

# Solutions for Financial Services and Insurance Companies

FoxT Provides Tried-and-Tested IT Controls for  
Identity and Access Management

A FoxT White Paper

---

## ● About FoxT Enterprise Access Controls Management

FoxT Enterprise Access Controls Management provide identity and access management, security with strong authentication and time-saving, simplified administration:

- BoKS® Access Control for Servers (Unix/Linux servers)
- BoKS® Access Control for Applications
- BoKS® Access Control for Desktops

FoxT Enterprise Access Controls Management enhance existing Identity and Access Management infrastructure. Features that can be integrated include:

- Centralized user administration
- Centralized policy management
- Centralized audit logging
- Access control with strong authentication
- Single sign-on
- Encrypted communication and
- Credential management.

“As a bank, our first priority is to make money, but we also need to keep our auditors happy.”

Network Manager, Top U.S. Bank Holding Company

## ● Financial Sector IT Challenges

With financial services and insurance companies facing IT challenges on a number of fronts, FoxT is proud to present a solution that has been successfully deployed in some of the world's largest financial institutions for many years.

CIOs and network managers at banks, insurance companies and other financial service providers are typically tasked as a first priority with growing the business by helping to:

- Minimize trading times and costs
- Optimize branch office services
- Facilitate online banking and
- Support B2B services

All of these activities are strongly dependent on networked access and performance.



Another priority that financial sector companies must consider is how to make sure they are in compliance with regulatory frameworks and can satisfy their auditors.

Financial services and insurance company CIOs need to address a number of practical questions to ensure their IT infrastructure supports these twin goals of business growth and compliance:

- How can I effectively and safely provide services to customers and partners?
- How can I maximize the efficiency of user provisioning and network management?
- How can I position my IT infrastructure to pass security and other audits?

FoxT Enterprise Access Controls Management is a family of solutions designed for deployment in the enterprise and built on tried-and-tested BoKS® technology. This paper explores some of the areas where financial services and insurance companies are today using IT Controls to help cement their business success:

- Providing highly-available, secure technologies for the trading floor
- Providing secure access to data from branch offices
- Effective, efficient controls for data centers
- Achieving effective user provisioning in large environments
- Passing audits

## ● FoxT on the Trading Floor

Trading floor IT infrastructure has two principal requirements, both of which can make the difference between earning or losing vast amounts of money:

- 1) Availability
- 2) Security

System downtime can mean that deals are lost and therefore availability is a prime concern for trading floor desktop infrastructure. However, a lack of security in busy trading rooms can lead to catastrophic consequences.

Banks are typically “Unix shops” and there are historical reasons for this. Twenty years ago only Unix workstations provided the performance required for running real-time applications on trading floors. And their strong Unix preference also explains why the BoKS system is a preferred solution among system administrators at large international banks: BoKS is one of the world’s leading Unix/Linux security platforms.



FoxT has been working to help provide secure desktops for financial trading for many years, starting with Unix desktops when these were the industry standard and today also providing comprehensive desktop security solutions for Microsoft Windows workstations. Some of the features provided by FoxT Enterprise Access Controls Management in this space includes:

- Flexible, strong authentication of users using smart cards, digital certificates and password tokens
- Centralized inactivity monitoring and controls
- Centralized logging of who logged in when
- Role-based authorization based on access rules

## ● FoxT at Branch Offices

Financial institutions want to provide a full range of services to customers via branch offices, but achieving this involves accessing a wide range of potentially sensitive information held on servers and mainframes at data centers.

For example, downloading confidential information about customer accounts, rate information for loans and mortgages, and also uploading details about transactions taking place at the branch all involve transmitting sensitive information across potentially insecure networks.



Ensuring that front-end applications at branch offices are secure and can communicate securely with head offices and data centers is vital for financial service providers who want to maintain their reputation for integrity while offering a full range of services via their network of branches.

FoxT Enterprise Access Controls Management include the following features to safeguard the integrity of front-end applications at branch offices:

- Strong authentication to workstations at branches using smart cards, password tokens, and certificates
- Secure, encrypted communications for applications between branches and data centers
- Centralized audit logging of access to controlled applications and servers

“The FoxT solution isn't just about security and compliance... the solution also makes it easier to administer and manage our mixed-vendor environment. We see it as a big win when a security product actually makes life easier for our administrators as well.”

CISO, Top U.S. Bank Holding Company

## ● FoxT in the Data Center

It is indispensable to financial services and insurance companies, but the modern data center is an expensive resource, and finding efficient ways to manage and secure data can make a real difference to your company's bottom line. Having said that, it is not always easy to achieve a balance between efficiency and security. You need to get the work done in time, but you also need to protect your customers' data and pass your audits.



With the scope and number of IT services financial institutions are providing both for private and corporate customers burgeoning, the demands on data centers are greater than ever. Services such as online banking often require sizeable dataparks with multiple servers often running different computer operating systems.

At the same time, the demand for effective Business-to-Business services is growing steadily, and as financial service providers strive to work more closely with partners and corporate customers the need for flexible, secure access controls in backend environments is growing too.

When it comes to compliance, while the first two years of SOX compliance audits focused strongly on the application side, today we see the requirements hitting the floor of the data centers. Auditors are reluctant to accept omnipotent administrators with unrestricted privileges. Today, server security is key.

Maximizing the efficiency of data center administration operations and ensuring that proper controls are enforced to protect digital assets and pass audits are top-of-mind concerns for CIOs in the financial sector. How do you give

your administrators the tools they need to work effectively without violating corporate security policies or getting points from your auditors?

FoxT responds to these concerns with a wide range of practical controls that give you the operational flexibility you need coupled with enterprise-class security mechanisms. Features provided by FoxT Enterprise Access Controls Management include:

- Highly granular access controls for heterogeneous Unix/Linux server environments
- A wide range of authentication options to prevent unauthorized access
- Secure, controlled single sign-on to maximize administration efficiency
- Domain-wide managed SSH providing encryption and access management
- A robust set of controls on privileged accounts
- Centralized management and policy enforcement

FoxT has a long history of providing robust controls designed to both simplify and secure management of data centers. With an outstanding track record in the financial services and insurance sector, FoxT Enterprise Access Controls Management offers a unique set of features in one solution that promotes efficiency, security and compliance.

“One administrator on any LDAP server can mess up our entire domain. LDAP is just too easy to break.”

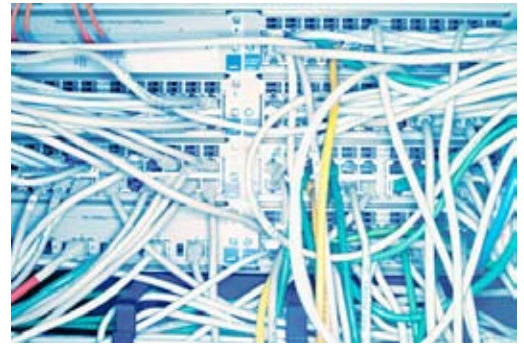
Network Manager, Top U.S. Bank Holding Company

## ● FoxT for User Provisioning and Network Management

Financial services and insurance companies typically work with extremely large IT environments that contain a lot of data, and large amounts of users. Added to this, the many mergers and acquisitions in this sector in recent years have compounded the challenges faced by IT departments when it comes to user provisioning, as it has often required them to quickly assimilate and organize new user and host populations.

This situation is compounded by the fact that some commonly-used network management utilities are increasingly falling foul of auditors due to their inherent lack of access controls. In the world of Unix and Linux, this is true of the NIS and NIS+ utilities, whose administration benefits are undermined by the difficulty of securing them and being able to show auditors that they are not open to misuse. Similar concerns are being aired about LDAP-based management systems and applications.

Quite simply, NIS and LDAP do not offer audit-proof user authorization and access controls, or central auditing of the system. It is all but impossible to enforce limits on the actions of NIS and LDAP administrators, or effectively trace what they have done. This is a serious flaw when it comes to compliance.



FoxT Enterprise Access Controls Management offers the secure and auditor-friendly solution to user provisioning and network management. Features include:

- Centralized, workflow-based user provisioning across heterogeneous operating systems
- Flexible management of user passwords, certificates and password tokens
- Integrates with existing infrastructure such as LDAP, Microsoft Active Directory, Tivoli, Sun and other provisioning systems
- Includes a range of useful tools to monitor and check the integrity of the BoKS domain
- Quickly provide users with precisely the access they need to systems to do their job
- Quickly and effectively remove access from users who leave the organization or change jobs

## ● FoxT at Audit Time

The financial services and insurance sectors have always been heavily regulated compared with many other industries, so in some ways banks and insurance companies were well prepared for the latest round of regulatory mandates including the Sarbanes-Oxley Act, Gramm-Leach-Bliley Act and HIPAA.

That said, challenges remain, particularly when it comes to achieving compliance in IT infrastructure. In approaching audits, it can often be tempting to focus on specific applications and making sure controls on segregation of duties are in place for those applications. While efficient Application Controls are crucial to ensure compliance in financial reporting, limiting compliance efforts to this can cause organizations to overlook the equally necessary controls on the hardware and operating systems those applications are running on. After all, there's no point in running SoD checks within financial applications if the servers they are running on are unsafe.



FoxT Enterprise Access Controls Management focus on providing a robust controls framework at the operating system level, ensuring that common policies can be enforced across different operating systems. Coupled to this, domain-wide reporting tools and centralized audit logs provide invaluable input for audits and allow organizations to prove that they are actually enforcing data controls as designed.

These are things the auditors want to know regarding your organization's IT controls:

### Security Policies

- Who can access which system and service today?
- What policies do you have for authentication (password aging, tokens, etc.)?
- How do you enforce them?
- How do you verify the integrity of sensitive configuration files?

### Audit Trail

- What exactly are administrators and other privileged users doing on systems with sensitive data?
- Which systems were accessed last month?

- Who accessed the systems?
- When did they access the systems?
- How did they get in?
- Where did they come from and was it permitted?

With FoxT Enterprise Access Controls Management in place, you can easily and quickly answer questions like these.

Key IT Controls features for auditing include:

- Flexible design of access controls
- Baseline reporting of access controls
- Centralized logging across the domain
- Powerful audit log reporting
- Key stroke logging

## ● About FoxT

FoxT offers a comprehensive and effective controls solution for corporate governance, risk, compliance and information security management. FoxT combines corporate controls, application controls and secure IT controls software into a single, integrated platform that provides continuous visibility into business processes and performance. Through smart integration and automation, FoxT solutions reduce total cost of ownership, deployment risk, and time to market, making compliance sustainable and transforming it into a source of competitive advantage. Headquartered in Mountain View, California, FoxT serves Global 1000 customers in 32 countries. For more information, contact Elliott Zember at +1 650 687 6248 or visit [www.foxt.com](http://www.foxt.com).



FoxT  
883 North Shoreline Blvd.  
Building D, Suite 210  
Mountain View, California 94043  
[www.foxt.com](http://www.foxt.com)  
650.687.6300

Copyright © 2007 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 and BoKS is a registered trademark of Fox Technologies, Inc. Other product and company names herein may be registered trademarks and trademarks of their respective owners.