



Preventing Data Leaks on USB Ports

Check Point Endpoint Security Media Encryption simply regulates access and data for any plug-and-play peripherals

Contents

Executive summary	3
USB ports: A new vector for data leaks	4
How USB exposes endpoints to leaks	5
Ease of data movement with USB storage	5
Pod slurping and other techniques.....	6
Check Point Endpoint Security Media Encryption: A simple solution for USB port security	6
Enterprise port control	6
Device management, content filtering, optional encryption	7
Centralized management	7
Learn more	8

Executive summary

Regulating the electronic flow of information stored in a 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 may be 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 usually 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 bad publicity often triggers consumer outrage, regulatory scrutiny, and/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 the Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley, and Basel II.

The Check Point strategy for securing physical ports on enterprise-wide mobile devices is called Data Leak Protection. This strategy addresses a variety of risks affecting enterprise data security. This white paper explains how organizations can easily stop data leaks through storage devices attached to USB ports—or any other plug-and-play connection including Bluetooth, FireWire, WiFi, serial, or parallel ports. It describes parameters of the risk and how a solution called Check Point Endpoint Security Media Encryption™ simply controls access and data for external storage devices plugged into PCs.

USB ports: A new vector for data leaks

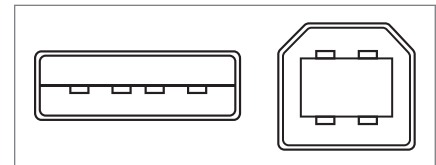
Organizations are under enormous pressure to do a better job securing enterprise and personal data. A continuous flow of news stories shows that data leaks are widespread. According to the Privacy Rights Clearinghouse, more than 100 million records containing private personal information have been lost or stolen since the massive leak from ChoicePoint in 2005.¹ Odds are the real number is higher due to reluctance by organizations to disclose data leaks or related problems with cyber security.

The public scrutiny, embarrassment, and 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.² 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 perimeter and desktop firewalls, antivirus and anti-spyware software, VPNs, intrusion detection and prevention, encryption, and network access control (NAC) 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 Microsoft Windows, Macintosh 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 PCs to upload music, wallpaper images, or transmit digital photos over the Internet. Their intent may be innocent. But the capability to also siphon off corporate data from an endpoint through a USB port onto a portable storage device places organizations at considerable risk of undetected data leaks and exposure to malicious files.



USB (Type A and B) connectors



A USB series “A” plug

¹See chronology of data leaks at www.privacyrights.org/ar/ChronDataBreaches.htm.

²2006 CSI/FBI Computer Crime and Security Survey, Table 2 on p. 24 at 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. However, this physical blocking tactic will do little to stop users with malicious intent from simply unplugging existing USB peripherals and connecting their unauthorized storage devices.

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 photo below). 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 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 undemanding 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)
- High 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 plugin 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 being used to swiftly and secretly steal data. 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. A user simply plugs a USB storage device into a USB port, launches Windows Explorer, and then clicks and drags target files onto the storage device. This action can be performed by malicious insiders—or even well-meaning insiders who are trying to do their jobs but are unaware of security policies designed to prevent data leaks.

One of the most popular USB storage devices is the iPod multimedia player from Apple Computer. Consequently, some people have coined “pod slurping” as a slang 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 by way of 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 for nefarious purposes by unauthorized people.

Check Point Endpoint Security Media Encryption: A simple solution for USB port security

The Check Point Media Encryption product is a simple software-based solution for enterprise-wide control of storage device access through USB and other I/O ports and the data flowing through those connections. It provides a policy-driven port security system to an administrator for granular control of USB access to endpoints that denies all access (blacklists), provides read-only access, or allows full authorized access (whitelists). 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. Check Point’s objective is to offer a customized port management solution that minimizes changes to end-user behavior, while also addressing the most critical elements of security policy.

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

Enterprise port control

Check Point Media Encryption is the only solution to support both whitelist and blacklist 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 whitelist security, Check Point Media Encryption can deny access to all devices except for those specifically permitted. Using blacklist security, it can grant access to all devices apart from explicitly untrusted devices. Device control can be either on a global device-type basis or as specific as a particular model or brand of device.

Check Point Media Encryption provides the following modes of operation:

- 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

All device access can be type-, model-, or brand-specific.

Device management, content filtering, optional encryption

Check Point Media Encryption 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 reauthorization 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 name or file type such as Excel spreadsheet or PDF. By ensuring that only digitally signed devices can be accessed, Check Point Media Encryption 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.

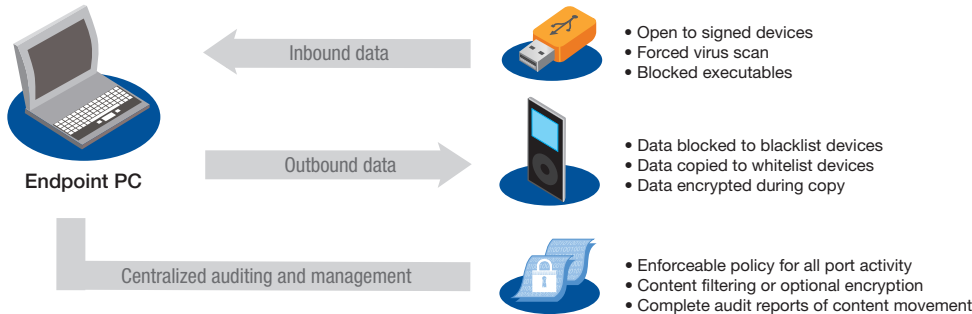
Check Point Media Encryption also can leverage an organization’s investment in the full line of industry-leading encryption solutions. This centrally managed optional capability automatically encrypts files stored on external storage devices and decrypts them when they are accessed by an endpoint—without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

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 agents 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 is sufficient to implement endpoint security policy with no further effect on user behavior.

“Check Point Endpoint Security Media Encryption 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 to the extensive auditing capability, but, most important, we are also sure that the data is secure at all times.”

MARK HEATHCOTE
IT Architect and Design Manager
Allen & Overy (U.K. law firm)



Check Point Media Encryption defends enterprise data at the points at greatest risk of exposure.

Learn more

Check Point, the global leader in mobile data protection, invites you to contact us for more information about Check Point Media Encryption as a simple solution for enterprise-wide port security. Deployment is rapid, automatic, and nonintrusive. Centralized management and operation make Check Point Media Encryption an efficient, cost-effective way to control data leaks via USB ports. To learn more, please contact a Check Point sales representative at 800-579-3363 or visit the Web site at www.checkpoint.com/.checkpoint.com/products/datasecurity/protector/index.html.

CHECK POINT OFFICES

Worldwide Headquarters

5 Ha'Solelim Street
Tel Aviv 67897, Israel
Tel: 972-3-753 4555
Fax: 972-3-575 9256
email: info@checkpoint.com

U.S. Headquarters

800 Bridge Parkway
Redwood City, CA 94065
Tel: 800-429-4391 ; 650-628-2000
Fax: 650-654-4233
URL: <http://www.checkpoint.com>

©2003–2008 Check Point Software Technologies Ltd. All rights reserved. Check Point, AlertAdvisor, Application Intelligence, Check Point Endpoint Security, Check Point Express, Check Point Express CI, the Check Point logo, ClusterXL, Confidence Indexing, ConnectControl, Connectra, Connectra Accelerator Card, Cooperative Enforcement, Cooperative Security Alliance, CoreXL, CoSa, DefenseNet, Dynamic Shielding Architecture, Eventia, Eventia Analyzer, Eventia Reporter, Eventia Suite, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, FloodGate-1, Hacker ID, Hybrid Detection Engine, IMsecure, INSPECT, INSPECT XL, Integrity, Integrity Clientless Security, Integrity SecureClient, InterSpec, IPS-1, IQ Engine, MailSafe, NG, NGX, Open Security Extension, OPSEC, OSFirewall, Pointsec, Pointsec Mobile, Pointsec PC, Pointsec Protector, Policy Lifecycle Management, Provider-1, PureAdvantage, PURE Security, the puresecurity logo, Safe@Home, Safe@Office, SecureClient, SecureClient Mobile, SecureKnowledge, SecurePlatform, SecurePlatform Pro, SecuRemote, SecureServer, SecureUpdate, SecureXL, SecureXL Turbocard, Security Management Portal, Sentivist, SiteManager-1, SmartCenter, SmartCenter Express, SmartCenter Power, SmartCenter Pro, SmartCenter UTM, SmartConsole, SmartDashboard, SmartDefense, SmartDefense Advisor, Smarter Security, SmartLSM, SmartMap, SmartPortal, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartView Tracker, SMP, SMP On-Demand, SofaWare, SSL Network Extender, Stateful Clustering, TrueVector, Turbocard, UAM, UserAuthority, User-to-Address Mapping, UTM-1, UTM-1 Edge, UTM-1 Edge Industrial, UTM-1 Total Security, VPN-1, VPN-1 Accelerator Card, VPN-1 Edge, VPN-1 Express, VPN-1 Express CI, VPN-1 Power, VPN-1 Power Multi-core, VPN-1 Power VSX, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecuRemote, VPN-1 SecureServer, VPN-1 UTM, VPN-1 UTM Edge, VPN-1 VSX, Web Intelligence, ZoneAlarm, ZoneAlarm Anti-Spyware, ZoneAlarm Antivirus, ZoneAlarm ForceField, ZoneAlarm Internet Security Suite, ZoneAlarm Pro, ZoneAlarm Secure Wireless Router, Zone Labs, and the Zone Labs logo are trademarks or registered trademarks of Check Point Software Technologies Ltd. or its affiliates. ZoneAlarm is a Check Point Software Technologies, Inc. Company. All other product names mentioned herein are trademarks or registered trademarks of their respective owners. The products described in this document are protected by U.S. Patent No. 5,606,668, 5,835,726, 5,987,611, 6,496,935, 6,873,988, 6,850,943, and 7,165,076 and may be protected by other U.S. Patents, foreign patents, or pending applications.