ROXIO®

Securing Data on Portable Media

www.roxio.com

Contents

Intro | Securing Data on Portable Media

Storing data on removable storage media including CD and DVD (and increasingly, Blu-ray Disc) and USB flash memory are a daily part of today's computing environment. Small businesses and large enterprises use removable media to archive and share data internally and externally.

However, the very portability of portable media and its convenience make it an easy target for breach of sensitive data. Data breaches harm customers and employees, and can be extremely costly for organizations. Furthermore, regulations increasingly mandate that sensitive data must be protected.

In order to protect sensitive data and to comply with regulations, organizations require a solution that enables data to be encrypted on removable storage devices, while at the same time maintaining the convenience and ease of use that makes this storage so useful.

This paper shows how Roxio Secure solutions can be used by organizations for reliable and secure data storage and sharing on optical and USB flash media.

1 | The Importance of Data Security

Security of data stored on portable and removable storage media has become a major concern in today's world. Organizations continue to lose data stored on portable media through theft and carelessness. There are frequent reports of 'data breach' and the associated costs. A simple Google News search on 'data breach', or a look at Open Security Foundation's DataLossDB at http://datalossdb.org/ reveals how serious and widespread the problem is.

Security is an important consideration when developing an organization's portable media policy. Optical discs and USB flash devices are easy to transport, and easy to steal.

Data breach can be extremely costly. Poneman Institute conducted a Cost of Data Breach Study, published January 2009, and their research indicated that:

- The average organizational cost of data breach was $6.65 million in 2008, rising annually
- Costs include lawsuits, process costs and lost business opportunity costs
- While conditions vary across states, the organization may not be required to notify individuals when the breached data is encrypted.

Compliance is a major factor driving organizations to adopt encryption policies for data stored on removable media. For example:

- According to a Department of Defence Policy Memorandum, the Department of Defense requires encryption of data stored on CD and DVD. Data must be encrypted using a FIPS 140-2 encryption module.
- State and federal regulators have created new privacy laws and are strictly enforcing previous requirements, e.g, privacy protection in healthcare (HIPAA), banking (GLBA) and credit card processing (PCI-DSS), etc.

Data security is important not only because it protects customers and employees, but also because it can potentially save a company huge costs and loss of reputation.

2 | Roxio Secure

Roxio Secure solutions are designed to meet the data security needs of personnel at multiple levels of the organization: management, IT administrators and end users.

Management requires a cost effective way to prevent data breach on removable media in compliance with corporate policies. Furthermore, data written to removable media needs to be logged in order to respond to reporting requirements.

IT Administration needs a solution that is easy to deploy, easy to support, and easy to manage.

End users require a solution that makes it easy and transparent to secure, write and access data on removable media, whether in the office or on the go.

The following sections outline how Roxio Secure products meet organizational requirements at every level.

Security Means Strong Encryption

In the simplest terms, the data on secure portable media needs to be encrypted so that only authorized users can access it. The encryption needs to be strong enough to prevent circumvention; some organizations must also comply with specific encryption standards such as US government approved standards.

Roxio Secure offers strong encryption on optical and USB flash media.

Roxio's secure burning component, called Roxio Secure Burn, uses an AES 128 bit encryption key; specifically the FIPS 140-2 certified Microsoft RSAENH Cryptographic Provider. The USB flash media encryption component, called LDD Flash, uses a non certified proprietary strong encryption module using AES and SHA (HMAC) algorithms with 256-bit key.

With Roxio Secure, business decision makers as well as employees responsible for transporting data can be confident that encrypted data cannot be breached.

Policy Control of Encryption

Different organizations have different policies and requirements for ensuring that encryption and authorization procedures are properly implemented.

Small businesses may simply require that secure data is protected with a password, and that employees can optionally secure the media, depending on the nature of the data. Other organizations may require that employees use a password to protect all data on portable media.

In organizations where data is shared frequently, it may be preferable to make the encrypted media readable on authorized PCs within the organization without the need for a password. The password is only required when carrying the media outside, where it can be easily stolen.

Larger enterprises, especially organizations dealing with highly sensitive data such as banking, medical or military records, require a higher level of security. Not only is encryption required, but central control of authorization is typically desired. The IT administrator needs to be able to control access to media in compliance with organizational policies. If an employee leaves the organization and carries media, or if a piece of media is stolen, it is important that the media cannot be accessed even with a password.

Managers may also be required to log data on which employees are copying data to portable storage, and to generate reports about this.

Following are some typical organizational policies for controlling encryption, which will vary depending on the size and nature of the enterprise:

- Encryption of media may be optional or mandatory.
- Encryption may be initiated by the end user or by the system administrator.
- Password strength must meet minimal requirements
- Encrypted media can be accessed within the organization, and not outside; or access is permitted outside the organization, but authorization is required.
- Likewise, encrypted media can be accessed within determined groups of PCs, Users or devices, and not outside; or access is permitted outside the groups, but authorization is required.
- Encrypted media can be accessed within the organization, and not outside; or access is permitted outside the organization, but authorization is required.

- In case an employee leaves the company, data on discs and USB flash devices must be made inaccessible that that employee.
- In case the media does not connect to the domain for a selected period of time, the data on the media becomes inaccessible.
- In case incorrect credentials are used to try to access the data a given number of times, the data becomes unreadable without administrative intervention.
- All data written to and read from media must be logged.
- All administrative changes to policies must be logged.

Not only do organizations require clearly defined policies, but management of these policies needs to be easy and transparent for executives and IT managers. What works for a small business is not necessarily so for a large enterprise. Appropriate policy management solutions need to be devised for the organization.

Roxio Secure solutions are customizable to meet the policy needs of most organizations.

Examples of Policy Control of Encryption

Here are some typical examples of how an organization might use one of Roxio's secure burning solutions.

A small business of around 25 employees has personnel with different levels of responsibility. The company policy is to encrypt all data stored on disc, and to compartmentalize it so that different users have different rights to access the data. For example, according to the policy the business owner can read discs created on any PC in the company, whereas a contractor can only read discs created on his own computer. The owner can add a password to the disc so it can be read at home, whereas the contractor cannot.

Roxio Secure Burn Plus is a solution that enables departmental permissions. Even though discs burned with Secure Plus are encrypted, they can be read on PCs within permitted groups and restricted outside of the groups. So, for example, if a disc is burned on a business owner's personal PC, the disc can be read back on other PCs selected by the owner for internal use, but not, for example, on PCs that external contractors or customers use. Discs burned by the owner can include a password for home use, whereas discs created by the contractor can only be read on PCs within the business.

Setting unique policies for each department is easily accomplished using the Roxio Permissions Manager application.

As a second example, we will consider a company that has thousands of employees. This company has deployed Roxio Secure Managed on all user PCs within the organization.

The company policy is that employees may not keep any company data on CDs, DVDs or USB flash drives if they stop working for the company. However, realistically, some employees will retain discs or USB flash drives that contain company data. Furthermore, it is company policy to log all data copied to USB flash drives and optical discs, and to periodically generate reports of such data for auditing.

Using the web console component of Roxio Secure Managed, the system administrator will be able to easily keep track of exactly which discs and devices the user has burned data to, what files have been burned, and will even be able to render discs and USB flash drives unreadable after the employee leaves. In fact, data on USB drives can even be triggered to be destroyed if the user is not authorized.

Additional Factors for a Robust and Successful Solution

Apart from encryption, there are other factors that make Roxio Secure a robust and successful solution that meets the needs of management, IT administration and users, especially:

- Ease of deployment
- Scalability
- Flexibility and Reliability
- Ease of use in accomplishing tasks
- Support

The following sections will discuss each of these factors.

Ease of Deployment

Ease of deployment is important for IT administrators. Without this, it would be difficult or impossible to bring the solution to the entire enterprise and keep it up to date. Typical deployment tools include SMS and System Center Configuration Manager 2007, Altiris, and Active Directory Group Policy including installation via a script file. Roxio Secure solutions are compatible with all of these, and include command lines in the installer for customized deployment, such as silent install, language selection, etc.

Scalability

Scalability is important for two reasons. As an organization grows, security policies tend be become more rigorous. A scalable solution allows additional policy controls to be added without disrupting the existing system. Furthermore, it is a cost efficient way to allow the security capabilities to grow as the business grows.

Roxio Secure is offered in three scalable solutions to meet any size of organization, and to enable easy upscaling as the organization grows.

Flexibility and Reliability

Very few organizations are standardized on a single platform or set of devices. Typical organizations use computers, CD/DVD burners and USB flash devices from a variety of manufacturers.   Some organizations use Windows XP in certain departments where change is disruptive, whereas Vista or Windows 7 are used in other departments.

However, enabling a solution to work on a wide range of systems can result in decreased reliability, because of the number of test scenarios that must be considered.

Roxio solutions have a proven track record of reliability in supporting a broad spectrum of systems and devices. Roxio has been an industry leader in digital media since 1986.   Customers include government, military, corporations, all major PC manufacturers including HP, Dell, Acer, Lenovo, etc.

Roxio is the provider of the optical disc recording technology for Windows XP, Windows Media Player, Audible.com and other key partners. The USB component used in Roxio Secure Managed is especially designed to work independently of make or model of device, PC or version of Windows.

Roxio Secure solutions are based on technology that has a record of reliability and flexibility.

Ease of Use in Accomplishing Tasks

Whether the business or organization is small or large, it requires easy installation of the encryption software on multiple systems, and easy and transparent reading/writing on the media.

- Logical Workflow, with the ability to accomplish tasks with just a few steps even if the underlying technology is complex
- Meaningful visual cues, including icons and other graphics
- Attractive design, so the experience is pleasing
- Well organized help and documentation

Roxio's dedicated user experience team has guided the design and workflow of Roxio Secure solutions to ensure best possible usability.

Support

Any sophisticated technology solution requires a learning curve and periodic customer support. Support can take many forms including both self help options such as FAQs, support forums and knowledgebase articles, as well as 1:1 support via email or phone. Roxio has a rich and mature support infrastructure to support Roxio Secure customers from beginners to experienced IT administrators.

3 | The Roxio Secure Product Line

Roxio Secure products consist of an end-user friendly family of enterprise applications that helps protect businesses, government agencies, and other institutions from data breach. The products enable users within an organization to quickly secure data on CD, DVD, Blu-ray Disc and flash devices using powerful data encryption that safeguards the contents from being accessed by unauthorized persons. Roxio Secure offerings go beyond simple encryption on stand-alone machines to provide advanced end-point security features for networks of computers in small workgroups to multi-departmental global enterprises. Roxio Secure offerings arm companies with the tools to not only meet internal security policies, but also comply with industry and government-mandated privacy measures and regulations.

Roxio Secure line of products includes:

Roxio Secure Burn:

- Burns data on CD, DVD and Blu-ray Disc using an easy drag & drop interface
- Copies discs and disc image files
- Encrypts data on disc using a FIPS 140-2 certified encryption module
- Spans files too big to fit across multiple discs
- Reads and writes disc image files
- Includes dynamic language support in a single installer for international organizations
- This product is specifically targeted at OEM customers

Roxio Secure Burn Plus adds:

- Discs can be read on PCs within permitted departmental groups of PCs
- Restricts permission to read discs on PCs outside permitted departmental groups
- Group read permissions are set at installation via command line
- Read permissions can be changed after installation with the included Roxio Permissions Manager applet
- This product is ideal for VARs as well as large enterprise customers

Roxio Secure Managed adds:

- Discs can only be written by permitted users
- Discs can only be read by permitted users
- An authorization server controls permissions per organizational policies
- Permissions can be changed in real time by the system administrator via a web control panel
- Data on USB flash devices is encrypted, and can be destroyed if a device is lost or stolen
- Supports logging and reporting of files burned to disc, files sent to USB devices, and administrative changes to permissions
- This product is targeted at larger enterprise customers

4 | Typical Use Case for a VAR Customer – Using Roxio Burn Secure Plus in an SMB

A doctor’s office has several employees including 3 doctors (the owners of the business), 3 nurses, 2 administrative assistants, and an office manager. In addition, they contract an accountant to handle bookkeeping and taxes and an IT expert to handle the computer network.

Each of these employees has their own PC. The company deals primarily with three kinds of data:

- Confidential patient records
- Company finances
- Appointments, daily communications, and other data that is not particularly sensitive, but should remain in the office

Data is sometimes burned to disc so that the doctors or the bookkeeper can carry data out of the office to work on at home (or in the accountant’s office). The doctors are concerned about patient confidentiality for both ethical reasons, and to comply with privacy legislation (HIPAA). Furthermore, the doctors and the accountant want to ensure that the company’s finances remain confidential.

To ensure proper levels of privacy while still enabling employees to conveniently share data on disc within the office, the IT expert has set up several groups of PCs. Employees in the office are divided into groups with the following policies and privileges:

	Management PCs	Medical PCs	Admin Staff PCs	Finance PC	Outside Office
	Doctors, IT, Office Manager	Nurses	Admin Assistants	Bookkeeper	Working at Home
Discs burned on Mgt PCs can be read on:	X	X With Password	X With Password	X With Password	X With Password
Discs burned on Med Staff PCs can be read on:	X	X	X With Password		
Discs burned on Admin Staff PCs can be read on:	X	X	X		
Discs burned on Finance PC can be read on:	X	X With Password	X With Password	X	X With Password

Using Roxio Secure Burn Plus, it is easy to set up the office according to these policies, to ensure that the more senior staff members have access to the data when and where they want, while junior staff and contractors are restricted.

5 | Conclusion

History and experience continue to teach us that it is a lot less expensive to prevent a disaster from happening than it is to clean up after the disaster occurs. Data breaches on portable media occur every day, but many of them could be prevented. Roxio Secure solutions can save companies time and money by ensuring that confidential records stored on optical and USB flash media are only viewable by authorized personnel.

Contact

To request a quote, contact the Volume Licensing Sales team at:

North America:

Tel: 866-825-7694 or 972-713-8110

Email: vlp@roxio.com

Europe:

Email: vlp.emea@roxio.com

ROXIO®

www.roxio.com/secure