Government on Demand Means Simple, Secure Fleet Management

On the heels of advances in digital government come equally sophisticated security threats, with government agencies being a top target for ransomware attacks. However with the need for government on demand, government cloud market size is expected to grow upwards of $28.8B by 2022[1]. In addition, government agencies are reporting significant benefits from cloud integration, including better citizen experiences and lower IT costs.

Bridging physical and digital workflows, print infrastructures are especially prone to cyberattacks, making secure fleet management a top priority. With a continuum of capabilities, we designed Xerox® Intelligent Workplace Services to go beyond Managed Print Services (MPS). Not only does it optimize your print infrastructure, it also provides end-to-end security.

TURNING DATA INTO OPPORTUNITY WITH FLEET MANAGEMENT ANALYTICS.

With easy-to-navigate dashboards, our fleet management analytics puts the information you need to stay productive and cost efficient at your fingertips. Data visualizations make it easy to turn information into actionable insights.

FULLY VETTED, FEDRAMP-AUTHORIZED CAPABILITIES YOU CAN COUNT ON.

As the first vendor in our class with FedRAMP authorization, we offer the safest, most reliable and trusted services you need to protect citizen data, navigate change and stay productive.

[1] **Government Cloud Market by Solution (Cloud Storage, Disaster Recovery, Identity and Access Management, Risk and Compliance Management), Service, Service Model (IaaS, PaaS, SaaS), Deployment Model, and Region – Global Forecast to 2022**
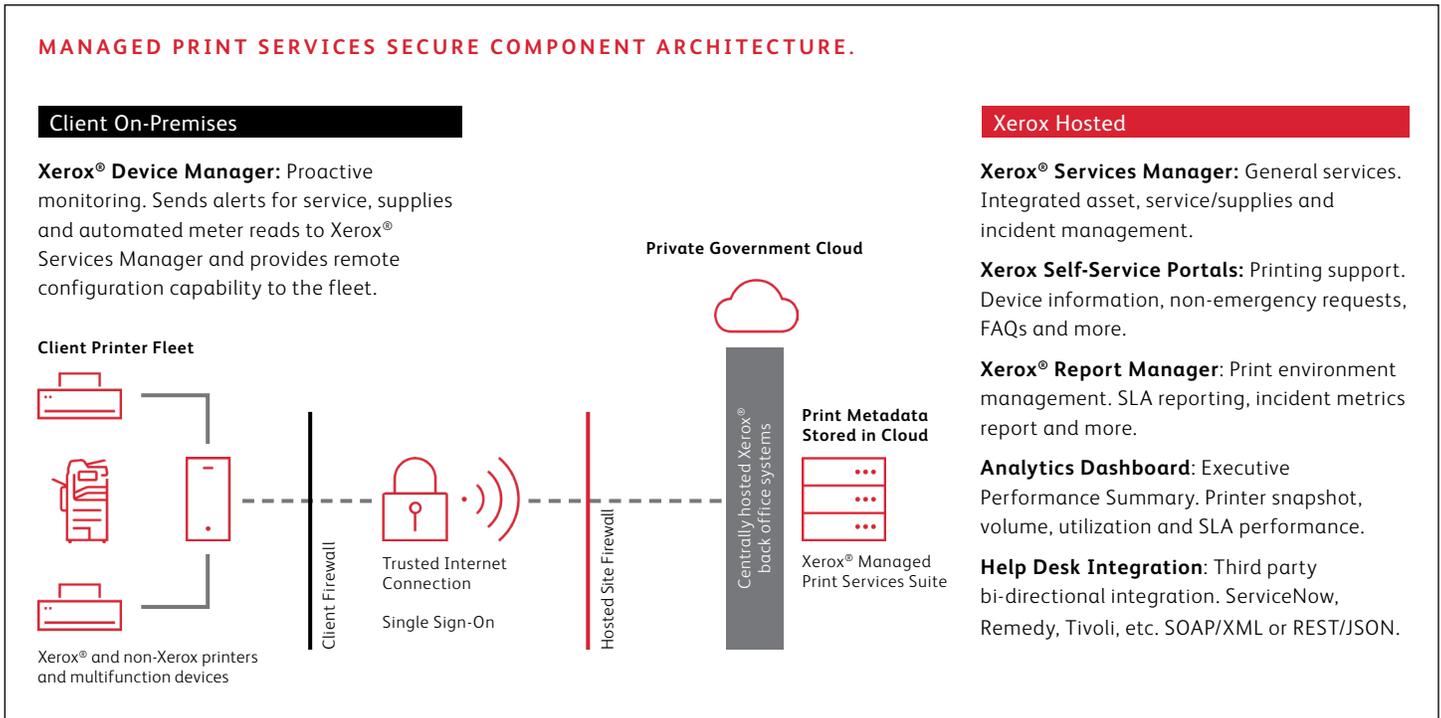
xerox™

Do more with multi-layered security.

We provide centrally hosted back office systems that are ISO 27001 certified and use secure HTTPS port 443. In addition, Xerox is FIPS 140-2 and FIPS 199 compliant, meeting over 325 technical, managerial and operational controls under NIST 800-53. And our MPS solution covers both Xerox® and non-Xerox devices.

MANAGED PRINT SERVICES SECURE COMPONENT ARCHITECTURE.

Client On-Premises

Xerox® Device Manager: Proactive monitoring. Sends alerts for service, supplies and automated meter reads to Xerox® Services Manager and provides remote configuration capability to the fleet.

Client Printer Fleet

Xerox® and non-Xerox printers and multifunction devices

Client Firewall

Trusted Internet Connection

Single Sign-On

Hosted Site Firewall

Private Government Cloud

Centrally hosted Xerox® back office systems

Print Metadata Stored in Cloud

Xerox® Managed Print Services Suite

Xerox Hosted

Xerox® Services Manager: General services. Integrated asset, service/supplies and incident management.

Xerox Self-Service Portals: Printing support. Device information, non-emergency requests, FAQs and more.

Xerox® Report Manager: Print environment management. SLA reporting, incident metrics report and more.

Analytics Dashboard: Executive Performance Summary. Printer snapshot, volume, utilization and SLA performance.

Help Desk Integration: Third party bi-directional integration. ServiceNow, Remedy, Tivoli, etc. SOAP/XML or REST/JSON.

XEROX IS THE FIRST FEDRAMP-AUTHORIZED SUPPLIER.

With a holistic approach to security and best-in-class, built-in security features, Xerox is the only FedRAMP-authorized supplier that has Printer Security Management. Xerox® Printer Security Audit Service delivers comprehensive, multi-layered security that includes:

Security configuration: A policy-based compliance solution that automates print fleet security by configuring device settings to your security standards baseline. It provides ongoing reporting to show compliance and highlight gaps.

Password management: Part of automated print fleet security

management that allows you to stay safe and steps ahead of cyber threats.

Firmware management: Proof of compliance with security standards with full reporting and historical information on any firmware update activities.

Certificate management: Part of our remote configuration capabilities, an automated process to deploy and configure device certificates signed by a certificate authority. A policy can be created to push out a new device certificate on a scheduled basis, preventing certificate expiration.

Security monitoring: Security Information and Event Management (SIEM) integrations allow security events to be managed through a single dashboard,

providing quick access to the detailed information administrators need to respond to events faster than ever.

WE HELP GOVERNMENT DO IT ALL.

With decades of experience in helping governments manage change, we're uniquely positioned to help governments navigate the new challenges and pressures of now while keeping citizens connected, informed and safe.

From mail processing to seamless citizen communications, Xerox® Intelligent Workplace Services is just one out of several customizable services and solutions we offer agencies across all levels of government.

Safer print infrastructure, better citizen experiences.
Our services help you protect data, cut costs and streamline workflows so employees can focus on what matters most: delivering better citizen services that drive satisfaction. Learn more at **xerox.com/IntelligentWorkplace**.

xerox™