

## Improving network access security for unmanaged devices

### Avenda Systems offers tips on how to keep unmanaged handhelds, laptops and guests under control

By Linda Musthaler, Principal Analyst with Essential Solutions Corp.

"Lions, and tigers and bears! Oh, my!" Anyone who has ever seen The Wizard of Oz knows that's the sum of the fears of Dorothy, Scarecrow and Tin Woodsman as they head into the woods on their way to Oz. For the network security administrator dealing with unmanaged devices, that refrain might be something like "handhelds, and laptops and guests! Oh, my!"

Fortunately for Dorothy, the menacing lion who jumps out of nowhere is no real threat. Alas, the security administrator is not so fortunate. Just one unmanaged device such as a contract worker's laptop can wreak havoc if it brings a nasty virus onto the network, or the person is allowed to access unauthorized data. Cleaning up the malware mess can feel a bit like being attacked by flying monkeys.

I turned to the experts at [Avenda Systems](#) to get their best practices advice about network access security and how to keep the unmanaged handhelds, laptops and guests under control. They talked about the issues their customers are facing. Perhaps you see your own organization in these scenarios.

The top menace these days is the proliferation of handheld devices that people want to use to access the corporate network. At one time these devices were primarily the domain of top executives and road warriors who simply wanted access to e-mail. Now, however, everyone with an iPhone, BlackBerry or some other smartphone wants access to enterprise applications beyond e-mail. The security admin can't

say no to the executives and knowledge workers who simply want to increase their mobility, agility and productivity.

A second problem is how to safely let guest users onto the corporate network. Temporary workers, contractors, vendors and business partners all may have legitimate needs to access at least portions of your network. Usually these guests want to or must use their own equipment, and you have little or no control over the health of the devices. It's imperative to restrict access to ensure the health and well being of your network as well as the security of your information assets.

Guest users aren't the only ones who bring their own equipment to the table. The Avenda Systems people say there is a trend toward employees using their own devices that are not company-issued. The problem here is the unknown status of the device's health. Are antivirus signatures up to date? Is a firewall fully enabled?



The problem of user-owned equipment is especially acute in higher education. On college campuses everywhere, security administrators struggle constantly with securing network access via devices that aren't managed or controlled by the school. What's more, students are notorious for using their computers in ways that practically invite trouble; for example, peer

-to-peer file sharing and extensive use of social networks. There's no easier way to pick up a computer virus. These same threats exist within enterprises as well; viruses disrupting a network and the potential for enterprise data corruption can be much more serious than in a school environment.

Like Dorothy and her friends facing their fears at the edge of the woods, the network security administrator faces his fears at the edge of the network where the unmanaged devices lurk. So, let's look at the best practice recommendations from our friends at Avenda Systems.

The first step is authentication of users and devices. Avenda recommends you take authentication to the highest level available to you. 802.1X is the best way to go, but if you can't do that, then use MAC address based or Web-based authentication. You need to have all your users -- employees, guests, temporary or contract workers and so on -- authenticate in some way so you are aware they are on your network. Then you can decide the amount of information to collect about that person or device and how you handle them from there.

The next step is to create rules for how to treat a person based on who he is, what device he is using, and how he connected to the network. For example, if an employee comes into the network from his office location using his company-owned PC, he can have broad access. However, if he's on his iPhone and coming in from a Starbucks down the street, you can limit the portion of the network he has access to; perhaps just his e-mail account. The rules should allow you to establish trust based on numerous variables, including the person's identity, as well as his location, device, connection method, and even the time of day.

You'll also want the ability to categorize the devices as they come onto your network. You should be able to identify a device and distinguish what it is; for example, a PC, smartphone, printer, specialty device such as a medical cart, DVR or game console, and so on. Then you can have a policy to treat specific classes of devices in the same way.

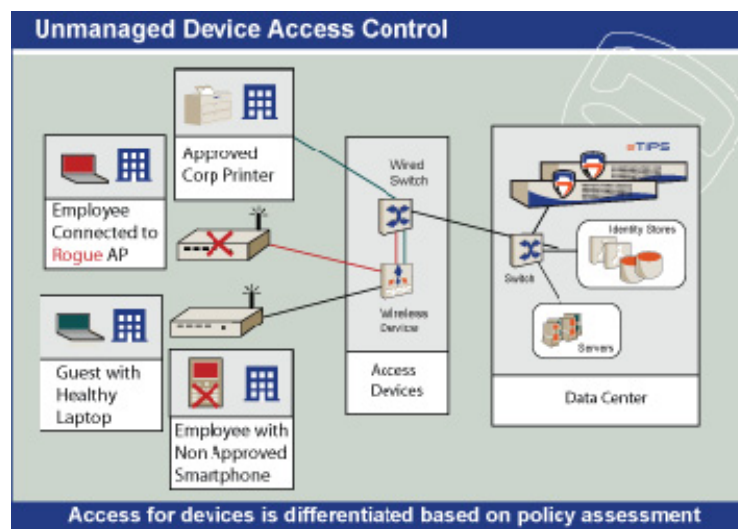
An absolute must for every network is a comprehensive guest access management system. The Avenda experts recommend that you be able to identify a guest and treat him appropriately by mapping security to the guest's purpose for being there, how long he is expected to be there, and what resources he should have available to him. For example, a vendor who comes in to give a product demonstration should be limited to outside Internet access only, but a temporary worker who is assigned to a weeks-long project may need access to certain resources behind your firewall. This level of ability is a specialized offshoot of identity-based access control, and every organization has a need for this.

Overall, network access security can be a daunting task, especially for extensive networks. However, it's OK to take incremental steps as you go through the deployment process. The Avenda folks recommend you get a baseline of the use of unmanaged devices -- who is using them, where they are connecting and so on. Use a network analysis tool to scope the size of the problem

and understand the impact to the network before you turn on enforcement or force changes on your network. As for the incremental steps, chip away at the issues and solve some real problems before you move on to the next set of challenges.

There are benefits to addressing the issue of unmanaged devices. For one thing, it raises the level of security on your

network and gives you more visibility into how the network is being used. It yields trend information and aids in compliance. It allows for a better user experience if you can allow more flexible use of multiple devices per user. And, of course, it gives you a healthier network if you can force a health check or assessment of unmanaged devices to reduce the likelihood of viruses and malware.



Avenda Systems, Inc.  
3255 Scott Blvd. Bldg. 2, Suite 102  
Santa Clara, California 95045  
Main Number: +1 408 748 0902  
Fax: +1 408 748 0906  
Sales: +1 408 748 0902 x123  
[www.avendasys.com](http://www.avendasys.com)

#### About Avenda Systems

Avenda Systems introduced the industry's first multi-function platform for network access security that breaks through past deployment barriers – complexity, compatibility, compliance and cost. Avenda's flagship eTIPS solution is a scalable AAA platform that utilizes identity-based policies for access control, endpoint health and device authorization for wired, wireless and VPN networks in multi-vendor environments. Further information: [www.avendasys.com](http://www.avendasys.com).