



Access Control Excellence

## Securing Access to the IT Infrastructure: Predictions for 2012 that Every IT Security Pro Needs to Know

*The growing use of mobile devices and movement of resources to the Cloud are adding further complexity to access management administration, enforcement, and auditing. However, there are still some basic access management challenges that need to be addressed. Here is how we see it all playing out in 2012.*





## 1. Solutions Will Be Available to Centrally Administer and Enforce User Access Across Diverse Operating Systems, Business Applications, and Databases on Networked and Mobile Devices.

Software applications, databases, and the operating systems that support various networked and mobile devices are the lifeblood of any organization. Creating secure access to these components without hindering productivity is therefore a critical priority for security teams. The current heterogeneous mix of hardware and software components will force many organizations to use a mixed bag of approaches and access management point solutions, increasing risk exposure and the chance of breach.

There are two sides to the access management coin. Let's first look at how to control privileged user access. To control privileged user access and actions at the operating system level, some organizations invest in password vaulting to control administrator access to servers, a partial resolution to the bigger problem. Other organizations are using inefficient sudo tools to control access to Unix and Linux based systems, without doing anything to address access control to (and creation of) local accounts on Windows servers and desktops. Others may use two different privileged user management systems: one for Windows and another for Unix/Linux, again increasing administrative challenges and operating costs. And with the movement of IT resource dollars to the Cloud, further gaps in access control and regulatory compliance have surfaced.

On the flipside, let's look at end user access management. Controlling end-user access to the dozens of packaged and legacy applications and databases used by the typical organization is even more varied and challenging. To add to that complexity is the growing use of mobile devices and tablets, running on a variety of new and unique operating systems.

To control access to applications themselves, organizations are typically using some combination of built-in access controls for core systems such as SAP and Oracle, with perhaps a different single sign-on solution for basic end user authentication to other packaged and legacy applications. Neither option provides a holistic approach to multi-factor authentication and server-side authorization, leaving organizations open to man-in-the-middle attacks and the inability to ensure user accounts are effectively removed upon status changes. And as to the mobile devices and tablets, organizations are just beginning to explore how to tackle that access control challenge, with many still working to control access and local account creation on Windows desktops.

In all cases, administrative resources are struggling to efficiently and effectively adding and remove user accounts and access entitlements to all of these components. In most cases, accounts and access entitlements fail to be removed as employees are promoted and leave, creating longer term security and audit problems.

In 2012, *organizations will look to vendors for a unified platform that can cover both granular access control policy management and enforcement across their complex IT infrastructure.* Enterprise-grade access management solutions need to centralize policy administration and enforcement, including multi-factor authentication, granular authorization, and the consolidation of user activity logs across diverse operating systems, applications, databases for both networked and mobile devices, including resources managed in the cloud. The ability to define, administer, enforce and audit those policies from a single solution will become crucial. Organizations that fail to move towards a centralized access management platform will find it nearly impossible to effectively control access policy management and enforcement, further increasing the risk of a data breach. As well, without a centralized platform, organizations will be hindered from being able to fully embrace new mobile devices, the Cloud, and innovations in authentication capabilities.

These single platform enterprise access management systems need to easily integrate with existing IDM and Directory systems to automate the inclusion of access policy assignments as well as the provisioning and removal of user accounts from across the diverse operating systems and applications. Not only does the automated administration reduce operating costs, it also removes a key security risk of orphaned accounts that can be exploited for fraudulent purposes, as seen in 2011 headlines.

The ability to administer, enforce, and audit granular access policies across the software infrastructure from a single platform reduces operating costs, greatly simplifies IT audits and compliance reporting, as well as closes a number of security gaps to reduce the risk of costly insider fraud.



## 2. Controlling Privileged User Access Will Remain a Compliance and Security Challenge.

Organizations are offered a variety of solutions and approaches to privileged user access and identity management. Password vaulting provides the ability to control the check in/out of privileged passwords, but isn't effective for day-to-day privileged user authorization. Privileged user management solutions on the other hand provide a great way to remove the sharing of privileged passwords for day-to-day operations, but still require a vaulting capability for cold-start and break-glass situations. Bridging solutions enable Unix/Linux systems to operate fully within a standard AD environment, but don't provide full privileged access control or vaulting. As well, some vendors focus on either coverage for only Windows or Unix/Linux.

Because automated privileged delegation, vaulting and AD Bridging across mixed platforms are all needed in the ideal privileged access management solution, several vendors are moving towards more complete offerings.

The combination of *privileged user management* to control the daily actions of administrators for Unix, Linux and Windows servers with *password vaulting* for break-glass situations, and the ability to seamlessly administer the privileged access policies through an *AD bridge* or other IDM systems will give organizations greater flexibility in their approach to controlling privileged user access. As well, the complete approach to privileged user access management will find organizations implementing more centralized and comprehensive access management controls.

## 3. Controlling Local Windows Accounts on both Desktops and Servers Will Eliminate a Critical Security Threat.

Windows has become a significant platform for web applications and corporate transaction processing. Microsoft Active Directory also has graduated into a scalable platform for user management, including the distribution, operation, and action of Group Security Policies. Organizational reliance on the integrity of data held inside these server environments and the expectation of the correct use of the Active Directory security model has become essential.

Here's what's at stake: Each Windows server install will typically have between three and six additional powerful privileged accounts (in addition to Windows "Administrator"), controlling the operation of backup, monitoring software, and owning the files and data of application

and database software environments. *The setup, operation, and audit of these local accounts are outside the control of Active Directory Group Policies, creating a significant security risk for insider fraud.*

Local Administrator accounts available on Windows Desktop systems within an organization also create a critical security threat. These accounts might be used as service accounts for certain applications and are needed in order for them to run properly. However, if malicious software gains access to execute with permission of these accounts, then a great deal of damage could be done, not only to that specific system, but to the entire organization.

Semi-manual mitigations to protect these “local privileged accounts” from your privileged support staff include ad-hoc scripting, the use of shareware third party tools, or the implementation of Microsoft’s PowerShell. Each has their weakness and failing for controlling local accounts. Moreover, audit reporting on Windows local accounts requires the support staff to access these accounts on each server and desktop operating system, which takes on average two hours per operating system install, per audit cycle. And by default, the Windows operating system reports only on actions taken in the past; by then, inappropriate and fraudulent actions would have already occurred.

Insider threats on Windows servers will increase in 2012 as organizations play catch up in managing user access. In 2012, vendors will begin to offer comprehensive access management platforms, making it easier to centrally provision, administer, and enforce access control policies for privileged local Windows accounts, along with all of the other diverse operating systems used by networked and mobile devices. As well, the user activity logs will be automatically consolidated from across the enterprise for significantly streamlined IT audit and compliance reporting.

#### 4. The Realization of Role-Based Access Control (RBAC).

A few early adopter organizations began to explore RBAC in 2011 for controlling access to their Unix and Linux servers because RBAC provides the ability to control privileged user access down to the operating system resource and file level, offering greater security and segregation of access, without costly kernel intrusion.

The challenge still remained in that each Operating System vendor took a different approach to RBAC, which required additional work on the part of the organization to leverage OS-



Based RBAC, stifling its adoption. Leading Access Management solution providers also began to offer some RBAC 'harmonization' capabilities with their solutions in 2011. We predict the fundamentals of RBAC will become a subset of the broader Attribute-Based Access Control (ABAC) approach. In ABAC, roles are defined as a set of attributes in conjunction with a rule that is applied to the attributes. The attributes define the level of allowable access and can be used to control access to specific servers. As well, the attributes could be used to enforce access to other systems, databases, and applications. This creates a more flexible and dynamic way of applying and updating the access a certain user or group of users are given based (or denied) on attributes. The ability to leverage ABAC and the underlying OS vendors RBAC capabilities will provide even deeper and broader access management and control capabilities, and starting in 2012, organizations will look for vendors who can offer ABAC as part of their enterprise access management offerings.

## 5. Access Management Will Be Critical for Securing Resources in the Cloud.

Cloud-based resources are becoming more widely adopted than ever for unmatched scale, ease of use and cost containment.

From an access management standpoint, Cloud-based architecture is straight-forward. The server runs within a cloud network, such as Amazon Web Services (AWS), instead of inside the perimeter of the organization. As with physical servers, methods should be in place to remotely manage and control access policies for Cloud-hosted servers. The good news is that controlling access to servers in the cloud is similar to controlling the access to systems hosted internally. We predict one of the crucial aspects to access control in the Cloud will be automating the management and enforcement of privileged user access entitlements.

Organizations need the ability to take advantage of cost savings inherent in Cloud environments without jeopardizing security. In 2012, enterprise access management solutions will need to provide centralized, unified access control administration and enforcement across all heterogeneous devices, whether servers are located within the organization's perimeter or virtually available through the Cloud.

Copyright © 2011 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.

