Protect Your Network From USB Drives and Smart Phones

By [Sam Grier](http://itmanagersinbox.com/author/sam-grier/)

[](http://itmanagersinbox.com/wp-content/uploads/2009/03/itsecurity.jpg)The need to protect your network from USB drives and smart phones is more important. Your employees bring the through the door each day and have no thought of plugging them into your company computers.  USB drives and smart phone devices pose a serious threat to your data and your network.

Data theft via portable devices has become increasingly easy using portable devices such as USB thumb drives, flash memory cards, external USB drives, and smart phone devices. This puts sensitive data such as Social Security numbers, customer or company and any information on your network at risk.

With increasingly larger storage capacities, within minutes an employee or unauthorized user can walk away with large amounts of your company data. These devices also represent a threat to your network by introducing viruses or other malicious code.

Employee USB Drive Use is a Risk

Do you know what your employees are doing?

SanDisk recently warned that IT is unaware of how many employees bring personal USB flash drives into the workplace. Their study found that 77% of corporate employees surveyed admitted to using personal flash drives for work related purposes. IT departments estimated the number to be 33%.

Those are staggering numbers which will only increase in the future. IT should be proactive to lock down USB ports. Many protection suites such as Symantec allow you to totally block all but authorized USB devices. Using group policy you can totally block USB access.

USB Drive Solutions

For IT departments that need to allow certain employees access with USB drives SanDisk offers an innovative solution with their [Central Management System](http://www.sandisk.com/business-solutions/usb-flash-drives) which allows you to centrally manage company issued [Cruzer Enterprise](http://www.sandisk.com/business-solutions/usb-flash-drives) USB drives.

Most IT departments try to address this issue with group policy rules that disable the use of USB storage devices.  Cisco also recently announced a fully integrated endpoint security solution in their [Cisco Security Agent](http://www.cisco.com/en/US/products/sw/secursw/ps5057/index.html) that addresses not only USB flash drives, but also other devices.

IT departments need to address this risk and stay on top of it as devices become more sophisticated and capacities increase. You only have to look at the news to see companies reputations damaged by data theft. What are your doing to protect your network from this threat?