Real Identity in a Virtual World

By Juan Martinez, Indigo Identityware, Inc.
Introduction

It seems as though we have come full circle. In the early 90’s we began pushing everything out to our client desktops. Most employees had their own PC, each loaded with the applications necessary for their work and each with access to the enterprise network. Now we seem to be bringing everything back to our servers. However, does the shift to VDI (Virtual Desktop Infrastructure) enhance, change, or affect our approach to Identity and Access Management? Are there any solutions out there which work equally well in both a client-based and a virtual world? This white paper will bring to light the challenges in store for the enterprise and what it takes to be on the leading edge of Identity and Access Management with VDI.

Since the dawn of the personal computer, there has been a need to control who can gain access to the computer, what information they can see, and what applications they can use; this is Identity and Access Management (IAM).
What is VDI?

Virtual Desktop Infrastructure, VDI, is the practice of publishing the desktop of a virtual machine that is stored on a central server. An end user may gain access to this virtual desktop through a local area network connection or a web interface. Since all processing and computing for applications within that desktop is performed by the virtual machine located on a central server, there is less regard to what hardware or operating system utilized by the local client to access the virtual desktop. The benefit and overall drive toward VDI stems from the ability to reduce hardware cost and easily maintain the virtualized desktops. Instead of applying changes and upgrades to each separate employee’s workstation, upgrades to applications and other changes can be easily pushed out to each one (or even all at once) in a fraction of the time. These factors all contribute to the appeal and attraction to VDI, but we cannot ignore the need to secure and control access to this new virtual world.

What is Identity and Access Management?

Since the dawn of the personal computer, there has been a need to control who can gain access to the computer, what information they can see, and what applications they can use; this is Identity and Access Management (IAM). One of the first and longest lasting tools used to control access is the username and password. While simple in the beginning, usernames and passwords have become extremely complex as a result of the fight against hacking and unwanted access. Now incorporating numbers, letters, case sensitivity, and even symbols, the strength of passwords has risen and, unfortunately, so has the difficulty to remember them. Newer tools in the IAM industry now include smart cards, proximity cards and personal identification numbers (PIN), password dongles and biometric devices. What impact does moving toward a virtual world have on utilizing some of these tools for authentication?

Challenges of Identity Management in a VDI environment

Though there are many benefits to move to the VDI environment, there are also challenges for IAM to secure access to the virtualized world. Resting the responsibility of protecting the enterprise’s private data and information within the virtual desktop (which can be accessed from anywhere in the world) solely on usernames and passwords is an open invitation for malicious activity. Here are some of the challenges ahead:
• Where do I add strong authentication for accessing the virtual environment?

• Can I extend an authentication device into the virtual world? I may want to authenticate the user again while they are in their desktop.

• What if I still want security in my local environment? I may also have local applications that need to authenticate the user again. Can I have both?

• What if I have a multi-user, “generic” workstation? How will that affect access to the virtual desktops? Can I rapidly switch users within the virtual environment?

Solutions to the Challenges

Where do I add strong authentication for accessing the virtual environment?

Answer: The first thought for managing access to the virtual environment may be to simply secure the access point; add strong authentication software and devices (proximity cards + PIN or biometric fingerprint readers) on the client workstation only. You may know, at that point, who is accessing the virtual desktop but that is not the only avenue for reaching the virtual world. Employ strong authentication, on the server side, within the virtual machine. A strong authentication vendor that can utilize the best authentication devices (proximity cards + PIN and/or biometric fingerprint readers) with little to no software on the local workstation allows for a minimalist approach to the thin client or other remote workstation that may be used to access the virtual environment.

Can I extend the authentication device into the virtual world? I may want to authenticate the user again while they are in their desktop.

Answer: YES. Not all strong authentication vendors allow a wide range of devices to be used in the virtual world. Some can only use a smart card and others no more than a proximity card. Make sure the vendor can provide the flexibility to support a wide array of authentication devices in the VDI environment; this gives you the freedom to choose what is best for you.

What if I still want security in my local environment? I may also have local applications that need to authenticate the user again. Can I have both?

Answer: YES. In the past you were able to have strong authentication devices for applications on the server side, but not for local applications. This was because vendors providing authentication in the virtual environment captured the authentication device as long as the VDI “portal” was open, making it unavailable for local use. That has changed. There is a small segment of
vendors now on the leading edge of the IAM industry that have developed the ability to share the device both locally and remotely (in the virtual environment).

What if I have a multi-user, “generic” workstation? How will that affect access to the virtual desktops? Can I rapidly switch users within the virtual environment?

Answer: YES. Make sure your strong authentication vendor has developed the means to log a user into a workstation using generic credentials, while maintaining the correct user in memory. These credentials are what are used to establish the virtual desktop connection the end user gains access to their personal virtual desktop. At the generic workstation, a new end user can authenticate locally and the virtual desktop connection is quickly switched to the new user’s personal desktop. These switches can be done repeatedly, each time establishing a connection to each individual’s own personal virtual desktop.

Summary
There is a definitive and powerful movement within companies and organizations toward the VDI environment, with expectations of cost savings and ease of maintenance. This calls for an equally important move for those in the IAM industry to provide methods for securing those connections and the applications within those virtual desktops. Only a vendor on the leading edge of software development possesses all of the tools necessary to overcome the challenges set by the VDI environment. Indigo Identityware, Inc’s strong authentication and SSO solutions give you the flexibility you need for the virtual environment; remote strong authentication, secondary authentication, local and remote strong authentication and SSO, and one-touch “live-user-switching”. Ask for our Proof-of-Concept and we’ll show you what we can do in your environment.

As an aide in assessing IAM VDI vendors and solutions, please see the attached Indigo VDI Challenge. It is an excellent tool to help break through various vendors’ claims of their IAM VDI capabilities.

Indigo Identityware’s strong authentication and SSO solutions give you the flexibility you need for the virtual environment; remote strong authentication, secondary authentication, local and remote strong authentication and SSO, and one-touch “live-user-switching”.

About the Author
Mr. Martinez is an Implementation Engineer at Indigo Identityware, Inc, in Minneapolis, Minnesota. He can be reached at jmartinez@indigoidware.
The Indigo VDI Challenge

All technical industry sectors have quality benchmarks and/or testing methodologies to assess the intrinsic capabilities of a product. For example, diagnostic imaging uses resolution phantoms. Filtration systems measure parts per million (PPM) of a desired (or undesired) chemical. If the intrinsic technical capability of a product is superior, the potential utilization of that product will most likely be superior.

In regard to identity management with VDI, we suggest that an organization consider the following four technical product capabilities as a “bell weather” for the clinical workflow capabilities of identity management in a VDI environment.

1. VDI with Remote Strong Authentication
   **Clientless server-based authentication**
   In a thin client VDI environment, show proximity card + PIN and one-touch biometric with the authentication and single sign-on functions occurring on the server...with no software located on the client.

2. VDI with Secondary Authentication
   **Multi-layer verification in virtual applications**
   Within that same environment, show multiple authentications occurring within the published application(s). Describe how many “layers” of authentication can be performed.

3. VDI with Local and Remote Strong Authentication (SA) & Single Sign-on (SSO)
   **Virtual & local applications simultaneously**
   With both a published desktop functioning and local applications functioning on a thick client, display one-touch biometric authentication and SSO functionality for each.

4. VDI with One-touch “Live-User-Switching”
   **“Generic” desktop with instant user recognition**
   While a desktop is published on a generic workstation, display proximity card + PIN and one-touch biometric authentication user-switching within the published desktop.

Requesting a VDI or Identity Software vendor to demonstrate these capabilities will facilitate a very interesting discussion about their ability to meet your secure workflow requirements.