

Secure Business Intelligence with Brio Enterprise

Meeting users' needs for flexible data access, while providing robust security with Brio Enterprise 5.5.

Security White Paper

November 1998



P/N 05-991-1340

| | |
|---------------------------------------------------------------------------------------|-----------|
| EXECUTIVE SUMMARY | 3 |
| SECURITY IN THE CLIENT/SERVER ENVIRONMENT- DIRECT DATA ACCESS..... | 5 |
| THE CLIENT/SERVER ENVIRONMENT: INTRODUCING THE BRIO REPOSITORY | 6 |
| Creating the Brio Repository- Security Implications | 6 |
| Repository Access Management | 7 |
| Brio Repository Objects | 7 |
| MANAGED QUERY ENVIRONMENT – INTRODUCING THE BROADCAST SERVER | 9 |
| User Group Access Control..... | 10 |
| Enabling Output Directories..... | 10 |
| INTRANET- DATA ACCESS: "THE POWER OF THE WEB" | 12 |
| Open Authentication Model | 13 |
| Adaptive Reports | 14 |
| SECURING YOUR EXTRANET ENVIRONMENT WITH BRIO ENTERPRISE | 16 |
| Distribution via the Broadcast Server in a Pure SSL environment..... | 18 |
| The Diverse Extranet User Base..... | 18 |
| BRIO ENTERPRISE MANAGES SECURE DATA ACCESS THROUGHOUT THE ENTERPRISE | 19 |
| APPENDIX A BRIO ENTERPRISE 5.5 PRODUCT SUITE | 20 |
| Client/Server Clients..... | 20 |
| Brio Enterprise Server | 20 |
| Web/Intranet Clients | 20 |

EXECUTIVE SUMMARY

The popularization of client/server query and reporting tools in the early 1990s gave clear competitive advantages to organizations that employed just a relatively small number of savvy data analysts. The ever-increasing competition since then demands timely, informed decision-making at all levels of the organization, not just in Finance and Operations. The expansion of the Web promises to meet that need by allowing cost-effective data access and analysis for all decision-makers. IT departments must now support multiple network architectures and serve a very diverse user population, each with different needs and access privileges. However, as the number and types of users increase, invariably so does the potential for security breaches.

Database administrators (DBAs), whose job has always been to keep data safely *in* the database, need to know how to open up the data warehouse or mart so that only the right data flows to the right people—but there are admittedly many people to serve. This white paper addresses Brio's design philosophy and the methods that administrators can use to widely deploy Brio's business intelligence products without sacrificing security.

Brio's design philosophy has always been to give the user the right tool for the job and to avoid redundant work and maintenance burdens. In the case of data security, Brio allows you to control data flow through a combination of proprietary Brio features and support for standard security systems and protocols. This seamless integration is a critical factor in ensuring that you can set up, maintain, and deploy a secure environment where all users get exactly the data they need to do their jobs.

Depending upon whether your network supports data access via traditional client/server connections or the Web, security for the Brio Enterprise product suite can occur at any of these levels:

| Level | Brio feature or support for existing system |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Document | <ul style="list-style-type: none">· Adaptive Reporting· Locked data models |
| Brio Enterprise product suite | Products that range from: <ul style="list-style-type: none">· Viewing only, to· Full ad-hoc query, analysis, and administration |
| Application/File servers | <ul style="list-style-type: none">· Open Authentication Model for additional user names and passwords (OnDemand Server)· Authorized directories and printers (built into Broadcast Server)· Built-in Web, FTP, and file server authentication |
| Meta layer | <ul style="list-style-type: none">· Hide, show, and rename tables and columns· Store data in a central repository with restricted access privileges· Group privileges |
| Database server | <ul style="list-style-type: none">· User names and passwords· Row level security |
| Network | <ul style="list-style-type: none">· Compressed binary file transmission (as opposed to sending data over the Web "in the clear")· SSL· Digital signatures (for Brio Web client software)· Firewalls· Encrypted password transmission |

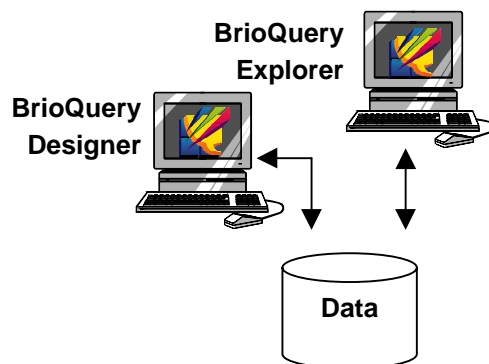
As mentioned in the introduction, security considerations are compounded by the increasing number of and types of users and their respective network environments. This white paper addresses the security requirements and options available for the following user communities:

| User Community | User Profile |
|------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Administrators and Sophisticated Data Analysts | <ul style="list-style-type: none">· Users who connect directly to the database via traditional client/server APIs |
| General Business Users | <ul style="list-style-type: none">· Users who pass through a meta layer to the database via traditional client/server APIs· Users who receive or pick up data sent to them by a batch server during the off-hours (also known as "push")· Users who pass through a meta layer to the database via their Web browsers; data is transmitted safely within a trusted network or intranet |
| Business Partners | <ul style="list-style-type: none">· Your company's business partners or customers who pass through a meta layer to the database via their Web browsers; these users are part of an extranet and typically pass through a firewall and require secure data transmissions over the Internet |

SECURITY IN THE CLIENT/SERVER ENVIRONMENT- DIRECT DATA ACCESS

In any client/server environment, the most effective way to secure data is to grant and revoke privileges for users and user groups at the database level. If security is not implemented on the database, but rather by an application that sits on top of the database, the DBA has to set up redundant security systems for each application or tool. Worse, those systems can get out of sync and there is always the potential that someone could infiltrate the database through an alternate application. When a product requires a heavy semantic layer, users may not even have the option of directly accessing clean well-designed data warehouses or data marts.

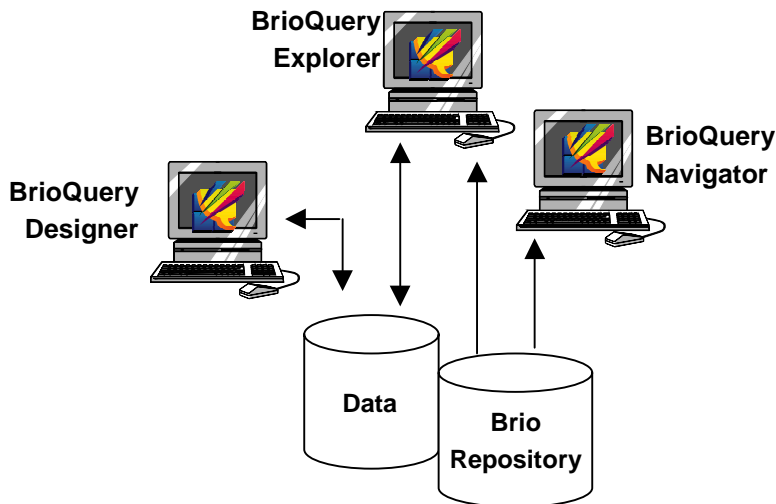
BrioQuery Designer and BrioQuery Explorer are Brio's client/server products that provide direct database access. These products can be made available to administrators or savvy, professional data analysts for ultimate ad-hoc query capabilities. The database server itself manages user access security. For example, in order for BrioQuery Designer or Explorer users to process a query against the database, they must first enter a username and password. Once the username and password are supplied, the connectivity API securely transmits it to the database for authentication.



At the more granular level, organizations that require row level security can control data flow on a row-by-row basis. Typically, a database administrator (DBA) designs and implements this level of security. The DBA creates a database View that implements additional "join" and "where-clause" logic that constrains the rows returned based on predefined conditions, such as User ID. The DBA then grants View access and restricts access to the source database tables. Any query against the database View—whether from a Brio product or any other—automatically and transparently inherits the conditions defined in the View.

THE CLIENT/SERVER ENVIRONMENT: INTRODUCING THE BRIO REPOSITORY

The previous section on direct data access used no proprietary security features. In this section we look at a more structured, managed query environment, which extends our model beyond professional data analysts to a much broader set of users within an organization. Since these users are still connected via client/server APIs, the database password authentication and row level security discussed previously still applies. We introduce the Brio Repository to store and manage standard queries, reports, and data models. These objects expose the database elements and information that users need, yet shield them from items they should not have access to.



The Brio Repository provides an efficient way to manage and distribute Brio data models and documents to BrioQuery Explorer and Navigator users. By storing standardized objects in a Brio Repository, BrioQuery Designers can provide password-protected, version controlled data models and documents for user groups as needed.

In this model, database logins provide password-protected access to the Repository. Using BrioQuery Designer, administrators create and administer the Repository, define access privileges for users and groups connecting to the Repository and upload documents to the Repository.

Creating the Brio Repository- Security Implications

Before creating the Brio Repository, there are security implications to consider.

Will the Repository contain highly sensitive documents that only a small select group of users should have access to?

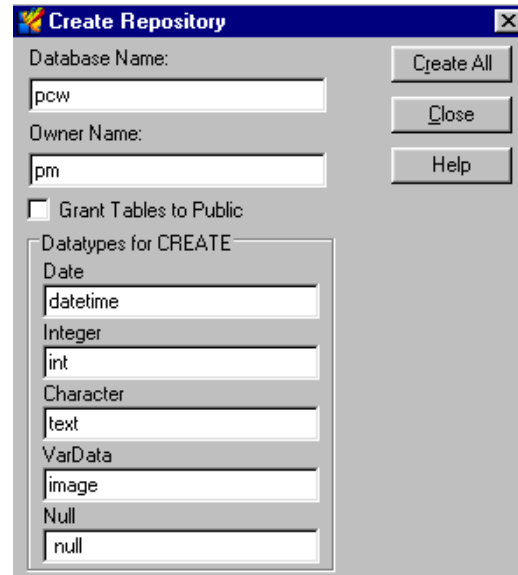
Is it necessary to provide general user access to the Repository with the ability to tightly control access on a document basis?

The Brio Enterprise architecture is flexible enough to implement multiple repositories for specific subject areas of the data warehouse, or to implement a single Repository managed for specific user groups.

Repository Access Management

Upon creation of the Brio Repository, a database table owner is specified. This owner name is a powerful tool to restrict repository access by using database grant privileges to define access to the repository.

Within the Brio Repository, a public database group may be allowed “grant table” access. This option executes a “Grant Select” statement for the Public group for each of the Repository tables. Public access allows all users logging on to the database access to the Repository. It is important to note that having access to view the Repository does not necessarily mean that a user will have access to all the data models and reports stored within that Repository. The Brio approach provides each user with a catalog of data models and documents that have been granted to their user group. If restricted documents exist on the Repository, they would not appear in the user's Repository catalog.



As an alternative to granting public access to a Brio Repository, administrators can create a Repository specific to certain users. The users can then access Repository tables with Select privileges manually granted. This tightly secured Repository is designed for sensitive data that must be inaccessible to the general public, such as a finance repository. This model leverages database security in conjunction with the user group protection inherent in the Brio Repository.

Brio Repository Objects

Three types of Brio objects are stored in the Brio Repository: data models, standard queries, and standard queries with reports. All objects are created with BrioQuery Designer to manage end-user data access. With a locking feature contained in the Brio Repository, data models and standard queries cannot be altered by the end-user.

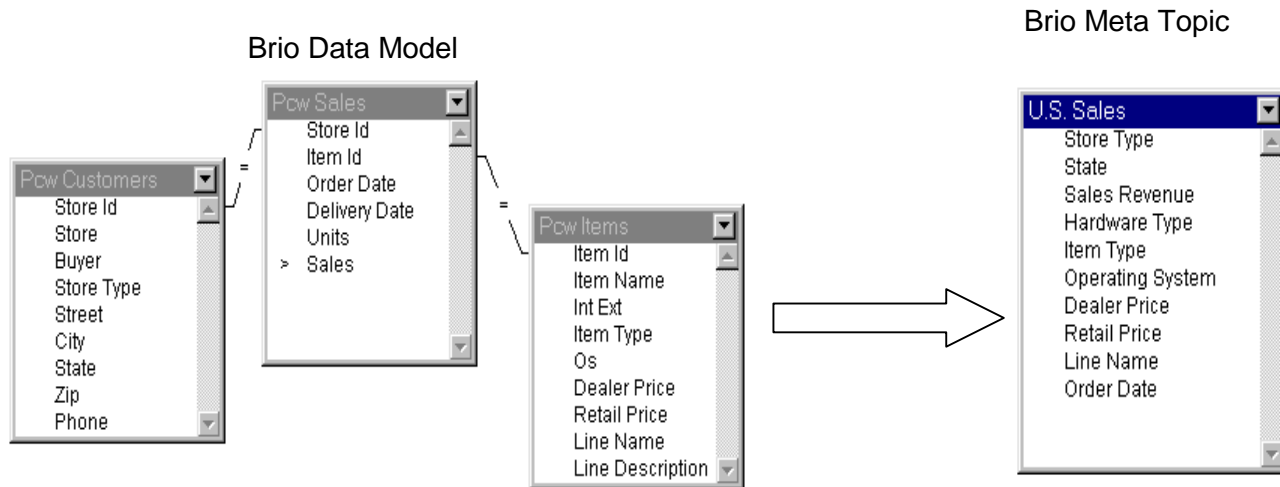
Data Models

BrioQuery Data Models enable an administrator to tightly manage access to database tables and columns while still allowing end-users flexibility to perform ad hoc queries. Data models are a graphical representation of underlying database tables and join structures (*Note the Brio Data Model displayed below.*)

Using BrioQuery Designer, administrators can further manage access within data models by creating meta topics, which provide a customized view of the underlying data model structure. When a meta topic is created, the original data model structure becomes hidden from the end-user. Join logic, physical database tables and column names can be altered and/or hidden from the end-user. A partial view of a database table, comprising a subset of the table columns and computed items, may be represented as a meta topic.

The example below depicts a Brio Data Model and a Brio Meta Topic derived from that Data Model.

Notice in the meta topic that the join logic is hidden, topics are renamed, the limit icon is not displayed next to Sales, and only a subset of the topics are available to the user.



Data models allow administrators to grant access to information necessary to a particular user group while restricting the same users from database columns or computed item calculations. For example, employee contact and salary information may be contained in the same table on the database. A Human Resources employee may need to query employee contact information but this person should not be privy to salary information. An administrator can handle this situation with BrioQuery Designer by creating a Repository data model with a meta topic view consisting of employee contact information only. With this in place, users can build their own queries, but only from items made available in the data model by the administrator.

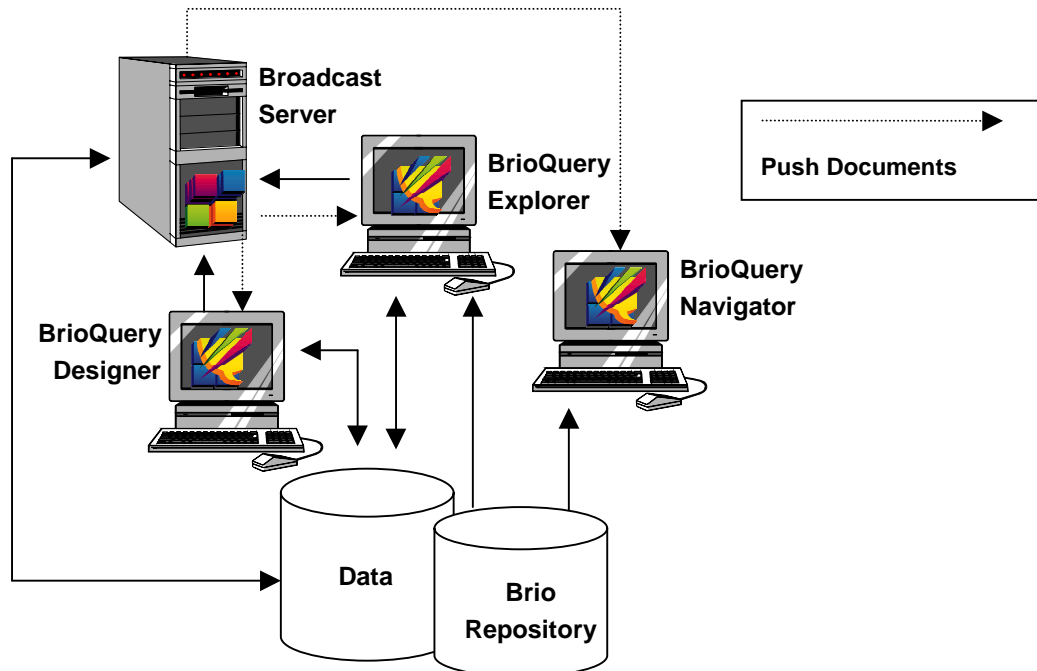
Standard Queries

Standard queries are Brio documents downloaded from the Brio Repository that contain a data model and a predefined query (Standard Queries with Reports also contain preformatted reports). Standard queries enable administrators to manage data access more tightly than they can with data models. End-users are restricted from adding or removing an item from the query request line, but they can refresh their results set, analyze and create reports. Standard queries ensure that users run predefined queries that cannot be modified by the end user.

Locked Brio Repository objects remain 'linked' to their parent data model or standard query in the Brio Repository even after the document is saved onto an end-users local desktop. The document link is hard coded into the file and cannot be unlinked. When BrioQuery users open a locked document, they are prompted to login to the database. The database then authenticates their password and the linked Brio document is refreshed against its "parent" document. Any change made to the parent document will be automatically reflected in the linked document. This process is called Automatic Distributed Refresh (ADR). ADR controls the content of Brio Repository documents even if an end-user has saved a Repository document locally to their desktop. ADR give administrators confidence that every end user working with a linked document has the latest version of that document.

MANAGED QUERY ENVIRONMENT – INTRODUCING THE BROADCAST SERVER

The Broadcast Server is a batch-processing server that automates query processing and report distribution. BrioQuery users create queries and reports and then schedule them to be processed at a later time. Scheduling can be one-time or recurring based on date, time or an event, such as a database update. The results are automatically published to specified users or groups of users who can view and/or analyze the data without impacting the network or the database during peak processing hours. The Broadcast Server can be one of the most effective tools for extending the reach of your data warehouse—both in and outside your organization.



Although the Broadcast Server can deliver large amounts of data to many people, security safeguards are built into the product to enable administrators to tightly control database access and document distribution. The database server administrator defines the database connections the Broadcast Server uses to process scheduled Brio documents. Documents may be scheduled by a select group of trusted data stewards within each department or the Broadcast Server may be opened up as a scheduling resource for all users.

Opening up scheduling to trusted data stewards offers an effective way to restrict access to the database, yet still deliver data and reports to the user population. For each scheduled job, the Broadcast Server queries the database, retrieves the results set, and formats any reports. These updated documents may then be broadcast out to others in the user population via e-mail, printer or saved to file server directories. These end users receive Brio documents with just the data they need without compromising database security by the issuance of extra database accounts.

The Report Bursting feature of the Broadcast Server enables the convenience of scheduling a report once and distributing the same report with variable inputs and unique destinations. Each user receives only the subset of data they are authorized to receive.

The Broadcast Server can retrieve data sets based on different needs or access privileges. Scheduled documents can run in multiple cycles, each cycle constrained to a specific data set based on the access privileges of the recipient. Users schedule just one document, and the Broadcast Server delivers controlled data sets to diverse audiences.

For example, a sales report can be scheduled to the Broadcast Server to process and distribute different data to different sales regions. The eastern region will receive a report restricted to the eastern sales totals, the western region to their totals, and the sales manager may receive a report that shows the sales totals for both regions.

User Group Access Control

If the Broadcast Server administrator chooses to enable end-users to schedule jobs, the first step is to grant scheduling privileges. Only users that are granted access by the administrator can schedule jobs.

Using the Broadcast Server's administrative tool, administrators assign access privileges to users or user groups. Administrators then control access to output directories to preserve the integrity of network security. For example, an administrator may want to restrict access to the color printer, or restrict a certain output directory to upper management. These privileges can be defined and applied through Broadcast Server's "user groups" feature, which associates lists of users, output directories and printers for each group.

User group access can be managed in three ways. With the user group model, network privileges can be differentiated based on specific criteria such as departmental mission or geographical location. The database user ID determines user group membership and the options available when scheduling a job.

- **Custom Groups:** Custom groups assign specific privileges to a group of users. When a user schedules a document from BrioQuery, only the resources available to his or her respective group will appear as scheduling options.
- **Public Groups:** Public groups offer scheduling privileges to those not assigned to a custom group. Public groups can be used in place of custom groups if assigning differentiating user privileges isn't necessary. Administrators can also combine the Public group with other user groups to implement a hybrid group arrangement, while maintaining their distinct access privileges. For example, the custom group members will have more comprehensive access privileges than the users belonging to the Public group.
All forms of general access to Broadcast Server can be prohibited by deleting the Public group. This will create secured access by ensuring that every user who has access to Broadcast Server is a member of a custom group.
- **Administrator Groups:** Administrator group users can access all Broadcast Server resources and options when scheduling a job. In addition, Administrators can monitor all jobs in a given job list (other users can only view the jobs scheduled under their own database user ID).

Enabling Output Directories

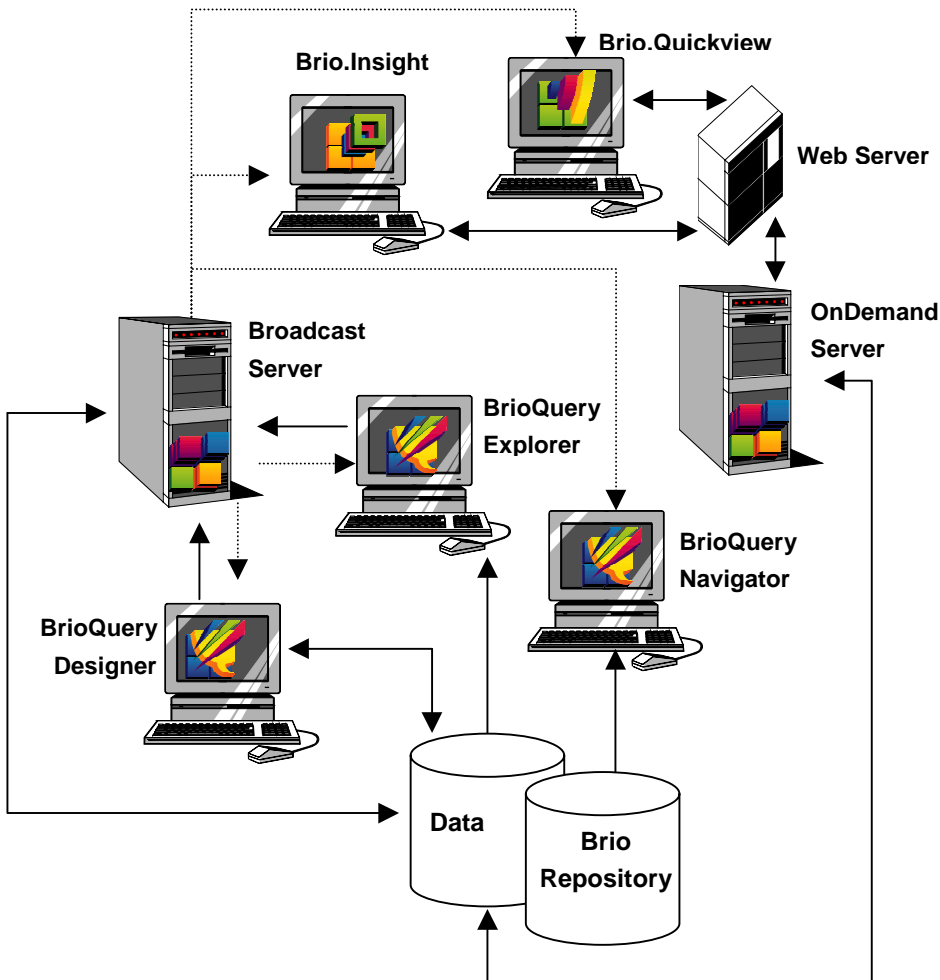
- **Saving to LAN or FTP server directories:** The Broadcast Server allows a user to save Brio documents to a LAN directory or to a remote FTP location. Through the Broadcast Server Administration tool, access is granted to selected user groups to output jobs to specific, predefined directories. The Broadcast Server itself needs to be running as a background process with full

access privileges to all target directories. The user and user group security of the Broadcast Server filters the appropriate choices for the user so that when users schedule a job, they are only given predefined locations choices. When the Broadcast Server runs the job, it will place the output file in the proper location using the system privileges of the appropriate account.

- **Printing:** Similar to saving to directories, a scheduled document can be specified to output to a local or LAN printer. When a user schedules a job and selects the print action, a printer picklist appears, populated with only those printers available to that user's group.

INTRANET- DATA ACCESS: "THE POWER OF THE WEB"

We examined how to secure data for various users within a client/server environment, including directly-connected data analysts, managed query users who access data through the Brio Repository, and recipients of documents sent to them by the Broadcast Server. In this section we look at some of the security issues related to making a data warehouse accessible via an intranet. We also discuss how Brio's OnDemand Server addresses these issues with its Open Authentication Model and Adaptive Reporting features. The following diagram shows how the OnDemand Server and Brio's Web clients, Brio.Insight and Brio.Quickview, interact with other Brio products to retrieve and share data.



The OnDemand Server is a Web-based application server that enables users to view and select from a list of authorized Brio documents. These documents may be Standard Queries with Reports or they may simply contain Data Models from which a user can build an ad-hoc query and reports. Each document available from the OnDemand Server is assigned a privilege level to define the level of interactivity that individual users may have with the document. Document interactivity levels range from simply viewing a report in the Web browser to full query and analysis capabilities.

The OnDemand Server maintains strict security over database information. The administrator of the OnDemand Server has centralized control over who can access the OnDemand Server, which documents a specific user can view, and what interactivity level the user has with a particular

document.

The Administrator can thus restrict access to files at the user, document and database levels to halt information from flowing beyond authorized channels. Access information is stored centrally in the OnDemand Server's Repository. Physical documents are stored on a file system located on the same machine as the OnDemand Server, obeying standard network system privileges.

Note: The OnDemand Server Repository tables are a superset of the Brio Repository tables. When creating the OnDemand Server Repository, the same security considerations apply as they do with the Brio Repository, such as repository owner and grant tables to public. Refer to the preceding section Creating the Brio Repository- Security implications for information regarding security implications to consider when creating the OnDemand Server Repository.

Open Authentication Model

At the OnDemand Server login page, users are required to logon with a username and password. This password is authenticated before the user is permitted to view the document list. Password authentication is also repeated, transparently to the user, each time the user selects a new document from the job list. This allows any changes to access privileges to take immediate effect. If the administrator removes a document from a user's job list after the user has logged on, the user will be denied access when he or she attempts to select the document link.

Brio allows the OnDemand Server administrator the flexibility to choose between three different password authentication methods. Brio's Open Authentication Model leverages previous investments made in setting up secure application environments. It also saves maintenance and setup time and simplifies access when deploying Brio Enterprise across your Intranet.

The three authentication methods are:

- **OnDemand Server Password Authentication:** Password information is encrypted and then stored in the OnDemand Server Repository. When a user logs on to the OnDemand Server, the OnDemand Server will authenticate the given password by verifying it against the encrypted password stored in the OnDemand Server Repository. The user's password information is stored in a temporary cookie, in the RAM of the user's PC, for repeated access during the browser session. This cookie is encrypted and stored in temporary memory only.

Change Password: When using OnDemand Server authentication (as opposed to database or JavaBean), the OnDemand Server allows users to change their passwords directly from the logon screen. Users may change their OnDemand Server passwords as often as they wish. When the change password authentication option is set for OnDemand Server authentication, the OnDemand Server encrypts the new password and overwrites the old password in the Brio Repository.

- **Database Password Authentication:** This authentication method allows the OnDemand Server administrator to leverage the username and password security already set up in the corporate database. In this model, the OnDemand Server attempts to logon to the database using the username and password entered on the OnDemand Server logon form. If the connection is successful, the user is authenticated and the document list is displayed. The OnDemand Server does not permit the Web user to proceed to the document list until the database has authenticated

the given password. If the database password authentication model is selected, the list of available users is generated from the users already defined on the database. This allows the OnDemand Server administrator to leverage existing user groups for OnDemand Server access.

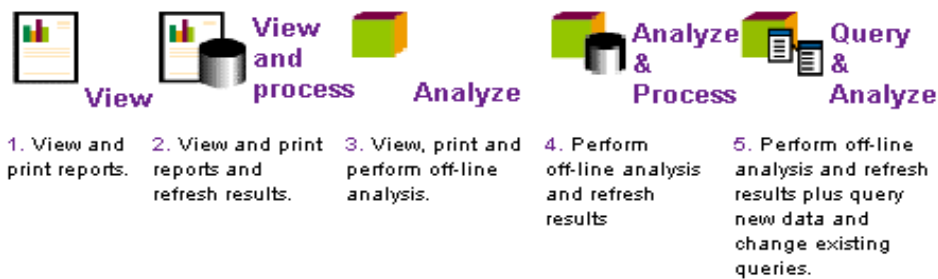
- **Custom JavaBean Authentication Model:** Custom JavaBean password authentication allows the OnDemand Server to integrate with an organization's existing security systems allowing for a single source of password authentication. The OnDemand Server transmits the given password to the JavaBean and will not allow the Web user to proceed to the document page until the JavaBean runs the password through a custom algorithm and passes back a 'true' or 'false' to the OnDemand Server. Refer to the tech note 'OnDemand Server Custom User Authentication', available on Brio's Web site (www.brio.com/support/tn2.html), for more information on how to implement JavaBean password authentication.

Adaptive Reports

The OnDemand Server Administrator assigns users to groups, where each user group not only has authorization to use different documents, but different user groups can have different interaction privileges—ranging from simple viewing to full ad hoc query—for the same document. The ability to change the interaction level for a document on a user-by-user basis is called Adaptive Reporting.

Note: Users and documents can be added to more than one group. If a user is part of multiple groups, and a document is registered to multiple groups, then the user will receive the highest privilege level available of all of the groups. Documents registered to the Public group will appear in every user's document list, with the access functionality determined by the document at registration time.

A Web client's adaptive state is based on the privilege level assigned to a user group and a registered document or Repository Model. The document privilege setting is graphically displayed next to each document in the document list. The five adaptive privilege states that may be set are:



< - Brio.Quickview View & Process - >

< - - Brio.Insight adapts between View and full Query & Analyze - - >

When a user logs in via the OnDemand Server login page (see the previous section on the Open Authentication model), an Adaptive Report list appears displaying the available documents based on the user's privileges. Only those documents to which the user has authorized access will appear in the document list. When the user selects a document, their username and password is re-authenticated and the document is downloaded to the user's Web browser. The Brio Web client opens the document and reads a token passed in the file to adapt to the specified level of functionality.

At the document level, registered documents that are opened and saved from a Web client application

to a local directory retain the token that contains the privilege level with which they were originally retrieved. When these documents are opened, processing a query triggers re-authentication to the OnDemand Server to verify user privileges. This functionality allows an administrator to retain access to documents even if they've been saved locally.

Note: Adaptive Report technology is used only when Brio Web clients are used to open documents registered with the OnDemand Server (Brio's Web clients can open unregistered documents as well). A user may be given a document from another user, or published to a network directory by the Broadcast Server. When a user opens an unregistered document, it will open with the default privileges of the user's Web client application. Default Privileges of Brio Web clients provide the following functionality:

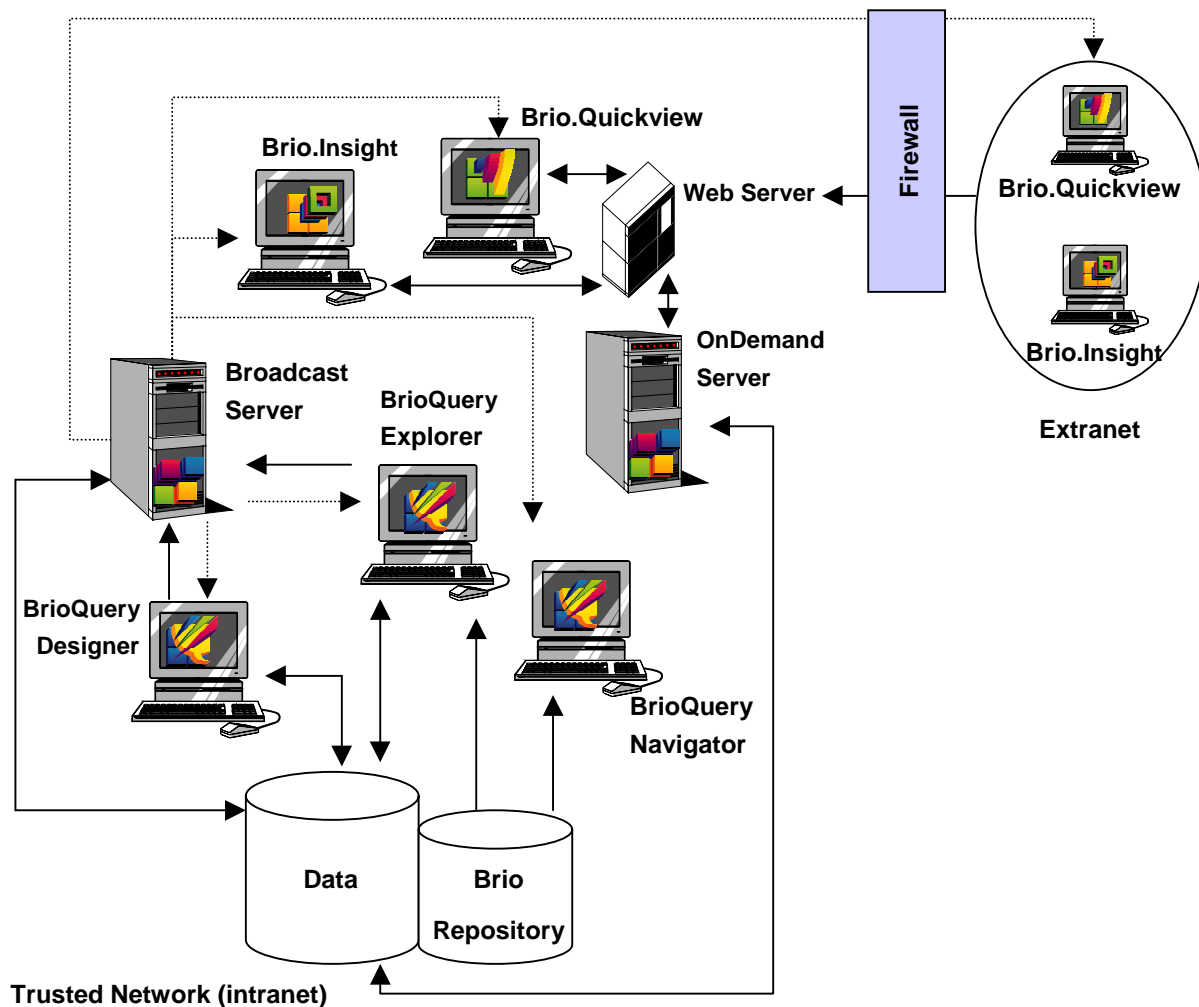
| Product | Default privilege level | Default functionality |
|----------------|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Brio.Quickview | View (1) | End-users can tab through BrioQuery documents and print out report portfolios in BrioQuery format. |
| Brio.Insight | Analyze (3) | Complete OLAP and reporting functionality in a Web browser. Users can pivot, group and drill everywhere. They can also build completely new charts and reports from a document distributed through the Intranet. A Web client's default privilege level is used when opening an unregistered document. |

SECURING YOUR EXTRANET ENVIRONMENT WITH BRIO ENTERPRISE

Extranets depend upon firewalls and secure data transmission techniques to make a company's intranet Web servers accessible by authorized users via the public Internet. This is different from a company's public Web site, which anyone can access. Extranets typically extend beyond the corporate user base in order to share information or operations with suppliers, vendors, partners, customers, or other businesses. Typical information exchanges on an extranet include:

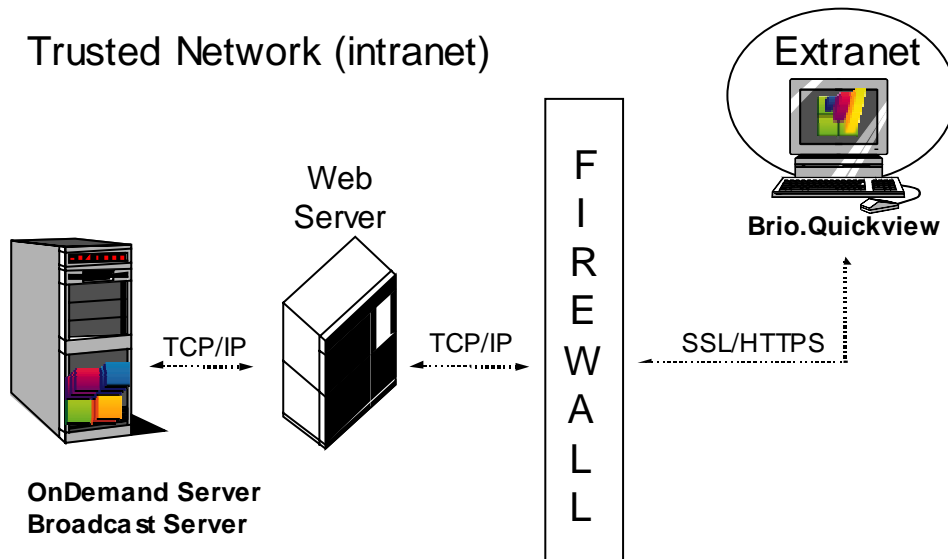
- Sharing product catalogs exclusively with wholesalers or those "in the trade"
- Collaborating with other companies on joint development efforts
- Sharing news of common interest exclusively with partner companies
- Providing status reports and report cards to suppliers and customers

From a business perspective, an extranet can be viewed as part of your company's intranet that has extended to users outside your company. From an IT perspective, extranets create great security concerns because in business-to-business information exchanges, data is transmitted not within a trusted network, but over the public Internet.



The previous architecture diagram shows how Brio Enterprise products access and share data within a secure intranet. This section discusses how extranet users can use full-featured Brio products to access the corporate intranet without compromising data security. Later we will discuss how data can be securely transmitted to the extranet using third-party file formats, such as Microsoft Excel, text, or HTML.

An Extranet requires security and privacy. This typically requires user authentication to ensure that only trusted individuals can request data. Once the data is obtained, it needs to be securely transmitted over the public Internet so that only the person who requested it can read it.



Companies often install firewalls to protect all computers within the trusted network from unauthorized access via the Internet. To allow extranet client workstations to communicate to the Web server, they must first be authorized to pass through the firewall, typically on port 80 (the default port for Web servers). The Web server communicates directly with the OnDemand Server through a distinct TCP/IP port (the default port is 5500). Once the extranet user is authorized access to the network, both the OnDemand Server and the database server authenticate the user either through passthrough methods or additional prompts. In this way, only authorized users can request data.

The OnDemand Server may perform password authentication, serve up document lists, and retrieve documents to the client's browser while connected to an SSL enabled Web server. This allows for secure transmission of the user's logon information. Once the data is retrieved, the OnDemand Server packages the data in Brio's compressed, binary file format. Unlike some products that send data "in the clear," data stored in Brio files cannot be read by picking up packets transmitted over the Internet.

Additionally, the Secure Sockets Layer (SSL) protocol can in some cases manage the security of Brio file transmissions between the Web server (within the trusted network) and the client's Web browser (in the extranet). SSL is based on public-and-private key encryption. Brio's Web clients support the Secure Socket Layer (SSL) protocol for "View (1)" and "Analyze (3)" Adaptive Report modes. However, interaction between the Brio Web client and the Web server is based on standard HTTP. This means that documents with query processing privileges (2, 4 and 5) may not be reprocessed to the database via SSL. As mentioned above, these requests are still transmitted in a compressed binary format, not in a clear text format.

To protect your critical data transmissions (such as password authentication) via SSL while still supporting users who need processing functionality (Adaptive Report modes 2, 4, and 5), a JavaScript "onClick" event can be defined. The onClick event redirects the processing request to a non-SSL enabled Web server for processing. This way, you can use an SSL-enabled server to handle the password authentication transmissions at login and to retrieve documents, while still allowing for the processing of documents. When a user processes or shows limit values, the "onClick" event is triggered and the request is sent to a non-SSL enabled Web server. Support for pure SSL is a future direction for Brio. A technical note describing how to implement the "onClick" event described above is available on Brio's Web site (www.brio.com/support/tn2.html).

Distribution via the Broadcast Server in a Pure SSL environment

Another option for pure SSL environments is to use the Broadcast Server to automatically process documents based on a variety of events, such as a database update, and then to re-post the document to the OnDemand Server. This ensures that a user's document list is always populated with documents and reports containing the most current data. By eliminating the need for users to refresh their data set, you reduce network traffic during peak hours, while still granting users access privileges to analyze data and create new reports.

The Diverse Extranet User Base

Your company's extranet community has access privileges and preferences as diverse as the needs of your internal user base. Some Extranet users will be licensed Brio.Quickview and Brio.Insight users, viewing and analyzing Brio documents via their Web browsers. Others wish to view or analyze data exported from BrioQuery to various other file formats such as Microsoft Excel. Brio's extranet solution extends to those partners or distributors who do not wish to use or are not licensed to use Brio's Web products.

The Broadcast Server can send e-mail attachments to specific individuals, or post files to secure FTP or Web servers. In each case, you can leverage the security built into the servers themselves. Jobs can be set up such that when the Broadcast Server posts a Brio file to a Web or FTP server, it also sends an e-mail to the intended recipients notifying them that the latest data is posted and where to locate it.

BRIO ENTERPRISE MANAGES SECURE DATA ACCESS THROUGHOUT THE ENTERPRISE

Information distribution mechanisms are constantly changing to provide and share information with people around the world. Brio is on the cutting edge of this technology and is the proven leader in providing secure business intelligence to your organization.

As we have seen in this white paper, Brio effectively manages data access throughout the complex user base in today's enterprise, while still allowing IT personnel and DBA's the flexibility to utilize their security systems already in place. Brio's broad set of security features, combined with your built-in database security, allows for security down to the row level. Meta layer objects in the Brio Repository, such as data models and standard queries, allow the BrioQuery Designer to provide access to only those tables and columns that each user group has privileges to. Linking and locking these documents adds extra security through ADR (Automated Distributed Refresh), ensuring that even if a user groups' access privileges change, they will always have the most up-to date version of a given document.

With the Broadcast Server handling the processing of documents, DBA's need only grant database access to a few specific users, enabling the DBA to have tight control over database access. In addition, since the output methods for the Broadcast Server are protected, those users with scheduling privileges cannot post sensitive information to users lacking the proper access privileges.

With end-users increasingly demanding the increased productivity promised by Web-based analytical tools, the network of users and the specific security implications have become more complex. Brio has a uniquely flexible, yet powerful solution for managing Web-based data access. Adaptive Report technology sets a new standard for balancing security with functionality in business intelligence tools. This capability enables organizations to safely deploy a full range of functionality to end-users across the Web without compromising security or deploying and managing incompatible systems. Reporting, combined with Brio's Open Authentication Model, create a safe environment for information producers that is both easy to maintain and very secure.

As customers increasingly prefer online interactions and business-to-business partnerships become more crucial to your company's success, corporate information needs to travel outside the corporate firewall. Information must be made available in a flexible and time-effective manner, without exposing sensitive and proprietary data to hackers or competitors. Brio's extranet solution uses its own and standard Internet security methods to allow you to open up portions of the data warehouse to selected customers, partners, distributors, and supplier—without compromising the security of your internal systems or computers.

APPENDIX A

BRIO ENTERPRISE 5.5 PRODUCT SUITE

Brio Enterprise is the first enterprise query, reporting and analysis product line to deliver no-compromise, full-featured business intelligence for Web, client/server and mobile users. Brio's product line is fully integrated, easy to use, and delivers high performance in direct connected, disconnected and distributed Web environments. Since Brio's products run across all the platforms that are critical in today's growing enterprise, they work within existing IT infrastructure and give IT managers choice when purchasing new client and server systems.

With Brio Enterprise, everyone in today's enterprise can access the information they need to make qualified, informed business decisions. Whether you are an information producer, an information consumer, a road warrior, occasional user or an every day user, insight into important business issues has never been easier. The Brio Enterprise product family includes three categories of products.

| <i>Client/Server Clients</i> | |
|-------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| BrioQuery Designer | Query, analysis and reporting with database administration functionality, security, auditing, and Repository setup (for IT departments). |
| BrioQuery Explorer | Query, analysis and reporting with direct access to database tables and a Repository of pre-defined data models and reports (for power users). |
| BrioQuery Navigator | Query, analysis and reporting with access to Repository of pre-defined data models and reports (for active analysts). |

| <i>Brio Enterprise Server</i> | |
|--------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| The OnDemand Server | A Web application server that enables querying over the Web, zero administration clients, report level security and Adaptive Reports™. |
| The Broadcast Server | A query server that schedules and automates query processing and report distribution via Email, networks, printers, FTP and the Web. |

| <i>Web/Intranet Clients</i> | |
|------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Brio.Insight | Browser-based query, analysis and reporting with varying levels of functionality based on report information and user security (for active analysts and report users). |
| Brio.Quickview | Browser-based report viewing and refreshing of data views (for report viewers). |

Please visit Brio Technology at www.brio.com for further product and company information. You can also call (650) 856-8000 or (800) 879-BRIO.