BlackBerry AtHoc

Redefining Secure Crisis Communications with FedRAMP High Authorization

Executive Summary

Reliable and secure communication during critical events is vital in any organization. BlackBerry® AtHoc®, a critical event management platform, redefines secure communication during crises by achieving FedRAMP High authorization. This achievement underscores the ability of BlackBerry AtHoc to protect sensitive data while ensuring business continuity in the face of cyberattacks, natural disasters, and other operational disruptions.

With over 421 stringent security controls, FedRAMP High sets the highest bar for safeguarding critical organizations such as government agencies and critical infrastructure operators. For users of the BlackBerry AtHoc platform, this means uninterrupted, encrypted communication, operational resilience, and rapid recovery.

BlackBerry AtHoc provides real-time situational awareness, centralized command and control, and compliance with global security standards. It enables organizations to prepare for, respond to, and recover from critical events without compromising security compliance.

This white paper explores the importance of FedRAMP High authorization in relation to BlackBerry AtHoc. It details the milestones BlackBerry AtHoc has reached in achieving FedRAMP High certification, underscoring the dedication of BlackBerry in delivering secure and trustworthy communication during crises.

Navigating the Complexities of Secure Communication in a High-Risk Landscape

Modern organizations operate in a heightened threat landscape where secure and reliable communication is non-negotiable. Sophisticated cyberattacks, extreme weather events, unpredictable mass gatherings and public safety emergencies place an unprecedented strain on organizations operating within complex compliance requirements.

- **Cybersecurity Threats:** Advanced persistent threats (APTs), ransomware, and insider risks jeopardize the confidentiality and integrity of organizational data.
- **Compliance Pressures:** Regulatory mandates, such as FedRAMP or industry-specific standards (e.g., HIPAA or GDPR), demand stringent security controls and continuous compliance vigilance.
- **Operational Risks:** Public safety, financial stability, and infrastructure reliability can be jeopardized when communication channels fail during crises.

Organizations need a critical event management platform that addresses these vulnerabilities with robust encryption, secure identity management, and compliance with the most stringent global security protocols.

Understanding FedRAMP

The Federal Risk and Authorization Management Program (FedRAMP) is a U.S. government initiative that standardizes the security assessment and authorization for cloud-based SaaS solutions. FedRAMP provides a robust framework that helps government and private organizations use secure cloud technologies to protect the most sensitive data while remaining compliant. Achieving FedRAMP authorization involves a rigorous process that requires organizations to demonstrate that their cloud services offering meets an exacting set of federal security and privacy standards.

Levels of Authorization

FedRAMP divides its certification into three distinct authorization levels based on the sensitivity of the data a system handles.

FedRAMP Low	• For cloud solutions managing non-sensitive, publicly available data, such as public-facing websites or platforms with minimal security risks. • Represents 7% of all FedRAMP authorizations.
FedRAMP Moderate	• For systems storing and processing data critical to organizational operations. Solutions that manage moderately sensitive information, such as personally identifiable information (PII), fall under this category. • Represents 76% of all FedRAMP authorizations. • BlackBerry AtHoc achieved FedRAMP Moderate authorization in 2017.
FedRAMP High	• For systems managing highly sensitive data, such as Controlled Unclassified Information (CUI). The loss of confidentiality, integrity, or availability in these systems can have severe or catastrophic impacts on national security, public safety, or organizational operations. • Represents 17% of all FedRAMP authorizations. • BlackBerry AtHoc achieving FedRAMP High involves compliance with 421 security controls outlined in NIST SP 800-53, making it the most demanding level of authorization.

The FedRAMP Authorization Process

Achieving FedRAMP authorization entails a rigorous evaluation process, requiring Cloud Service Providers (CSP) to validate that their cloud service offerings are compliant with 421 federal security and privacy standards outlined in NIST SP 800-53. These controls protect sensitive data with precision and resilience. FedRAMP authorization is comprised of the following steps:

1. **Sponsorship:** A federal agency must sponsor the CSP or the provider must proceed via the Joint Authorization Board (JAB) Provisional pathway. For agency-sponsored authorizations, the agency works with the vendor throughout the security assessment process.
2. **Initial Review by 3PAO:** A FedRAMP-accredited third-party assessment organization (3PAO) independently evaluates the service. This includes testing components such as encryption

protocols, access controls, and system resiliency to ensure compliance with FedRAMP's stringent criteria.

3. **Authorization to Operate (ATO):** Following the evaluation, the CSP submits a detailed Security Assessment Report (SAR) to the sponsoring agency or JAB. If approved, the product is granted an Authority to Operate (ATO) at the designated impact level (Low, Moderate, or High).
4. **Continuous Monitoring:** Authorization does not mark the end of compliance efforts. FedRAMP mandates continuous monitoring measures, including recurring vulnerability scans, routine audits, and security updates to ensure sustained protection and compliance over time.

Significance of FedRAMP High Authorization

Securing FedRAMP High authorization signifies compliance, underscoring a Cloud Service Provider's readiness to meet the most stringent security and operational standards. This certification demonstrates a provider's capability to address advanced threats, mitigate risks from nation-state actors, and safeguard sensitive information from insider and sophisticated attacks vectors.

Key Components of FedRAMP High:

- **Enhanced Security Controls:** FedRAMP High incorporates 96 additional controls beyond the Moderate level, covering critical areas such as end-to-end encryption, continuous environmental monitoring, and granular event logging to facilitate forensic investigations. It mandates rapid incident response mechanisms and requires thorough personnel vetting, including background checks for individuals with privileged access.
- **Operational Resilience:** Stricter recovery time objectives (RTOs) and recovery point objectives (RPOs) ensure minimal downtime and data integrity in critical systems. Frequent, comprehensive audits reinforce ongoing operational readiness, providing unmatched reliability across infrastructures.
- **Nation-State Threat Mitigation:** Advanced threat intelligence and response mechanisms are integral to countering highly sophisticated adversaries. These capabilities are essential for organizations managing sensitive data or operations frequently targeted by nation-state actors.

FedRAMP High authorization is vital for any system where uncompromising reliability is crucial to maintaining public safety, national security, or core organizational operations. It is a non-negotiable requirement for specific U.S. federal systems and a key advantage for sectors that demand unparalleled assurance in their security frameworks.

Industries and Systems Benefiting from FedRAMP High Authorization

Law Enforcement and Emergency Services	Platforms supporting real-time coordination of responses to public safety threats or critical incidents.
Financial Institutions	Systems safeguarding critical financial data and sensitive transactions, ensuring financial stability.
Healthcare Providers	Infrastructure managing protected health information (PHI) and enabling emergency medical operations.

Critical Infrastructure	Systems supporting essential utilities, energy grids, and transportation integral to public welfare.
Enterprises Handling CUI	Businesses entrusted with sensitive government data or intellectual property requiring the highest levels of confidentiality and protection against breaches.

Why FedRAMP Matters

FedRAMP establishes a rigorous framework for secure cloud operations, ensuring cloud service providers meet advanced security and operational benchmarks. It is not just about compliance but reflects a provider's ability to safeguard sensitive data and respond swiftly to complex cybersecurity threats.

By choosing FedRAMP-authorized solutions, organizations gain access to critical features like robust encryption and continuous monitoring, which are imperative for maintaining system integrity and operational resilience. This level of assurance is particularly vital in industries where accountability and data protection are essential.

BlackBerry AtHoc, with its FedRAMP High certification, exemplifies this commitment to security and reliability. It empowers organizations to confidently operate in high-risk environments, ensuring stability and trust while meeting the highest standards of operational excellence.

BlackBerry AtHoc: Engineered for Resilience and Security

BlackBerry AtHoc is an advanced critical event management platform, purpose-built to deliver unmatched security and reliability when it is needed most. Designed to keep organizations operational in high-stakes scenarios, BlackBerry AtHoc facilitates secure communications, coordinated action, and real-time responses in the face of disruptions such as cyber threats, natural disasters, or operational crises.

Key Capabilities of BlackBerry AtHoc

- **Secure, Resilient, Two-Way Communication:** BlackBerry AtHoc enables organizations to send and receive secure, encrypted messages across multiple channels, enabling uninterrupted communication even under extreme conditions.
- **Real-Time Incident Insight and Situational Awareness:** With comprehensive data and actionable insights, BlackBerry AtHoc empowers decision-makers with the knowledge to inform rapid and effective responses during a crisis, minimizing delays and ensuring timely action in critical moments.
- **Streamlined Emergency Planning and Automation:** Robust workflows, task assignments, and pre-configured messaging templates to streamline and automate crisis management processes, reducing the chaos in the most challenging times.
- **Centralized Command and Control:** Seamless integration with diverse devices, communication channels, and third-party systems enables unified and efficient management with all stakeholders during critical events.

BlackBerry AtHoc provides an unparalleled lifeline, helping organizations maintain operational continuity during events when traditional communication systems fail or cannot be trusted.

Regulatory Leadership and Trust

BlackBerry AtHoc sets a benchmark for meeting the most rigorous compliance standards in the industry, reinforcing its commitment to security, reliability, and operational excellence. It integrates with FEMA's Integrated Public Alert & Warning System (IPAWS) and Canada's National Public Alerting System (NAAD), affirming its role in delivering critical public safety alerts. The platform is both FedRAMP- and GovRAMP-authorized, ensuring that it complies with strict federal and state security requirements.

With its achievement of FedRAMP High authorization, BlackBerry AtHoc sets a gold standard for resilience and assurance for government agencies and enterprises with stringent security demands.

Real-World Use Cases

Incident Response Coordination During Cyberattacks

- **Challenge:** Ransomware attacks and data breaches require a coordinated and secure response to mitigate operational impacts. Without secure communication channels, response teams risk exposing sensitive strategies to threat actors.
- **Solution:** BlackBerry AtHoc provides a secure, encrypted communication platform that enables real-time collaboration among internal security teams, executives, and trusted vendors. It eliminates the risk of intercepted communications, enabling organizations to maintain the confidentiality of their response plans and tactics.
- **Outcome:** Organizations can respond to incidents more quickly, minimize downtime, and limit potential damage, ensuring operational continuity and resilience during cyberattacks. This approach fosters seamless collaboration between security teams, executives, and trusted vendors, enabling a more effective and unified response.

Executive Communication and Collaboration During Crises

- **Challenge:** Critical situations, including legal investigations, financial crises, or sensitive negotiations, require absolute confidentiality to protect organizational interests and maintain trust. Standard communication tools are insufficient for these high-stakes scenarios.
- **Solution:** BlackBerry AtHoc serves as a highly secure communication hub for executives, equipped with robust encryption and strict access controls. This ensures sensitive communications are restricted to authorized personnel only, reducing the risk of unauthorized access or data leaks.
- **Outcome:** Executives can confidently make critical decisions, align on strategies, and collaborate effectively during high-pressure situations while maintaining the integrity and security of their communications.

Natural Disaster Recovery Coordination

- **Challenge:** Natural disasters like hurricanes, wildfires, and floods often disrupt traditional communication channels, complicating recovery plans and leaving teams unable to coordinate effectively.
- **Solution:** BlackBerry AtHoc delivers a resilient communication framework that operates in even the most adverse conditions. It enables organizations to rapidly disseminate updates, activate business continuity plans, and coordinate efforts with employees, emergency responders, and partners across affected areas.

- **Outcome:** Organizations can minimize downtime, protect assets and lives, and streamline recovery efforts, fostering a more resilient response in the aftermath of natural disasters.

Safeguarding Sensitive Customer Communications

- **Challenge:** Organizations managing high-profile customers or VIPs must ensure the privacy of sensitive communications, especially during outages, crises, or tailored service responses.
- **Solution:** BlackBerry AtHoc offers a secure and compliant platform for managing these critical interactions. Built with advanced encryption and regulatory compliance in mind, the platform safeguards conversations and ensures data confidentiality.
- **Outcome:** Organizations can build stronger customer relationships while ensuring contractual and regulatory obligations. This enhances trust, strengthens reputation, and ensures service reliability, particularly in highly regulated industries like healthcare and finance.

High-Stakes Product Launches and Press Releases

- **Challenge:** Coordinating the launch of flagship products or releasing critical financial information requires precision and total discretion to prevent leaks, sabotage, or premature disclosures.
- **Solution:** BlackBerry AtHoc provides a secure collaboration platform with advanced encryption and restricts access to unauthorized participants. Teams can collaborate on strategies, supplier arrangements, and sensitive press release details, knowing that their communications are protected.
- **Outcome:** Organizations can safeguard intellectual property, prevent premature disclosures, and execute high-impact initiatives with confidence and control.

Talk to an expert

Contact us today to learn more about AtHoc or visit blackberry.com/securecomms

ABOUT BLACKBERRY

BlackBerry (NYSE: BB; TSX: BB) provides enterprises and governments the intelligent software and services that power the world around us. Based in Waterloo, Ontario, the company's high-performance foundational software enables major automakers and industrial giants alike to unlock transformative applications, drive new revenue streams and launch innovative business models, all without sacrificing safety, security, and reliability. With a deep heritage in Secure Communications, BlackBerry delivers operational resiliency with a comprehensive, highly secure, and extensively certified portfolio for mobile fortification, mission-critical communications, and critical events management.

For more information, visit BlackBerry.com and follow @BlackBerry.