Highlights from a recent webcast on enterprise network management

ADDING MACS TO YOUR ENTERPRISE? START WITH IDENTITY MANAGEMENT

Macs are in the enterprise to stay, and companies need to integrate them. Here's why IT should start with identity management.

Enterprise environments have traditionally been dominated by the PC, but in recent years, organizations of all sizes have seen an influx of Macs. Some attribute this trend to the fact that the Mac is the only computer that is able to run all three major desktop operating systems – OS X, Windows, and Linux. Others suggest that users who own iPads and iPhones became curious about what else Apple may offer and thus began adopting Apple computers such as the iMac or the Mac Book Pro. Still others have suggested that users have become dissatisfied with Windows because of Windows 8 and therefore began looking for an alternative. Whatever the reason, Macs appear to be here to stay.

Organizations that support both Macs and PCs have found that doing so can be challenging, even beyond the obvious support issues. In order for Macs to be a viable option in an environment that has long been dominated by PCs, Macs must provide an experience that is at least as good as that of a PC. Otherwise, there will be pushback from the users and / or the IT staff.

When it comes to enterprise usage, Macs are at somewhat of a disadvantage. Windows PCs are natively capable of being joined to an Active Directory and managed through various domain level policies. Although a Mac that is running a Windows operating system can be domain joined, a system that is running OS X cannot. This has historically made it more challenging to manage Macs than PCs.

If Mac computers are to be viable for use in highly managed enterprise environments, then there are four points of integration that must be achieved. These points are:

- **Identity Integration** – A user's account should ideally be valid across the entire enterprise regardless of which device type they are using and what resources they are accessing.
- **Security Management** – Users should be able to perform multi-factor authentication regardless of the type of device that they are working from.
- **Policy Integration** – Most enterprise class organizations have invested a lot of time into defining a comprehensive collection of group policy settings that provide the level of protection required by the organization. These group policy settings should ideally be applied regardless of device type.
- **Device Validation** – Over the last several years there has been a massive and totally unprecedented proliferation of devices. Administrators need a way of knowing which devices are being used on their networks and also need to know that those devices are being properly secured.

As previously explained, Macs are relatively new to the enterprise workspace. Although it was not completely unheard of for large organizations to have a few Macs, the Mac usage tended to occur in one-off situations. Only recently has Mac adoption occurred at any significant scale in the enterprise.

The rampant adoption of Mac computers has left IT professionals scrambling in search for a solution that will allow them to manage both PCs and Macs. One popular solution has been the use of the so called magic triangle.

The magic triangle refers to a three-pronged approach to device management. It is based on the idea that it is in an organization's best interest to adopt a best-in-class management solution for each device type. Windows Active Directory

> "The rampant adoption of Mac computers has left IT professionals scrambling in search for a solution that will allow them to manage both PCs and Macs."

for example, which is one of the three components that makes up the magic triangle, is probably the best environment for managing PCs, but it doesn't work very well for managing Macs because Mac computers running OS X cannot be Active Directory joined. Similarly, Apple's Open Directory for OS X Server works great for managing Mac computers running OS X, but it isn't an ideal solution for managing Windows PCs or Apple computers that are running Windows.

The magic triangle is made up of three components. These components include:

- Open Directory OS X Server
- Windows Server AD
- Mobile Device Management

These three magic triangle components collectively make up a best of breed management solution, but there are some major disadvantages to using this approach. One of the most obvious disadvantages is the cost. If an organization is maintaining three separate management systems, then they will incur roughly three times the hardware costs and three times the licensing cost that they would if they were operating a single management system. Of course there is also the administrative cost to consider. Administrators must be trained to operate, manage, and service three completely different systems.

A much bigger issue is that of creating IT silos. What happens for instance, if a OS X user decides that they need to log into a PC? If siloed systems are being used, then the user's account will only be valid for use on OS X.

In a situation like this, the administrative staff has three options. The first option is to limit users to working from their platform of choice. This is essentially telling the user that once they are a Mac user, they will always be a Mac user. The user remains locked into using one specific platform. This might be OK for day to day operations, but this approach can prevent a user from being able to get their job done in the event that a special project requires the user to temporarily work from an alternate platform.

A second approach would be for the administrative staff to create accounts on all three magic triangle tiers. Although this approach would theoretically allow users to work on whatever platform they choose, in practice this approach is completely impractical. Not only does it create more work for the IT staff who must create all those accounts, it can also increase licensing cost substantially. Furthermore, without some sort of synchronization solution in place, it will only be a matter of time before passwords fall out of sync, which means that users will constantly have to call for password resets.

The third solution is by far the most practical of the three. This solution is to adopt a third party identity management product such as Centrify Identity Service, Mac Edition that can provide identity management across multiple platforms. Such a solution would likely cost far less to implement and maintain than the magic triangle. Centrify's solution has the added benefit of addressing the four key points that were previously discussed – identity integration, security management, policy integration, and device validation. For example, Centrify Identity Service, Mac Edition allows you to apply group policy settings to both PCs and Macs.

Administrators who suddenly find themselves having to support Macs must carefully consider how they will support a multi-platform environment. Although a number of different solutions are available, neither Apple nor Microsoft offers a fully comprehensive solution. Administrators should strongly consider looking at third party management products.