



Access Control Excellence

## The New Gold Standard for Privileged Account Management

*The inherent limitations in the “all-or-nothing” administrator role, as super user in standard Unix, Linux and as local administrator in Windows servers, has created a market for privileged account management solutions. However, adding policy-driven privileged account protection to control session changes or privileged command execution using SUDO have been technical “band-aids” to overcome the architectural weaknesses of the operating systems.*





Controlling The inherent limitations in the “all-or-nothing” administrator role, as super user in standard Unix, Linux and as local administrator in Windows servers, has created a market for privileged account management solutions. However, adding policy-driven privileged account protection to control session changes or privileged command execution using SUDO have been technical “band-aids” to overcome the architectural weaknesses of the operating systems. In addition to still utilizing privileged passwords, all be it in a more controlled fashion, these technical band-aids also fail to control the root user from opening, changing and deleting pre-defined files and directories, making it difficult for organizations to achieve compliance with the latest PCI and HIPPA-2 regulations.

## How OS Vendor Role-Based Access Control (RBAC) is Changing the Privileged Account Management Game:

The maturing of role-based access control capabilities embedded in the OS and provided by the OS vendors has the potential to completely change the game in how organizations control administrative access to servers and data. Some of the core capabilities of the OS Vendor RBAC include:

- **Enables fine-grained, file-level segregation of duties:** RBAC enables organizations to implement fine-grained access controls to system administration commands, files and devices. Now IT organizations can easily specify and enforce, by role, who can access which files and system devices. You can protect files even from security and system administrators. For example, a system administrator can be granted the authorization to manage system files and objects, but not the authority to access the security system, nor database and application resources.
- **Remove all access to privileged system accounts:** RBAC provides the ability to easily allocate sub-administration rights to roles. Now you can delegate what have normally been “root only tasks” to normal, unprivileged users. The “super-user and “administrator” accounts are depreciated to such a point that they can be permanently locked away from normal use and that can be invoked only in a break-glass situation. Not only do you avoid the risk of assuming privilege with “su” and “sudo”, you can also utilize lower-cost personnel to perform system maintenance and administration.
- **Simplify administration and audits:** RBAC uses a more modern and robust security metaphor than current third party privileged account management solutions. A role-based enforcement model, where fine-grained controls are attached to roles, is a more straightforward approach both for user and support staff, and easier to audit.

## How FoxT Is Making RBAC a Reality for Organizations:

The vendor based RBAC is very exciting. However, because each OS vendor has implemented their own version of RBAC, it has been very difficult for organizations to leverage the value across diverse servers. FoxT is changing that with its new FoxT ServerControl – Extensible RBAC solution.

- **Common role-based access policies across all server platforms:** FoxT solutions are now leveraging the RBAC enforcement modules from the operating system vendors and adding value by providing a unified, cross-platform method for defining common policy and administration of RBAC across the diverse OS platforms. Vendor neutral policies are applied in vendor-specific mappings using the innovative FoxT mapping capabilities.
- **Automated RBAC-level administration and sub-administration:** Role-based policy is defined centrally by the FoxT solution and automatically deployed and activated on the disparate technical platforms from a single administration point. Now you can centrally define, distribute, and delegate privileged policies across various administrator roles.
- **Centralized logging and reporting:** Role-based access enforcement is typically logged locally per node in the OS vendor's unique RBAC module. FoxT centralizes and consolidates the OS vendor RBAC logging information and provides a single reporting and access control point.
- **Non-intrusive:** Unlike other access control solutions, FoxT, by leveraging RBAC from OS vendors, can provide file-level access control without kernel intrusion. With no association between your access control solution and the OS vendor, you won't have to recompile the UNIX kernel after applying critical operating system patches and then have to undertake extensive regression testing of mission critical applications.
- **Rapid implementation:** It is as simple as activating the RBAC module in your operating systems and linking them to the FoxT solution.

The latest compliance regime requirements are changing, demanding specific, granular controls that are approaching the outer boundaries of the capabilities of current third party Privileged Account Management solutions. By enabling organizations to leverage the capabilities of the OS vendor RBAC via the FoxT ServerControl solution, FoxT continues to lead in the delivery of cross-platform, centrally administered, enterprise access management with a low total cost of ownership.

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.

