omnissa®

Protecting government data is protecting what matters most

Safeguard federal mobile endpoints with robust security that's both FedRAMP-authorized and NIST-compliant

Key use cases include:

- **Demonstrate compliance** with NIST, EO mandates, and FedRAMP through audit-ready reporting
- **Protect sensitive government data** from mobile-borne threats
- **Enforce zero-trust policies** across mobile devices
- **Secure mobile endpoints** for remote and field personnel

Omnissa Workspace ONE® Mobile Threat Defense™ (MTD) detects and helps mitigate threats across mobile and endpoint devices. MTD solutions continuously monitor devices for anomalous behavior and activity, helping protect against phishing and unauthorized access.

With MTD organizations can enforce security policies, lock screen settings, and ensure data encryption. Mobile Threat Defense assesses application risk and blocks malicious downloads to thwart malware installation attempts and monitors suspicious activity to prevent theft of sensitive and protected data. All of this is achieved while staying within government regulations and compliance.

Visit **omnissa.com/platform/federal-government/** or contact your Omnissa Federal government representative for more information.

omnissa®