BlackBerry AtHoc

Brochure

AtHoc Cloud Services

Security and Availability Overview

AtHoc is the pioneer and recognized leader in network-centric, interactive crisis communication. We serve the security, life safety and business continuity missions of commercial enterprises and government agencies worldwide. A trusted partner to the most demanding customers, AtHoc is the #1 provider of interactive crisis communication solutions to the U.S. Department of Defense, U.S. Department of Homeland Security and leading healthcare, industrial and commercial organizations.

Now, AtHoc is offering secure **AtHoc Cloud Services**, designed to provide an unprecedented level of customizable features, from comprehensive end-to-end crisis communication to secure communication service.

AtHoc Cloud Services features:

- Full compliance with federal security and privacy regulations
- Flexible deployment options that don't compromise your security needs
- Integration with on-premise emergency communication services and systems

Security Framework, Compliance and Auditing

- AtHoc Cloud Services is certified per NIST SP 800-53 Rev 3 (at a moderate FIPS 199 classification), complying with government and DoD security mandates
- NIST SP 800-53 certification goes beyond the typical SAS 70 Type II / SSAE 16 certification to include actual assessment of service security provisions:
    i. Continuous monitoring (per latest federal mandates)
    ii. Security scans and compliance with DISA (Defense Information System Agency) STIGs (Security Technology Implementation Guides)
    iii. Facility and system inspections
    iv. Failover testing
- Secure communications using AtHoc Cloud Services has been certified and accredited through the Defense Information Assurance Certification and Accreditation Program (DIACAP) by all Military Services (Army, Navy, Air Force and Marines)
- AtHoc Cloud Services is currently being evaluated for authorization under the Federal Risk and Authorization Management Program (FedRAMP)

Data Center Certifications

- AtHoc Cloud Services is hosted in highly reliable, advanced Equinix data centers in Santa Clara, CA and Ashburn, VA. They are separate from AtHoc business operations.
- Equinix hosting facility is a SSAE-16 SOC I Type II Certified and LEED Certified Data Center
- These certifications are widely recognized and indicate that this facility has been comprehensively reviewed and meets stringent security standards

Physical Security of Facilities

- 24/7/365 on-site security guard and technician
- Comprehensive security system monitors gates, doors, mantraps and alarmed doors
- Physical and biometric controls

Environmental Safeguards

Fire Detection and Suppression

To reduce risk, automatic fire detection and suppression equipment has been installed. This comprehensive system features:

- Smoke detection sensors in all data center environments
- Mechanical and electrical infrastructure spaces
- Chiller and generator equipment rooms
- Protection via either wet-pipe, double-interlocked pre-action or gaseous sprinkler systems

Power

The data center electrical power systems:

- Are designed to be fully redundant and 24/7/365 maintainable without impact to operations
- Feature uninterruptible power supply (UPS) units that provide backup power in the event of electrical failure
- Employ generators to provide backup power for the entire facility

Climate and Temperature Control

Climate control is required to maintain a constant operating temperature for servers and other hardware, which prevents overheating and reduces the possibility of service outages. Data centers are conditioned to maintain atmospheric conditions at optimal levels.

Monitoring systems and data center personnel ensure temperature and humidity are at appropriate levels.

Management

To ensure potential issues are immediately identified, data center staff monitor electrical, mechanical and life-support systems and equipment. Preventative maintenance is performed to maintain the continued operability of equipment.

Redundancy and Service Availability

Data Center and Service Provider Redundancy

AtHoc Cloud Services is hosted at redundant and highly available data centers, which feature:

- Multiple telecommunication carriers and aggregators to diversify, protect against outages and ensure the continuity of operations during a failure – without impacting alert delivery services. Any blocked or busy trunk forces traffic to the next available carrier and carrier circuits.
- N-tier architecture with redundancy at every point in the system (e.g., server components, databases, phone carriers, SMS carriers, ISP, etc.)
- Online data replication, which ensures that – should a data center become unavailable – others are available to provide service

System Redundancy

AtHoc Cloud Services is 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. All data is replicated online to avoid data loss. Service redundancy is tested on a quarterly basis.

Infrastructure Redundancy

AtHoc Cloud Services is a carrier-grade infrastructure that:

- Resides on fully redundant hardware, including ISP/DIA, routers, firewalls, switches, load balancers, all hardware nodes and dual power supplies
- Features hardware from Cisco, EMC, VMware, F5 and VCE / VBLOCK. The VBLOCK system by VCE is the world's most advanced infrastructure, and includes best-in-class components and the industry's most robust configuration.

VBLOCK systems are designed to deliver 99.999% uptime at hardware level.

Service Availability

AtHoc Cloud Services offers a minimum of 99.95% service availability. In the past three years, AtHoc has consistently exceeded the service-level agreements.

Network Security

Firewalls and Intrusion Detection

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

Independent Testing and Audits

AtHoc uses a third party to perform periodic independent penetration testing, vulnerability scans and audits.

Network Access

Access to the network is limited and on a needs-only basis. All access to infrastructure is provided via RSA 2 factor authentication.

Application Security

Encryption

AtHoc Cloud Services uses strong encryption via FIPS140-2 compliant SSL/TLS in our application. By using encryption, we minimize the chance of intruders intercepting username/passwords and/or other sensitive information.

Passwords

- All passwords and other sensitive fields are encrypted and/or hashed at transaction tier
- We enforce strong passwords via minimum length and complexity requirements, complying with DoD password management policy
- We monitor and manage unsuccessful trial blocks

Logging and Auditing

All activities are logged at multiple levels, to provide full audit of system activity for monitoring and troubleshooting.

The auditing function complies with applicable federal regulations.

Safety Act Designation

Based on our reliable software and infrastructure, AtHoc was awarded the Support Anti-Terrorism by Fostering Effective Technology (SAFETY) Act Designation by the Department of Homeland Security (DHS). And recognized as a Qualified Anti-Terrorism Technology (QATT). This makes AtHoc the only supplier of emergency mass notification technology to receive the SAFETY Act Designation. Get more details about: AtHoc's SAFETY Act Designation.

Data Storage and Retention Policies

All data is continuously backed up in real time and stored on dedicated SAN and in a hot standby system. Backups are stored online on separate disk space for one year.

Incident Management Policies

We have implemented service checks – some of which run as often as every minute – to advise us of abnormal activities. All system events are logged and unusual events are flagged for review by a member of our operations team.

All user actions are logged, which records user information.

Change Control

All updates to AtHoc Cloud Services are performed following strict change control processes, including thorough analysis of implied security impact and risk assessment. Detailed records of applied changes are maintained.

Access to Customer Data

As part of normal operations, AtHoc employees don't have access to customer data. In some cases, customers give certain employees access to their application and specific data.

Employee Screening and Policies

- All AtHoc employees undergo background checks and agree to company policies regarding security and acceptable use policies
- Access to AtHoc Cloud Services is on a need-only basis. All AtHoc employees that have such access undergo mandatory security awareness training and annual refresher training.
- Many employees hold U.S. Government and DoD security clearance
- Strict rules of behavior policy is enforced

Go to AtHoc.com or call 650-685-3000

About BlackBerry

BlackBerry is securing a connected world, delivering innovative solutions across the entire mobile ecosystem and beyond. We secure the world's most sensitive data across all end points – from cars to smartphones – making the mobile-first enterprise vision a reality. Founded in 1984 and based in Waterloo, Ontario, BlackBerry operates offices in North America, Europe, Middle East and Africa, Asia Pacific and Latin America. The Company trades under the ticker symbols "BB" on the Toronto Stock Exchange and "BBRY" on the NASDAQ. For more information, visit www.blackberry.com.