



Industry-Leading Solutions for Mobile Data Protection

# Preventing Data Leaks On USB Ports

Pointsec Device Protector Simply Regulates Access  
and Data for Any Plug-and-Play Peripheral



**pointsec**  
[www.pointsec.com](http://www.pointsec.com)



## Executive Summary

Regulating the electronic flow of information stored in digital format has never been so hard. Most organizations have attempted to reduce the risk of data leaks from servers and networks with firewall, intrusion prevention, authentication and access controls. The mobility trend driving widespread use of laptops for remote and mobile computing has recently spurred the use of encryption solutions for protecting data on devices that are lost or stolen. But now, a new risk is sidestepping these controls – one that creates the opportunity for data to slip outside the protective net without detection. The culprit is any plug-and-play storage device attached to a stationary PC or laptop USB port.

The USB port enables use of many peripherals, including storage devices. Digital music players can host huge quantities of MP3 files – and hold files in any other format such as word processing, PDF, spreadsheet, database, photo or multimedia. USB memory sticks do the same thing, albeit without the capability to play back stored multimedia. Digital cameras can store files. So can cell phones, portable hard disks, personal digital assistants, and many other mobile devices.

The danger stems from operating systems that almost always recognize and authorize any USB-connected storage device the instant it is plugged into an enterprise endpoint. This Achilles heel effectively makes all endpoints susceptible to data leaks. Danger can also flow in the other direction when newly attached storage devices send virus-infected files or malicious applications onto the endpoint device – and potentially throughout the enterprise network.

When data leaks out, the resulting glare of public exposure often triggers consumer outrage, regulatory scrutiny, or punishment by financial markets. Civil and criminal convictions also may occur for individuals responsible for conditions leading to a leak in organizations subject to laws such as HIPAA, Gramm-Leach-Bliley, and Basel II.

The Pointsec strategy for securing enterprise-wide endpoints is called Data Leak Protection. The strategy addresses a variety of risks affecting enterprise endpoint security. This white paper explains how organizations can easily stop data leaks through storage devices attached to endpoint USB ports – or any other plug-and-play connection including Bluetooth, FireWire, WiFi, serial or parallel port. It describes parameters of the risk, and how a solution called Pointsec Device Protector simply controls access and data for external storage devices plugged into PCs.

### Contents

Executive Summary	2
New Vector for Data Leaks	3
How USB Exposes Endpoints to Leaks	4
Pointsec Device Protector for USB Security	5
About Pointsec	7

## USB Ports are New Vector for Data Leaks

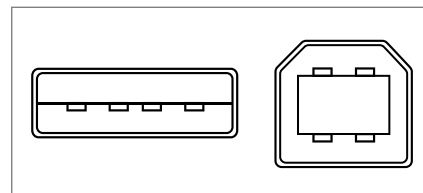
Organizations are under big pressure to do a better job securing enterprise and personal data. A continuous flow of news stories show that data leaks are widespread. According to the Privacy Rights Clearinghouse, more than 100 million records containing private personal information have been lost or stolen since the massive leak from ChoicePoint in 2005.<sup>1</sup> Odds are the real number is higher due to reluctance by organizations to disclose data leaks or related problems with cyber security.

The public scrutinies, embarrassment, financial and judicial penalties triggered by data leaks have stimulated steady efforts to strengthen security. Among the “most critical issues” are data protection, compliance, data leaks, viruses and worms, and access control, according to a recent survey by the Computer Security Institute and the Federal Bureau of Investigation’s Computer Intrusion Squad.<sup>2</sup> In addressing these issues, enterprises have discovered a requirement to deploy different solutions that solve particular vulnerabilities at each layer of the networked information system. Some of the most common security technologies include firewall, antivirus and antispyware software, intrusion detection and prevention, encryption, and access control and authentication.

Enterprises are becoming aware of another significant vector for data leaks that evades control by traditional layered security technologies: the innocuous USB port on endpoint devices.

USB stands for Universal Serial Bus, an interface standard natively supported by popular operating systems such as Windows, Mac OS X, and Linux. The USB standard is intended to ease the interconnection of PCs and laptops with peripheral devices. Its hallmark is automatic recognition of any device that is plugged into a USB port without requiring a user to intervene with mouse clicks or keyboard commands. USB has become commonplace for keyboards, printers, televisions, home stereo equipment, video game consoles, and storage-related devices. Unfortunately, the technology that has streamlined the operational cost of interconnection also has become a critical point requiring the attention of security administrators.

The last category is a point of danger for data security because people constantly plug personal storage devices into their work PC to upload music, wallpaper images, or transmit digital photos over the Internet. Their intent may be innocent. But the ability to also siphon off corporate data from an endpoint through the USB port onto a portable storage device places organizations at considerable risk of undetected data leaks and exposure to malicious files.



The USB (Type A and B) Connectors



A USB series “A” plug

<sup>1</sup> See chronology of data leaks at [www.privacyrights.org/ar/ChronDataBreaches.htm](http://www.privacyrights.org/ar/ChronDataBreaches.htm).

<sup>2</sup> 2006 CSII/FBI Computer Crime and Security Survey, Table 2 on p. 24 at [http://i.cmpnet.com/gocsi/db\\_area/pdfs/fbi/FBI2006.pdf](http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2006.pdf).

## How USB Exposes Endpoints to Leaks

A standard corporate desktop PC may have up to eight USB ports. Some are required for peripherals such as a keyboard or security token reader, but there are usually one or more unused ports. By default, USB ports are “always on,” ready to serve any USB-enabled device that is plugged into the endpoint computer.

An enterprise may choose to disable USB via the Windows Group Policy and an ADM template. Unfortunately, this capability does not provide administrators with granular control. It's all or nothing, so all USB ports on an endpoint are either available or not. And since most endpoints now require USB for mandatory peripherals, this control is practically useless.

One alternative is physical restraint of unused ports. A popular urban myth in IT circles involves the injection of epoxy glue into unused USB ports, but it's hard to imagine inflicting such permanent damage on expensive business equipment. Some vendors sell plug-in USB “locks” to physically secure unused ports. The physical blocking strategy will do little, however, to stop a user with malicious intent from simply unplugging an existing USB peripheral and inserting their unauthorized storage device in its place

### EASE OF DATA MOVEMENT WITH USB STORAGE

A typical device in this category is a USB flash drive, which stores digital files on NAND-type flash memory (see adjacent photo). The flash drive may also be called a “USB key,” “pen drive,” “thumb drive,” or “chip stick.” When a flash drive is plugged into an endpoint's USB port, the endpoint computer's OS automatically recognizes the device, loads its device driver, and enables file transfers with Windows Explorer or similar applications. Some endpoints may allow execution of programs that are stored on a flash drive.

Currently, storage capacity on a flash drive may be up to 16 gigabytes. Connections are implemented with a set of standards called the USB mass-storage device class. Designers did not intend for USB to serve as a primary bus for an endpoint's internal storage such as SCSI, but it can do a fair job for non-demanding applications. The USB standard supports three data rates:

- Low Speed, 1.5 Mbit/s (187.5 kB/s); used for Human Interface Devices (mice, keyboards)
- Full Speed, 12 Mbit/s (1.5 MB/s)
- Hi-Speed, 480 Mbit/s (60 MB/s)

The USB flash drive appears to a user exactly like another internal drive on the endpoint computer, so its plug-in capability and size make it ideal for sneaking out sensitive data from the enterprise. The flash drive is not the only USB device capable of swift and secret data theft. Users may employ any of the USB storage devices mentioned above for the same purpose.



USB Flash Drive

## POD SLURPING AND OTHER TECHNIQUES

Stealing data with USB storage does not require a long script. One simply plugs the USB storage device into a USB port, fires up Windows Explorer and drags target files onto the storage device. This action can be performed by a malicious insider, or even a well-meaning insider who is trying to do their job but is unaware of security policies that might otherwise prevent a data leak.

One of the most popular USB storage devices is the iPod multimedia player from Apple Computer, Inc. Consequently, some people have coined “Pod Slurping” as a hip term for transferring files to a USB storage device.

A synonymous term is “camsnuffling,” which applies to using a digital camera to photograph documents or objects and then transfer them to an unauthorized recipient. Likewise, “bluesnarfing” entails stealing data from a wireless device through a Bluetooth connection.

Whatever the term, it’s very easy to move digital files from an endpoint to a USB storage device. These transfers usually happen undetected by enterprise security controls. And once data has moved to a small storage device, it’s usually easy to carry it outside the enterprise and on to nefarious use by unauthorized people.

## Pointsec Device Protector: A Simple Solution for USB Port Security

Pointsec Device Protector is a simple software-based solution for enterprise-wide control of storage device access through USB and other I/O ports, and of the data flowing through those connections. It provides a policy-driven port security system to a system administrator for granular control of USB access to endpoints that denies all access (black list), provides read-only access or allows full authorized access (white list). The level of control is configurable by a security administrator, which is critical for striking the best balance between security and cost. In some enterprises, implementing a rigid security policy puts new strain on end user work patterns. Pointsec’s objective is to offer a customized endpoint security solution that minimizes changes to end user behavior, while also addressing the most critical elements of your security policy.

As a client-server solution, Pointsec Device Protector is implemented with management software on a server and small-footprint client software installed on each enterprise endpoint. Black list and white list capability is enabled on clients with kernel mode filter drivers. Pointsec Device Protector’s Removable Media Manager enables unique identification of each device on the network using a digital signature. Client software can be silently deployed using any existing Microsoft Windows Installer (MSI) or command line-compatible software distribution package. Pointsec Device Protector also provides a Deployment Server for distribution and management of the product. The solution integrates transparently with the existing network infrastructure.

## ENTERPRISE PORT CONTROL

Pointsec Device Protector is the only solution to support both white list and black list control of removable media and I/O devices on any port (USB, FireWire, IDE, Bluetooth, etc.). The system administrator can centrally manage access to all devices both known and unknown.

Using white list security, Pointsec Device Protector can deny access to ALL devices except for those specifically permitted. Using black list security, it can grant access to all devices apart from explicitly un-trusted devices. Device control can be either on a global device-type basis, or as specific as a particular model and brand of device.

Pointsec Device Protector provides the following modes of operation. All device access can be type-, model- or brand-specific.

- No access
- Read only access
- Read only signed access
- Full access
- Full encrypted access (using the Encryption Policy Manager)
- Full encrypted access with the ability to access data offline

## DEVICE MANAGEMENT, CONTENT FILTERING AND OPTIONAL ENCRYPTION

Pointsec Device Protector includes a unique media authorization system that digitally tags and authorizes devices based on content. A digital signature is written to each device to mark it as “authorized.” The digital signature is automatically updated when storing information within the protected environment. If changes to the media are permitted outside of the organization (such as sharing data with a business partner), the device requires re-authorization before it can be used again within the protected environment.

To further simplify user operation, content written to a plug-and-play storage device can be filtered by file names or types of files, such as Excel spreadsheets or PDF. By ensuring that only digitally signed devices can be accessed, Pointsec Device Protector can provide device-specific security rights for content. These rights prevent accidental or deliberate attempts to transfer protected files onto unauthorized portable storage devices.

The solution also prevents transfer of files with malicious content from storage devices onto enterprise endpoints. Administrator-defined file types can be controlled on a user or group basis. New software packages can only be installed by trusted users and applications.

Pointsec Device Protector also can leverage an organization’s investment in the full line of industry-leading Pointsec encryption solutions. This centrally-managed optional capability automatically encrypts files stored on external storage devices and decrypts them when they are accessed by an endpoint – without requiring extra action by end users. In this manner, an organization can fully protect access to data that passes outside its layered controls for network security.

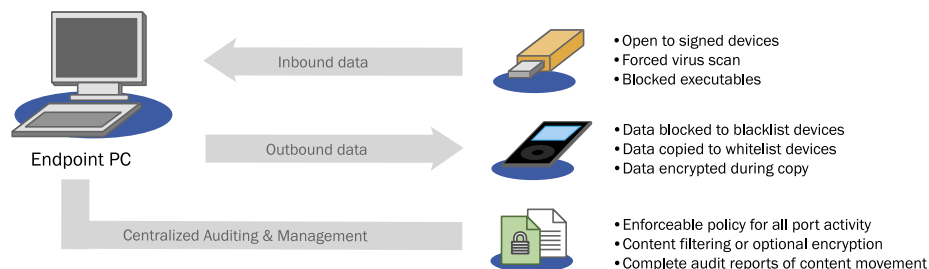
*“Pointsec Protector was chosen due to the simple fact that the technology met the demands of today’s business needs placed upon Allen & Overy. Having fully implemented the product across the firm we now know what data is being removed, due the extensive auditing capability, but most importantly are also sure that the data is secure at all times.”*

**MARK HEATHCOTE**  
IT Architect and Design Manager  
Allen & Overy (UK Law Firm)

## CENTRALIZED MANAGEMENT

Management is performed using a familiar Microsoft Management Console (MMC) interface. Centralized auditing and alerts signal all attempted security breaches and device usage. Audit information is encrypted and filtered on clients before moving to the server at defined intervals. Email alerts can be configured for administrator-defined events. In many cases, just being able to track the flow of specific data files or types of plug-and-play devices used within the organization are sufficient to implement endpoint security policy with no further impact to user behavior.

### Pointsec Protects Enterprise Data at Points of Greatest Risk of Exposure



## Learn More

Pointsec Mobile Technologies, the global leader in mobile data protection, invites you to contact us for more information about Pointsec Device Protector as a simple solution for enterprise-wide port security. Deployment is rapid, automatic and non-intrusive. Centralized management and operations makes Pointsec Device Protector an efficient, cost-effective way to control data leaks through USB ports. To learn more, please contact your Pointsec sales representative at 800-579-3363, or visit our web site at [www.pointsec.com/Protector](http://www.pointsec.com/Protector).

## About Pointsec

Pointsec is the global leader in mobile data protection – with the most customers deployed, highest level of certification and more complete device coverage than any other company. Pointsec delivers trusted solutions for automatic data encryption and port and device control that guarantee proven protection for sensitive enterprise data stored on mobile devices. By securing sensitive information stored on laptops, PDAs, smartphones and removable media, enterprises and government organizations can protect and enhance their image, minimize risk, shield confidential data, guard information assets, and strengthen public and shareholder confidence. Pointsec's customers include blue chip companies and government organizations around the world. Founded in 1988, Pointsec Mobile Technologies AB is a wholly owned subsidiary of Protect Data AB, publicly traded (PROT) on the Stockholm stock exchange. The company has operations in 14 countries, and is represented through partners on all continents. Pointsec can be found on the web at: [www.pointsec.com](http://www.pointsec.com).



**U.S. Headquarters**  
 2441 Warrenville Road  
 Suite 210  
 Lisle, IL 60532  
 800-579-3363 or 630-392-2300  
[www.pointsec.com](http://www.pointsec.com)

**World Headquarters**  
 Pointsec Mobile Technologies AB  
 Box 5376, Humlegårdsgatan 14  
 SE-102 49 Stockholm  
 Sweden  
 +46 8 459 54 70