BlueBin

Technical Specification And Overview

BlueBin Tech

Table of Contents

Version History

Version	Author	Date	Description
1.0	John Ratte	1/10/2015	First Version Complete.
2.0	Gerry Butler	9/1/2015	Updates inserted for hosted model
3.0	Gerry Butler	10/1/2015	Notifications Updated

BlueBin Product Overview

Introduction

The BlueBin platform is the single solution for all your hospitals' supply chain needs.

Document Scope and Purpose

The purpose of this document is to provide the technical specification and overview of the BlueBin system. The following categories will be discussed.

BlueBin Architectural and System Data Flows Overview

BlueBin delivers a Supply Chain Intelligence solution from the cloud, offering Software as a Service (SaaS) model that minimizes a healthcare systems' technical footprint. Through the use of a variety of data transport technologies, data is moved from the customer's network (typically the customer ERP system, see below) into the BlueBin data center where BlueBin processes the data into a variety of reports and operational metrics.

BlueBin Components Description

BlueBin integrates with the customer's ERP system and Supply Chain management processes.

Interface Requirements

BlueBin utilizes Integration Services (SSIS) packages as the primary method of data exchange and data processing. These packages can be initiated from either the Client side or BlueBin. Other technologies are required for secure connection, transmission, and optional workflow integration.

BlueBin Intelligence Platform

Tableau for BlueBin Intelligence report rendering and availability.

BlueBin SaaS

BlueBin uses SaaS-based servers within each environment that work to perform collection, services, transmission, storing, and presentation of data to the BlueBin hosting environment. BlueBin utilizes Amazon Web Services (AWS) for all remote server hosting and application availability

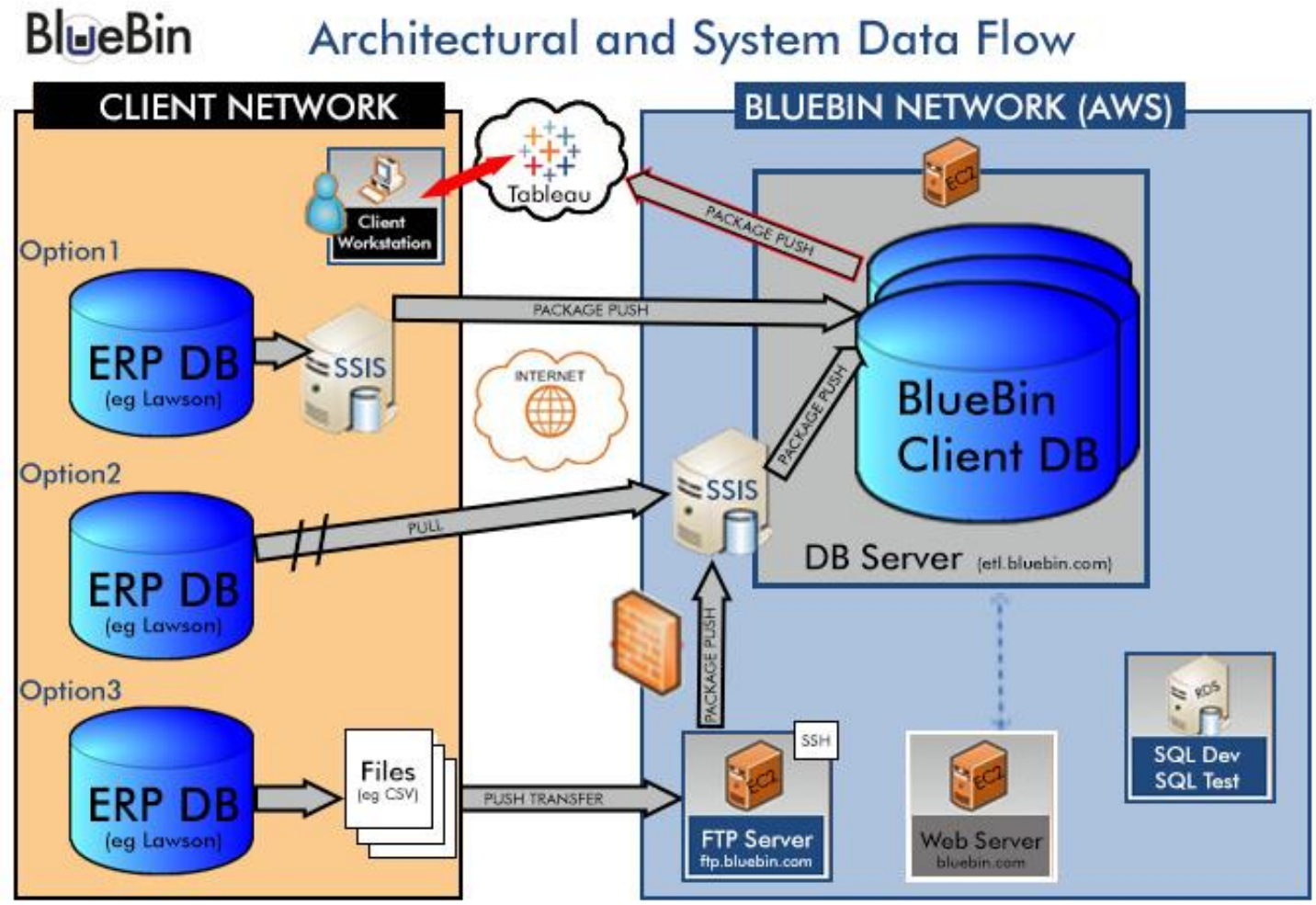
BlueBin Security

BlueBin provides the best practices in required physical and environmental security measures to prevent unauthorized access to, and otherwise physically and electronically protect, the software and customer data as applicable. Additionally, BlueBin will provide industry best practices for virus protection and security as provided by AWS.

Architectural and System Data Flows Overview

The BlueBin Architectural and System Data Flows Overview are best described by reviewing the *BlueBin Architectural and System Data Flow* diagram below.

PLEASE NOTE: Transmission is **one-way only**. The BlueBin system is currently a **read-only** application.



Components

BlueBin consists of a series of components that transfer data and communicate either internally or externally via defined protocols. The following describes the system's main components and their primary functionality. Please refer to *Client Requirements* section for workstation requirements.

BlueBin Data Processing Server (etl.bluebin.com)

The BlueBin Data Processing Server is a hosted server utilizing Microsoft SQL Server Integration Services (SSIS) to process incoming Client ERP data sent via secure transport methods into the BlueBin Client Database.

BlueBin Client Database(s)

The BlueBin Client Database is an isolated, hosted database containing processed client data and BlueBin proprietary data algorithms for purposes of managing and reporting on the BlueBin Kanban program.

BlueBin Secure Transport (ftp.bluebin.com)

The BlueBin Secure Transport server is a file directory server running an SSH Shell for SFTP and FTP protocol transfer of client ERP data.

BlueBin Client Portal (bluebin.com)

The BlueBin Client Portal is an access protected web site for distribution of various pieces of the BlueBin Kanban solution.

BlueBin Intelligence Dashboard (dashboard.bluebin.com)

The BlueBin Intelligence Dashboard is an access protected collection of Supply Chain, Sourcing, and Operational Performance Reports specific to your Client site created from processed inbound Client ERP data utilizing the Tableau Engine.

Interfaces

Data Access/Interface Methods Supported

Direct SQL Connection

Direct Database (DB) connection with encrypted data transfer utilizing TLS and registered Certificate Authorities (CA) is the preferred interface method and is used whenever possible due to its national standardization and acceptance.

Microsoft SQL Server Integration Services (SSIS) Packages

Microsoft SQL Server Integration Services (SSIS) Packages are the preferred method of initiating data transfer.

SFTP/FTP

BlueBin can accept flat data file transfer utilizing SFTP or FTP transfer protocols prior to SSIS Package processing if no direct DB connection is available.

ERP Data Requirements

The typical data required from the Client ERP system is outlined below. BlueBin and the Client will engage in data mapping sessions to accurately determine the location of each data element in the Client-side ERP data stores and the full capabilities of the BlueBin Intelligence solution based on available data. Detailed documents will be provided and reviewed during Client implementation.

ERP Tables/Data
Purchase Orders
Receipts
Inventory Transactions
General Ledger (GL) Transactions
Requisitions
Item Master
Par Master
Vendor Master
Buyer List
Location Profile

Interface Requirements

The data migration processes between the Client ERP system and BlueBin, as mentioned previously, require an active data connection, specific data fields, and data manipulation packages to modify the provided Client ERP data.

Receiving Client ERP Data is done in two parts. The order of these two parts can be switched depending on the specific capabilities of the Client:

ERP Data Manipulation

Client ERP Data, whether through direct Database (DB) connection, or through Flat Files is run through Microsoft SQL Server Integration Services (SSIS) Packages to scrub and populate the BlueBin Client Database .

Data Transfer

Complete Client ERP data can be transferred via flat file or direct SSL database connection. All data transfer is done across SSL utilizing existing certificate authorities to be provided.

> ***For example***: The Client maintains an instance of Microsoft SQL Server Integration Services (SSIS). BlueBin Technical Operations sets up a specific package(s) on the Client-side installation configured for the specific data mapping determined during implementation. Through a direct connection from the Client-side server and BlueBin's DB servers utilizing an SSL CA, the data is transferred in a nightly job into the Client Named Database on the BlueBin DB Server. Once proprietary algorithm processing is complete, all Intelligence Reports are available via designated Client distribution.

Product Security

Password/Login Functionality

Access to the BlueBin components is controlled by two separate logins that maintain identical parameters. It is not necessary for each user to have access to all components.

1) Access to the BlueBin Client Portal
2) Access to the BlueBin Intelligence Dashboard

Each method supports role-based access and allows users to access only the necessary operations to perform his/her job. Once authenticated, user permissions within the application are determined by the role assigned to the user.

Password Parameters

- Account Password Minimum Length = eight (8) Characters
- Contain Upper and lower case letters
- Contain a number OR non-alpha-numeric character
- Cannot contain:
  - User's login ID
  - Blanks

Authentication

All users required to access the application are loaded into SQL tables. Hashing is used to encrypt password information.

Application Logging and Auditing

BlueBin supports robust logging of security relevant events. Below is a list of the events that are logged within the application:

- User ID of user
- Successful login attempts
- Date/Time of event
- Type of event

Customers will need to request audit logs from BlueBin Support.

Application and Database Safeguards

In the BlueBin multi-tenant SaaS deployment, the data of multiple enterprises is located in separate data stores. Safeguards (described below) have been adopted to ensure that data of one tenant is not accessible to other tenants.

- In the multi-tenant SaaS environment, data will be segregated and isolated by separate Client databases.
- Data processed in the BlueBin solution utilizes unique data connections and SSIS packages.
- User data access will be authenticated based on user credentials mapped to that user's organization and will be verified on every transaction.
- Direct database access is not available to end users.

Development Security Practices

BlueBin adheres to a Software Development Life Cycle (SDLC) methodology. It follows commonly used best practices for designing, developing, and deploying with secure features. Every release containing architecturally significant change requires an architecture review and comparison of data integrity and performance versus pervious versions.

Product Software Patch Policy

In the event that a critical BlueBin Product Software Patch is required, BlueBin shall certify and install all patches within seven (7) days from the date that the patch is made available. This applies to critical patches only, including, but not limited to, security issues, incorrect operation of the Software that materially impacts the safe or correct operation of the Software, etc.

Hosting Infrastructure Security

General Security

The physical infrastructure (servers, routers, switches, SAN, etc.) for the BlueBin application is hosted in Amazon Web Services (AWS), while the reporting application is available through Tableau Online. Detailed Whitepapers on each environment are located here:

Tableau - http://www.tableau.com/learn/whitepapers/tableau-online-security-cloud

AWS - https://media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf

BlueBin's Technical Operations department maintains current architecture documents, which include full network diagrams of the BlueBin hosted environment. These plans are reviewed and updated annually as part of BlueBin's Business Continuity Planning.

Network Security

All data communications between BlueBin and the Client are encrypted during transport and at rest. Access to the BlueBin Data Center is limited to Clients accessing via Secure Socket Layer (SSL) transport with approved ips added to internal whitelist.

Physical Safeguards

All BlueBin engineers with datacenter access have undergone background checks and compliance training prior to gaining access to the production datacenter.

Server and Network High Availability

The BlueBin application is built around a highly scalable and redundant network and server design topology that guarantees high availability across networking and server components. The database servers utilize SQL Server 2012 AlwaysOn Technology for high availability. The Servers that host the BlueBin are Enterprise-grade systems.

Backup Policy (Production, Preview and UAT)

BlueBin backs up both data and computer images for disaster recovery and business continuity purposes.

Frequency and Timing of Backups

A full back up of practical data is taken every day, including:

- All clinical records and system audit trail.
- All files required for BlueBin network operations.

All BlueBin relational databases are backed up daily including:

- All transactional log data is backed up at least twice an hour.
- Incremental backups are performed nightly.
- Copies of the weekly full backups are stored local and securely offsite.

All BlueBin servers are imaged daily:

- System image recovery is used to restore a server in its entirety, to a baseline OS state.

BlueBin engages in periodic infrastructure audits to ensure compliance with the BlueBin policies and standards. Non-intrusive network audits (e.g., basic port scans, OS patch level baselines, etc.) are done weekly. More intrusive network and physical audits are conducted at a minimum annually.

BlueBin's Technical Operations department maintains current architecture documents, which include full network diagrams of the BlueBin application environment, full data flowchart that details where BlueBin data resides, and the security thereof. These plans are reviewed and updated annually as part of BlueBin's Business Continuity Planning.

BlueBin's formalized Information Risk Management (IRM) security committee meets weekly to review and/or approve any suggested enhancement or remediation request related to the BlueBin environment.

Operations Auditing/Logging

BlueBin product support is handled by a dedicated Technical Operations department with tools and procedures to gather metrics on BlueBin performance. BlueBin engages in periodic infrastructure audits to ensure compliance with the BlueBin policy and standards.

Database

- All successful and unsuccessful logins are logged at the database server
- All application-related auditing will remain in the production database and will be partitioned by date. All SQL logs are archived and maintained for one (1) year.
- SQL Server implicitly uses journaling via transaction logs. These logs are backed up on a scheduled basis and will be depended upon for recovery.

Disaster Recovery and Business Continuity Planning

The BlueBin data processing protocols allow for rapid recreation of any Client environment within a 48 hour period.

Antivirus Policy

BlueBin application host systems employees a multitier solution for antivirus, malware, and network access control protection. The following minimum requirements shall be enforced:

- The antivirus product shall be operated in real time on all servers and Client computers. The product shall be configured for real time protection.
- The antivirus library definitions shall be updated at least twice per day.
- Antivirus scans shall be done a minimum of once per week.
- Due to built-in BlueBin security that will only accept files from the original origin point, the following URL's will need to be added to the exception list for anti-virus scanning on download: Https://*.BlueBin.com and http://*.BlueBin.com. Redirected files to a new cleaned URL will not function properly.

SLAs

The Hosted System will be available for User access (uptime) **99%** of the time 24x7x365, subject to the terms of this Service Level Agreement measured monthly. This does not include any local Client system or communications failure. Uptime excludes (i) scheduled maintenance; (ii) emergency maintenance required by BlueBin Technical Operations to comply with the published Patch Policy that must, by its nature, only be conducted outside the scheduled maintenance window - provided that BlueBin shall notify Client as soon as practicable of the need for such emergency maintenance before the Hosted System is taken offline; (iii) downtime caused by any unauthorized use of the Hosted System by Client or Users; and (iv) circumstances beyond BlueBin's reasonable control. BlueBin is not responsible for issues that might occur with global internet.

Subject to scheduled maintenance, it is intended that the software will be continuously available. However, the customer acknowledges that access to the Internet and to the software is subject to factors outside of BlueBin's control and that BlueBin will not be responsible for any unavailability of the software.

Uptime Warranty Standards

Uptime: BlueBin system "uptime" is defined as a system condition whereby users can retrieve designated reports and perform critical functions in supply chain management.

Uptime calculations exclude the following conditions:

- Planned system preventative maintenance requiring system downtime (proper notification will be sent to Clients prior to planned maintenance outside the regular scheduled maintenance window);
- Hardware upgrades requiring system downtime;
- Operating system or database system upgrades requiring downtime;
- Upgrade and installation of core system or additional modules requiring planned system downtime;
- Downtime caused by non-application related conditions (e.g., network infrastructure, wireless infrastructure, third party applications installed on the same server/workstation, acts of God, etc.);
- Measurement will begin ninety (90) days post productive use.
- Software upgrades.

Maintenance Windows/Scheduled Restarts

Consistent with sound industry operating practice, BlueBin will take down the software for scheduled routine maintenance as identified in our Service Level Agreement. The customer will be advised/reminded in advance of the times for such scheduled maintenance (noting that maintenance is typically scheduled to occur during less active times of the day).

BlueBin hosting environment maintenance occurs monthly as applicable. The scheduled maintenance window takes place on the first Wednesday of the month at 7:00pm PST until 12:00am PST if needed.

In addition to standard maintenance windows, System Down updates can occur with no notice.

Tableau Online Maintenance follows the standard update procedures setup by Tableau, occurs automatically as needed, and do not normally affect report use. BlueBin has no responsibility for the frequency and impact of Tableau Maintenance and Updates that occur. Should there be detrimental performance experienced (including system down) by the Client due to Tableau scheduled maintenance, BlueBin shall investigate and provide updates as applicable.

Amazon Web Services (AWS) follows the standard update procedures setup by Amazon, occurs automatically as needed, and do not normally affect application access. BlueBin has no responsibility for the frequency and impact of AWS Maintenance and Updates that occur. Should there be detrimental performance experienced (including system down) by the Client due to AWS scheduled maintenance, BlueBin shall investigate and provide updates as applicable.

Monitoring

BlueBin Technical Operations manages a wide variety of information systems to support the BlueBin application. In order to ensure that BlueBin Technical Operations adheres to its requirements under The Data Protection Act and the Employment Practices Data Protection Code – Part 3, it is essential that monitoring of these systems occur in order to protect data and manage risks to the systems and applications. This monitoring may consist of automated tools to collect and record information and/or human monitoring and auditing.

Disk Space

Automated check of disk space free size will trigger alerts when the level falls below a defined threshold.

IDS Monitoring & Unauthorized Access

BlueBin systems will be monitored for unauthorized access or system alteration. Proactive monitoring of BlueBin will occur on a regular basis, dependent upon the system capability and appropriate resource allocation. This monitoring will take the form of scheduled audit reports produced by the system manager using an automated tool set. Monitoring will also be undertaken at the request of an appropriate BlueBin Technical Operations management where suspected abuse of the system has been identified and reported or in the event of an incident.

Client Requirements

Hardware/Software Requirements

The **minimum** BlueBin implementation requires one Enterprise resource planning (ERP) environment inside the Client's hospital network environment. The servers hosting this environment act as a hub for the collection and transmission of data to the BlueBin hosting environment.

Recommended Workstation Requirements

OS	CPU	RAM	HD	Display	Browser
Windows 7 or later	Minimum 2.4 GHz processor	2 GB RAM or higher	20 MB Disk Space	1280x960 display or higher	• Android Browser (Android 3.2 or later) • Apple Safari 3.x or later, including Safari on the iPad (iOS 5.1.1 or later) • Microsoft® Edge or Internet Explorer 10 or later • Mozilla Firefox 3.x or later (not supported on mobile devices) • Google Chrome, including on Android devices

					• Tableau Mobile iPad and Android Apps, available at the Apple App Store and Google Play Store, respectively

Connectivity and Bandwidth Requirements

For transfer of data from Client network to BlueBin Server Environment, a 1.5Mbps connection is the minimum required.

Port and IP Requirements

Whitelist Requirements

TCP Port Requirements

Workstations

Port Number	Usage
80	Browser requests-automatically forwarded to port 443
443	Browser requests, secure web service communications from GUI (all systems)
1443	Secure web service communication

DB Server

Port Number	Usage
80	Browser requests - automatically forwarded to port 443
443	Browser requests, secure web service communications (all systems)

Notes:
Port 80 is required to ensure the user does not receive an error if they forget to type “https” into the browser. It is immediately redirected to port 443. Port 443 is always needed (all systems), as this is the main port for communicating to web services.

RDP access to servers is controlled by whitelisted ips on obscure port.

Application Version Upgrades and Updates

BlueBin will notify each Client by email (from Client manager or support) when a new product release or update is available. The email notification will contain detailed information regarding the product update (release notes) and the timeline for which the updates will be implemented.

- Standard release cycle is four major version updates per year (per quarter), however smaller minor updates may be necessary. All updates will be applied to a customer test/preview environment for validation. The Client will have time (depending on specifics of update) to validate updates in test. After the determined testing timeline is met, the product update will be applied to the hosted production environment.
- Regulatory or security updates will be applied during the regularly scheduled maintenance window and/or if a special hotfix is required to resolve a critical (system down) incident.

Client Notification

BlueBin communicates important information or updates to our Clients so they can quickly and easily understand what is happening and what impact it may have on their operations.

NOTIFICATIONS

To keep it simple, we've created a color coding process for the notifications that will be sent (as applicable). This process is intended to help clearly and consistently communicate about planned activity, activity completed, system incidents, and announcements.

Planned Activity – Title of activity

System Incidents – Title of Incident

Announcements – Title of Announcement

Activity Completed – Title of Corresponding Activity Completed or Incident Resolved