SOLUTION OVERVIEW

Trusted solutions for secure, mission-focused government operations

For government agencies, security and efficiency aren't optional—they're essential. Delivering public services, safeguarding national security, and maintaining critical infrastructure all rely on a workforce that thrives on both productivity and robust security.

Modern challenges such as evolving security threats, the growing need for flexible work environments, and increasingly complex IT infrastructures amplify the pressure on these institutions.

To meet these demands, your agency needs a strategic approach that seamlessly combines advanced security, cutting-edge IT solutions, and productivity enhancements—without compromising compliance or operational integrity.

This is where Omnissa steps in. Our comprehensive framework is designed to empower your government agency, helping you **strike the perfect balance between security, efficiency, and innovation.**

At a glance

Discover how Omnissa secures data to optimize uninterrupted access to essential resources and empower government employees to do their jobs more efficiently and effectively.

omnissa™

Promote compliance, reduce security risks, and boost productivity

With unified endpoint management (UEM), you can centralize endpoint security and management to give IT full visibility and control over government-issued and BYO-devices. This ensures compliance with security policies while allowing employees to work from any location.

- **Zero trust security** is designed to allow only authorized users and devices to access sensitive data.
- **Automated patching and policy enforcement** helps reduce vulnerabilities and enhance compliance.
- **Device and application management** simplify IT operations across all endpoints.

Enhance flexibility while maintaining strict control

With virtual desktops and apps, you can deliver secure, scalable access to apps and desktops, ensuring your employees can work efficiently while minimizing security risks. A centralized approach enables your agency to provide secure digital workspaces without relying on physical hardware.

- **Data remains on secure servers** rather than local devices, reducing the risk of breaches.
- **Employees can securely log in** to government-approved virtual desktops from any location.
- **Centralized IT admin can reduce operational overhead** and extend device lifespans.

Proactively manage risks, optimize performance, and improve the employee experience

Empower employees to work efficiently—without unnecessary IT bottlenecks, downtime, or disruptions. Streamline IT workflows, automate issue resolution, optimize incident management, and improve responsiveness with digital employee experience (DEX).

- **Detect and resolve issues** before they disrupt productivity.
- **Identify patterns in IT incidents** and automate issue resolution.
- **Optimize apps and devices to perform at peak efficiency** so employees can stay productive.
- **Reduce manual IT workloads** by automating incident response.
- **Leverage predictive analytics** to anticipate and mitigate IT disruptions.

Solve today's top challenges

Our solutions enable your agency to create a unified ecosystem where apps, desktops, data, and services come together securely so you can easily meet today's most pressing demands, including the following:

- **Modernization** – Increase operational efficiency and reduce costs.
- **Always-on availability** – Provide continuous delivery of services.
- **Securing sensitive information** – Reduce risk and automate compliance.

Simplify endpoint management and secure app and data access on any device. Adopt desktop virtualization to optimize IT infrastructure to cut costs, boost performance, and enable flexible access. Integrate zero trust security to protect both physical and virtual endpoints while delivering a seamless, low-effort user experience for government employees. Put visibility and proactive remediation at your fingertips.

64%
of federal IT leaders are worried about not having the existing infrastructure to use emerging tech.

57%
say their agency's IT infrastructure is simply not built to handle emerging tech.

Source: Ernst & Young LLP, "2024 EY federal, state and local trends report: key findings." US SCORE no. 22296-241US. 2024.

Omnissa benefits

Visibility and proactive remediation

- Continuously monitor endpoints for unauthorized users, compromised devices, and other risks.
- Automatically block access to data if a threat is detected.
- Leverage machine learning and predictive insights to optimize IT resources and maintain high-performance environments.

Tighter security and risk mitigation

- Utilize multi-tenancy.
- Maintain adherence to regulations like FedRAMP, NIAP, and NIST.
- Secure document transmissions with 256-bit TLS encryption.
- Control restrictions on user access, document editing, and app usage.
- Mandate SCL environments for document security.
- Adopt strong user authentication with AD/LDAP.

Higher productivity

- Build internal apps with integrated features like robust user authentication and comprehensive security policies.
- Accelerate identification and resolution of problems with a prioritized, real-time list of experience-related anomalies.
- Combine robust telemetry across devices, virtual desktops, and applications with user data.

Key features for government	Important certifications
• Manage multiple operating systems, device types, and mobile deployments from a single admin console. • Prevent unauthorized devices from entering mobile environment with strict enrollment policies and security. • Manage devices by geographic function, role, and location with strict role-based access controls. • Secure and track devices with FIPS 140-2 validated modules and automated compliance engine. • Meet security requirements for installation on DOD networks with STIG approval. • Enforce strict security settings specific to employee function with highly scalable, multitenant architecture. • Secure management and distribution of internal and public apps available to employees for official use. • Maximize data loss prevention and secure content collaboration. • Encrypt, secure, and containerize email as an alternative to native email clients on devices.	• NIAP Common Criteria Security Certification • FIPS 140-2 and 140-3 • NIST MIP, CMVP • DISA STIG • CSA STAR Level 1, CAIQ • C5 Certified • Cyber Essentials Plus • G-Cloud Certified • ISO 27001 – Information Security Management Compliant • ISO 27017 – Cloud Specific Information Security Guidance Compliant • ISO 27018 – Cloud Specific Standard for Protecting Personally Identifiable Information (PII) Compliant • ISO 9001 Quality Management Systems Compliant • PCI DSS Compliant • SOC 1, SOC 2, SOC 3 Compliance • DOD CC SRG IL2 • DOD CC SRG IL5 • FedRAMP Authorized • StateRAMP Authorized

Modernize without compromise

With Omnissa, you can enhance IT efficiencies, drive innovation, and deliver a better experience to government employees—all while maintaining the highest security standards to protect sensitive government data. Now's the time to meet today's challenges head-on, and bring new levels of efficiency, productivity, and security to your government agency.

Get started

To learn more about how Omnissa can help your government agency operate more securely and efficiently, visit the **Public Sector Tech Zone** or **contact** an Omnissa representative today.

omnissa™