

# Supporting the secure, digital-ready government of tomorrow

Balancing public sector security, productivity, and cost-efficiency  
for mission success



# Table of contents

- 3 Streamline security and compliance with an efficient digital workspace
- 4 Empower government operations
- 5 Fortify security with AI-powered threat defense
- 6 Minimize unauthorized access with least-privilege principles
- 7 Optimize IT service management for mission readiness
- 8 Strengthening government resilience
- 9 Get started

# Streamline security and compliance with an efficient digital workspace

Government agencies face the constant challenge of balancing mission-critical security with the mobility and efficiency required for modern government operations. While the workforce increasingly relies on mobile access, cyber threats continue to evolve rapidly. The need for a robust, flexible IT infrastructure has never been greater.

Omnissa provides a suite of products designed to enhance security, mobility, and operational efficiency across the government. By leveraging modern tech, your government agency can stay ahead of threats while improving productivity and reducing IT complexity.

## Why it matters

Our solutions are designed to support your agency's mission with operational, security, and compliance benefits.

### **Enhanced security and compliance**

Government agencies handle sensitive and classified data, requiring strict security measures, zero trust access, and compliance with regulations like FISMA, FedRAMP, and NIST standards.

### **Operational continuity and resilience**

Secure digital workspaces keep mission-critical operations running smoothly, even in the face of cyberthreats or disruptions.

### **Remote and mobile enablement**

Government employees, military personnel, and contractors need secure access to apps and data from any location or device while maintaining strong data protection standards.

### **Cost efficiency and IT optimization**

Centralized management of apps, desktops, and security can help reduce IT overhead and extend device lifespans.

### **Improved productivity and collaboration**

Secure digital workspaces provide a seamless, high-performance user experience enabling government teams to collaborate efficiently while maintaining data security.

### **Data sovereignty and controlled access**

Support data sovereignty by keeping sensitive government data within controlled environments while enforcing access policies based on roles, locations, and device security posture.

# Empower government operations

For government employees, having seamless access to mission-critical apps from any location is essential. Here's how Omnissa delivers.

- **Effortless workforce support** – Empower your mobile workforce while helping reduce costs. Rapidly deploy devices and provide secure access to apps for improved productivity.
- **Seamless performance anywhere** – Designed to deliver fast, reliable desktop performance across all locations, networks, and devices. Keep teams connected and efficient, no matter where they work.
- **Simplified IT workloads** – Streamline app management to help alleviate IT burdens, ensuring users have the tools they need to succeed.
- **Optimized for every environment** – Advanced adaptive protocols provide low-latency performance, even in remote or low-bandwidth conditions.
- **Centralized security and compliance** – Reduce the risk of data breaches with robust security controls, supporting compliance with cybersecurity standards.
- **Productivity made easy** – Enhance user experiences with tools and infrastructure designed to keep your teams focused and efficient.
- **Future-forward solutions** – Support innovation with cutting-edge technology that adapts to your organization's evolving needs.

## Our flagship product families



Workspace ONE®

### Omnissa Workspace ONE®

Integrated endpoint management, security, and experience across any use case.



Horizon®

### Omnissa Horizon®

A modern approach to the secure delivery of desktops and apps across hybrid cloud.

# Fortify security with AI-powered threat defense

Omnissa products feature real-time threat detection and automated remediation to safeguard government employees from attack while maintaining operational flexibility. Direct integration with **Omnissa Intelligence** and **Omnissa Workspace ONE® Mobile Threat Defense™**, as well as products from third-party providers, offers seamless deployment and management. This helps reduce complexity for your IT teams and enhance security without disrupting productivity or causing digital friction.



## Automated security from endpoint to endpoint

Automation enhances threat detection and response by identifying vulnerabilities in real time and enforcing security policies across all endpoints.

**Omnissa Workspace ONE® UEM** enables your agency to support consistent policy enforcement, zero trust access, and real-time monitoring of devices, apps, and networks.

**Omnissa Horizon** provides secure access to desktops and apps while helping reduce data exposure and supporting compliance with federal standards, including FedRAMP.

**Omnissa Workspace ONE® Experience Management** is designed to help reduce downtime, optimize resources, identify potential vulnerabilities, enforce policies, and improve operational efficiency.

## Minimize unauthorized access with least-privilege principles

Implementing zero trust and contextual security models is essential for controlling access to sensitive data. By adhering to least-privilege principles, zero trust ensures that users and devices are granted only the minimum level of access necessary for their specific roles. This can significantly reduce the risk of unauthorized data exposure.

A zero trust approach is complemented by contextual security measures, which dynamically adapt security protocols based on the device in use, user identity, and geographic location. This adaptability allows for more granular control and real-time adjustments to security measures, ensuring that access remains secure and appropriate under varying conditions.

### Deliver a great experience, securely

Securing access to apps and devices is essential for protecting sensitive data in government agencies. But with Omnissa, advanced security doesn't have to come at the expense of usability. Create login experiences that combine simplicity with robust protection. Leverage tools like multi-factor authentication alongside single sign-on to safeguard critical systems while supporting seamless workflows. Empower government employees to be productive while protecting them—and their data.



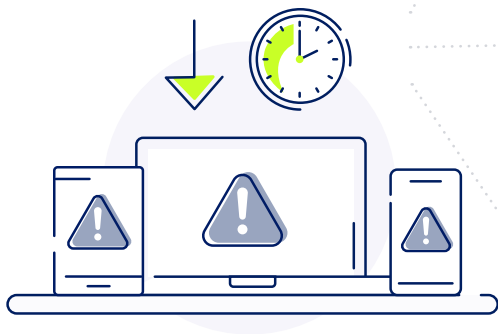
## A secure and mobile workforce

As mobile devices become more integral to government defense, ensuring their security is a priority. Omnissa Workspace ONE Mobile Threat Defense delivers advanced, AI-driven protection against a variety of threats, including phishing, device vulnerabilities, and malicious apps.



# Optimize IT service management for mission readiness

Governments can't afford to be reactive when it comes to IT issues. Problems must be anticipated and addressed before they disrupt operations. That's where IT service management (ITSM) plays a critical role. By integrating Omnissa with your existing ITSM tools, your agency can gain deeper visibility into potential issues and automate proactive remediation workflows. This helps reduce mean-time-to-resolution (MTTR), increase uptime, and boost productivity—resulting in a more resilient, agile IT infrastructure that supports mission-critical operations without unnecessary delays or security risks.



## **Automated issue resolution and incident management**

By integrating Omnissa with your existing ITSM platform, your agency can streamline ticketing, issue detection, and resolution workflows. This minimizes downtime and ensures that critical systems remain operational—even during high-stakes missions—helping your agency maintain mission readiness.

## **Proactive system monitoring and predictive maintenance**

Your ITSM platform and monitoring tools can integrate with Omnissa to detect potential failures before they impact operations. By leveraging AI-driven analytics, your agency can proactively address IT vulnerabilities, ensuring continuous availability of mission-critical infrastructure.

## **Compliance and security enforcement**

Integrating Omnissa with your ITSM framework helps you enforce security policies, track incidents, and maintain compliance with government regulations such as NIST and FedRAMP. With automated workflows and real-time telemetry, your agency can respond quickly to security threats—protecting sensitive data and preserving operational integrity.

# Strengthening government resilience

With a commitment to protecting sensitive data, streamlining workflows, and enhancing productivity, Omnissa helps governments achieve resilience and agility in an increasingly dynamic world. The path forward for government IT is clear: Adopt Omnissa solutions to facilitate a secure, efficient, and future-ready digital ecosystem that ensures success in every mission.



## Compliance monitoring

- Continuously monitor for unauthorized users, compromised devices, and other risks.
- Automatically block access to data if a threat is detected.



## Enhanced security

- Enable strong user authentication through AD/LDAP.
- Leverage certificate-based access to email, Wi-Fi, and VPN.
- Adopt comprehensive protection for apps and documents.



## Secure content locker

- Safeguard document transmissions with 256-bit TLS encryption.
- Maintain control over user access, document editing, and restrictions on app usage.
- Mandate SCL environments for document security.



## Government networks

- Automatically provision Wi-Fi and VPN profiles for seamless integration to networks and file systems.
- Provide secure access to specific websites through an encrypted VPN tunnel.



## App management

- Build internal apps with integrated features like robust user authentication and comprehensive security policy.
- Seamlessly add advanced security and management capabilities to existing internal apps.



Supporting the secure, digital-ready government of tomorrow

# Get started

Learn more about how Omnissa can help your government agency enhance security, efficiency, and productivity. Visit the **Public Sector Tech Zone** or **contact** an Omnissa representative today.



omnissa™

Copyright © 2025 Omnissa. All rights reserved. This product is protected by copyright and intellectual property laws in the United States and other countries as well as by international treaties. Omnissa, the Omnissa Logo, Workspace ONE and Horizon are registered trademarks or trademarks of Omnissa in the United States and other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies. "Omnissa" refers to Omnissa, LLC, Omnissa International Unlimited Company, and/or their subsidiaries. FY25-7930-OMN-SECURE-MISSION-READY-IT-WP-USWEB-A4-20250523 5/25