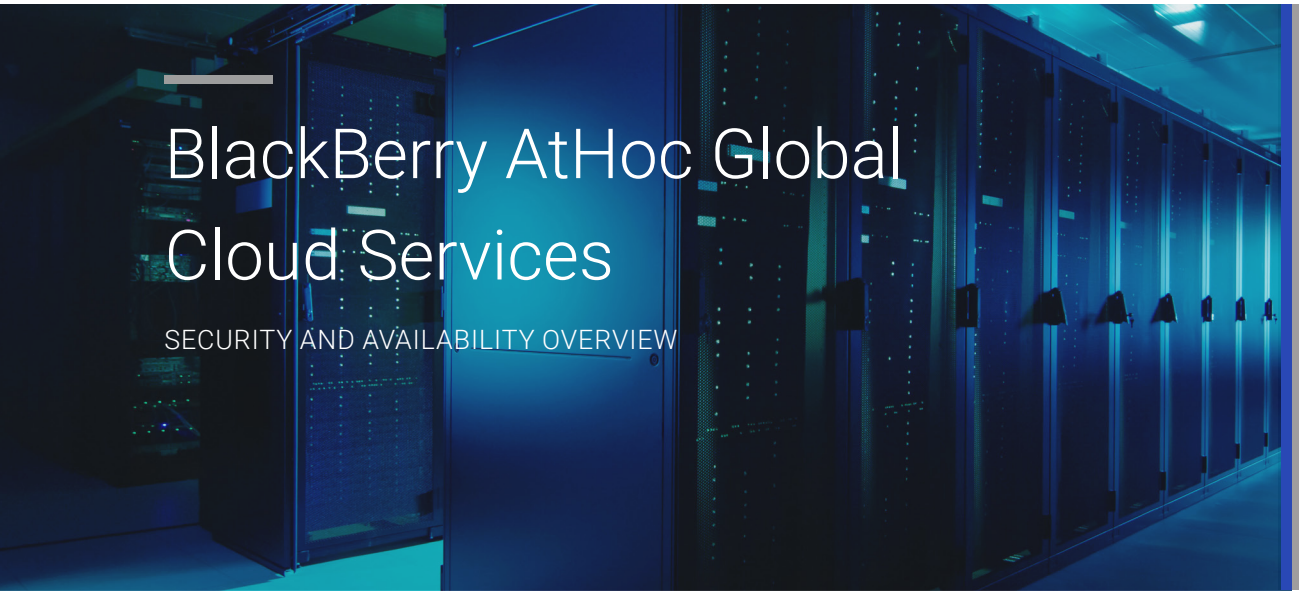


BlackBerry AtHoc Global Cloud Services

SECURITY AND AVAILABILITY OVERVIEW

BlackBerry AtHoc

Availability Overview

BlackBerry AtHoc is a FedRAMP-authorized mass communication solution and a networked platform enabling corporations and government agencies to communicate around the world and collaborate securely with their personnel and with other organizations through multiple devices. BlackBerry AtHoc is a prime provider of interactive mass communication solutions to governments globally and leading industrial, transportation and commercial enterprises.

BlackBerry AtHoc Global Cloud Service is designed to provide an unprecedented level of customizable features, from comprehensive end-to-end mass communication to secure accountability service. BlackBerry AtHoc Global Cloud Services features:

- Complies with applicable privacy regulations
- Flexible deployment options that don't compromise your security needs
- Integration with on-premise emergency communication services and systems
- Provides free unlimited support
- Delegate system management to local points of contacts (PoCs) while maintaining control

AtHoc Global Cloud Service is designed to serve global customers outside of the US, specifically customers in Europe and in Canada.
BlackBerry AtHoc is providing a US-based service for US based customers; please contact BlackBerry sales for additional details.

Security Framework, Compliance and Auditing

BlackBerry AtHoc Global Cloud Services are ISO 27001 certified as a SaaS service, under BlackBerry Corporate ISO 27001 certification. This certification means the BlackBerry AtHoc Global Cloud services have passed a rigorous security and risk management review.

ISO/IEC 27001:2013
ISO/IEC 27001 provides a model for establishing an information security management system (ISMS), which aligns people, resources, and controls, to create a series of measurable security practices to protect information assets. BlackBerry has an established record of integrating secure practices. In 2002, BlackBerry was one of the first organizations in North America to receive accreditation against the BS7799 Security Standard. This standard was later adopted by the International Standards Organization as ISO/IEC 27001:2005 and, most recently, ISO/IEC 27001:2013. This makes BlackBerry the only supplier of emergency mass notification technology to receive the SAFETY Act Designation. Get more details

SAFETY Act Designation
In 2013, BlackBerry AtHoc was awarded the SAFETY Act designation by DHS. The BlackBerry AtHoc networked platform was the first emergency mass notification system to receive a SAFETY Act designation as a Qualified Anti-Terrorism Technology (QATT). BlackBerry AtHoc customers are now protected against property or personal injury claims. BlackBerry AtHoc is deployed across DHS itself in the U.S. Coast Guard, the Transportation Security Administration (TSA), and Customs and Border Protection.

Data Centers

BlackBerry AtHoc Global Cloud Services are globally hosted in highly reliable, advanced Microsoft Azure data centers.

- Specifically,
- Hosting UK customers from redundant Azure data centers in the UK
- Hosting North European customers from redundant Azure data centers in Ireland
- Hosting West European customers from redundant Azure data centers in Netherlands
- Hosting Canadian and global customers from redundant Azure data centers in Canada

Microsoft Azure is SSAE-18 SOC 1 and SOC 2 Type II Certified, Cloud Security Alliance (CSA) STAR Attestation and ISO 27001 certified

- These certifications are widely recognized and indicate that the Azure services, processes and facilities has been comprehensively reviewed and meets stringent security standards.
- More information on the security and governance of the Microsoft Azure environment may be found here.

24/7 Internal Network and Security Operations Centers

BlackBerry's monitoring practices include:

- BlackBerry AtHoc Global Cloud Services are 24/7 monitored by a Canadian based manned Network Operation Center (NOC) and Security Operation Center (SOC)
- The monitoring covers 24/7 continuous security and operations monitoring
- NOC and SOC are providing 24/7 response by trained personnel

Redundancy and Service Availability

Data Center and Service Provider Redundancy

BlackBerry AtHoc Global Cloud Services are hosted at redundant and highly available data centers, which feature:

- Multiple communication vendors to diversify, protect against outages and ensure the continuity of operations during a failure without impacting alert delivery services.
- N-tier architecture with redundancies in the system (e.g., server components, databases, management components, etc.).
- Online data replication, which ensures that – should a system or a data center become unavailable – others are available to provide service.

Systems Redundancy and Contingency

BlackBerry AtHoc Global Cloud Services are configured with multiple logical nodes and multi-tier architecture to avoid single point of failure. In a catastrophic situation, the same configuration is maintained ("hot" and online) in a geographically separate data center in the same region. Data is replicated online to avoid data loss. Additionally, backup files are periodically copied across the protected sites within region, to support disaster recovery situations.

Service redundancy and disaster recovery readiness are tested at least twice a year.

Service Availability

BlackBerry AtHoc Global Cloud Services offer a minimum of 99.95% service availability. BlackBerry AtHoc consistently exceeds service-levels.

Network Security

Firewalls and Intrusion Detection
BlackBerry AtHoc has implemented strict firewall rules that allow access only to required and approved traffic only. BlackBerry AtHoc has also implemented intrusion detection, real-time monitoring and logging systems.

Independent Testing and Audits
BlackBerry regularly undertakes external third-party testing encompassing penetration testing, vulnerability scans and auditing against multiple industry security frameworks.

Network Access
Access to the network is limited and, on a needs-only basis. Access to network infrastructure is provided via multi-factor authentication.

External Systems
Access to the BlackBerry AtHoc Global Cloud Services environment from external systems or networks is prohibited.

Application Security

Development
BlackBerry AtHoc application is designed and developed with security in mind and using industry best practices and BlackBerry's deep experience with security engineering.

Developers are trained in following Open Web Application Security Project (OWASP) guidelines, embedding security principles into all stages of design and development. Use of third-party components, commercial and Open Source Software (OSS) is evaluated and vetted while considering security and supportability.

Encryption
BlackBerry AtHoc Global Cloud Services uses strong encryption via FIPS140-2 validated TLS 1.2 in the application to ensure **protection of data-in-transit** for all web-based communication. Communication to end user devices is implemented via industry standard protocols, such as text messaging, email and voice telephony, which may not use the same levels of encryption.

Application databases use FIPS 140-2 validated encryption to ensure **protection of data-at-rest**. Database backup files are protected and encrypted using same level of encryption to support protection of **data-in-storage.**

By using encryption, we minimize the chance of intruders intercepting potential Personal Identifiable Information (PII) – such as names and contact details used for mass communication - and other sensitive information.

Authentication and Passwords
BlackBerry AtHoc Global Cloud Services supports authentication via SAML 2.0. BlackBerry AtHoc services can also enforce strong passwords to comply with password management best practices.
Passwords and other sensitive fields are encrypted and/or hashed at transaction tier using FIPS 140-2 validated cryptography.
Unsuccessful access attempts are monitored by the application and system and respective accounts are automatically blocked after successive unsuccessful access failures per policy.

Data Storage and Retention Policies
Databases is continuously backed up in real time and stored on dedicated storage and replicated to a hot standby system in the regional redundant site. Periodic backups are stored online for three years.

Role Based Access Control (RBAC)
The BlackBerry AtHoc application employs a granular role-based access control framework, ensuring users and administrators are granted only privileges they need for their role and responsibilities.

Logging and Auditing
Application activities are logged at multiple levels, to provide full audit of system activity for monitoring and troubleshooting. The auditing function complies with applicable industry regulations and is hardened to prevent tempering with audit logs.

BlackBerry AtHoc application access and operator audit logs are available to customer's authorized users for review and download via the application console.

System Component Security

Hardening
System components are hardened following hardening guidelines by Center for Internet Security (CIS) Workbenches and / or DISA Secure Technical Implementation Guides (STIGs), including network devices, operating systems, databases servers, web servers and security components.

Authentication
System components admin access is done via Multi-Factor-Authentication (MFA).

System Auditing
System components logs are centrally collected, aggregated and correlated to detect distributed attacks and abnormal behavior patterns.

Vulnerability Scanning and Detection
BlackBerry AtHoc had implemented a multi-layer vulnerability scanning approach, to ensure vulnerabilities are identified as early as possible across the system, to include –

- Static Application Security Testing (SAST) on checked-in source code, to detect insecure coding practices
- Dynamic Application Security Testing (DAST) on applications prior to release and periodically on production systems to identify common vulnerabilities such as SQL and JavaScript Injections, or cross-site scripting
- External vulnerability scans are executed, at least monthly, from outside the BlackBerry AtHoc Global Cloud Services to detect attack vectors on the external system surface

- Internal vulnerability scans are executed internally, at least weekly, using credentialed scans on network components, operating systems and databases
- File integrity monitors are detecting unauthorized configuration changes to system components
- End point protection agents are installed on operating systems to detect and handle malware

Identified findings are reported, assessed, verified and action plans are put in place, based on Common Vulnerability Scoring System (CVSS) ranking and security posture analysis.

Additionally, BlackBerry security team regularly monitors public sources including US- CERT and vendor updates to identify vulnerabilities that are applicable to AtHoc Global Cloud Services systems.

System Management Process

Change Control

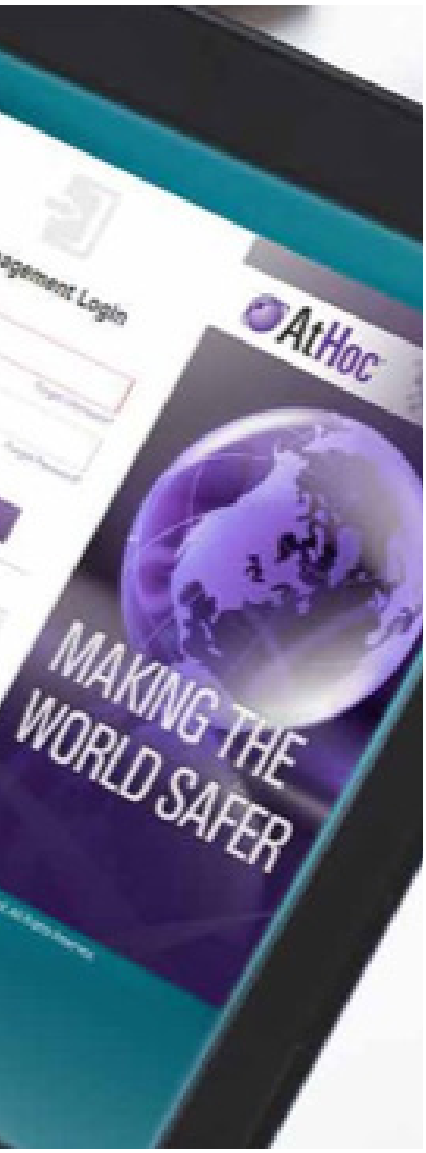
Updates to BlackBerry AtHoc Global Cloud Services are performed following strict change control processes, as led by its Change Control Board (CCB) including thorough analysis of implied security impact and risk assessment. Detailed records of applied changes are maintained.

Access to Customer Data

BlackBerry employees are not allowed access to hosted customers' data. In some cases, customers might explicitly grant select BlackBerry employees' access to their application and specific data; for example, for training or support purposes.

Incident Response

Incidents are managed in a well-defined Incident Response Process, which includes isolation, assessment, remediation, recovery and internal and external communication steps, as applicable to the situation. The BlackBerry Incident Response team is cross functional in order to provide end-to-end and timely action to the incident. Incident response activities are tracked and managed using automated workflow tools to ensure follow up and effective handling of the incident.



Employee Screening and Policies

BlackBerry employees, external contractors, security guards, janitorial services, and so on, are subject to background screening before an offer of employment. We have engaged with several third-party service providers who specialize in this area.

Background screening of candidates includes checking their social presence, education, certifications, and prior work experience, in addition to performing criminal and financial checks. Successful candidates are required to sign non-disclosure agreements and code of conduct agreements as a condition of hiring.

Employees are trained in both general and specific information-security procedures and the correct use of information processing facilities to minimize the likelihood of a security breach through our Security Essentials training, regular awareness communications, and targeted security campaigns. Our awareness program emphasizes that security and privacy are part of the employee's role at BlackBerry and that the employee has an obligation to act in a manner consistent with our security goals.

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.