BEST PRACTICE GUIDE

MAKING USB PORTS SECURE WHILE KEEPING EMPLOYEES PRODUCTIVE

USB ports have become such a security risk that some admins are using epoxy to prevent employees from using them. This helps prevent users from leaking data, introducing malware, and so on, though it also hampers productivity–USB ports are crucial for so many things. Rather than sacrifice productivity in favor of security, why not develop policies that give users the freedom they need while also giving admins the security and compliance they require? In this guide, we'll look at best practices for policy-based USB-port administration including which tools to use, how to set up new policies, and how to ensure that the humble USB port isn't a massive security risk. But first, let's look at why USB port management is so critical.

SECTION 1

3 REASONS WE MUST SECURE USB STORAGE AND USB PORTS

REGULAR USB DRIVES SPREAD MALWARE AND RANSOMWARE

Attackers commonly use USB drives to infect computers with malware that can lock up machines with ransomware, give attackers control over endpoints, or even disable machines using an electrical shock. In fact, in 2021 over 30% of known malware is designed for USB-based infections.[1] USB-based attacks are simple to carry out, requiring a threat actor or unsuspecting user to plug a USB drive into a target computer. The problem is so bad that guides on how to create a so-called "bad USB" are ubiquitous online. USB malware is also easily updated,[2] such that it can sneak by anti-malware defenses and continue its spread to other networked systems and USB drives.

REGULAR USB DRIVES ARE DATA THEFT TOOLS

The USB drive is the tool of choice for data thieves, including both external threat actors and even internal threats. In a matter of minutes, thieves can harvest gigabytes of data including an organization's most sensitive intellectual property, customer information, or even protected financial and health-care records. And it's all just a simple process of copying files to an every-day USB drive. Compare that to the hours or even days it can take to steal the same data over a network and it's easy to see why 60% of IT workers said that the USB drive would be the tool of choice for stealing data.[3]

REGULAR USB DRIVES CAUSE INTENTIONAL AND ACCIDENTAL DATA BREACHES

USB flash drive sales have been growing for years and will continue to do so.[4] And while data breaches keep happening, many go unreported. Few employees would report losing a USB drive if their organization didn't have a policy governing such things, and worse, some may have lost drives without realizing it for a period of hours or days–just take the example of an attorney who lost a USB drive with 3 years worth of crucial work files.[5] It happens all the time.

But the risk of data breach gets worse due to the nature of data storage. USB drives create what we'll call Shadow Data. Essentially, data that still lives on a drive and can be recovered, even once it's "deleted." A regular USB drive stores all the data you store on it, never fully removing it, even if you delete it. When you delete a file, empty the trash can, or even perform a quick format on a regular USB drive, all the data is still there. The drive doesn't remove anything or overwrite it, it just changes the file table. Recovering even deleted data is simple using many of the free tools available online. While these tools have legitimate uses such as recovering accidentally-deleted family photos, they can also be used by cyber criminals to restore data a business thought was safely deleted.

This makes it crucial for security professionals to ask themselves a few questions if a regular USB is lost or stolen: Was there sensitive data on the device? But also: Was there *at any point in time,* sensitive data on the device? If drives are not properly sanitized, that sensitive data can still be recovered.

USB drives pose a significant risk to organizations. Luckily, there are a few steps you can take to ensure that the humble USB port is not a massive data leak waiting to happen.

SECTION 2

LOCKING DOWN USB PORTS STEP BY STEP

STEP 1

ASSESS CURRENT USB USAGE

Use port control software that can run in the background. This software should be able to collect and send metadata to a central server, allowing you to audit USB port usage. This way, you can understand how ports are commonly used, which will allow you to better assess the impacts any new USB policies will have on your organization. USB ports are still crucial tools for employees, so you must consider how best to keep them secure without compromising employee productivity.

STEP 2

DEVELOP A NEW USB POLICY

Next, you must determine how and when USB ports should be used. This should include things like who this policy affects, when it will go in place, what exclusions look like, what changes, and what specifically you expect from your users. We've included a sample policy in a later section that you can quickly adapt to your own needs.

STEP 3

INFORM AND TRAIN STAFF ABOUT POLICY CHANGES

It's crucial to help your users understand why policies are changing and what's included in them. Schedule a quick training session to highlight the risks of non-compliance for the organization and the employees. Ensure that staff understands the risk of regular USB drives, and the threat of malware and data breaches. You may also cover the risk of temporarily storing sensitive data on USB drives. You'll also want to go over how to use any new devices you might roll out, and what your expectations are in terms of their usage.

STEP 4

GET MANAGED SECURE USB DRIVES AND ENDPOINT DEVICE CONTROL TOOLS

Many of the issues discussed above can be solved through a blend of endpoint management software and password-protected, hardware encrypted USB flash drives. Together, these help mitigate the threats posed by malware, leaks, and breaches, while also allowing staff to remain productive. Note: while many businesses feel they can rely on software-based encryption along with everyday USB drives, there are limitations. Rather than trust users to encrypt their data using software, a hardware-based option keeps all data encrypted and password protected by default. Furthermore, many drives can be managed remotely, allowing for additional security features, auditing, reporting, and more.

STEP 5

ENFORCE THE POLICY BY LOCKING ALL UNSECURE USB DRIVES OUT OF YOUR NETWORK

This can be achieved by using an endpoint device control tool. Create a strict usage policy during deployment of the new solution to ensure that users must only use approved devices. Your endpoint device control software will make it easy to ensure future policy compliance once set up and configured.

STEP 6

PROVIDE USERS WITH APPROVED MANAGED SECURE USB DRIVES

Next, it's time to make sure employees have safe, secure encrypted USB drives. Look for solutions that allow for self-service deployment and offer one-click automatic enrollment. Each device will be claimed by an authenticated user in the corporate directory (if a directory is available). Solutions like DataLocker's SafeConsole also allows admins to help users recover forgotten passwords, remotely destroy data, and much more. See the section on DataLocker solutions below for more information.

STEP 7

COLLECT AND DESTROY "OLD" DEVICES.

Collection and destruction are best handled with endpoint data erasure software or an outsourced physical destruction service provider. This step is crucial. As noted, users may be tempted to take home old USB drives, which as we discussed, can still contain sensitive data even after it's been "deleted."

STEP 8

CONFIGURE, CONTROL, AND ENHANCE THE SECURE SOLUTION

The right central device management platform gives an authenticated administrator the opportunity to granularly configure policy, audit for compliance, and assist users with remote password resets and monitor the compliance using port control software.

STEP 9

SEE USERS EMBRACE THE NEW SOLUTION

Users will rely on your new solution to transport and share data, distribute data securely,, and collaborate, all while they remain compliant with policies and regulations.

A solid removable media policy is an essential security step for your organization. With one in place, your organization will quickly see an impressive return on investment when quantitative risk analysis shows a massive decrease in the risk of data breach or malware infection.

SECTION 3

SAMPLE BEST PRACTICE USB POLICY[6]

[COMPANY NAME] REMOVABLE MEDIA POLICY

1. Overview

Flash drives, large-capacity storage drives, and other USB media are common sources of malware. Their accidental loss or misuse often results in an organization's loss of sensitive intellectual property, customer data, and more.

2. Purpose

This policy is designed to reduce the risk [company name] faces with regard to the loss of sensitive data, either through loss, theft, or destruction. It is also designed to help reduce [company name] networks risk of acquiring malware infections.

3. Scope

This policy covers systems operating at [Company name]. It covers all workstations, servers, and any machine or piece of equipment which makes use of USB port technology.

4. Policy

[Company name] employees must only use USB devices provided to them by [Company name] IT or security staff. No other removable media can be used with [Company name] systems, including USB flash drives, USB mass storage devices, or other USB technologies, without the explicit permission of [Company name] IT or security staff. Sensitive data should only be stored on USB-storage devices when strictly necessary for staff to perform their duties, or when required by state or federal agencies. In these cases, all sensitive information used in the performance of duties by [Company name] staff must be stored on [Company name] provided encrypted drives. Users may request exceptions to these policies by contacting [Company name] IT or security staff. Exceptions will be managed on a case-by-case basis.

5. Policy Compliance

5.1 Compliance Measurement

[Company name] IT or security staff will regularly verify adherence to this policy using central management software which may include: endpoint management tools, device control software, password-protected hardware encrypted USB drives, on-site visits, video monitoring, as well as via internal and external security audits.

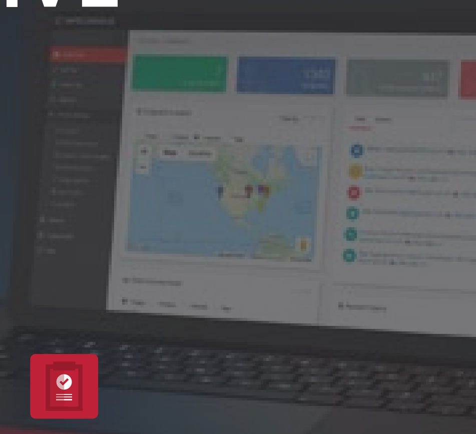
5.2 Exceptions

Users may request exceptions to these policies by contacting [Company name] IT or security staff. Exceptions will be managed on a case-by-case basis and will be determined as needed by IT or security staff.

5.3 Non-Compliance

Employees guilty of violating policies will be subject to disciplinary action.

SECTION 4
SAFECONSOLE FOR USB DRIVE AND PORT MANAGEMENT



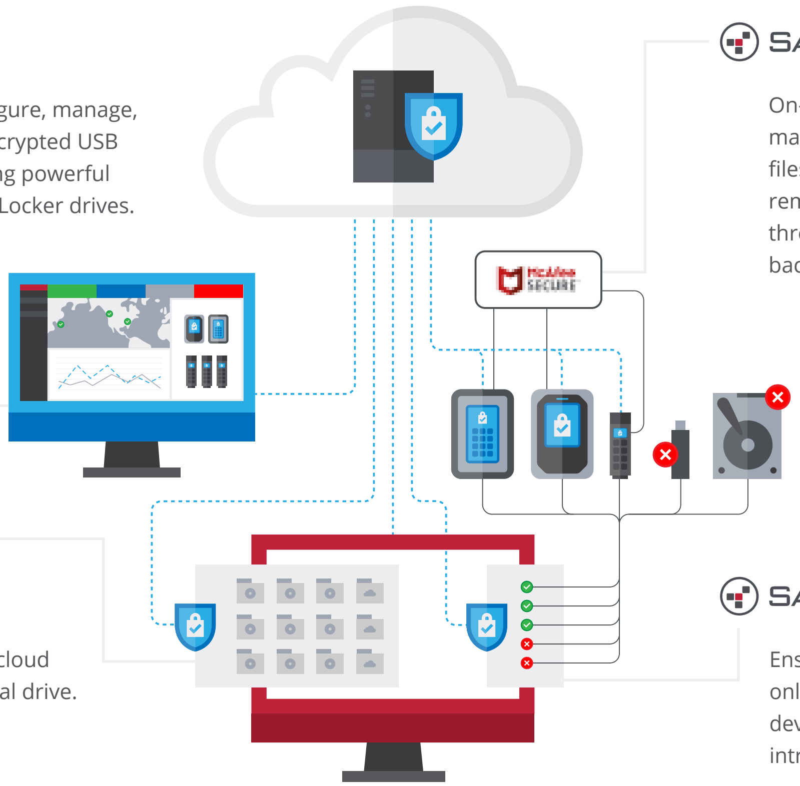
DataLocker's platform lets you easily provision, secure, manage, and audit encrypted USB drives, USB ports, and encrypted virtual drives from anywhere. Ask about custom cloud roll-outs, Premium support, and our enterprise features.

Enhance security for portable USB drives and workstation USB ports

Reduce time spent deploying and managing secure USB drives

Make tracking and compliance for secure USB drives simple with sophisticated auditing and reporting tools

Keep your workforce productive with easy-to-use devices and dynamic security postures



SafeConsole® DEVICECONTROL

Remotely provision, configure, manage, and audit your fleet of encrypted USB drives, while also unlocking powerful security features for DataLocker drives.

SafeConsole® ANTI-MALWARE

On-board McAfee® anti-malware is always on to scan files on secure USB drives, remove or quarantine malware threats, and report information back to SafeConsole.

SafeConsole® SAFECRYPT

Store and secure local or cloud data in an encrypted virtual drive.

SafeConsole® PORTBLOCKER

Ensure that your workforce only uses approved USB devices to prevent malware intrusion or accidental file loss.

[1] https://www.prnewswire.com/news-releases/honeywell-cybersecurity-research-reports-significant-increase-in-usb-threats-that-can-cause-costly-business-disruptions-301317360.html

[2] https://techwireasia.com/2021/10/cyber-attacks-today-zero-day/

[3] https://www.prleap.com/pr/178226/survey-usb-drives-are-the-greatest-breach-risk

[4] https://www.marketwatch.com/press-release/usb-flashdrives-market-trend-key-players-analysis-and-forecast-to-2028-2021-08-16?siteid=bigcharts&dist=bigcharts&tesla=y

[5] https://www.legalfutures.co.uk/latest-news/solicitor-lost-unencrypted-usb-stick-full-of-client-information

[6] http://www.sgcybersecurity.com/images/resource/SOPs/Other_Policies/removable_media_policy.pdf

DATALOCKER
+1 913-310-9088

sales@datalocker.com
To find your local DataLocker Reseller please visit
datalocker.com