USB Key Products

Be aware of USB keys! These are the small, colorful flash drives that you can plug in, download data, and unplug, all in a few seconds. And they are now one of the greatest security concerns facing IT managers. The marketing spin on these keys is intriguing, but don't let this or any other sales gimmick destroy your credibility or violate your client's trust.

Even trustworthy employees can cause problems with these devices. Few users encrypt sensitive data stored on their network servers, let alone the files stored on a personal flash drive. However, the keys are so small that they're easy to misplace or lose. Once lost, they become someone else's data. This would not make your client happy.

Most importantly, IT managers understand that a hacker may be able to install a virus, back-door keyboard logger, remote control software or other malicious virus or software onto the machine in which the USB key is plugged.

If the user is logged in and has active secure sessions running against an enterprise application, or is using a VPN, the unauthorized user may be able to search and retrieve selected information from within the company's critical applications or servers. If the device's owner is logged in as an administrator, the unauthorized user may even be able to set up fictitious accounts or access administrative privileges.

Access to non-data files, such as caches, configuration files, "preferences" and registry keys, might allow the application to be installed or run on a second machine. Even if not, those files might include sensitive data, such as customer information, embedded passwords, encryption keys, network IP addresses and TCP port numbers, or other material that could be used to reverse-engineer hacks into an otherwise secure data center.

Your customer may trust you, but they have no idea how secure your key is, who last had access to it, or what it's capable of once it's plugged in.

The security vulnerability is real. Not only may you not get permission to utilize the key, but it's important to realize that many companies are actually beginning to install software designed to block the use of USB storage devices.

It's also important to realize that every time you use one of these devices, you have to request permission, your client will need to take time out of their busy schedule to run a virus scan, and sit with you through the process to make sure that you're not accessing anything you shouldn't. And in order to retrieve any meaningful data at all, you will have to request permissions and utilize the key more than once.

With the Miracom Solution, there are no security vulnerabilities, and IT permissions are required only once, and you get continuous real-time data, not a one-time isolated snap shot!

Real security concerns require *real* solutions. You can trust Miracom.

Miracom Network, Ltd. • 100 N. Central Expressway, Suite 500 • Richardson, TX 75080
Phone: 214.292.2931 • www.miracomnetwork.com