

Using its cloud-native, container-based architecture, Kasm Workspaces supports scalability and adaptability in even the most secure operational environments, including air-gapped and classified networks. Agencies can instantly provision virtual desktop environments specific to their operational requirements, whether to support routine remote work or tactical field deployments under challenging conditions.

Building on the flexible hardware foundations provided by Harvester Government, Kasm Workspaces delivers specialized support for data science and AI workloads. The platform offers pre-built deep learning environments with popular frameworks and tools, such as Jupyter Notebooks, TensorFlow, and PyTorch. Integrated GPU resource scheduling and monitoring features allocate compute power for deep learning workloads.

For data science teams requiring reproducibility and version control, Kasm Workspaces provides structured, version-controlled Python environments to support precise replication and auditing of research and experiments. The platform also supports distributed AI model training so agencies can use multiple resources and scale AI workloads more efficiently. Integration with widely adopted developer tools like VS Code, enriched with specialized AI extensions, further improves collaboration, productivity, and developer experience across distributed teams.

- **No Endpoint Software Required:** Users access workspaces through a browser
- **Configurable Desktop Environments:** Supports persistent or non-persistent sessions
- **AI/ML Developer Workspaces:** Pre-configured for GPU-based workloads and data science applications

Multi-Cluster Kubernetes Management

Centralized administration across hybrid environments

Incremental VMware Migration

Supports phased transitions from VMware infrastructure

Automated Infrastructure as Code (IaC)

Reduces manual provisioning and configuration time

Unified Management with Rancher MCM

RGS offers seamless management of Kubernetes clusters through Rancher Multi-Cluster Manager (MCM). IT administrators can manage containerized workloads, legacy virtual machines, and VDI environments from a single control plane. This approach aligns with DevOps and Infrastructure-as-code (IaC) methodologies for automated deployment, scaling, and updates.

The unified management extends to migration scenarios, where organizations can:

- Run parallel to existing VMware infrastructure
- Migrate workloads incrementally
- Maintain existing operations during the transition
- Convert VMs to containers systematically

Migration components include:

- Parallel infrastructure operation with shared storage access
- Network bridge configuration and identity federation
- Phased user transition with profile conversion
- Automated workload transformation

Built for Defense-Grade Security

Recognizing the stakes government and defense organizations face, RGS embeds security at every layer of Kasm Workspaces. The result is a battle-tested workspace delivery platform resilient enough to withstand the sophisticated threats common in classified and sensitive operations.

At its core, the solution uses a zero-trust, web-native architecture that eliminates the need for endpoint-installed software to reduce the attack surface and prevent common vectors of compromise. Administrators gain control over workspace activities, enforcing strict data loss prevention policies through clipboard restrictions, upload/download management, and session monitoring capabilities. Out-of-the-box compliance with federal security standards, including FIPS 140-2, NIST 800 controls and DISA STIG guidelines, means agencies exceed regulatory guidelines from day one.

For security identity management, Kasm Workspaces supports enterprise-grade Single Sign-On (SSO) integration with widely used identity providers such as Azure AD, Okta, and Google Workspace, complemented by local two-factor authentication (2FA) options. Additionally, the platform allows agencies to tailor desktop persistence to specific mission parameters, either retaining user data across sessions for continuity or enforcing non-persistent environments to strengthen security further.

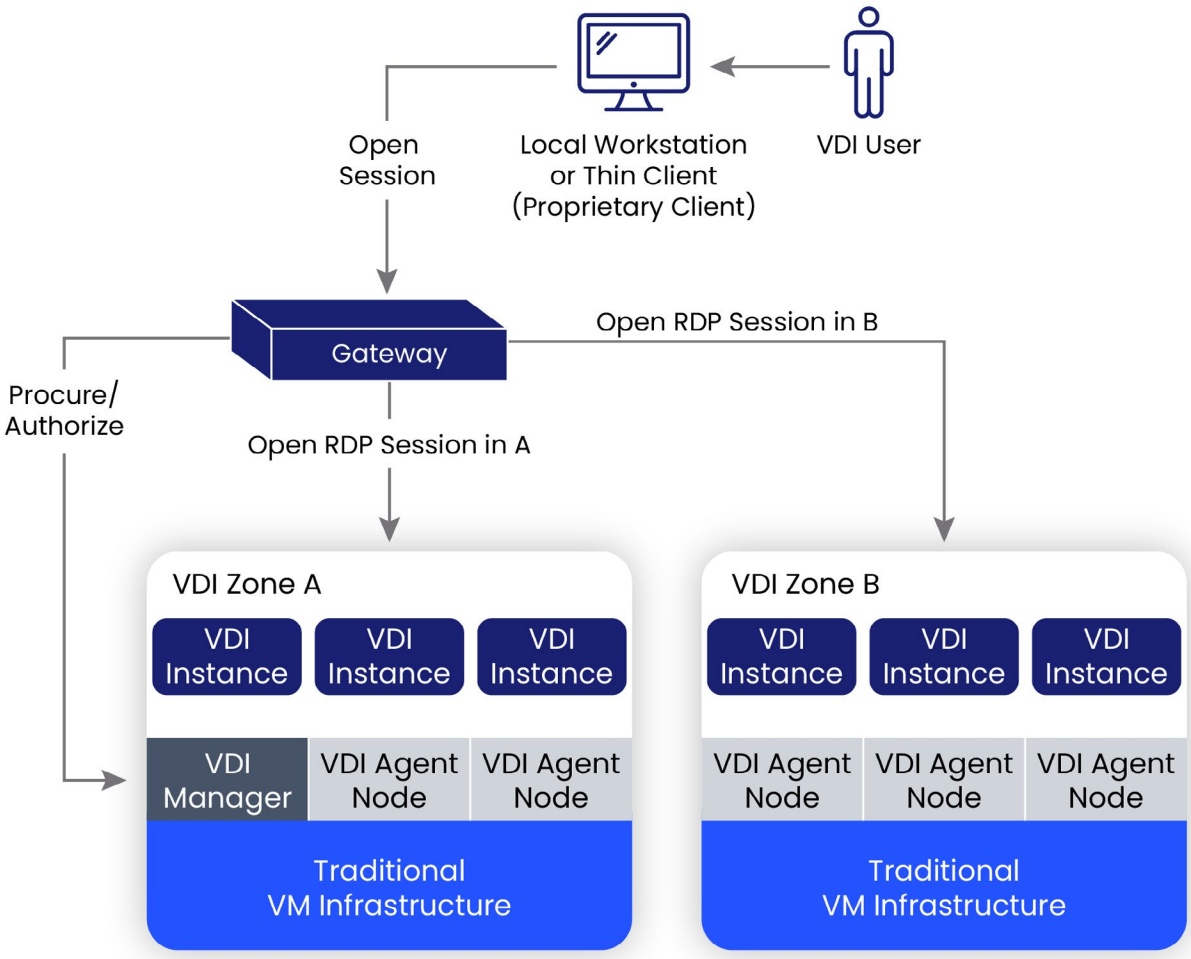
Traditional VDI fails in disconnected, low-bandwidth, or high-security environments. The RGS - Kasm partnered solution is purpose-built for these missions, providing:

- **Air-gapped deployment support:** Secure, self-contained workspace environments with no external connectivity.
- **Low-bandwidth optimization:** Remote work in austere environments with minimal data transfer.
- **Portable containerized desktops:** Deploy workspaces on forward-operating bases, classified networks, and mobile units.
- **Zero-trust security enforcement:** Strict access controls and unauthorized data exfiltration protection.

Solution Architecture Overview

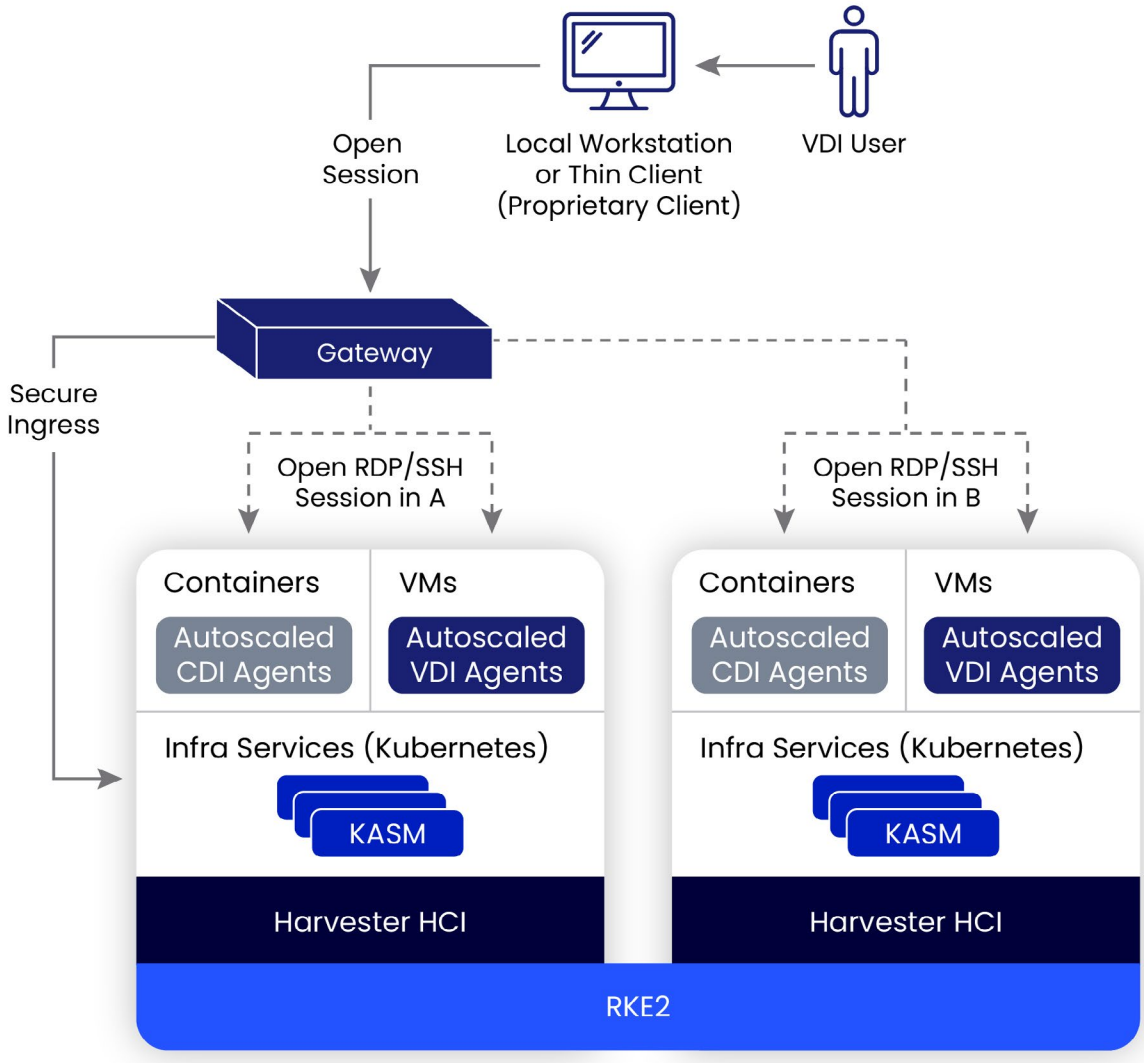
Legacy Virtual Desktop Infrastructure

The first diagram illustrates a traditional VDI stack built on proprietary hypervisors, siloed networking and storage, and agent-heavy endpoint access. Each virtual machine requires dedicated resources, increasing complexity and cost. Endpoint software expands the attack surface and creates management burdens. This architecture lacks the flexibility to support hybrid, edge, or air-gapped environments and falls short of zero-trust security mandates. Designed for static data centers, it struggles with modern mission demands—especially those requiring rapid scale, distributed access, and secure operations. The result is an inflexible, costly solution unfit for today's defense and government use cases.



Modern Cloud-Native Workspace Architecture

The second diagram shows a modern, cloud-native workspace built on Kubernetes. Harvester Government provides hyperconverged infrastructure, while Rancher MCM centralizes management of VMs and containers. Kasm Workspaces deliver secure, browser-based desktops—no endpoint agents required. The stack supports x86, ARM, and repurposed hardware, and operates in hybrid, air-gapped, or disconnected environments. Security is built-in through zero-trust isolation and workload controls. This architecture simplifies operations, improves agility, and strengthens compliance. It's purpose-built to meet mission-critical needs with scalable, portable, and secure workspaces—ideal for government and defense deployments.



Core Rancher Government Solutions Components

Combining Kasm with RGS's technology stack creates a defense-grade workspace platform significantly more capable than either solution alone. Core Rancher components — RKE2, SUSE Security (NeuVector), and SUSE Storage (Longhorn) — extend Kasm's capabilities through:

- **RKE2:** Full CNCF-certified Kubernetes distribution with FIPS validation and DISA STIG compliance.
- **SUSE Security (NeuVector):** Zero-trust container security with real-time vulnerability scanning and runtime protection.
- **SUSE Storage (Longhorn):** Distributed and resilient storage solution with automated backup and disaster recovery capabilities.

The RGS-Kasm Solution: Capabilities and Advantages

- **Silicon-to-Browser Security:** The integrated platform establishes security controls at every layer, preventing unauthorized access and protecting sensitive data.
- **Confidential Computing:** Container isolation protects data in use, allowing security mechanisms to focus on access control and threat prevention.
- **Streamlined Operations:** The unified approach simplifies deployment, management, and compliance across diverse computing environments.
- **Performance Impact:**
  - **Reduced Latency:** Native container performance with minimal overhead
  - **High Availability:** Distributed architecture ensures continuous operation
  - **Operation Excellence:** Automated management reduces administrative burden

How the RGS-Kasm Solution Stands Out

Feature	Kasm Workspaces with Embedded RGS Stack	Traditional VDI
Deployment Flexibility	On-prem, hybrid, air-gapped	Primarily on-prem, cloud add-ons
Security	Zero-trust, workload isolation	Perimeter-based security
Cost Efficiency	No hypervisor licensing fees	High licensing and support costs
Scalability	Kubernetes-native, elastic scaling	Limited by hypervisor constraints
Management	Centralized Kubernetes management	Requires agent-based VDI infrastructure

Future-Proofing Government Workspaces

The partnership between RGS and Kasm offers government agencies a scalable alternative to legacy virtual desktop infrastructure workspace delivery for government agencies and defense operations. By replacing proprietary hypervisors with a Kubernetes-native approach, agencies can improve security, control IT management, and reduce costs without sacrificing performance.

This partnership is purpose-built to meet the demands of government and military operations, Providing secure operations in on-prem, hybrid, and air-gapped environments. With zero-trust security principles, workload isolation, and flexible deployment options, agencies retain complete control over their IT infrastructure while avoiding vendor lock-in constraints.

Agencies transitioning to this approach will gain greater control over their infrastructure, minimize security risk, and strengthen IT investments to meet future mission needs.

See the RGS - Kasm partnered solution in action. Explore an on-demand demo today to see how secure, cloud-native workspaces can modernize your agency's IT strategy.

About Rancher Government Solutions

Rancher Government Solutions is designed specifically to address the unique security and operational needs of the U.S. Government and military as it relates to application modernization, containers, and Kubernetes.

Rancher is a complete open-source software stack for teams adopting containers. It addresses the operational and security challenges of managing multiple Kubernetes clusters at scale while providing DevOps teams with integrated tools for running containerized workloads.

Rancher Government supports all Rancher products, with U.S.-based American citizens currently supporting programs across the Department of Defense, the Intelligence Community, and civilian agencies.

To learn more about Rancher Government's products and solutions, visit: www.ranchergovernment.com

info@ranchergovernment.com
844-RGS-7779
1900 Reston Metro Plaza
Suite 600
Reston, VA 20190

About Kasm Technologies

Kasm Technologies inc. is a leading provider of enterprise VDI solutions. Kasm Workspaces enables secure, scalable, and efficient delivery of desktop infrastructure through cloud-native, Kubernetes-based architectures. Kasm is dedicated to supporting organizations in their transition to modern DevOps environments and providing the tools needed for the future of VDI. To learn more about Kasm Technologies visit kasmweb.com.