



Access Control Excellence

Controlling Access To Business Applications

Best Practices Guide

Effectively controlling access to various business applications requires a centralized approach, enabling you to implement and enforce uniform robust security policies across your organization and easily collate activity data for both internal and external audit and compliance needs.





Mitigating Security Risk in Regulated Industries With Access Controls for Applications

As your business make more use of technology, and operations become more complex through globalization, outsourcing, telecommuting, and on-line customer relationships, you must also be more flexible when it comes to sharing information and applications.

However, providing adequate access controls for the extensive flora of critical applications containing confidential or personal data while keeping security risk at acceptable levels is no easy feat. It requires the right internal controls to make sure that your organization's business processes are correctly followed within the application, such as enforcement of Segregation of Duties (SoD). As well, these internal controls must be equally safeguarded by the proper external controls, protecting the integrity of the applications themselves against such threats as unauthorized access, eavesdropping, and man-in-the-middle attacks.

Controlling Access to Applications - The Key Components

In addition to having a well-organized patch management program and proper procedures for application change management, the ability to control access to applications is a vital aspect of securing your organization. Access control includes implementing mechanisms to make sure only authorized users access applications and that you can protect the data that is being processed.

Access control for applications enables you to establish and enforce security policies including:

- Allocation of end-users to defined roles in your provisioning workflows
- Allocation of application and data sets to clearly scoped and protected entitlements
- Attachment of user roles to defined entitlements

- Fine-grained authorization, enabling the correct access to entitlements by users
- Definition and enforcement of encryption requirements for user sessions
- Targeted authentication of users, including the ability to utilize second or third factors of authentication on the user's desktop before sessions are activated
- Centralized logging of all events around the user session
- Reporting and profiling capabilities to track user behavior
- And lastly, the ability to Single-Sign-On (SSO) to a selection of your applications

Fine-grained authorization refers to putting external controls in place to ensure that users can only access systems they are authorized to view and use including rules around when they can access an application, from what desktop, and using what communication protocols. Users can be organized by roles to ease administration.

Targeted authentication of users means that you can flexibly determine which method you want to use to identify that users are who they claim to be. Because applications and the data they are processing vary greatly in their sensitivity...you need the ability to selectively target where you want to require and enforce the use of strong authentication methods such as PKI, biometrics and tokens, and where it is appropriate to require the relatively weak form of user-selected password authentication.

Strong authentication of hosts means using mechanisms to identify that computers are who they claim to be, avoiding the comparatively weak identification provided by IP address and DNS name. The reason strong authentication of hosts is needed is that IP addresses and DNS names can easily be faked, allowing third-party computers to masquerade either as a client or as an application server, or as both in a so-called "man-in-the-middle" attack, giving potentially unauthorized individuals access to an organization's confidential information.



One way to *protect data traffic* is to encrypt it. This renders data unusable to eavesdroppers and protects sensitive information, including usernames and passwords, from sniffing programs. Data traffic transported in clear text across networks is clearly a security risk that can compromise the effectiveness of internal application controls.

Consolidated audit log and traceability is another aspect of external application controls that is important for organizations to consider. While an organization may have every confidence that its business applications are protected with adequate internal and external controls, it is essential to be able to prove that this is the case to internal and external auditors. Thus systems must not only enforce access, they must also produce records showing that the controls in place have indeed worked and security procedures have been properly adhered to. The ability to consolidate audit logs from across diverse applications greatly simplifies audits and compliance activities.

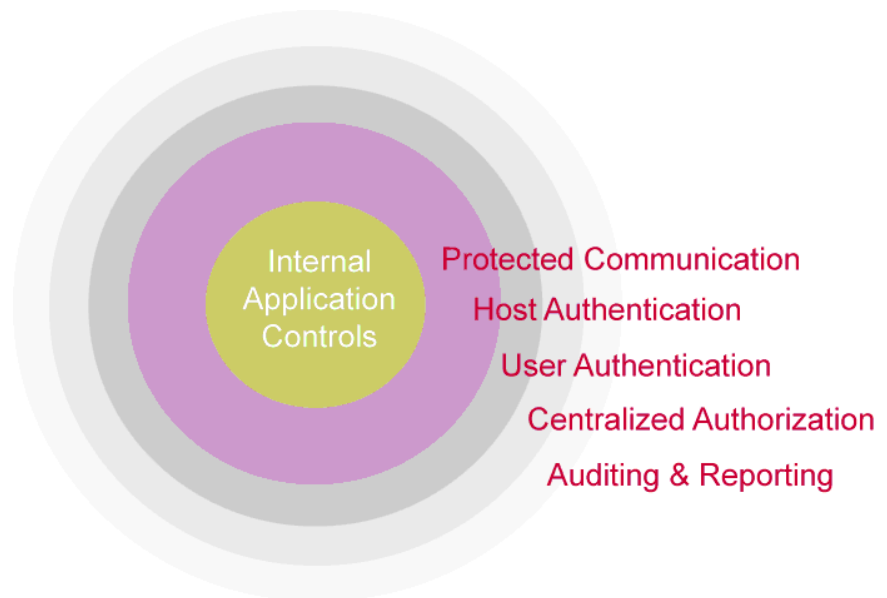


Figure 1: Multiple Levels of Assurance With External Controls

Taken together, these external controls can help ensure that applications operate according to an organization's security policy and can greatly reduce the operational risk associated with mission-critical applications.

FoxT ApplicationControl

In application security, it is an advantage to have only one general security system to protect many applications, rather than one security system for each application. A single system greatly simplifies administrators' work and provides centralized audit logging, giving an enterprise overview that makes it much easier to monitor application access and achieve compliance.

FoxT ApplicationControl helps organizations manage user access to networks that may include numerous local, client/server, and Web-based applications, each with its own authentication mechanism.

The access control solution from FoxT enables organizations to manage access rules to all applications from one central point in the network. Administrators have complete control over who can access applications, how much of the application can be accessed, when applications can be accessed, what authentication is required by specific applications, and from where the application can be accessed.

In such environments, FoxT ApplicationControl also enables users to log on just once to gain secure access to all of the applications they are authorized to use. As a result of this transparent single sign-on (SSO) service, users no longer need to create, maintain, and memorize multiple passwords and security procedures for different networked applications, and help desk calls related to forgotten passwords are reduced.

Once the user is logged on, FoxT ApplicationControl encrypts all communication between the user's workstation and the application server, including usernames and passwords, thus protecting data from interception.

Typically, no modification to the protected applications is required, and the FoxT Agent (the component that protects the application) is quick and easy to install.



FoxT ApplicationControl enhances an existing network infrastructure by providing:

- Centralized, flexible rule-driven control of user access to applications
- Flexible determination of authentication methods for both hosts and users with support for public key technology and two-factor devices such as tokens, biometrics, and virtual smart cards
- Protected communication between workstations and application servers
- Auditing and centralized logging of application access attempts
- Single sign-on for users
- User role mapping to allow users to log on to specific applications for a specific purpose.

Centralized, rule-driven authorization—FoxT ApplicationControl enables organizations to manage access rights to all applications from one central point in the network. Administrators have complete control over who can access which applications, how much of the application can be accessed, and when applications can be accessed. Administrators do not need to log in to all application servers to enable or disable an account. Instead, the user is added, removed, or blocked temporarily in the central security database for greatly enhanced security during lay-offs, mergers and acquisitions, and promotions.

Flexible authentication of hosts and users—FoxT ApplicationControl enables organizations to flexibly determine what authentication methods they want to utilize by application. The solution includes support for strong two-factor authentication using a variety of authentication devices, including virtual smart cards, biometrics, and tokens. Strong authentication ensures that only authorized users gain access to the network. Organizations that want to continue using password authentication have the option of using randomly generated, frequently changed passwords that the user never knows. In addition to strong authentication for users, FoxT ApplicationControl

performs authentication of application servers to make sure they have not been replaced by an unauthorized machine.

Protected communication between desktops and servers—In a typical desktop-to-application communication scenario, information, including usernames and passwords, is transferred in clear text over a network, which can result in passwords being compromised or other sensitive information being obtained by unauthorized persons. FoxT ApplicationControl encrypts communication between the desktop and the application host using strong encryption.

Consolidated audit logs and reporting—The auditing function of FoxT ApplicationControl provides a consolidated, centrally located audit log of all successful and unsuccessful user logon attempts for all protected applications. Instead of obtaining separate logs from each application, the administrator can consult the FoxT ApplicationControl's central audit log available from FoxT Manager (the security server component of the solution). This consolidated log makes it easier for administrators to monitor system access across applications and provide reporting data to auditors.

Single sign-on for end users—The single sign-on (SSO) service provided by FoxT ApplicationControl means that users need log on just once a day. They are then logged on to the various networked applications they are authorized to use transparently and automatically. Users no longer need to remember multiple passwords and security routines for applications because passwords are stored securely in the user credential. This capability has been shown to greatly reduce help desk traffic within organizations by minimizing logon-related calls, thus providing significant economic benefits.

Role mapping—Users who must access applications for different purposes, for example, as an administrator, tester, or ordinary user, may need different user credentials for each type of session. Role mapping allows users to indicate which set of credentials they need for a given session by allowing each set of credentials to be mapped to a unique role name. The user logs on using the appropriate role name for the



task he or she needs to perform, and the correct credentials are used to log the user on transparently. Other than the role name, the user does not need to know any details, such as passwords, about the user account and credentials with which he or she logs in.

FoxT ApplicationControl can be deployed on a wide range of platforms, including Sun Solaris, HP-UX, IBM AIX, Windows NT/2000, and Linux. In addition to several standard application interfaces, an SDK makes developing interfaces for other applications you may have very straightforward.

Summary

In an age where organizations in both the private and the public sector are increasingly required to protect certain information while making other information and process more transparent to outside scrutiny, gaining control over information and IT infrastructures is a pressing and difficult challenge.

Major Telcom Provider Secures Mission Critical Applications

Like most major services organizations, this leading telcom provider has mission critical applications processing a tremendously high volume of transactions. The company needed to secure their transaction information (3.5 million transactions per hour) because the information is used for billing customers and contains sensitive data. The company wanted to start off with a project that would protect one of their primary applications...SAP R/3.

The company required certificate-based logon to applications, role-mapping for federated identities, single sign-on, encrypted communication with application servers, and centralized logging of all user access activity. After reviewing several offerings, they selected FoxT ApplicationControl. The initial FoxT implementation enabled certificate-based authentication and centralized audit reporting for approximately 10,000 users accessing the organizations SAP applications, including those at affiliated organizations. The implementation also featured a seamless interface with the telcom's LDAP repository via SiteMinder.

Using the FoxT Agent SDK, a powerful toolkit for programming new application-specific agents, the organization has now expanded the FoxT solution footprint to include controlling authorization and authentication for over 40,000 users accessing 35 different applications including Oracle databases running on a variety of operating systems, the billing system, and a statistics package.

Copyright © 2010 FoxT. All rights reserved.

The document is provided for informational purposes only and the contents herein are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. The document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior permission.

FoxT logo is a trademark of FoxT, Inc. Other product and company names herein may be registered trademarks and trademarks of their respective owners.

