SECURE YOUR REMOVABLE MEDIA

Intelligently control the use of USB sticks and other portable storage devices
Intelligently control the use of USB sticks and other portable storage devices

The Situation

One of the largest security vulnerabilities today is the widespread use of removable media: USB sticks, smartphones, backup drives, and more. Usually, this vulnerability exists because employees are accustomed to having no restrictions on removable media, and many organizations believe users will not tolerate policies being enforced. However, according to the Ponemon Institute, in the past two years, 70 percent of businesses have traced the loss of sensitive or confidential information to removable media. Ponemon also states that only 21 percent of organizations with USB device security policies on the books use data loss prevention (DLP) tools. Besides the loss of sensitive data, removable media may also introduce malware.

Operating systems have no controls in place to regulate the use of removable media—or audit it. As a result, many organizations have little to no visibility into how their employees use removable media. They don’t appreciate their risk, so they haven’t invested in policies or controls that could protect the business and its data.

Driving Concerns

Many organizations have sensitive information and a need to protect it, but have not addressed the use of removable media. There are special circumstances that make removable media security a difficult and complex challenge:

- **Understanding how the organization uses removable media.** It is difficult to determine who is using removable media, what they are using it for, and which uses constitute legitimate business activities.
- **Determining policies for appropriate use of removable media.** With no operating system controls in place to enforce removable media security policies, organizations must look to third party solutions for enforcement. Most of these solutions are point products, so it takes several products from several manufacturers for comprehensive control.
- **Encrypting data on removable media.** If a user copies something that the organization has deemed confidential, it should be encrypted. However, wholesale encryption can frustrate users and consume time and CPU. Selective encryption is desirable, but requires an understanding of the data or files being transferred. Once the decision has been made to encrypt the data do we want it to be accessible only on corporate owned assets or can the removable media be used on any computer?
- **Gaining user acceptance of policies and tools.** Solutions can be cumbersome and affect the productivity of users. User acceptance of the corporate removable media policy is important. They must understand the serious risk of loss and how and why to comply with policies.
Solution Description
Best practice for removable media security follows a path from risk reduction to risk mitigation to proof of compliance. First, you limit data loss risks by controlling which specific devices, if any, can be connected to corporate systems. Second, you limit what data can be transferred to devices. Third, you protect the data once it is on the device. If a device is lost, the most important questions are: “What data was on it?” and “Was the data encrypted?” Proof of encryption at the time of loss can let your organization avoid breach disclosures, such as those required by privacy laws.

The appropriate approach will depend on your organization—users may have legitimate needs for removable media, while your regulatory environment may dictate more or less stringent rules on disclosure. Here are the practical steps:

• **Understanding how the organization uses removable media.** Data loss prevention (DLP) solutions provide visibility to help you understand and monitor removable media usage. These products can allow discreet auditing to discover what data is being copied where and tie each event back to specific users. Through the reporting mechanisms of the DLP product, a clear picture can be drawn of current usage and trends.

• **Developing policies for controlling appropriate use.** With an understanding of legitimate business needs, you can structure an appropriate policy for removable media usage.

  » Define acceptable use of removable media. The most rigid policy would use a DLP solution to block all removable media for any users who lack business justification. For those users that have a reason for using removable media, the policy would dictate that the approved media be encrypted.

  » Utilize antivirus and antimalware. Many forms of malware including Stuxnet and Conficker have been introduced to organizations via removable media. Your policy could require an approved device include antimalware to automatically scan all content copied to or from a device looking for code that could spread infection.

  » Determine which systems can access sensitive data on removable media. Many companies choose to limit sensitive data access by removable media attached to corporate-owned laptops and PCs. The alternative is that the sensitive data can be accessed on any system, whether company owned or not.

Decision Elements
These factors could influence your architecture:

• Do you utilize a removable media policy to enforce blocking or encryption of removable media?

• Do you want removable media to be tied exclusively to corporate owned devices?

• Do you need malware protection for removable media?

• Do you currently use McAfee ePolicy Orchestrator® (McAfee ePO™)?
• **Encrypting data on removable media.** Military-grade encryption should be used to protect the data. The implementation will vary depending on the systems and the data itself. For reliable protection, simple, straightforward encryption is imperative, which often means taking the decision away from the end user through automated encryption.

  » All data. With most DLP solutions, a rule can be set to automatically encrypt anything going to a removable device or to encrypt files selectively based on content in the file. For the most coverage, a rule should be set to automatically encrypt if the user simply plugs in a device.
  
  » Select data. DLP solutions can trigger encryption based on pre-defined content rules such as a credit card number, a HIPAA ICD9 diagnostic code, or a document labeled “company confidential.” If a file tagged by the DLP solution is copied to removable media, the appropriate encryption policy can be enforced.
  
  » Corporate assets. If the data should only be accessible on corporate assets, file level encryption is the preferred method. An encryption tool should be used to encrypt any file going to any removable media. Only corporate assets should be allowed to open the file.
  
  » Any asset. A container can be used to encrypt data on removable media for access using any device. This way, although the media might be plugged in anywhere, only a user with the encryption password will be able to access the data.

• **Gaining user acceptance of policies and tools.** Automated encryption removes a significant part of the end-user compliance burden, but DLP solutions can also help with education. DLP solutions can push a warning to the end user when they plug in removable media. This warning could be a message that the user’s actions are being monitored or a link to the corporate removable media policy.
Technologies Used in the McAfee Solution
The solution proposed by McAfee has several options: McAfee® Device Control, McAfee Data Loss Prevention, and McAfee Endpoint Encryption for Files and Folders. The architecture streamlines implementation with a single management console, McAfee ePolicy Orchestrator® (McAfee ePO™), and a single agent on the client system, the McAfee Common Management Agent. This single agent minimizes resource consumption on client systems.

McAfee protections use centralized management to efficiently enforce policies for use of removable media

McAfee ePolicy Orchestrator
This policy and management platform configures and pushes the software and policies for McAfee Data Loss Prevention and McAfee Endpoint Encryption for Files and Folders to client systems. Using one console, you deploy and maintain the McAfee software on managed clients. This single console has the ability to report and alert on the status of both solutions, as well as other McAfee endpoint software. You can perform and automate all compliance reporting and alerting with McAfee ePO. For example, from the McAfee ePO console you can report on the contents of a user’s removable media as well as the encryption state. This report may be required in the event the device disappears.
Securing Removable Media

McAfee Host Data Loss Prevention Endpoint
The McAfee Data Loss Prevention (DLP) suite controls the distribution of regulated and sensitive information. The component of the suite that is installed on client machines is McAfee DLP Endpoint, which includes McAfee Device Control. McAfee Device Control prevents users from accessing removable media on company-owned systems. For example, with McAfee Device Control, you could choose to restrict access to CD burning applications. For content aware control, use McAfee DLP Endpoint to monitor or block sensitive content from leaving the system. With McAfee DLP Endpoint, you can configure rules for specific types and sensitivities of content. For example, you can prevent users from copying files with credit card numbers to the removable media. Removable media control is just one facet of this product. Controls and content-specific rules can be applied to other situations, including distributing files in web-based and client-based email applications. All rules can be configured to either block or simply monitor content. The application is wizard driven and includes many examples to ease the process of deployment.

McAfee Endpoint Encryption for Files and Folders
McAfee Endpoint Encryption for Files and Folders offers software-based encryption for generic removable media. You can easily set a policy to encrypt all content being copied to removable media. Depending on the policy, the content could be accessed only on a corporate-owned device (such as a laptop) or be available on any device. As an alternative to this automated approach, when the user inserts a piece of removable media, they can be asked if they wish to encrypt it. If they select “Yes,” the product prompts the user to enter a password and confirm it. If they select “No,” the device is put into read-only mode, and no sensitive data can be copied to the device.
Impact of the Solution

McAfee allows you to serve user demands for removable media use without giving up data protection controls. Our single console, single agent solution helps you audit and understand the legitimate needs of your users, then implement policies and automated controls that make protection both consistent and palatable to the user community. Flexible encryption options ensure you can protect your data while freeing users to work with it on more types of systems and in more places.

Through central management, McAfee reduces the cost of implementation, policy maintenance, visibility, reporting, and alerting. With McAfee, USB controls can be practical, even for today's complex organizations.

Since data can escape in many ways, McAfee solutions use policies to enforce appropriate controls.
Additional Resources
www.mcafee.com/epo
www.mcafee.com/hostdlp
www.mcafee.com/endpoint-encryption

For more information about the Security Connected Reference Architecture, visit:
www.mcafee.com/securityconnected

About the Author
Bruce A. Boyd is a Senior Sales Systems Engineer for McAfee. Bruce specializes in data loss prevention, firewalls, forensics, and encryption. He has spent over 15 years providing and implementing information security solutions for enterprise customers. Bruce holds a Bachelors degree in Business Administration from the University of North Texas. He has proudly used McAfee products since the late 80s, starting with scan.exe. Bruce has worked for other industry leaders, such as EMC, RSA, 3Com, and Network Intelligence. Bruce is a Certified Information Systems Security Professional.

As quoted in Information Week, August 8, 2011: http://www.informationweek.com/news/storage/security/231300434