omnissa®

WHITE PAPER

Guarding what matters for the government

Multi-level security and a compliant-ready workspace

Table of contents

Enabling government transformation with multi-level, adaptive security

Digital transformation is no longer optional. Today's government agencies must modernize operations, deliver digital services, and protect sensitive data. From defense systems to civilian services, modern governance demands secure, scalable infrastructure at every level.

Transformation, however, introduces significant risk. Government IT systems are prime cyberattack targets, and regulations like FedRAMP, NIST, and GDPR now dictate strict data access controls. Distributed workforces expand attack surfaces, complicating endpoint security and policy enforcement across multiple classification levels.

Air-gapped infrastructure, designed for physical separation, now creates inefficiency. Legacy systems drive data duplication, disconnected operations, and workarounds that undermine security, leading to communication breakdowns, hardware sprawl, and inconsistent access control.

Enter Omnissa.

A secure platform for modern governance

Omnissa enables and supports multi-level security (MLS) enforcement through integrated authentication and identity federation aligned with government clearances. **Omnissa® Access™** dynamically maps user roles to security labels, ensuring clearance-based mandatory access control that restricts users to data and apps appropriate to their authorization level. Micro-segmentation and zero-trust enforcement via **Omnissa Workspace ONE®** and **Omnissa Horizon®** create secure compartments and deliver granular per-app tunneling that isolates sensitive data according to need-to-know principles.

The Omnissa platform deploys entry, intermediate, and secure zones that manage session integrity, enforce device compliance, and isolate classified workloads within trusted computing environments. Real-time telemetry and AI-driven analytics through **Omnissa Intelligence™** enable automated risk scoring, conditional access controls, and rapid response to anomalies or policy violations, strengthening insider threat detection and compliance adherence. Strong authentication mechanisms including MFA, Smart Cards, PIV-D, and certificate-based logins combine with device posture validation to ensure only compliant, trusted devices connect. Centralized management consoles provide comprehensive audit trails and automated reporting that streamline compliance with FedRAMP, FISMA, and NIST standards, simplifying regulatory oversight.

In the following pages, we'll take a closer look at how the Omnissa platform helps protect what matters for government agencies.

Government security needs

MLS systems enforce mandatory access control by labeling data with classification levels and compartments that represent specific programs or missions. Every user and object carries a security label, and the operating system enforces strict “no read up, no write down” rules that create hard access boundaries users can’t override. This approach is essential for government agencies and defense contractors hosting multiple classification levels on shared infrastructure, as it helps prevent data leakage and enable controlled sharing without physical system separation.

The challenges of MLS

Despite its necessity, implementing MLS introduces significant challenges. Complex networks running multiple operating systems and apps force users to juggle incompatible devices, creating workspaces cluttered with computers and monitors dedicated to different classification levels. Managing varying security clearances while preventing unauthorized access is further complicated by persistent security issues like covert channels—through which classified information bypasses controls and reaches lower-clearance users—and by the rapid pace of technological change that outpaces system modernization.

Ironically, security architectures designed to protect data often create new vulnerabilities. System incompatibility forces manual data transfers and physical movement between networks, leading to logging errors, forgotten deletions, and theft opportunities. Collaborative government work involving employees, contractors, and agencies drives proliferation of incompatible networks and devices, resulting in a sprawling IT environment that is complex, time-consuming, error-prone, costly, and vulnerable to data leaks.

Modern MLS must balance various conflicting requirements: preventing unauthorized information flow, supporting efficient workflows, integrating legacy apps, ensuring usability across mixed-sensitivity environments, and scaling effectively—all while guaranteeing that information flow rules cannot be bypassed by misconfigurations, bugs, or covert channels. Traditional approaches have struggled to reconcile these disparate requirements, creating fundamental tensions between security, efficiency, and operational sustainability. The Omnissa platform helps solve this dilemma.

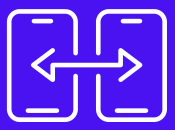
Security architecture overview

The Omnissa unified platform integrates endpoint management, digital experience monitoring, access control, and security compliance into a single automated framework. This approach allows your government agency to centrally manage diverse device types while monitoring user experience and security posture in real time. By consolidating these capabilities, Omnissa helps reduce operational complexity while enabling your IT teams to enforce consistent policies, streamline workflows, and accelerate incident response across your entire digital estate.

Authorized access only

The platform is built on zero-trust principles, enforcing least privilege access, continuous verification, and segmentation across identities, devices, networks, and apps. Users access only the resources they're explicitly authorized to use, with risk continuously assessed based on context—device health, location, and behavior. Multi-tenancy and granular segmentation features allow your organization to align security controls with complex hierarchies and operational silos. Policies can be inherited or overridden to match agency, department, or mission-specific requirements, ensuring MLS environments maintain strict isolation while enabling authorized collaboration.

Tailored for government use, Omnissa products ensure compliance with federal standards including FedRAMP, CMMC, and NIST frameworks while supporting both modern and legacy systems. Scalable deployment options adapt to your evolving needs. Key Omnissa components for MLS include Omnissa Access for granular identity and access management, Workspace ONE® UEM™ for device posture assessment and policy enforcement, Horizon for virtual desktop infrastructure, and Omnissa Intelligence analytics for real-time threat detection and compliance monitoring. Together, these create layered protections that align with federal security requirements.



TL;DR

A unified platform approach integrates endpoint management, digital experience, access control, and security compliance within a single data and automation layer.

Zero-trust principles emphasize least privilege, continuous verification, and segmentation by identity, device, network, and app.

Multi-tenancy and segmentation provide policy inheritance and override capabilities for aligning security posture to organizational hierarchies and operational silos.

The Omnissa approach to MLS

Omnissa helps enforce MLS in a variety of ways.

- **Compartmentalization and policy enforcement** – Workspace ONE delivers micro-segmentation and zero-trust network enforcement through software-defined security controls. Granular per-application tunneling and secure remote desktop protocols from Horizon restrict access within isolated compartments.
- **Continuous monitoring and risk assessment** – Telemetry gathering and AI-driven analytics through Omnissa Intelligence provide real-time detection of access anomalies and policy violations. Automated risk scoring and conditional access controls mitigate insider threats.
- **Audit and compliance reporting** – A centralized management console providing logs and audit trails helps support compliance with FedRAMP, FISMA, NIST, and other regulations.
- **Security labeling and access enforcement** – The use of strict user authentication and identity federation integrated with security clearances helps ensure alignment with MLS's mandatory access control. Omnissa Access provides role mapping to MLS labels for dynamic, clearance-based access enforcement.
- **Trusted computing and secure zones** – Implementation of entry, intermediate, and secure zones promotes session integrity and device compliance. Secure virtual desktops and restricted access environments help isolate classified workloads.
- **Strong authentication and device posture validation** – Support for multi-factor authentication (MFA), PIV-D cards, and certificate-based logins helps ensure alignment with government credentialing standards. Device compliance checks integrated with access decisions support trusted and managed device policies.

From desk sprawl to single device

Consider a federal regulatory or intelligence-support agency facing a common operational dilemma: Staff members and cleared contractors need to work with both Unclassified and Controlled Unclassified Information (CUI) throughout their workday, yet current security protocols require separate physical devices for each classification level. This creates desk clutter, escalates hardware costs, and introduces security risks during manual data transfers. What the agency needs is a solution that maintains strict data separation while consolidating endpoint infrastructure.

Implementation approach

The agency applies MLS principles through strict data classification, policy-driven access, and logical separation of work contexts delivered via unified digital workspace technology. Virtual desktop infrastructure creates hard security boundaries between classification levels while presenting users with a seamless single-device experience.

Technical architecture

Horizon-hosted virtual desktops and apps are segmented by classification (general business VDI versus CUI VDI) and presented through a single Omnissa workspace portal. Workspace ONE UEM continuously validates device posture—encryption status, OS version, FIPS-validated cryptography—and blocks access when devices drift from compliant states.

Role- and attribute-based access controls determine which virtual desktops, apps, and data classifications each user can access, aligning with NIST 800-171 and CMMC practices. A FedRAMP High or DoD IL-aligned Omnissa deployment hosts the platform, with network and data tiers mapped to classification levels. Omnissa manages identity, device compliance, and session policy at the access layer, while underlying MLS and network controls enforce hard boundaries between tiers.

Business value

Contractors and federal employees work from anywhere on mixed-device fleets while meeting FedRAMP, CMMC, and agency security baselines. Eliminating separate physical machines per classification reduces endpoint and operational costs. Centralized policy enforcement and monitoring improve auditability and simplify compliance demonstrations during inspections and certifications. Users experience a unified workspace that dynamically adapts security based on resource sensitivity, satisfying both mission requirements and security mandates.

How our products help maintain data separation while consolidating endpoints

Workspace ONE UEM provides endpoint management to enforce device compliance (e.g., encryption, FIPS modules, posture checks) across federal and contractor laptops, ensuring only compliant devices can connect to sensitive virtual environments.

Horizon serves as the core for delivering virtual desktops and apps segmented by classification levels, enabling users to access only permitted workloads through a unified workspace portal while enforcing MLS-style boundaries via policy-driven session isolation.

Omnissa Access handles identity federation, role-based access control, and MFA integrated with agency directories, dynamically assigning users to classification-appropriate app entitlements and preventing cross-domain spillage.

Omnissa Intelligence adds unified observability, anomaly detection, and automated compliance reporting to monitor access patterns, flag potential MLS violations (e.g., unusual data flows), and generate audit trails for FedRAMP/CMMC assessments.

Secure multi-classification operations for forward deployed

Consider a forward operating base where a logistics officer must coordinate supply movements on unclassified systems while simultaneously accessing mission planning tools handling CUI. An intelligence analyst working nearby requires even more sensitive apps. Both operate from rugged tablets over unstable satellite connections in an environment where space is limited and mission tempo is relentless.

Traditional approaches demand separate devices for each classification level. Multiply this across a deployed unit and the hardware burden becomes unsustainable. Operators juggle devices, manually transfer information between disconnected systems, and navigate constant friction—slowing missions, escalating costs, and increasing spillage risk.

The solution

Omnissa helps deployed forces maintain strict classification boundaries while achieving operational tempo through unified digital workspace architecture. Personnel can access classification-separated virtual environments from a single rugged endpoint—dynamically validated, continuously monitored, and rigorously controlled.

Horizon virtual desktops deliver distinct environments for each classification tier through the Omnissa workspace portal as a seamless experience while maintaining hard security boundaries. Workspace ONE UEM orchestrates device-level security through role-based policies, geofencing, and continuous compliance validation. Defense identity integration with zero-trust controls creates continuous verification—strong MFA confirms identity while conditional access evaluates device health, location, and behavior in real time.

The architecture

An Impact Level-authorized EUC environment in a defense data center or GovCloud region connects via secure gateways to tactical networks at forward locations. Omnissa operates at identity, device posture, and workspace layers, while underlying MLS/segmented networks and cross-domain solutions enforce hard separation between classification tiers.

Mission impact

Units gain faster mission app access, with no need to use multiple devices per security domain. A single rugged tablet replaces three laptops, reducing hardware footprint. Central enforcement ensures DoD, NIST 800-171, and zero-trust compliance across thousands of endpoints with complete audit trails. Automated controls replace error-prone manual processes, reducing spillage risk. Security adapts dynamically without forcing workarounds, maintaining secure connectivity even over unstable networks and enabling forces to operate faster, lighter, and more securely.

How our products help keep multi-classification operations secure

Workspace ONE® UEM

Workspace ONE UEM manages rugged and tactical devices with geofencing, compliance checks, and conditional access, ensuring field devices meet posture requirements before connecting to higher-sensitivity virtual apps.

Horizon®

Horizon delivers the virtual desktops for NIPRNet-style unclassified workloads and separate CUI/mission desktops, enabling deployed users to access only permitted environments through a unified, secure workspace portal that aligns with MLS boundaries via role-based session isolation.

Omnissa Access

Omnissa Access provides identity federation with DoD systems (e.g., DoD365 integration), strong MFA, and dynamic entitlement assignment by unit/role/clearance, preventing unauthorized cross-domain access while supporting tactical authentication in low-bandwidth scenarios.

Omnissa Intelligence

Omnissa Intelligence offers real-time threat detection, anomaly monitoring across endpoints/sessions, and automated compliance reporting for DoD/CMMC audits, flagging potential MLS violations and enabling rapid response in deployed environments.

Strengthening security posture while reducing complexity

Omnissa can help your government agency overcome the challenges of traditional MLS by taking a modern, efficient approach. Benefits include the following:

- **Compliance and security** – Zero-trust enforcement, session isolation, and anomaly detection reduce spillage risks across sensitivity levels while simplifying audits for mixed-classification workloads.
- **Operational efficiency** – Dynamic VDI provisioning mapped to clearances eliminates the need to use separate devices per classification domain, cutting hardware costs and administrative overhead.
- **Integration and agility** – Seamless federation with DoD IAM systems, tactical network support, and automated posture-based access enable secure hybrid operations for deployed and contractor personnel while adapting to evolving threats.

The Omnissa unified platform demonstrates that MLS principles can be enforced without the hardware sprawl, manual processes, and operational friction that have plagued traditional MLS implementations. By delivering classification-aware virtual desktops, zero-trust access controls, and AI-driven threat detection through a single consolidated framework, we can help your agency achieve measurable security improvements while simultaneously reducing costs, accelerating mission tempo, and simplifying compliance.

Take the next step

As cyber threats evolve and digital transformation accelerates, agencies equipped with modern MLS-aligned infrastructure gain the adaptability to meet emerging challenges without sacrificing the security mandates that protect national interests. The path forward is clear: Adopt a unified platform that enforces strict security boundaries while enabling the operational excellence modern governance demands.

Ready to modernize your MLS infrastructure? Visit the Omnissa federal **webpage** today to learn how our unified platform delivers compliance, efficiency, and mission readiness for defense and civilian agencies, or **reach out** to your federal government representative today.

omnissa®

 FY26-8062-OMN-GUARDING-WHAT-MATTERS-USWEB-WP-A4-20260302 3/26