BUSINESS INTELLIGENCE

Birst security and reliability

Dedicated to safeguarding your information

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

The following sections of this white paper cover the key areas of Birst security in detail, including physical security, system security, operational security, reliability, and application and data security.

Birst has passed the rigorous security audits of leading financial services companies and corporations in the Global 1000.

The key tenets of Birst's security initiatives are:

- Security is designed from the ground up in the application, network, hardware, and operational procedures.
- Birst is SOC 2 Type 2 audited, HIPAA/HITECH attested, and **ISO-27001:2013 certified**.
- Modern Tier-4 data centers that are SOC 2 Type 2 audited and are ISO 27001 certified or follow ISO 27001 policies.
- Adherence to security best practices for code development, testing, and operations is followed.
- Regular external review of the policies and procedures for Birst security and operations is conducted.
- Regular penetration and vulnerability testing by third parties is completed.
- Birst personnel maintain security and privacy certifications.

Birst has passed the rigorous security audits of leading financial services companies and corporations in the Global 1000.

Physical security

A key aspect of security is the physical security of the hardware containing customer data. Birst uses the leading hosting providers—INAP (US) and Amazon (EU and APAC)—for its data centers.

Birst data centers have the following physical safeguards:

- Data centers are staffed 24 hours a day, seven days a week.
- At INAP, data center access is limited to INAP technicians and the Birst operations team. At Amazon, data center access is limited to Amazon data center technicians only.
- Entry to data centers is regulated by photographic identification, biometric scans, man traps, and secured shipping/receiving areas isolated from the data center floor.
- Interior and external security camera surveillance monitoring, with the video stored for review.
- Unmarked facilities maintain a low profile.
- Physical security audits are conducted by third parties.

Further information about Birst data center operations, security policies, and procedures is available at:

- **https://www.inap.com/data-centers/colocation/secure-data-center/**
- **https://aws.amazon.com/compliance/**
- **https://aws.amazon.com/security/**

In addition to ensuring that the infrastructure containing customer data is physically secure, Birst ensures that the networks and hardware containing customer data are hardened and tested against attack.

Hardware security requirements include:

- New hardware is provisioned with a hardened operating system following documented procedures (for example: only necessary programs and services, default accounts disabled, default passwords changed, and all security patches applied).
- Security patches are applied on a regular basis
- All systems are firewall protected, with firewalls at multiple points in the network.
- All public-facing machines are in a demilitarized zone (DMZ), in which a firewall separates public-facing from internal hardware.
- Intrusion prevention systems and host-based intrusion detection systems constantly monitor the internal network, providing alerts to operations staff, daily status emails, and weekly vulnerability scans of all internal machines.
- Web application firewalls (WAF) are utilized.
- Virus scanning and detection on all machines, with signatures updated every 24 hours.
- 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 secure physical and network environment; they must also be operated securely. Birst and its data center providers work as a team and have the following operational security provisions.

Data center operational security includes:

- Policies and procedures that are SOC 2 Type 2 audited and ISO-27001:2013 certified.
- Access to confidential information is limited to authorized personnel only, by documented processes.
- All employees are trained on documented information security and privacy procedures.
- Multiple and thorough background security checks are conducted for all data center personnel.
- 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 and business continuity plans are independently reviewed and regularly tested.

Birst corporate operational security includes:

- Birst has fully documented policies and procedures that are independently reviewed.
- All employees are trained and tested (on hire and annually) on documented information security and privacy procedures. Regular updates on security are provided via email and forums.
- Background checks (on hire and annually) are performed on all employees who have access to customer data.

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

- Access to the production network is limited to authorized personnel, who access it using a secure, site-to-site virtual private network (VPN) with multifactor authentication through a jump server.
- Access to customer data is limited to authorized personnel only, according to documented processes.
- Disaster recovery and business continuity plans are independently reviewed and regularly tested.

Reliability

In addition to securing your data, Birst makes certain your data will be available when you need it:

- Birst data centers provide a very reliable infrastructure to host the Birst application.
- 100% infrastructure and network uptime is ensured.
- Distributed denial of service (DDOS) mitigation is provided.
- Support 24 hours a day, seven days a week is guaranteed.
- Regular backup of critical customer data is provided. Backups are encrypted using industry standard strong encryption and stored on disk both onsite and offsite at the appropriate regional Birst disaster recovery site.
- 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.

Additionally, system redundancy is provided at all levels, to ensure that your data is still available even in those rare situations when components fail. This includes:

- N+1 redundant HVAC is provided (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 is available.
- Power—N+1 redundant uninterruptable power supply is available, including onsite and regularly tested diesel generators for utility outages, with onsite fuel storage, are available.
- Network—Multiple internet service providers (ISPs) are provided; fully redundant, enterprise-class routing equipment is included.
- Intentional network underutilization is utilized, so spikes are easily managed.

Application and data 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.

Application security

User access to Birst and your data is controlled by authentication and authorization.

Authentication

Authentication controls whether or not you can access Birst. This involves checking credentials, determining if the user is enabled, and if they are logged in from an allowed network.

- Customers can authenticate themselves to the Birst application via multiple routes: forms-based authentication (with support for RADIUS), Open ID Connect, SAML 2.0, integration with cloud portals (Salesforce and NetSuite), or custom single sign-on.

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

- Birst provides customers with full control over their password policies, including complexity, history, expiration, and change on first use.
- Birst automatically locks account access after a customer-configurable number of failed login attempts within a customer specified period.
- When Birst maintains credentials, they are never stored in clear text; they are hashed using PBKDF2 (with a minimum of 10,000 iterations) to defend against offline attacks.
- Birst can automatically disable account access after a customer configurable period since the last login.
- Birst logs all login attempts, logout, access to sensitive data, and administrative events for compliance auditing (self-service downloading).
- Passwords maintained by Birst can only be reset, never recovered.
- Birst supports customer configurable idle timeouts.
- Birst supports IP whitelisting so that customers can control from which networks that their users are allowed to access Birst.

Authorization

Authorization controls how the user can use the system and what they can view.

- The Birst solution contains role-based access controls that administrators can use to control and manage the breadth of functions and features available to their end users.
- Birst administrators can define dashboard, report, row, and column level security to allow end users only to see the information that they are allowed to access.

Application development and testing

- Security is built into the Birst software development lifecycle, based upon guidelines from the **Open Source Web Application Security Project** and **SANS**.
- Birst development staff are regularly trained on secure coding.
- Birst runs manual and automated security tests and analyzes third-party libraries for security issues on each build, utilizing third-party web application vulnerability analysis on a continuous basis (**Whitehat Security**), penetration testing (Whitehat Security), and third-party static security analysis (**Veracode**) on major releases. Reports from the third-party scans can be provided upon request (also posted to the Birst user community).

Data security

- Customer data is fully encrypted during transit via TLS 1.1+ channels. The status of the Birst TLS 1.1+ support for all endpoints is validated daily and can be checked at any time via **Qualys SSL Labs**.
- Customer data is AES-256 encrypted at rest using self-encrypting storage.
- All customer data remains in the primary data center, with encrypted backups at the designated BC/DR location for the primary site.
- Birst logs logins (success and failure), all administration operations, access to sensitive data, queries, and all access to dashboards and reports.
- When a customer cancels their account with Birst, their data is permanently deleted from the Birst data center and is no longer accessible.

Certifications

Birst maintains a number of independent security-related audits and certifications.

- Birst is SOC 2 Type 2 audited (report provided upon request).
- Birst is ISO-27001:2013 certified (**https://cert.schellmanco.com/?certhash=bfvRQWEwLi4p**).
- Birst is HIPAA/HITECH attested (report provided upon request).
- EU-US Privacy Shield certification (**https://www.privacyshield.gov/participant?id=a2zt0000000GnPZAA0**).
- Birst personnel maintain security and privacy certifications, including CISSP, CCSP, CIPT, and CIPP/E.

Also, all Birst data centers are SOC 2 Type 2 audited and either ISO 27001 certified or follows the ISO 27001 policies.

Security reporting

Birst security policies and procedures are designed to minimize the risk of the breach of customer data. However, in the rare event of a breach of customer data Birst has a documented policy for investigating the breach and reporting it to customers, working with the customers to mitigate the risk, and if necessary, reporting to regulators and legal authorities.

Also, Birst has a responsible disclosure policy for those that find security vulnerabilities in the Birst application and marketing web site. The Birst responsible disclosure policy can be found at **http://www.birst.com/security-reporting**.

Summary

To protect the privacy of its customers and the safety of their data and 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.

Birst has passed the rigorous security audits of leading financial services companies and corporations in the Global 1000. In addition to securing your data, Birst ensures that it will be available when you need it, across any device. Our business intelligence (BI) platform has been designed from the ground up to protect the security of your data and information.

Learn more ›

INF-2065244-en-US-1018-1