Six Reasons for Blocking USB Storage Usage

Technology has seen some drastic developments in the last few decades. From CRT to LED monitors, Microsoft Paint to Google Tilt Brush, and floppy disks to flash drives, everything has changed with respect to size, quality, and performance. Although these technological developments offer improvements, they also bring new threats along with them.

The universal serial bus (USB) was invented to replace the various connectors at the back of PCs, address the usability issues of existing interfaces, and streamline device software configurations. USB also enabled higher transfer rates for external devices. From the first USB released in 1994, to USB 3.1 released in 2013, this technology has seen massive change regarding performance and storage. However, as USB devices—particularly flash drives and external hard drives —have evolved, so have the threats and risks they carry with them.

1. Disgruntled employees can easily steal data using USB drives.

When a USB or any other portable device is used in an unsupervised way on your network, it can lead to data theft or the introduction of viruses. As a cheap, easy way to transfer files or back up data, organizations often overlook the threats posed by USB drives. A single flash drive can collapse an entire network if managed improperly.

Unlike email or other online services that enterprises audit, USB devices are essentially a blind spot for businesses. Disgruntled employees can exploit this blind spot by transferring confidential information to a USB drive when they leave, including client databases, emails, calendar appointments, and contact lists. They can then distribute this information as they please, and even give it to competitors.

Organizations can employ a USB security management system to set restrictions on USB devices in their network. USB security systems help organizations avoid unnecessary data theft, while also protecting against malware introduced by employees' devices.

2. USB drives aren't always used for work purposes.

Data theft isn't the only threat to enterprises. Lost productivity is a huge issue, too. Employees might work on hobby-related tasks during business hours. That's why a USB security system that monitors user machines and can tell you who is accessing a USB port from what computer and when, is crucial in any enterprise. See which files employees are transferring to and from their work computer to identify non-work activities.

3. Booby-trapped USB drives can destroy your network.

Did you know hackers can control your keyboard without your knowledge? There are USB drives, nicknamed booby-trapped USBs, that can control users' computers without permission.

In 2015, hackers developed a USB pen drive that can deliver a 220-volt charge to a computer, destroying it instantly. Just a few years earlier in 2010, the infamous Stuxnet worm infected Iranian nuclear facilities decreasing efficiency by 30 percent. Named the most sophisticated computer virus ever created, the Stuxnet worm is believed to have originated from a worker's USB drive. Once this worm infects a USB drive, it attacks that drive first, then quickly moves toward other computing systems.

Booby-trapped USBs are dangerous because users are unaware of the damage being inflicted. Even with a proper network management system, threats like these can slip through the cracks. So a secured network is not just about deploying a network management system, it's about deploying a complete desktop management solution that can also take care of USB security.

4. Unidentified devices can wreak havoc in your organization.

The utility and ubiquity of USB devices means that they can't be banned from organizations outright, so organizations need to implement a system that allows these devices while also protecting their business. To secure these devices, you might have a database or inventory system that contains information about all the portable storage devices in your corporate network. Once you've done that, you can schedule periodic scans to monitor how the USB devices are being used.

5. Encrypting USB drives isn't enough to effectively secure them.

In extreme cases, organizations have to limit USB device use to specific employees or restrict access to USB ports. Organizations can encrypt USB drives or disable Autorun, so programs on a USB drive don't run automatically when the drive is inserted; however, these strategies aren't enough. Limiting the use of devices based on workgroups and domain membership can also help you avoid USB threats and keep your organization secure.

6. The ability to block and unblock USB devices improves USB security.

An enterprise can avoid the above threats by controlling all the USB devices in its network. Controlling USB devices is as simple as blocking and unblocking them according to your needs.