SAFECONSOLE®

WHITE PAPER

7 Steps to Solve the Problem with USB Drives and Make them a Vital Part of your Mobile Device Strategy

What is the problem with USB drives? How does the USB drive fit into an ever more connected world and BYOD strategies?

INTRODUCTION – USB DRIVES REMAINS THE BIGGEST IT SECURITY CULPRIT

More than 10 years after the USB flash drives was first introduced most companies in the world still struggle with the painful issues these small and convenient storage devices cause:

- **USB Drives Spread Malware** –The Confickr infection and other malware that spread over the Sneakernet (download on a USB and walk the infection over to the next machine) remains the most serious malware issue according to Sophos latest 2012 Threat Report[1] .
- **USB Drives are Data Leak Tools** – The USB drives is the tool of choice for data thieves. It is not only the high profile data leaks[2] and those that have been posted on WikiLeaks that utilize unsecure USB drives to steal data off networks. When IT workers where pulled in a survey 60% stated that the USB drive would be the tool of choice.[3]
- **USB Drives Cause Data Breaches** – 71% of USB drives that store business information remains unguarded by passwords or encryption. 65% of people losing USB drives do this without notifying appropriate authorities about the incident.[4] Gartner indicates a strong growth on unsecure USB flash drive sales for years to come which means there will be an influx of potential data breaches.

The Other Side – Benefits of Solving the USB Problem the Right Way

Today there are managed secure USB drive solutions available that eliminate all the threats of standard USB drives. The right managed secure USB flash drive solution stops malware, prevents data leaks and protects against data breaches in one swift move. Putting in place a managed secure USB solution:

- Allows you to easily achieve compliance for the data on the secure USB drives. Strict access controls, full audit logs and encryption of data-at-rest provides organization plug-and-play regulatory compliance. Secure USB flash drives provide security for portable data that is unmatched by other portable devices.
- Provides users with the ability to transfer files quickly: on secure networks, where data charges are high or where the network speeds are low.
- Offers a portable storage experience end-users are accustomed to.
- Provides a low-cost personal device that can complement new BYOD strategies. The cost of issuing and maintaining a managed secure USB drive is 5-10% of the cost of a standard smart phone. By loading portable browsers or virtualization onto the secure drives they become hybrid offline/online devices and can act as secure workspaces.
- Runs off an extremely ruggedized hardware technology with no moving parts and a low component count. Secure USB drives can take a beating and can have hardware failure rate numbers as low as 0.5%. Normal smart phone or laptop breakdown numbers are in the range of 10-20%.[5]

The 7 Steps to Solve the Problem with USB Drives and Make them a Vital Part of your Mobile Device Strategy

1. Standardize on a managed secure USB drive solution that provides hardware encrypted secure USB flash drives that are put under central device management to achieve compliance and control. To grasp the current state of USB usage on your network you can run a device discovery.[6] The device discovery tool also provides a chance to follow up on policy compliance after the implementation is completed.
2. Inform and train staff to comply with the new policy. This provides the opportunity to highlight the risks of non-compliance for the organization and the employees.
3. Enforce the policy by locking all unsecure USB drives out of your network. This can be achieved with an endpoint control tool.[7] It is recommended that the usage policy is strict during the deployment of the new solution to ensure that the switch takes place.
4. Provide users with the approved managed secure USB flash drive. Deployment must be self-service and offer one-click automatic enrollment in a scheme to recover from forgotten passwords. Each device will be claimed by an authenticated user in the corporate directory (if a directory is available).
5. Collect and destruct “old” devices. Collection and destruction is best handled with fileshredder software or an outsourced physical destruction service provider. Make sure not to skip this step as it could mean a fatal mistake with unsecure quick-formatted flash drives with access being spread, well, all over.
6. Configure, control and enhance the secure solution. The right central device management platform offers the authenticated administrator with the opportunity to granularly configure policy, audit for compliance, and assist users with remote password resets. It is also possible to push files and install software that is streamed down from the central server onto the user’s devices when they unlocked.
7. See users embrace the new solution. Users will rely on the new solution to transport data, share data, distribute data securely, work off the devices, and collaborate all while they remain compliant to policy and regulations. The organization will quickly achieve an impressive return on investment as a quantitative risk analysis shows.[8]

Security Warnings when Selecting a Solution

- Avoid central management systems that have schemes that offer password backups. Storing an unencrypted, or even an obfuscated, list of password at a central location is a flawed security practice according to the SANS Institute: do not store passwords in clear text or in any easily reversible form[9]. It is creating an unnecessary aggregated information asset that will require additional steps to be protected. Also never accept the usage of master passwords as a substitute for a real password management scheme.
- Do not rely on portable software encryption to protect data on standard USB flash drives. This is a flawed approach that does not provide convenience or the required security.[10]
- Make sure to manage you secure USB flash drives. There is way of achieving regulatory compliance without having a central device management solution that can enforce strict access controls, full audit trails and that can remotely destruct a lost or stolen device.

1 http://www.sophos.com/medialibrary/PDFs/other/SophosSecurityThreatReport2012.pdf
2 http://www.computerworlduk.com/news/mobile-wireless/3285570/t-mobile-employees-fined-for-massivedata-theft/
3 http://www.prleap.com/pr/178226/
4 http://media.kingston.com/pdfs/Ponemon/Ponemon_research_EMEA_summary_UK_1111.pdf
5 http://www.squaretrade.com/pages/cell-phone-comparison-study-Nov-10
6 http://www.safeconsole.com/pricing/disco/
7 http://www.safeconsole.com/pricing/lockout/
8 http://www.blockmastersecurity.com/doc/BM_WP_benefits-of-centrally-managed-secure-USB-drives.pdf
9 http://www.sans.org/security-resources/policies/Password_Policy.pdf
10 http://www.blockmastersecurity.com/doc/BM_WP_why-software-encrypted-USB-flash-drives-g

SAFECONSOLE.COM

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