



USB Drives: Friend or Foe?

New User Trends and Exploits in USB Requires Security
Controls to Protect Endpoints and the Networked Enterprise

Contents

Executive Summary	3
Exploiting Risks of USB Drives and Portable Applications.....	3
Pod Slurping.....	3
Switchblade	3
Trojan	4
Bootable USB Drive with Administration Tools	4
Enabling Portable Applications on USB Storage.....	4
Portable Application Architecture	5
Alternate Ways to Run Portable Applications	5
Using Security Controls to Block Risks of USB	6
Administrative USB Environment Controls	6
Port Control	7
Application Control	7
Media Control	7
Check Point Endpoint Security Controls Risks of USB	7
Check Point Port Control	7
Check Point Application Control	7
Check Point Media Encryption	8
Check Point Program Security Guard	8
Check Point Full Disk Encryption	8
In Conclusion Check Point Can Identify Friend or Foe	8

Executive Summary

From an IT end user's perspective, a USB drive is almost as useful as a cell phone. As the name implies, Universal Serial Bus is everywhere so even the most casual, non-technical person can plug in a flash drive, music player, phone, camera or other USB storage-enabled device, and easily copy data to and from a host endpoint. Ultra portability and convenience makes USB storage a popular no-brainer.

To an IT security pro, USB can be a continuous nightmare of risks. Users can copy sensitive data to a USB storage device that is easily concealed and moved off-site. The devices are small and easy to lose. Most USB devices are not password protected so access to their stored data is unimpeded. People can also use them to inadvertently or maliciously copy virus- or worm-infested files to endpoints—placing the entire network at risk. USB multiplies the risk vectors to your organization by its total endpoints times the number of their USB ports.

But protector beware! The risks of USB have risen with the new phenomenon of portable applications. Traditional software applications must reside on a host computer for operations. Portable applications are software programs that do not require traditional installation on the host. They allow the portable application to store its executable program, configuration, and data files on the USB device. The portable application can run when the USB storage device is plugged into a host. Like any other application, portable apps are also subject to vulnerabilities affecting their operating system and executable code. Malware can automatically move from a USB storage device to the host endpoint, and on to other vulnerable targets in the network. Malware can also infect the USB device and the portable applications.

This whitepaper describes how security professionals can reduce risks of vulnerabilities to portable applications and USB storage. It surveys the current state of USB storage and explains architectural background on the operation of portable applications. The paper also provides several examples of attacks using USB drives that exploit endpoints. It concludes by noting how Check Point Endpoint Security can block risks to an enterprise such as information leakage and attacks using USB and portable applications.

Exploiting Risks of USB Drives and Portable Applications

The use of portable applications with USB storage devices opens a door to many exploits, which can compromise the confidentiality, integrity and availability of the host endpoint and potentially vulnerable points beyond on the corporate network.

Pod Slurping

Pod slurping is the simplest exploit with USB storage devices. Pod slurping is a data leakage exploit that entails the unauthorized copying of proprietary or sensitive data onto a USB storage device. Pod slurping takes its name from the Apple iPod, although the technique can be used with any device with USB storage.

Switchblade

Switchblade is an exploit used to steal sensitive system information from a Windows-based endpoint, such as password hashes, Local Security Authority secrets, and Internet Protocol information, and access information such as passwords stored by Internet Explorer and Firefox. It uses a special autorun loader on a USB drive that triggers granting of administrative privileges without modifying the system or sending network traffic that could alert a security administrator.

Trojan

A Trojan is an unauthorized software program that installs itself from a USB drive onto an endpoint. The Trojan application can then execute malicious operations, such as opening a backdoor to allow hacker entry to the endpoint and vulnerable points beyond on the corporate network.

Bootable USB Drive with Administration Tools

A bootable OS with common administration utilities is an effective method of circumventing security software installed on an endpoint. This technique bypasses most security software installed on the endpoint. Bootable USB drives can be configured with NTFS file utilities, password reset tools and any other type of software imaginable. If done correctly this technique would leave no traces, or logs of data being taken from the endpoint. Insert the drive and power on the computer. You are now free to copy any data on the endpoint.

Enabling Portable Applications on USB Storage

Portable applications are the new thing for enhancing productivity with USB storage. In addition to data portability, USB sticks now allow users to run applications virtually anywhere, even if the host endpoint does not have the required application installed on its system. Portable applications can fulfill almost any function. Examples include office productivity software, endpoint security, encryption, remote access to a gateway or virtual private network, virtual desktops, and, of course, games.

The USB device itself does not necessarily need to be modified in any way, unless the developer wants to provide it on a secure USB device. You may optionally place an operating system on a USB drive allowing non-typical corporate operating systems like Linux to run on enterprise endpoints.

Note that portable applications require “beefed up” USB storage devices with fast random read and write capability. Portable applications do not typically access data in a continuous sequential format. Portable apps also require a much larger storage capacity on USB storage devices for operating system, application, and library files.



USB sticks typically hold several gigabytes of data. This one holds up to 16GB of storage.

Portable Application Architecture

The most popular enterprise desktop operating system is Microsoft Windows, which is not meant to support portable applications. Windows applications are tied closely to the individual endpoint on which they run via the Windows registry. Standard applications extensively use the registry and often store state information throughout the file system. Authorization is another complication as Windows-based endpoints may require administrator privileges to install software applications.

A portable application for Windows bypasses these limitations in several ways:

- **Alternate configuration and storage.** Applications installed to USB storage devices would write all configuration and operation settings to a separate file or location on the USB device instead of through the Windows registry. Portable applications using this approach require serious modification. In addition to the portable application code, you would also have to copy required components such as libraries, COM and ActiveX to the USB device.
- **Application virtualization.** This approach works without modifying application code by sequencing a portable application through a run-time layer, which redirects calls to the registry and file system and writes all changes to the USB storage device. Components of the portable application are included in the run-time layer, such as libraries, COM and ActiveX. Everything bypasses normal registry and file activity, so the portable application and components do not require authorization for installation and management.

Other operating systems, such as Apple's Mac OS X, Linux and UNIX do not make the same assumptions as Windows for the registry and file system. Technically, applications on these operating systems are easier to convert to portable use.

Alternate Ways to Run Portable Applications

There are several ways to implement portable applications on USB drives. Here are the most popular techniques:

- **Live USB.** A live USB drive contains the full operating system, which enables it to be booted like a regular endpoint. Preparing a live USB drive is similar to preparing a live CD. After connecting it to the host endpoint, a bootable flag is set and MBR written to the primary partition. The partition is formatted, and then a bootloader is installed on the drive. Finally, required files are copied to the USB drive for the operating system, services and applications. The benefit of live USB is allowing other operating systems and applications to run on an endpoint in a clean computing environment. Drawbacks are potential of missing drivers and network configurations.
- **VMware ThinApp.** VMware sells a commercial application called ThinApp that allows you to package and run applications from a USB drive without installation on a host endpoint. No administrative privileges are required to run the applications. ThinApp does this by virtualizing the portable application and encapsulating it into one EXE file with the OS, registry keys, dynamic link libraries, third-party libraries, and frameworks. This solution does not require rebooting the endpoint or changing the endpoint. It does require minor development to package the applications. Be sure to check the license agreements of applications being packaged to ensure compliance.

Benefits of Applications on USB

- Convenient, easy to carry and use
- Works on many PCs
- Inexpensive way to carry data and applications
- Flexible way to work at an external sites without a laptop
- Enables business continuity by carrying data, applications and communications all on a simple device
- Can be configured with security, antivirus, encryption, VPN

- **Ceedo and MojoPac.** These companies allow portable computing environments to be installed on USB devices.
 - **MojoPac.** RingCube Technologies sells a commercial software virtualization product called MojoPac, which turns any USB 2.0 storage device into a portable computing environment. Applications must be installed into the MojoPac virtual environment. MojoPac only works with host endpoints running Windows XP and generally require Administrator rights.
 - **Ceedo.** Ceedo Technologies sells commercial software virtualization software that recreates a user's endpoint on a USB storage device—including an exact duplicate of applications and interface. Users can run their applications and settings from the USB device by plugging it into any endpoint PC.
- **PortableApps.com.** PortableApps.com offers a free open source platform of mobile applications that use the host OS resources. It does not require rebooting the host OS and does not run a virtual desktop. These applications are designed and compiled not to require traditional installation. Its applications include accessibility, development, education, games, graphics and pictures editors, browsers, music and video players, office productivity suites and operating systems utilities. These can be used on a variety of computers without modification.

Using Security Controls to Block Risks of USB

Security pros can take several proactive actions to secure endpoints and the enterprise from exploits using USB storage devices and portable applications. These actions include four types of controls: administrative, port, application, and media.

Administrative USB Environment Controls

Several steps can help to protect your endpoints and network from malicious portable applications run from USB storage devices. Most of these are useful for virtual operating systems and applications deployed by your organization, but are of little help for USB storage devices with portable applications deployed by external organizations or unauthorized individuals.

- **For Virtual OS on USB:** Applications and operating systems on the live USB device must be updated and patched just like any other endpoint. Enable automatic Microsoft Updates with Microsoft Group Policies. Use patch management software such as Microsoft SMS to keep the virtual operating system on USB storage devices current. Regularly scan the OS on live USB devices with antivirus and anti-spyware with the latest signatures.
- **For third-party application virtualization:** Ensure that applications are configured to not modify the host endpoint. For example, with VMware, configure virtualization to sandbox changes to the host endpoint and disallow full read/write access to the host file system. Do the same with MojoPac; however, it is currently possible for a user to modify MojoPac system files such that changes are mirrored to the host endpoint.
- **For scripting updates:** Create an automated update process triggered by a script to copy updated versions of portable applications such as ones from portableapps.com that reside on USB storage devices.

Port Control

Port control provides a higher level of security that is independent of a USB storage device or portable application. It allows a security administrator to implement a variety of access rights to individual USB ports on endpoints. Port control does not regulate execution of portable applications. Practical deployment requires centralized, automated execution of port control for all endpoints in the enterprise. Port control can be very granular, allowing only specific USB devices by Vendor Identification (VID) and/or Product Identification (PID).

Application Control

Application control provides a high level of security that is independent of a USB storage device or portable application. It allows security administrators to exercise granular control over what applications are allowed to run over a USB port. This control applies to portable applications run from a virtualized environment on a USB storage device. It cannot control live USB, which boots another operating system that bypasses the endpoint OS. As with port control, practical deployment of application control requires centralized, automated execution for all endpoints in the enterprise.

Media Control

Media control entails encryption of individual files or the entire fixed disk drive on endpoints. By encrypting the entire endpoint disk, security administrators can prevent data leakage from bootable USB drives.

Check Point Endpoint Security Controls Risks of USB

Check Point Endpoint Security (CPES) is the first single agent for total endpoint security. It combines the highest-rated firewall, network access control (NAC), program control, full disk encryption, antivirus, anti-spyware, data security, and remote access security controls. The solution provides five types of controls that are crucial for controlling risks related to USB storage devices and portable applications.

Check Point Port Control

Check Point Endpoint Security includes granular access controls for all USB ports on all enterprise endpoints, including:

- No unauthorized access (access by VID / PID)
- 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

Check Point Application Control

Check Point Endpoint Security includes granular program control for all applications run through all USB ports on all enterprise endpoints. The Program Control feature allows you to restrict network access between a particular program and either your Trusted or Internet Zone. Program Control uses program permissions applied to individual programs or program groups to control program activity. Program Control only moderates network access for programs. It does not prohibit the programs themselves. To require or prohibit a portable application on a USB storage device attached to a network endpoint, you would use Enforcement Rules.

Graham Taylor, Head of IT security for Michael Page International

said: “Full disk encryption means the user doesn’t have to make any decisions about what data needs protecting—unlike file-based encryption solutions. With Check Point, the security is always on and data is encrypted on the fly, keeping confidential records safe and removing the responsibility from users. What’s more, users report little or no difference in computer performance.”

“The Check Point solutions have been ‘fit and forget’ after initial set-up. We now have complete control over our endpoints, and any changes we need to make, such as giving a member of staff permission to use a USB device, are quickly done.”

Pod Slurping can be prevented by Check Point Port Control.

Check Point Program Security Guard and SmartDefense Program Advisor can defend against **Switchblade** exploits.

Check Point Antivirus defends against **Trojans**, and Check Point Program Control can pre-emptively stop Trojans from communicating.

Preventing unwanted access to local data via “**Bootable USB drives with administration tools**” can be done with Check Point Full Disk Encryption.

The SmartDefense Program Advisor is a supplemental service provided by Check Point that gives policy recommendations for programs. To help block malicious portable applications, use Program Advisor to get professional recommendations from Check Point security professionals about which permissions to assign common programs. Program Advisor also lets you choose to terminate malicious applications run through USB ports on endpoints. Common implementations of Program Advisor are to block known unwanted programs, or in other words prevent black-listed programs from working.

Check Point Media Encryption

Check Point Endpoint Security Media Encryption prevents unauthorized copying of sensitive information from enterprise laptops and PCs to USB storage devices through centrally managed media encryption policies. Only authorized parties can use encrypted USB drives.

Check Point Media Encryption allows employees to share data internally, while providing authorized users with transparent access to encrypted media. Read/write access to encrypted media is maintained when offline or traveling, without requiring third-party software.

Check Point Program Security Guard

Program Security Guard (PSG) is integrated within the media authorization process. Employing this module, users can be given the right to authorize their own media providing the device contains only permitted file types. PSG can be configured to allow the authorization of data-only files. Any executable or unapproved code can be rejected even if renamed or hidden. This can effectively block application on USB drives. PSG is centrally managed, and can be configured to allow authorized users to run applications on USB drives.

Check Point Full Disk Encryption

Check Point Full Disk Encryption secures all users' data with Advanced Encryption Standards and centrally managed policies. Encrypting the entire drive will prevent a bootable USB drive from accessing any user data, resetting system passwords and/or taking system and browser passwords. Booting from a USB drive will bypass security software installed on the host operating system. Full disk encryption will prevent unauthorized access to local endpoint's hard drives.

In Conclusion: Check Point Can Identify Friend or Foe

USB storage devices and portable applications are a paradox for the enterprise. They enable huge productivity and convenience, but open a deluge of security risks on every endpoint with USB ports. Check Point Endpoint Security provides the foundation for securing all endpoints in your organization – including every USB port on every PC. But securing only the USB ports is not enough. Granular, comprehensive controls are required to allow authorized portable applications to function – and block ones that are not. Check Point Endpoint Security (CPES) incorporates multi-layered security and centralized management that addresses these complex risks. Check Point, the worldwide leader in securing the Internet, invites you to contact us for more information about Check Point Endpoint Security. To learn more, please contact a Check Point sales representative at 1-866-488-6691 or visit the Web site at www.checkpoint.com/products/index.html#endpoint.



About Check Point Software Technologies Ltd.

Check Point Software Technologies Ltd. (www.checkpoint.com) worldwide leader in securing the Internet, is the only vendor to deliver Total Security for networks, data and endpoints, unified under a single management framework. Check Point provides customers uncompromised protection against all types of threats, reduces security complexity and lowers total cost of ownership. Check Point first pioneered the industry with FireWall-1 and its patented stateful inspection technology. Today, Check Point continues to innovate with the development of the Software Blade architecture. The dynamic Software Blade architecture delivers secure, flexible and simple solutions that can be fully customized to meet the exact security needs of any organization or environment. Check Point customers include tens of thousands of businesses and organizations of all sizes including all Fortune 100 companies. Check Point's award-winning ZoneAlarm solutions protect millions of consumers from hackers, spyware and identity theft.

CHECK POINT OFFICES

Worldwide Headquarters

5 Ha'Solelim Street
Tel Aviv 67897, Israel
Tel: 972-3-753 4555
Fax: 972-3-624-1100
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>

©2009 Check Point Software Technologies Ltd. All rights reserved. Check Point, AlertAdvisor, Application Intelligence, Check Point Endpoint Security, Check Point Endpoint Security On Demand, 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, INSPECTXL, Integrity, Integrity Clientless Security, Integrity SecureClient, InterSpect, IPS-1, IQ Engine, MailSafe, NG, NGX, Open Security Extension, OPSEC, OSFirewall, Pointsec, Pointsec Mobile, Pointsec PC, Pointsec Protector, Policy Lifecycle Management, Power-1, 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, the totalsecurity logo, 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.