

2009 WHITE PAPER

Birst Security and Reliability

Birst is dedicated to safeguarding your information



 **Table of Contents**

Physical Security 3

System Security 4

Operational Security 4

Reliability 5

Data and Application Security 6

Certifications 7

Birst has passed the rigorous security audits of leading financial services companies and corporations in the Fortune 500.

Birst Security and Reliability

Birst is dedicated to safeguarding your information

To protect the privacy of its customers and the safety of their information, Birst maintains high standards of data security. Birst relies upon a state-of-the-art secure data center, enforces strict internal product controls, and regularly audits its policies and procedures using third party auditors.

The key tenets of Birst's security initiatives are:

- Security designed "from the ground up" in the application, network, hardware, and operational procedures
- A modern data center that is SAS 70 Type II certified and follows ISO 17799 policies
- Adherence to security best practices for code development, testing, and operations
- Regular external review of the policies and procedures for Birst security and operations
- Regular validation and testing of system security by third parties.

Birst has passed the rigorous security audits of leading financial services companies and corporations in the Fortune 500.

The following sections of this whitepaper cover the key areas of Birst security in detail, including: Physical Security, System Security, Operational Security, Reliability, and Data and Application Security.

Physical Security

A key aspect of security is the physical security of the hardware containing the customer data. Birst uses the leading hosting provider, Rackspace, for its data center. Rackspace has the following physical safeguards:

- Rackspace staff mans the data center 24 hours a day, 7 days a week
- Data center access is limited to Rackspace data center technicians
- Entry to the data center is regulated by biometric scans (e.g., hand geometry or iris scan) and man traps
- Interior and external security camera surveillance monitoring, with the tapes stored for review

Birst makes sure the networks and hardware containing the data are hardened and tested against attack.

- Unmarked facilities, to maintain a low profile
- Physical security audits by an outside firm

Further information about Rackspace's security policies and procedures is available at www.rackspace.com.

System Security

In addition to making sure that the infrastructure containing customer data is physically secure, Birst makes sure the networks and hardware containing the data are hardened and tested against attack. This includes:

- Hardware security requirements include:
 - › New hardware is provisioned with a hardened operating system (only necessary programs and services)
 - › Security patches are applied on a regular basis
 - › Provisioning follows documented policies and procedures
- All systems are firewall protected
- All public-facing machines are in a Demilitarized Zone (DMZ), in which a firewall separates public-facing from internal hardware
- An Intrusion Detection System (IDS) constantly monitors the internal network and provides weekly vulnerability scans of all internal machines
- Virus scanning and detection are on all machines
- Quarterly vulnerability testing is conducted by a third party, in compliance with Birst's Payment Card Industry Data Security Standard (PCI DSS) certification.
- All machines can only be accessed by named accounts, so that a detailed log of activities is available

Operational Security

It is not enough to have a security physical and network environment, they must be operated in a secure manner. Birst and Rackspace, working as a team, have the following operational security provisions:

- Rackspace (data center) operational security includes:
 - › ISO 17799-based policies and procedures that are regularly reviewed as part of the SAS 70 Type II audit process
 - › All employees are trained on documented information security and privacy procedures
 - › Multiple and thorough background security checks are conducted for all

In addition to securing your data, Birst ensures that it will be available when you need it.

- data center personnel
 - › Access to confidential information is limited to authorized personnel only, in accordance with documented processes
 - › Systems access is logged and tracked for auditing purposes
 - › Secure document destruction policies and procedures are followed
 - › Change management procedures are fully documented
 - › Disaster Recovery (DR) and Business Continuity (BC) plans are independently audited
- Birst Corporate operational security includes:
 - › Birst has fully documented policies and procedures that are independently reviewed
 - › All employees are trained on documented information security and privacy procedures
 - › Background checks are performed on all employees who have access to customer data
 - › Access to the production network is limited to authorized personnel, who access it using a secure, site-to-site Virtual Private Network (VPN)
 - › Access to customer data is limited to authorized personnel only, according to documented processes
 - › Independently reviewed Disaster Recovery and Business Continuity plans

Reliability

In addition to securing your data, Birst ensures that it will be available when you need it.

- Rackspace provides a very reliable infrastructure for the hosting of the Birst application
 - › 100% infrastructure and network uptime from Rackspace
 - › System redundancy is provided at all levels, to ensure that your data is still available even in those rare situations when the first line of defense falters. This includes redundancy for electrical power, HVAC (heating, ventilation and air conditioning), fire suppression, internet service, networking hardware, application hardware, and data storage.
 - » N+1 redundant HVAC (i.e., there is at least one independent backup component to ensure system functionality continues in the event of a system failure)
 - » Advanced fire suppression
 - » Power
 - N+1 redundant Uninterruptable Power Supply

Birst solutions have been designed from the ground up to protect the security of your information.

- Onsite and regularly tested diesel generators for utility outages, with onsite fuel storage
- » Network
 - Multiple Internet Service Providers (ISPs)
 - Fully redundant, enterprise-class routing equipment
- Intentional network underutilization, so that spikes are easily managed
 - Distributed Denial Of Service (DDOS) mitigation
 - › Replacement or repair of hardware within one hour
 - › Data support 24 hours a day, 7 days a week
- Regular backup of critical customer data is provided onsite and offsite via Iron Mountain, a leading provider
- All devices within the Birst production infrastructure are fully redundant, highly available (HA) configurations. All devices are hot swappable, requiring no down time for hardware failure and replacement.

Data and Application Security

A secure infrastructure cannot protect your data if the applications providing access to your data are not secure. Birst solutions have been designed from the ground up to protect the security of your information.

- Solution security
 - › User access to Birst involves three components: Identity, Authentication, and Authorization
 - » Identity – confirmed email address serves as the public identity of the user. Email address must be confirmed by the user after registration in order to be granted access to an account.
 - » Authentication – Customers access Birst via the website must complete password based authentication.
 - Passwords are never stored in cleartext, but are hashed using Secure Hash Algorithm-1 with a random salt, to ensure uniqueness and to defend against offline dictionary attacks.
 - Passwords can be reset, but never recovered.
 - » Authorization – the Birst solution contains administrator access controls that an account administrator can use to manage the breadth of functions and features available to their subscribers
 - › Communication encryption –VeriSign certificates secure all communication
 - › Birst documents all login (success and failure), logout, administrative, and database events for auditing
 - › Birst automatically locks account access after a number of failed login attempts within a specified period

Birst, Inc.

153 Kearny St., 3rd floor

San Francisco, CA 94108

www.birst.com

Email: sales@birst.com

Toll Free Phone: (866) 940-1496

› Security is built into our documented software development lifecycle, based upon guidelines from the Open Source Web Application Security Project (OWASP www.owasp.org) and SANS Institute (www.sans.org)

- Data deletion and account closure
 - › Birst employs deletion tools that meet or exceed the United States Department of Defense and National Security Agency requirements for secure deletion.
 - › Once a customer cancels their account with Birst, their information will be securely maintained for the period of time specified in their terms of service or contract. During this period, the customer can access their information only if they re-activate their account. After this period is concluded, the account data is permanently deleted from the Birst data center and is no longer accessible.

Certifications

- The Rackspace data center is SAS 70 Type II examined, and PCI and Safe Harbor certified
 - › For more information on SAS 70, please visit http://en.wikipedia.org/wiki/SAS_70
- Birst is Payment Card Industry Data Security Standard (PCI DSS) certified
 - › Payment Card Industry Data Security Standard (www.pcisecuritystandards.org)

If you have additional questions regarding Birst security safeguards and procedures, please contact the Birst sales team at:

Email: sales@birst.com

Toll Free Phone: (866) 940-1496