DataLocker®
Simply Secure

WHITE PAPER

Reaping All the Benefits of Secure USB Drives Under Management Control

A secure USB flash drive instantly secures all stored data, using hardware encryption and a mandatory password. The point of introducing this technology into your organization is thus apparent:
Never again will you lose data on a stick.

There are a number of factors to consider as your organization prepares to procure secure USB flash drives, especially when it comes to central management of this technology.

Executive Summary

There are a number of factors to consider as your organization prepares to procure secure USB flash drives, especially when it comes to central management of this technology.

1. First among these is the speed and ease of deployment: How quick and easy will it be to distribute drives to users? Remember also that provisioning and delegation of rights to administrators should require as little effort and incur as few costs as possible.

2. A second factor to consider is the level of control you will have over end users of the USB flash drives. It is important to allow only authorized software content, and when distributing content and software, you must be able to verify whether it has been received. You must also ensure that the drives enjoy efficient and effective malware protection.

3. Consider also the need for privacy – don't store passwords centrally! – and how you will comply with existing legislation and your organization's policies. Ask yourself, can we audit the drive content? Does local law permit auditing of end users at all?

4. It is crucial that you determine methods for the administration of every task. How will you assist offline users with a forgotten password? Can data from a lost device be easily recovered to a new drive, and how can lost drives be tracked and retrieved?

5. A fifth element to think about is integration with your current infrastructure. How can you integrate the solution with your existing software? Does the software have hooks and APIs that you must know about? Is it possible to export data to your other systems?

6. Finally, consider the overall situation regarding access to your systems; it should be easy to deny access to users and administrators who have left the organization. Rather than having to remove users explicitly from several systems, you should be able simply to update your central user directory.

Introduction – Moving Beyond Locked-Down Devices

USB flash drives are an integral part of our working lives. Alongside laptops and smartphones, USB flash drives play an absolutely crucial role in enabling remote and flexible working patterns. Even more important, USB flash devices give us mobile access to all those files too sensitive or too large to be downloaded over a public network.

"Managed, secure USB drives can be productivity multi-tools that make it easy to share, transport, distribute, collaborate and work with data and virtual environments directly off the drive."

A secure USB flash drive instantly secures all stored data, using hardware encryption and a mandatory password. The point of introducing this technology into your organization is thus apparent: Never again will you lose data on a stick.

Serious data breaches and malware threats caused by exploited, unsecure USB drives have left no industry unaffected. A Manchester police department was closed for days when a single USB drive infected its entire system with the Conficker virus. Zurich Insurance was fined £2.8 million for the loss of a portable data storage device. All these issues can be prevented with hardware-encrypted, secure USB flash drives. But secure drives alone are only part of the solution.

Evaluating secure USB flash devices by themselves can be a complex task, especially in comparison to evaluating management systems against a clear baseline, which is a big timesaver. This paper offers a general discussion on some of the major problems a management system should help solve and on how you can get the most out of the solution.

Management Should Add Value to Your Investment

By adding a system to manage your secure USB drives, you can attain additional security benefits crucial to any organization. The right solutions will provide you with full control and visibility, and will support everyday usage by allowing you to manage your investment. But all management systems are not alike. Choosing the wrong solution can cause more harm than good. There is a risk of focusing so much on 'the ball' that you end up ruining your whole 'game' – that is, the wrong solution can create management chaos and disrupt end-user productivity. Simply put, there is a great incentive to get it right the first time around.

Managed, secure USB drives can be productivity multi-tools that make it easy to share, transport, distribute, collaborate and work with data and virtual environments directly off the drive.

Ask Yourself – How Do We Get Devices Connected to a Server and Under Management Control?

- How do we get managed devices into the hands of users?
- Is the process flexible? Can we ship devices and connect them at any point?
- Does each device need to be preregistered?
- How do we assign administrators to the central management system?
- How do we avoid creating a new user-group structure as we develop configuration and assign rights to users and administrators?
- Is the device connected to the server in a simple process that does not involve manual steps, extra codes or other means that might confuse end users?
- How secure and easy is it to connect a device to the server?

"Proper management can elevate the productivity of your organization's secure USB drives without increasing security risks..."

Devices Must Be Under Administrator Control

In order to attain any level of computer security, admin rights must not be assigned to users. With the right management system and the right person in the administrator role, users can relax and go about their everyday USB usage. The administrator should decide what is stored on the drive, authorize what software runs on the USB drives, install any needed software and send necessary files to the specific devices.

Contrast this approach with that of most organizations, in which use of unsecure USB drives has spun totally out of control and, in some cases, caused total havoc, including such consequences as data loss and malware infections. These issues often can be traced back to the devices being out of the administrator's reach. Even secure USB drives can cause issues if end users are left to fend for themselves when they are exposed to malware, phishing and social engineering attacks.

The danger of viruses tailored to fit USB drives currently ranks as the number one threat for several consecutive years in most of the major antivirus vendor reports. And yet by simply stripping the end user of admin rights, the likelihood of a malware infection is almost completely eliminated.

Proper management can elevate the productivity of your organization's secure USB drives without increasing security risks, by enabling secure data exchange and collaboration on both trusted and unknown machines.

Ask Yourself – Who Is in Charge of the Devices?

- How do we ensure that only preapproved software is used on the organization's devices?
- Are we able to roll out new portable software to remote devices without user interference or assistance?
- How does the solution protect against USB viruses that are not on the virus lists (day zero threats)?
- Does the malware protection still allow the user to work with the USB device?

Both Privacy and Compliance Must Take Precedence

A central management system is a powerful tool. Therefore it is important that a new solution does not cross the line between privacy and compliance. For example, when an organization implements a secure USB drive, it is imperative that the central system does not store copies of the device's password. Storing the passwords centrally in any manner or form would violate a basic security principal and, in some scenarios, would effectively render the hardware security useless.

Still, the organization should have full audit control if this is in accordance with the existing legislation within its jurisdiction. Management systems for USB drives normally collect information about the user's device and activity; an administrator is able to trace the user on a map within the central system. This can be an important tool for some organizations, while in other cases it can cause severe privacy and security issues. Therefore the organization must have the option of operating the system with all auditing modules in an 'off' mode.

When deciding upon a management solution, your organization must ensure both server and server-to-device security and integrity. In a best-case scenario, the organization will be able to lock down all communication using private certificates. This will ensure that eavesdropping and server breaches are not an issue.

You should also carefully assess what it means to bring in a new system and new users. When users leave the organization, how do you ensure that they can't access sensitive information on a USB drive or log in to any of your management systems, causing a serious data breach? Ideally, all authentication attempts will be synchronized with your central user repository. When you disable a user in your LDAP database, that user should be locked out automatically from any other systems or data.

"You want to give him the right answer – and that answer is not 'I need you to fly back to the office in order to access the presentation'."

Ask Yourself – Is the Solution Compliant with Legislation and the Organization's Policies?

- Do we prohibit storing user passwords centrally in plaintext?
- Can the auditing modules be turned off?
- Is it possible to deactivate privacy-sensitive features?
- How do we assure confidentiality of server-stored information?
- Does the solution accept private certificates?
- Who could possibly have access to server and server-to-device communication?

Devices Must Be Managed for Everyday Life

Naturally, your organization wants to enjoy the benefits of USB drives without the downsides. Users need to go about their everyday business at their own pace, without being limited by the security protocol. Any task that possibly can be made automatic and transparent for the end user should be implemented as such. This will ensure that users quickly adopt and accept the secure device as just another work tool and part of their day.

A secure USB drive is a small device living a hard-knock life. It will be dropped, forgotten, left in pockets to be laundered and sometimes even stamped upon. And compare these superficial, exterior dangers with the interior risks: reset forgotten user passwords, cloned data, enforce password policies and failure to adopt (and even later change) a security policy.

Secure USB drives are everywhere. That is why they were invented: to move data around. Securely. Therefore it is pivotal that the management solution does not require administrator, user and device to be in the same place to perform a procedure as simple as resetting a device password or recreating a lost device. Nor should the administrator have to rely on an internet connection to get the job done. For example, say an executive has forgotten a device password and the big presentation is five minutes away. You want to give him the right answer – and that answer is not 'I need you to fly back to the office in order to access the presentation'.

Given the right circumstances, the administrator should be able to factory reset, terminate and disable devices; assign devices to new users; and even recreate lost devices – without leaving his or her desk. And remember, these devices might be dispersed all over the world.

Ask Yourself – Is the Security Solution Built for the Real World?

- How do we assist a disconnected remote user with a forgotten password?
- Does the solution play well with other endpoint security systems?
- How do we recreate a lost device without interfering with the user's everyday work?
- Can the organization activate backup for all devices?
- Is the device backup automatic, transparent and incremental?
- Is the administrator able to clone a lost device onto a new, off-the-shelf device once the user simply plugs it in?
- Is it possible to display an organization-wide 'lost' message to devices that have been reported lost?
- Is the administrator able to control and support user devices with a click of a button, without having to be on location?

A Long-term Solution to a Moving Security Target

It has been ten years since the USB drive came on the market, and the benefits of managing secure USB drives are being recognised by the world's leading organizations. This is proven technology, an emerging industry that is demonstrating fast growth. New technological breakthroughs include running full virtual desktops of the devices and letting them double up as two-factor authentication tokens.

Ask Yourself – What Does the Future Hold for This Technology?

- Is it possible to get access to a software escrow?
- Is there a device API which will assure that future integrations will be possible?
- Is there a server API which can make it possible to securely access the central system?
- Does the device support a signed secure update?

Moving Forward – Managing Devices Can Be Easy and Quick

There is a sense of urgency when it comes to solving the USB drive's security problems; organizations must take the necessary steps to avoid losing data and attracting malware. Adding management power over your organization's secure USB drives can be a straightforward, no-fuss procedure.

The right central management system will make the most of these intelligent devices. It will empower the organization to manage each device's entire life cycle over the internet. It will permit the organization to assign secure drives to new users throughout each device's technical lifespan. With the click of a button – what seems like a stroke of magic – your USB security solution will be upgraded to a full-fledged, secure productivity tool, thus easing the burden for your organization, your central administrator, your support staff and your end users.

"Secure USB drives are everywhere. That is why they were invented: to move data around. Securely. "

Sources

1) http://www.scmagazineuk.com/greater-manchester-police-hit-by-conficker-from-infected-usb-that-leaves-it-unconnected-from-its-network-for-three-days/article/162904/
2) http://www.scmagazineuk.com/zurich-insurances-fsa-fine-should-act-as-a-warning-on-the-importance-of-protecting-sensitive-information/article/177482/

SAFECONSOLE.COM

UNITED STATES
1-913-310-9088
sales@safeconsole.com

To find your local SafeConsole Reseller
please visit datalocker.com for more information.