



Accario introduces the AccessStick DayXtender: BrianMadden.com Independent Review

At iForum 2007 in Las Vegas there were quite a few vendors, some talking about the same old stuff (thin clients, monitoring, etc.), and others with some pretty fresh solutions. One such company with a fresh take on remote access is Accario. Many of you know about Accario's EPAFactory and their excellent suite of utilities for the Citrix Access Gateway. Now Accario has added another product line called the AccessStick DayXtender. I had the opportunity to get my hands on one, and thought I'd give you the rundown.

The AccessStick DayXtender is, in short, a portable VPN client and access tool on a USB stick. But in reality, it's quite a bit more than that. It's a 1GB USB stick that, other than the built in software, you can use for your own storage. It's also got a fingerprint scanner to prevent unwanted access to your company's VPN and data. But perhaps the best part - AccessStick has created a technology called "VirtuaWrapper" to isolate file operations to the USB stick, and only to the USB stick, no matter what PC it is used on, which means it won't let you forget to delete the payroll spreadsheet off the PC at Kinko's - it was never really there in the first place.

Let's take a look a little more in-depth:

As I mentioned, it's a 1GB USB stick where you can put whatever you want and feel safe since the contents are only accessible after you swipe your finger across the biometric scanner. The initial setup of the device is pretty simple, and with a small note card, most end-users would have no problem making it work.

When you first insert the stick, you'll be prompted to enroll for biometric authentication (fingerprint scanning), after which you'll set up your CAG Advanced Single Sign On connection. For fingerprint scanning, you can scan many fingers, in case you have a cut or something (which, oddly enough, just paid off bigtime for me. Freak Christmas present accident).

After setup is complete, and every time the device is inserted thereafter, you'll be prompted for a fingerprint. Upon successful authentication, Internet Explorer is launched and you are authenticated through your CAG. But you're on a client site, and you don't have rights to install the CAG client, so how the hell did that get installed?

Actually, it didn't get installed. The makers of the AccessStick have managed to pack the USB drive with a handful of more or less "preinstalled" software packages that the workaholic needs to connect and do his or her job. Along with the CAG client, you've also got the ICA client and GoToMeeting. This means that a user can securely connect to his or her corporate network from any Windows machine (2000 or higher w/ a free USB port) without making changes or installing additional software on the local machine.

And that's not the coolest part...

VirtuaWrapper is the name of the technology the AccessStick uses to brand its file operation isolation technology. With VirtuaWrapper, they've addressed two issues - one where users save information to the local machine for whatever reason (printing, for instance) and forget to delete them, and the other where users need to save something to the local device but can't based on restrictions on the local OS (like a kiosk, for instance).

VirtuaWrapper intercepts any process (launched from the AccessStick) that is trying to access the local file system and redirects that write operation to the USB drive itself. This includes the cache, settings, files...you name it.

So, imagine you're trying to save a document from Word running in a Citrix session to the local C:\ drive (or whatever), since that's the easiest place to find it. What you don't know is that you don't have access to write to the folder C:\. The application will present itself just like normal, but when that write operation attempts to write C:\MyDoc.docx, it will automatically be redirected to a special folder on the USB drive. That way, the user can still save and access the data, but as soon as they pull the AccessStick from the machine, there is no trace of that user on the local machine since nothing was ever actually written to it.

Last, and this is taken straight from the website: "Each AccessStick has a unique ID that can be identified by the Citrix Access Gateway enabling the administrator to disable compromised sticks. This means that security is enhanced and user confidence is increased." This won't stop thieves or the like from having your data (if they can break past the fingerprint scanning, of course), but it certainly will stop them from gaining access to your corporate environment if they're using Single Sign On (again, if they can break past the fingerprint scanning). Seems like they might not be 100% confident in the biometrics, but they were nice enough to give you way to centrally disable the device.

That wraps up one of the eye-catching devices from iForum. It looks like the DayXtender is available through the channel, and they have a demo program that you can check out. It's a pretty cool product, and something I'll at least throw in my bag of tricks just in case I'm stuck somewhere and need a quick gadgety pick-me-up.