

# Solving the Top IT Security & Audit Issues

A FoxT White Paper

---

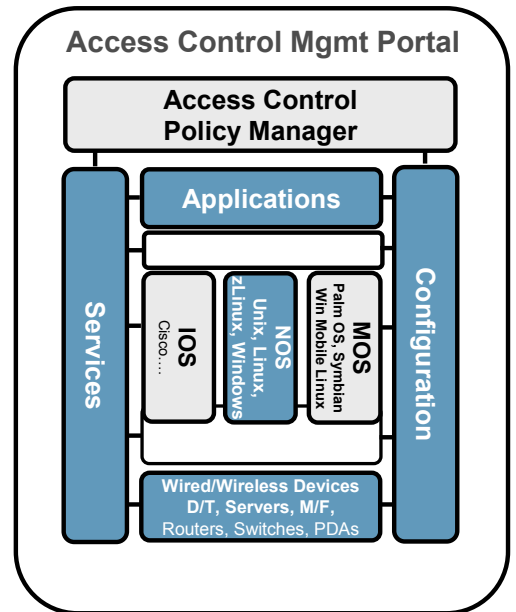
## The Source of IT Audit Pressure

There is increased scrutiny of how business applications, and the supporting IT infrastructure, are deployed, configured, and accessed. The scrutiny is translating into tougher IT audits, especially in server operating system services, data, and business applications security. Several macro trends are driving the increased IT audit pressure including new government regulations, globalization, and the need to improve energy efficiencies. Some of these trends have their roots in how auditors responded to Sarbanes-Oxley.

These macro-trends are creating several micro-effects for organizations including...

- Government regulations demand that businesses become more policy and audit driven, including the ability to provide proof that their information assets are protected from fraud and abuse, which can be initiated from within or outside the organization
- Business partners, in a globalized world, need to access portions of the information assets held within the partner organization in order to collaborate
- As the workforce becomes more mobile, and telecommuting more prevalent, there is a need to provide access from mobile devices and home offices to information assets held behind the firewall
- In a bid to reduce their carbon footprints, organizations are consolidating servers and using new technologies, such as virtualization, to maximize the capacity utilization of their data centers

These macro trends and micro effects make it imperative that physical and logical access controls are in place for both human and automated processes. And these access controls must cover the various layers of the enterprise information technology stack including hardware (in the form of wired and wireless devices), configuration and operating system services, databases and file systems, business applications, and other related services. In order to meet compliance and security policies, the access controls must be easily audited. As well, to address globalization, the controls need the flexibility to be enabled from both within and outside of the enterprise.



## What Are Some of The Top Audit Issues?

Besides physical access control, four of Gartner's "audit findings to avoid" relate to logical access controls:

- **Administrator Controls and Shared Accounts:** System administrator accounts have root account privileges to access any data and execute any application or transaction, typically with little or no tracking or control. Such accounts are not frequently tied to specific identifiable individuals making monitoring tools ineffective. There is a need for controlled delegation of privileged and root accounts with the support of appropriate (two-factor, if necessary) authentication and keystroke logging for sensitive sessions that can be later audited.
- **Identity and Access Management:** Access control and maintaining accountability becomes an exercise in futility if there is no authentication of the user or service that is accessing critical information related technologies. Having established the identity of the "user" it is critical that the "user" be authorized to perform only a specific set of actions be it access to operating system or configuration services, access to files or databases or to application services. Fine-grained authorization mechanisms with appropriate audit logging in place become critical features of an Access Control Management system.
- **User Activity and Log Analysis:** When appropriate logs are not recorded during the actual access of a system or service, it becomes impossible to produce a record of which employees have accessed which system when, and for what purpose. In other cases, the activity is recorded on the individual server or application...making it difficult to provide a consolidated record. The inability to provide appropriate log data can be a cause for failing an IT audit. Access Control Management systems need to centralize the user activity tracking and access logs to simplify audit reports, enable integrity checks, and facilitate real-time monitoring of user activity.
- **Segregation of Duties (SoD):** Segregation of duties (SoD) is an access control issue where the integrity of financial reporting could be compromised or fraud could be perpetuated if there are conflicting user access permissions across multiple business or custom applications. As the number of users for ERP and custom business applications increases, and business processes span multiple applications and instances, administrators are finding it very difficult to ensure that these conflicts of interest do not occur. SoD issues can also exist across the layers of the information technology stack. A good example: if a user is denied access to a business application, then (s)he also needs to be denied access to the database of the business application. It is crucial to bring SoD under the purview of the same central Access Control Management system that manages other layers of the information technology stack.

Another two of the Gartner audit findings relate to the inability of enterprises to protect data including:

- **Data Classification:** It is critical for enterprises to do an ABC analysis of their information assets and categorize such assets in a spectrum, from the most to the least sensitive, to minimize exposure to fraud and abuse. Such classification leads to consistent data protection policies that can be administered using manual and automated business processes. Enterprises that are unable to produce an inventory of assets and associated classifications may jeopardize their ability to pass an IT audit. These organizations need to find a solution that will help them classify data and protect information with auditable access controls and encryption methods.
- **Sourcing Controls and Partner Agreements:** With globalization comes the need for outsource partners to have access to information that may be considered sensitive to an enterprise. To pass audits, and protect sensitive information (either at rest or in transit), organizations need to produce evidence that they have agreements with their partners, have deployed appropriate business processes and remote access control systems, including the potential use of data encryption.

Businesses can also fail an audit when the right controls are not in place for documenting the changes that are made to applications, business processes, and underlying IT systems. Managing change in a controlled and auditable manner is critical. Organizations need a system that provides identifiable accountability for changes including automated approval mechanisms and detailed audit logs.

Other IT audit issues are introduced through the vulnerabilities of certain IT technologies. For example:

- Many auditors are asking companies to replace LDAP and NIS/NIS+ because they lack inherent support for authentication and authorization, making it difficult to track changes to user and host definitions
- Secure Shell (SSH) is another technology that creates audit issues. The problem: SSH provides a blank check to administrators to perform multiple, sensitive, operating system services that are not easily auditable. Fine-grained authorization for SSH is crucial to improving control.
- The use of SuDo is critical for many organizations. However, SuDo creates a security vulnerability that most auditors are not comfortable with. Organizations need an auditable control mechanism that will enable them to perform must-have, SuDo-like capabilities.

To avoid these IT audit issues and address the vulnerabilities exposed by certain technologies, organizations need a holistic, enterprise access controls management solution. Through better access controls management, organizations can proactively address the challenges that a highly regulated, globalized, energy-conscious world delivers.

## Access Controls Management: The Key to Simplified IT Audits

The ideal access controls management system should have the ability to:

- **Define policies:** The ability to centrally define access control policies across a complex IT infrastructure, including a diverse collection of servers, applications, desktops and other mobile devices, is the first step toward streamlining IT audits and security administration.
- **Administer policies:** Organizations need the ability to centrally administer access control policies. It is important to distinguish policy definition from policy administration. Policy definitions reflect the aspiration of a corporation and set a benchmark for evaluating and auditing the way the actual policy has been administered. Administered policy may deviate from defined policies due to the constraints of the deployment environment. Such deviations expose compliance vulnerabilities and risks to the corporation and must be mitigated.
- **Manage changes to defined and administered policies:** Defined and administered policies may change due to fluctuating business needs. However, it is important that all changes are controlled through an auditable (and ideally automated) approval process. The other critical piece of change management is that all changes be logged, including qualifying attributes, to facilitate external auditing and aid in resolution of any problems that arise from the changes.
- **Enforce policies:** The access control management system should determine the granting or denial of access based on administered policies and the credentials of the “user” trying to access systems. Most importantly, the access control solution should control access to IT systems that materially matter from a security and compliance perspective. Again, the access control management system must maintain a detailed audit of all access grants and denials.
- **Monitor and report to ensure compliance to security policies:** The last and perhaps the most important aspect of an access controls management system is that it enables a feedback loop for continuous improvement, while easing the process of auditing against defined

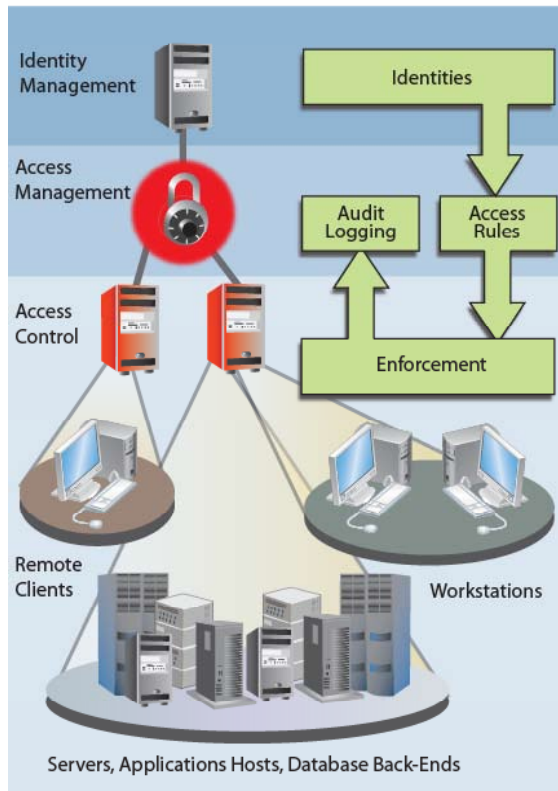
compliance and security policies. The system's ability to collect, correlate and correct enterprise-wide access controls, based on a centralized audit log, is a critical capability.

## FoxT's Enterprise Access Control Management Solution

Fox Technologies provides a comprehensive, highly scalable, enterprise access control management solution. The FoxT solution centralizes access controls management across operating system services, configuration services, applications, and information. This common infrastructure for managing access control policies across servers, applications and desktops combines the capabilities needed to effectively and efficiently address the top IT audit issues and core technology shortcomings.

Key capabilities of the FoxT Enterprise Access Controls Management solution include:

- Centralized enforcement and administration of security policies, access controls, and passwords across Unix, Linux and Windows servers including centralized audit logging
- Controlled delegation of root and privileged accounts with authenticated keystroke logging
- Managed SSH including host-based (2-factor, as needed) authentication and fine-grained authorization
- Data encryption of files on desktops and servers and encryption of communication between components to avoid man-in-the-middle attacks
- Single-Sign-On (SSO) capabilities to business applications and databases.
- Workflow-driven account and role management capability to streamline user provisioning and facilitate change management
- Centralized enforcement and administration of security policies and access controls across ERP, legacy and other packaged business applications
- Unified SoD and compliant user provisioning across applications to manage changes to application security models
- A highly customizable reporting capability to streamline audits and proactively identify areas for improvement



FoxT solutions are used by world-class IT organizations in the Financial Services, Manufacturing, and Telecom industries in Europe and the Americas. These large-scale, worldwide deployments of FoxT solutions control access to applications and tens of thousands of servers and desktops.



FoxT  
883 North Shoreline Blvd.  
Building D, Suite 210  
Mountain View, California 94303  
[www.foxt.com](http://www.foxt.com)  
650.687.6300

Copyright © 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.