



Protecting Valuable Enterprise Information

A White Paper from Brio Technology

TABLE OF CONTENTS

4	INTRODUCTION
4	PREVENTING UNAUTHORIZED ACCESS
4	SCALING TO MEET USER DEMANDS WHILE ENFORCING SECURITY
5	STREAMLINING SECURITY TO AVOID ADMINISTRATIVE BURDEN
5	BRIO.PORTAL: SCALABLE SECURITY FOR THE ENTERPRISE AND BEYOND
5	DISTRIBUTED ARCHITECTURE ENSURES SCALABILITY
6	THE GATEKEEPER FOR USER ACCESS: BRIO.PORTAL SERVICE BROKER
7	PREVENTING UNAUTHORIZED ACCESS WITH PERMISSION CLASSES
7	STREAMLINING LOGINS FOR DYNAMIC REPORT EXECUTION
8	REDUCING ADMINISTRATION WITH EXTERNAL AUTHENTICATION
8	FLEXIBILITY WITH EXTERNAL AUTHENTICATION OPTIONS
9	TRANSPARENT LOGIN WITH SINGLE-SIGN-ON
9	ENSURING SECURITY WITH SESSION KEYS AND SESSION COOKIES
10	SECURITY FOR EXTRANETS
11	ABOUT BRIO TECHNOLOGY

PROTECTING VALUABLE ENTERPRISE INFORMATION

Brio.Portal™ provides secure, streamline access to enterprise information.

Opening up information access across the enterprise does wonders for accelerating the business decisions that generate revenues. In fact, as companies explore business-to-business relationships, sharing critical information is becoming a necessity for making decisions together. The Enterprise Information Portal (EIP) plays a central role in open information access—organizing the flow of vast amounts of internal and external information, tying together structured and unstructured data, and steering decision-makers towards relevant content.

But providing open access to information can leave the enterprise vulnerable. EIPs must prevent unauthorized access to enterprise information—without adding administrative overload for overworked IT departments. This paper describes these challenges, and explains how Brio.Portal provides secure, streamlined access to enterprise information.

PREVENTING UNAUTHORIZED ACCESS TO ENTERPRISE INFORMATION

While the Internet has opened wide the doors to information—helping corporate decision makers to find relevant content via Enterprise Information Portals—it also raises many security concerns for enterprises. How can the enterprise keep its sensitive information secure so that only authorized individuals in the company can access it? As corporate boundaries dissolve with business-to-business arrangements, how can the enterprise ensure it's only sharing the information that's necessary? As enterprises extend access to business partners and customers, the corporate boundaries are beginning to blur. While extranets enable these new categories of users to access

enterprise intranets, they also raise a whole new set of security concerns. Inadvertently, extranets expose previously private network environments to any hacker or cracker with Internet access.

Enterprises need to ensure that their EIP does not provide the wrong kind of window into the enterprise—one through which unauthorized people can slip. EIPs must offer a permissions scheme that determines which users can access what information. To secure enterprise systems from external hackers, it must also offer robust authentication with secure network transactions.

SCALING TO MEET USER DEMANDS WHILE ENFORCING SECURITY

The Internet has truly caused an information revolution. Now hundreds to thousands of users are accessing the Enterprise Information Portal to find the precise information they need to make a decision—today. On the back end, the EIP is accessing critical data in all sorts of legacy systems to report back to the user. How can all of these users create the reports they need from the data in these legacy systems—without waiting an undue amount of time for the results?

To pass muster, the EIP must scale to meet the needs of the extended enterprise while maintaining the highest levels of security. To do so, the EIP must implement a distributed architecture that can replicate services to meet high user demands with fast response times. The EIP must protect these replicated portal services across widely distributed computing environments, and tightly secure user access to business intelligence content and systems.

STREAMLINING SECURITY TO AVOID ADMINISTRATIVE BURDEN

Many enterprises look to their IT staffs to shore up potential information leaks. But the systems issues abound when integrating legacy systems that each uses their own authentication methodology. The move to distributed computing has resulted in the proliferation of specialized servers, each with a separate set of user accounts. The need to define users and passwords in each of these systems individually, and to replicate changes and revoke access privileges or delete users across all of them, has created a huge administrative overhead. It also creates problems for users when generating reports that access data in multiple legacy systems because users have to remember multiple login names and passwords.

IT has more administrative overhead because they must secure information objects by assigning individual security attributes. As the numbers of objects and users has grown, IT departments have quickly become overwhelmed. How can IT managers ensure adequate security for accessing information from the EIP and the legacy systems that house the data it organizes—without creating an administrative nightmare?

EIPs must help IT managers by ensuring security across all business intelligence objects—without adding to IT administrative overhead or placing additional burdens on users. To achieve operational scalability, EIPs should minimize the need for users to remember (and administrators to manage) multiple user login names and passwords. Using a centralized authentication system stops the proliferation of passwords and accounts, and reduces administrative overhead. Better yet, EIPs should implement a single-sign-on scheme that authenticates users once, and then lets them initiate

multiple application sessions as they research information in the EIP.

BRIO.PORTAL: SCALABLE SECURITY FOR THE ENTERPRISE AND BEYOND

Brio Technology's Brio.Portal™ 6.0 is a robust enterprise portal platform with unmatched security that enables IT professionals to provide broad access to business intelligence systems and information—without compromising these systems in any way.

With Brio.Portal's proxy-based database access, administrators can define rules that govern object-level access, without creating an administrative nightmare. Brio.Portal's session-management features simplify user account management by offering several different user authentication schemes that can be adapted for unique enterprise environments. And Brio.Portal ensures secure business-to-business operations—enabling business partners and customers to access appropriate enterprise information via Web-based extranets.

Brio.Portal's distributed architecture easily scales to meet enterprise demands: ensuring fast response times for hundreds to thousands of users while maintaining security with its robust authentication.

DISTRIBUTED ARCHITECTURE ENSURES SCALABILITY

Brio.Portal's modular distributed platform scales across the entire extended enterprise without sacrificing performance or security. It includes several specialized service agents that implement services for storing, managing, and generating information objects. These services can be replicated to support a scalable and broad-based reporting and information delivery system.

- **ONE/Name Server™** provides directory lookup and initialization service to other service agents and manages their configuration information.

- **ONE/Service Broker™** provides session-management services and acts as a gateway server to the service agents that actually fulfill user requests.
- **ONE/Authentication Server™** authenticates users who connect to Brio.Portal through its ONE/WebClient client service.
- **ONE/Repository™** services requests to store or retrieve objects, or to search or browse through the object repository.
- **ONE/Job Factory™** requests services from external DBMS or ERP systems and then delivers the job output.
- **ONE/Event Server™** offers scheduling services to One/Job Factory agents, and also provides a notification service to which users can subscribe.
- **ONE/WebClient™** is a browser-based client service that controls what users can see and access through Brio.Portal.

Security is ensured by the ONE/Name Server. At startup, each service agent requests its configuration information from ONE/Name Server. This information includes the port number at which the service agent will “listen” for requests. Before requests from these service agents are fulfilled, the ONE/Name Server authenticates the service agent—thereby providing security for the distributed system, while enabling Brio.Portal to provide faster response times via agent replication.

THE GATEKEEPER FOR USER ACCESS: BRIO.PORTAL SERVICE BROKER

Brio.Portal enforces security across the network—even when it extends beyond corporate firewalls—so enterprises can provide access to customers, suppliers, telecommuters, and mobile users. Its network-level security incorporates a kerberos-like authentication scheme and robust session management that integrates with Secure HTTP for sending encrypted

information to and from browsers outside the firewall.

The key to Brio.Portal's user access security is ONE/Service Broker. This service provides a gateway to other Brio.Portal services. All Brio.Portal clients connect to the Service Broker—they do not interact directly with any other service. Service requests from users come in to the Service Broker, which then routes them to the appropriate service agents. For example, requests for browsing, searching, retrieving, and publishing tasks are routed by the Service Broker to the Repository agent. Similarly, the Service Broker routes scheduling and subscription tasks to the Event service agent for fulfillment.

To create sessions with Brio.Portal, users must identify themselves with registered user names and provide passwords for authentication. When users log onto the Service Broker, they are screened by an Authentication agent that compares the passwords they enter to the ones associated with their user names in the Brio.Portal database.

Passwords are never sent across the network in the clear. Instead, the client and Service Broker negotiate a random session key that is used to encrypt the password for transmission. Each session generates a unique session key that is valid only for the duration of the session and is not stored and reused.

This gateway architecture gives client components a single point of contact for a number of widely distributed services, and shields them from changes to the configuration and connection information for each individual service. This architecture also limits the number of systems that require access to secure information about services.

PREVENTING UNAUTHORIZED ACCESS WITH PERMISSION CLASSES

Brio.Portal ensures that users only see and access the content for which they have permissions—enabling enterprises to broaden information access to partners and customers without fear of security breaches. User access to business intelligence objects is restricted by Brio.Portal permission classes. All Brio.Portal objects—such as categories, reports, and documents—have an access-control attribute that administrators assign. This attribute defines two classes of permissions: level and type.

- **Permission level** determines which users can access the information object: the object's owner, specific individuals or groups, or all users.
- **Permission type** indicates what actions authorized individuals and groups can take: read, read/write, or read/write/execute.

Security is further enforced at the browser level because Brio.Portal customizes what each user or group sees—depending on their permissions. When users submit queries through Brio.Portal, they see only the objects to which they have some level of access rights. Other objects are completely hidden and don't appear to exist at all. Thus, a user who asks for a list of available reports might only see a small subset of the list that the same query generates for someone with broader access.

The administration of Brio.Portal access rights can be delegated to a "super user." This individual has access to any object and can create new Brio.Portal users and assign their rights. While each object can have only a single group associated with it, this group can consist of multiple groups, or a combination of groups and individuals. The administrator can further refine access rights to objects by assigning security

attributes that are associated with users. Administrators can also restrict which users are allowed to execute new reports, and which can only view existing reports.

STREAMLINING LOGINS FOR DYNAMIC REPORT EXECUTION

Brio.Portal generates reports that are populated dynamically by drawing the latest information from various data sources in the enterprise. With all of the legacy systems Brio.Portal accesses to deliver enterprise reports, users can quickly become overwhelmed with the multiple logins and passwords used by each system.

Brio.Portal supports a variety of methods for accommodating these external security systems. Administrators can assign database passwords to each application that queries a particular database; assign a certain level of database access privileges to specific reports; or base database access on the rights of the individual user who is running the report.

When access is based on the individual user's rights, Brio.Portal can be configured to prompt the user successively for the passwords to each data source. However, another option is to provide transparent access to these data sources without requiring a password from the user. Brio.Portal can store the database passwords for the report execution, protecting them with two-way, 64-bit DES encryption.

When a user then executes a report, Brio.Portal passes the stored password to the report server so that it can connect to relevant databases and collect the requisite information. The individual generating the report does not have to be defined as a user in any of these source databases, because Brio.Portal is serving as a proxy that provides access to them. Database security is not compromised because users

can only access the databases when executing Brio.Portal report jobs that they are authorized to run.

REDUCING ADMINISTRATION WITH EXTERNAL AUTHENTICATION

Although Brio.Portal includes an enterprise-class authentication system, companies may prefer to leverage investments in existing directory services, or to centralize authentication services altogether. To support these approaches, Brio.Portal can access the user-profile information in ERP systems or integrate with the directory services in LDAP, UNIX, or Windows NT environments. Brio.Portal thereby uses the existing authentication schemes of enterprise systems like databases and ERP applications. When objects are generated by external business applications, Brio.Portal automatically assigns security levels to them.

With Brio.Portal's external authentication, all servers use a centralized directory of user account and authentication information. Brio.Portal uses Lightweight Directory Access Protocol (LDAP)—defined by the Internet Engineering Task Force—to enable its external authentication. LDAP provides a standard, Internet-based API for directory access. Network applications and services that support LDAP can authenticate users through an external LDAP-compliant directory, which greatly reduces the password-management burden for administrators.

Using an external authentication system eliminates the need to create user accounts and store passwords in Brio.Portal, and saves users from authenticating themselves separately to the portal. When Brio.Portal is configured for external authentication, its Authentication agent uses a driver to interface with the external directory service and authenticate users. This driver can also be used to obtain a list of authorized users and information about their group memberships.

Brio.Portal comes with an LDAP driver that can be customized for particular LDAP-based directory services. It also includes an Authentication Driver API that enterprises can use to develop interfaces to any internally built directories or proprietary systems that manage user accounts and passwords. As an added security measure, the Authentication Driver treats all external authentication data as read-only information and does not provide a mechanism for altering it.

FLEXIBILITY WITH EXTERNAL AUTHENTICATION OPTIONS

Brio.Portal's modular architecture creates a very flexible environment that enables multiple modes of external authentication. It allows administrators to separate the authentication function from the user-account database and let an external directory service handle the former while maintaining the latter in local storage. Administrators can also choose between automatic and manual user-definition modes.

- **Automatic Mode:** The automatic mode is particularly useful when all users in an existing directory service are to become Brio.Portal users. As users log into the new Brio.Portal system for the first time, they automatically become Brio.Portal users. No intervention by the administrator is required.
- **Manual Mode:** When administrators want to be more selective about adding users to Brio.Portal, they can use the manual user-definition mode. Users are manually defined in Brio.Portal, but their passwords are not. When operating in this manual mode, the Authentication agent lets users login to Brio.Portal if they are defined in the external authentication system, and provide the correct password to the external system.

It then defines the user in the Brio.Portal database. The external directory handles the actual authentication.

Brio.Portal also offers flexibility for defining the groups to which users belong. Groups that have already been defined in the external authentication system can be readily used in Brio.Portal. This eliminates the need for administrators to recreate the same groups. Additionally, administrators can define and manage groups within Brio.Portal, even when users are defined by an external authentication system.

TRANSPARENT LOGIN WITH SINGLE-SIGN-ON

Brio.Portal supports single-sign-on so that users can be authenticated once, and initiate multiple application sessions. To accomplish single-sign-on, the ONE/WebClient agent establishes trusted relationships with other systems that have already authenticated users. These users can then start Brio.Portal sessions without entering passwords. Brio.Portal's transparent user login enables enterprises to use their Web server's security system to secure access to all of the Brio.Portal Web Client agent's URLs. Transparent user login is also useful for pre-authenticating users before allowing access to any Web-based application.

Trusted environments and single-sign-on systems can take many forms. In some environments, a Brio.Portal user has been pre-authenticated by an external system before accessing Brio.Portal for the first time. In this scenario, Brio.Portal can be configured to require that the user enter a password. Brio.Portal can also re-authenticate the user without requiring a password by seamlessly accessing the user's authentication credentials in the background. With the latter approach, the user name and password must be available to Brio.Portal. In either case, Brio.Portal creates a unique session token for each user.

With transparent login, the Web server passes the user name and a password to the Brio.Portal Web Client agent. In cases where both the Web server and the Brio.Portal Web Client agent are relying on the same external directory for user authentication, the user's actual password should be used. Brio.Portal can also use a pre-defined password that is the same for all users. If Brio.Portal is being used with its native authentication driver, and users are not being authenticated externally, this is the best choice.

Brio.Portal offers several methods of passing the user name and/or password to the ONE/WebClient agent: as part of a URL, as a cookie, or via the HTTP header by using the HTTP Basic Authentication Scheme.

ENSURING SECURITY WITH SESSION KEYS AND SESSION COOKIES

Brio.Portal enforces security across the network—even when it extends beyond corporate firewalls to support customers, suppliers, telecommuters, and mobile users. Using network-level security that incorporates a kerberos-like authentication scheme and robust session management, Brio.Portal prevents security breaches.

The Service Broker manages all user sessions initiated by Brio.Portal clients—whether the client is a ONE/WebClient, ONE/Administrator, ONE/Publisher, ONE/Script, or applications written using ONE/API. When the Service Broker receives a user's login request, it routes the request to the Authentication Server that uses public-key cryptography to generate a session key. First, the Authentication Server passes the public key to the client. The client then uses this public key to encrypt the user's password and a randomly generated client key. The resulting session key is used to validate all further service requests from the client. When the client requests a service, it passes the session key to the Service Broker which

forwards it to the server that will fulfill the request. This server decrypts the password and validates it against the authentication system. If the authentication is successful, the server generates a server session key and encrypts it with the client session key. This unique session key is the token that the client passes with each subsequent request from the user for the duration of the session.

When a user is accessing Brio.Portal from their Web browser, a session cookie is created and passed between the browser and portal with each user request. ONE/WebClient uses this session cookie to determine whether an active session exists for the user. If there isn't one, the user login process is initiated. The cookie is valid for the duration of the session, which ends either when the user logs out of Brio.Portal, or when the session is idle a certain period of time (timeout length can be configured in ONE/Web Client). When the session is closed, the session cookie and the session key are discarded.

SECURITY FOR EXTRANETS

To work more efficiently across corporate boundaries, enterprises must grant partners, vendors, and customers access to their EIP. Brio.Portal accommodates these new categories of users and enables them to access enterprise Intranets via extranets that run across the public Internet—without exposing the enterprise's private network environment to hackers on the Internet.

Brio.Portal protects Internet access points with SSL—integrating with Secure HTTP to send encrypted information to and from browsers outside the firewall. Brio.Portal also offers a number of different firewall deployment options. One option is a double-firewall configuration that puts the first firewall between the extranet user and

the Web server running the Brio.Portal Web Client agent. The Web server sits between the first firewall and a second one that isolates it from the corporate Intranet. This second firewall passes requests from the Web Client agent on the sandwiched Web server to the Service Broker agent, blocking any other type of access. The Service Broker and all other Brio.Portal agents—except the Web Client—are hosted inside the private Intranet, behind both firewalls.

For additional information about Enterprise Information Portals, visit **www.aboutportals.com**—the Portal about Portals.

ABOUT BRIO TECHNOLOGY

Brio Technology, Inc. [Nasdaq: BRIO] is the only business intelligence software provider to offer a complete platform that addresses the decision processing needs of today's Web-enabled e-enterprise.

The Brio ONE platform—which includes Brio.Enterprise, Brio.Report, and Brio.Portal—enables organizations to build and deliver business intelligence, enterprise reporting and analytical applications to users in intranet and extranet environments, all with unmatched ease of experience. Brio ONE also enables customers to derive higher business value from all of their enterprise information sources, including enterprise resource planning (ERP), sales force automation (SFA) and customer relationship management (CRM) applications as well as data marts, data warehouses and others.

Brio products are available through direct sales and professional services organizations located in the United States, Canada, the United Kingdom, France, Germany and Australia, and more than 40 countries worldwide through VARs, resellers and distributors. Brio has commercial relationships with companies such as Hewlett Packard, IBM, Microsoft, Oracle, PeopleSoft, SAP and Sun Microsystems.

Brio Technology

3460 W. Bayshore Rd.
Palo Alto, CA 94303 USA

650 856 8000 | Telephone
650 856 8020 | Facsimile
800 879 2746 | In the USA

For worldwide contact
information, please visit:
www.brio.com

