Federal compliance you can deploy with confidence

Securing federal workloads isn't just about doing the right thing—it's about meeting the right standards. The Omnissa government portfolio aligns with a variety of compliance frameworks across different deployment models to enable a diverse range of use cases. These certifications provide organizations with proven, trusted tools for securing sensitive workloads, ensuring mission continuity, and rapidly adapting to emerging threats.

Omnissa product portfolio

Omnissa Horizon® 8	Omnissa Workspace ONE® FedRAMP HIGH	Supporting appliances
Horizon 8 in customer on-premises	Workspace ONE SaaS	Workspace ONE Boxer
Horizon 8 in customer accounts on FedRAMP authorized public cloud	UEM ModStack • Omnissa Access and Workspace ONE Intelligent Hub™ Services • Omnissa Intelligence™	Workspace ONE Tunnel
DISA Stratus		Omnissa Unified Access Gateway (UAG)
Partner-managed solution	Partner-managed OSS	

Here's how each Omnissa product helps meet specific government compliance requirements.

Government compliance matrix

Product	FedRAMP	GovRAMP	CC NIAP	CSfC	CMMC[1]	STIG	FIPS 140
Horizon 8			✓	✓	✓	✓	✓
Workspace ONE UEM	✓	✓	✓	✓	✓	✓	✓
Workspace ONE Access	✓	✓			✓		✓
Workspace ONE Intelligence	✓	✓			✓		✓
UAG			✓	✓	✓	✓	✓
Tunnel			Planned	Planned	✓		✓
Boxer			✓	✓	✓		✓

1. Omnissa can help customers meet CMMC requirements with either FedRAMP authorization for SaaS or configurable hardening for on-premises software.

Key success factors

Government use cases require rigorous security controls and efficient delivery of services and resources. Omnissa helps meet these requirements with a broad range of certified solutions across a variety of environments and deployment models. With Horizon and Workspace ONE, government users can ensure that the distributed workforce has continual access to critical applications and data through secure, scalable, and manageable remote desktops and managed endpoints.

Protect sensitive data

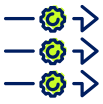
Keep data safe with layered security architectures.

Enforce strong identity controls, SSO, MFA, and encrypted communications.

Leverage unified observability, enhanced anomaly detection, and continuous device posture verification.

Meet FedRAMP, NIAP, STIG, and FIPS 140 requirements.

Enable confident deployment to highly regulated environments.



Empower productivity

Deliver hardened remote access to apps and desktops supporting sensitive workloads.

Streamline and secure device onboarding and management.

Monitor health and performance.

Ensure compliant, secure access to resources for distributed teams and personnel.

Modernize and reduce complexity

Maintain consistent security posture across environments.

Automate patching and compliance enforcement.

Consolidate tools to limit sprawl, reduce TCO, and simplify management.

Accelerate adoption and updates with aligned compliance frameworks. Achieve faster ATO readiness.

Get started

To learn more about Omnissa federal certifications, visit the Omnissa **Trust Center**.

omnissa®

 FY26-8060-OMN-FED-COMPLIANCE-DS-USWEB-A4-20250321 3/26