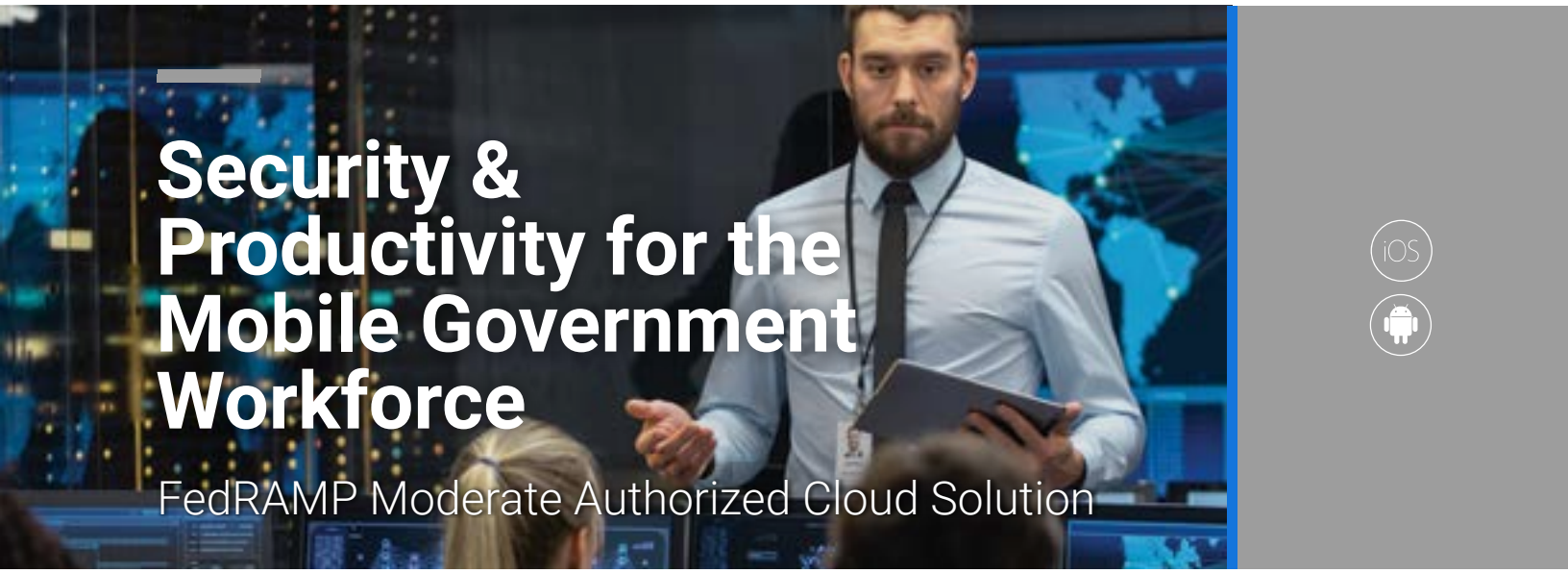

Security & Productivity for the Mobile Government Workforce

FedRAMP Moderate Authorized Cloud Solution

The Challenge of Conducting America's Business in These Unprecedented Times of Uncertainty

After the global pandemic outbreak, the U.S. government agencies have been tasked to conduct America's business remotely using both Government-issued devices and BYO devices. With the pervasive use of mobile devices and fast BYOD deployment, government employees can keep operating remotely and instantly communicate via text, email, and chat or access behind-the-firewall applications anywhere in the world. But these technologies and personal devices have also expanded the threat of cyberattacks, with ever-present hackers and rogue entities developing sophisticated, malicious methods to breach secure systems, and many government agencies are challenged to meet the stringent security requirements for safeguarding and monitoring federal data during these uncertain times.

Cloud computing and digital communications dominate the modern landscape, offering the ability to speed the flow of information, streamline processes, and fast-track new service offerings. Having a FedRAMP authorized cloud solution can help the U.S. government agencies prepare for the new normal.

The Benefits of FedRAMP

The federal government fully understands the benefits of cloud computing and, more importantly, a cloud-first strategy:

- Streamlined technology footprint within each agency.
- Eliminated costs of acquiring and maintaining on-premises hardware and software.

- Reduced cybersecurity overhead by shifting monthly compliance reporting, annual reassessments, and maintenance burdens from the government agency to the cloud service provider.

Federal agency cloud service providers must be certified and authorized by the Federal Risk and Authorization Management Program (FedRAMP) Program Management Office (PMO). This rigorous cybersecurity process validates that a cloud solution fully meets the federally-mandated, standardized approach to security assessment, authorization, and continuous monitoring for cloud products.

Introducing BlackBerry Government Mobility Suite

Hosted on the FedRAMP-approved Microsoft Azure Government platform, BlackBerry Government Mobility Suite is a FedRAMP-Moderate-certified, end-to-end cloud-based solution to securely manage endpoints and protect sensitive data

FIPS 199 System Categorization	Service Model	Deployment Mode	Cloud Stack	Offered in FedRAMP Marketplace
Moderate	SaaS	Government-Only Community	Microsoft Azure Government, Akamai FastDNS	Yes

sent via email and text, whether in transit or at rest. The solution also enables government employees and designated contractors to access applications behind the agency firewall to efficiently and securely work, communicate, and collaborate to conduct the business of the U.S. government.

BlackBerry Government Mobility Suite is based on BlackBerry Secure UEM & Productivity solutions and is specifically designed to meet the needs of U.S. federal agencies and contractors.

Single, Integrated Management Console
Based on a trusted end-to-end security model, the solution provides a flexible and centralized console to manage security policies that connect and protect:

- **Users**—regardless of location around the globe
- **Endpoints**—smartphones and tablets (government-issued or personally owned)
- **Applications**—custom and third-party
- **Operating systems**—iOS®, Android™

Mobilize Your Workforce
Allow employees to access business applications behind the firewall and ensure employees are productive wherever they are with seamless, secure integration to Microsoft® Office 365, on-premise Microsoft Exchange® infrastructure, SharePoint®, and OneDrive® for Business.

Secure Business Productivity
Boost employee productivity with a full array of apps for emailing, calendaring, instant messaging, collaborating, mobile web browsing, document editing, and task managing.

Streamlined, Flexible Identity and Access Management
BlackBerry Government Mobility Suite offers multiple security options for browser access, including Kerberos and SAML, as well as integrations with Microsoft Active Directory and KPI. More advanced capabilities are also available with single sign-on, token-based two-factor authentication, and complete cloud federation. The robust solution allows the agency's IT team to configure devices based on highly-specific authorizations for identity, role, and device functionality (e.g. allowing or turning off the camera on individual smartphones). Devices can be partitioned so employees and contractors can work securely to conduct government business and still use the phone or tablet as a personal device.

Lower TCO
By migrating to FedRAMP-authorized cloud technologies, federal agencies and contractors can eliminate the burden of deploying, managing, and upgrading on-premises hardware and software; simplify mandated cybersecurity monitoring and reporting overhead; decrease security-related costs; and reallocate IT staff to other strategic projects.

Trusted Technology Advice
The BlackBerry approach to support goes beyond issue resolution. With a highly trained, experienced account and support team, you can turn to BlackBerry as a trusted advisor for proactive guidance when planning a change to your mobility environment and get customized strategies from BlackBerry® Enterprise Consulting and BlackBerry® Cybersecurity Consulting experts.

BlackBerry's U.S. Cybersecurity Operations Center

The solution is deployed in the Microsoft Azure Government Community Cloud and is managed by the BlackBerry U.S. Cybersecurity Operations Center (CSOC). Based in Washington, D.C. and staffed with U.S. citizens, the CSOC is focused on providing the best level of service for BlackBerry government customers and will oversee all FedRAMP security functions, required monthly reporting, and annual reassessments.

FedRAMP-Ready: BlackBerry Government Mobility Suite

Learn more at https://www.blackberry.com/us/en/solutions/fedramp.

About BlackBerry

BlackBerry (NYSE: BB; TSX: BB) is a trusted security software and services company that provides enterprises and governments with the technology they need to secure the Internet of Things. Based in Waterloo, Ontario, the company is unwavering in its commitment to safety, cybersecurity, and data privacy, and leads in key areas such as artificial intelligence, endpoint security and management, encryption, and embedded systems. For more information, visit BlackBerry.com and follow @BlackBerry.