SAFECONSOLE®

WHITE PAPER

Benefits of Centrally Managed Secure USB Drives

To make sure your organization's data is kept safe, providing the users with secure USB drives is a great way to start. However, a central management solution will make sure that all risks of losing data are eliminated, and provide you with powerful productivity tools while at it.

EXECUTIVE SUMMARY

A secure USB drive uses password and hardware encryption to protect all stored information automatically. This technology ensures that your sensitive data is always kept private and that data breaches are avoided altogether. But it takes more than just a secure USB drive to ensure that your data is safe. A USB drive needs to be under central management control in order to be its most secure. A central management solution will take you beyond data confidentiality and further ensure the integrity and availability of your stored data.

WITH THE RIGHT CENTRAL MANAGEMENT SYSTEM YOU CAN DO THE FOLLOWING

- Limit or eliminate the risk of USB devices introducing malware onto your networks.
- Get an automatic inventory directory listing all users and their devices. As with all functioning inventory lists, this will limit waste of devices and assist you when assigning previously used devices to new users.
- Enforce your security policy by ensuring that stored data is protected with a password that meets your safety standards.
- Enforce central administrator privileges on the devices and let the device user perform work in a protected user state, making the solution foolproof. The administrator decides what can be stored on and run off the devices.
- Reset forgotten passwords using a secure, local self-service or a central help desk challenge response procedure.
- Re-create data from a lost device onto a new, off the-shelf device by centrally pushing the existing backup package onto the new unit at the user location.
- Centrally handle the state of the devices over the Internet, setting them as disabled or lost. You can even perform factory resets remotely.
- Enforce accountability and assist compliance efforts by activating a full audit trail on all device actions and file changes.

SCENARIOS HIGHLIGHTING MANAGEMENT POSSIBILITIES

A central management system benefits users, administrators and organizations by enabling secure USB devices to move beyond flat, secure storage and to reemerge as portable computing platforms.

TRANSPORT

A major benefit of secure, hardware-encrypted USB drives is that you can ensure the integrity and confidentiality of the encrypted data on the drives when moving to a remote site and then re-ensure them when bringing the device back to the home site. The security of a hardware-encrypted device cannot be deactivated, so all data is always secured and protected against tampering. If someone repeatedly logs in using an incorrect password, the device will destroy all stored data. If the device is left unlocked, the hardware will lock down the device after a preset time of inactivity.

A consultant is delivering a confidential work product on a secure USB drive to a customer site. He knows that the drive's safety technology will ensure the confidentiality of the sensitive work. He delivers his work and is handed a new batch of highly sensitive files. Because his USB device is foolproof, the consultant knows he can store only hardware encrypted files on the device. He leaves

the customer site and notices upon return to his home site that the device was lost in transit. The consultant immediately notifies the customer that no breach has been confirmed but he needs a new copy of the data. The administrator at the consultancy issues a factory reset state command to the lost device, thereby erasing all the data on the device. The administrator also has the option to prompt the device to display a custom return-to-owner message.

SHARE

USB drives were designed to transport data. With a secure USB drive, you can safely transport select files with the assurance that in the event the device is lost or stolen, your data is secure. A secure USB drive also safeguards against infecting customers or partners with USB malware when sharing data by ensuring that only authrorized users have access to it.

A salesperson can share a presentation on a secure USB device protected temporarily with a PIN. The main secure storage area, which houses confidential pricing strategies and quote drafts, is never exposed to the audience. Nothing but the authorized software can run off the secure device, so anyone who wants a copy of the presentation can download it from the salesperson's device and rest assured that his or her machine's integrity has not been violated.

DISTRIBUTE

Sometimes email is not enough, and file distribution can be both a hassle and a security risk. The right central management system for secure USB drives permits secure file distribution.

A project manager working on a sensitive project involving multiple companies is provided with a folder shortcut on his desktop. Files added to this folder will be securely distributed through a secure tunnel over the Internet onto the project team members' authenticated, secure USB drives upon unlock.

"The expected hardware failure rate for the standard portable computer is 10 to 20 percent. Secure USB drives, in contrast, have a failure rate below 1 percent."

COMPLY

Organizations can be strained when trying to fulfill auditing demands for compliance. When data goes beyond the network perimeter, the data audit trail often is lost. Organizations can comply with accountability and safety standards by activating full audit capabilities for device actions and file changes, even when the drives are offline and outside of the network perimeter.

WORK

Issuing laptops to employees who use them infrequently can be expensive. In addition, the expected hardware failure rate for the standard portable computer is 10 to 20 percent. Secure USB drives, in contrast, have a failure rate below 1 percent. Connecting your secure USB drives to a central management system will enable you to centrally issue and maintain portable virtual workspaces on the devices. This concept is often called a "managed thumbtop," and it provides organizations with a low-cost option that allows users to work securely off any host computer within a company-issued, protected workspace.

As part of a contingency plan, an organization pushes out a portable virtual workspace to select users. In case of an emergency, such as a pandemic, the workspace will allow users to work securely from home off their unverified home computers and still connect securely to the organization's system.

COLLABORATE

A USB drive can be a powerful, teamwork-boosting, productivity-enhancing tool. A secure, hardware-encrypted USB drive offers those same benefits plus additional levels of security. A centrally managed system unlocks devices automatically on trusted accounts, thereby saving users and administrators time. Administrators can even modify security policies to allow users to trust their teammates' devices and computers. If an account is not trusted, a user is prompted for his or her password.

Time literally is money at law firms, and USB device users at law firms may perceive security features on USB devices as roadblocks on their path to productivity and billable hours. Devices can be configured to unlock automatically, using an embedded certificate within the protected device user's individual account, thus saving time and frustration. The data stored on the device will always be secure, even if the user brings the device home.

MANAGING SECURE USB DRIVES SAFEGUARDS THE INITIAL INVESTMENT

From a quantitative risk analysis perspective, a central management system provides numerous benefits. It drives down the costs of lost work by enabling backup, and it limits device waste by maintaining an automatic detailed inventory of every device in the network. A central management system not only saves organizations money, but it also helps them improve control over and support of their private data.

Quantitative Risk Analysis	**Unsecured USB Drives**	**Managed Secure USB Drives**
AV - Asset Value		
USB Hardware	$10.00	$40.00
Stored lost work (recreation cost)	$40.00	$10.00
Stored sensitive data (avergae breach cost)	$30.00	$ -
Malware attack from USB	$20.00	$ -
EF - Exposure Factor	60%	5%
SLE - Single Loss Expectancy (single incident cost)	**$60.00**	**$2.50**
USB Hardware Purchased per Year, pieces	1250	526
ARO - Annual Rate of Occurance (of incidents)	750	26
ALE - Annual Loss Expectancy (accumualated incident cost)	$45,000.00	$65.75
Estimated Drives Left After 12 Months	500	499.7
Breakdown of one-time investment (with no risk costs)		
USB hardware cost per piece	$10.00	$40.00
Hardware Cost	$12,500.00	$21,040.00
Management server cost per device	$ -	$20.00
Management server cost	$ -	$9,994.00
Sum of one-time investment	$12,500	$31,034.00
Annual investment	$45,000	$10,059.75
*Note: Based on Quantitative Risk Equations, ALE = SLE*ARO, SLE= AV($)*EF(%)*		

SAFECONSOLE.COM

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