AlertBoot: Hardware Port Blocking and Access Control

How many of your employees listen to their MP3 players while working? These electronic devices connect directly to a computer via hardware ports. What would stop one of your employees from downloading valuable customer and corporate data assets onto their music player and taking it out of the office? If there is a data breach, your organization is the one that will pay the price — both financially and publicly.

AlertBoot hard disk encryption protects your data assets with advanced and powerful ciphers, but that's not all there is to protecting your confidential information. Data leakage is a huge concern in organizations around the world. Everyone carries a USB key these days, and all those personal music players and external hard drives are getting smaller and smaller.

Completely transparent to the end-user, AlertBoot Port Control prevents unauthorized use of serial, parallel, USB, Bluetooth, FireWire, IrDA, and other ports. AlertBoot Port Control

- Controls access and use of CD-R of DVD-R drives
- Accommodates new blacklisted or whitelisted devices
- Deploys selective access control based on device classes, brand and ID
- Synchronizes policy updates via AlertBoot Central

Centralized management, control, and reporting

AlertBoot Port Control is launched from AlertBoot Central — the central management console — and applies strong security access control to ports on your organization's laptops and devices in order to prevent unauthorized use. By blocking a user's ability to transfer data from a laptop, you can effectively prevent potential data leaks or breaches.

AlertBoot Port Control policies are pushed out from AlertBoot Central's management console and synchronized with devices remotely for easy configuration, efficient deployment, and optimal reporting of deployed policies for auditing compliance.

AlertBoot controls access to the following types of ports:

- Serial ports (PDAs, older communication devices)
- Parallel ports (Printers, older communication devices)
- USB ports (USB keys, personal music players, external hard drives, PDAs)
- FireWire (external hard drives, personal music players, PDAs)
- IrDA® (Infrared receivers, handheld portables, cell phones, cameras)
- CD-R / DVD-R (Burning data CDs or DVDs)

Extended features of AlertBoot Port Control allow an organization to adapt security control policies to accommodate new devices or ports. Organizations can also discriminate between "good" and "bad" devices – based on the device classes, brand, and ID. This allows organizations to continue to use selective USB tokens or keys that are approved for use while excluding the use of other devices on that USB port.

AlertBoot Port Control protects your company from breaches of data by controlling what can and cannot be attached to and used with your workstations and laptops. Prevent access to insecure ports and stop unauthorized access to critical and confidential data before it even starts.