



745 Atlantic Avenue  
Boston, Massachusetts 02111  
(800) 899-IRON

Iron Mountain operates in major markets worldwide, serving thousands of customers throughout the U.S., Europe, Canada, Latin America and the Pacific Rim. For more information, visit our Web site at [www.ironmountain.com/digital](http://www.ironmountain.com/digital)

# A Guide to Reducing the Risk of Costly Data Breaches: The 3 Pillars of Data Protection

## INTRODUCTION

### Data Security Regulations on the Rise

A recent study by Jupiter Research<sup>1</sup> revealed that after virus infection and unintended forward of emails, loss of mobile devices and password compromise are the greatest causes of data security breaches. In fact, there are numerous federal, state and international laws and regulations that govern the protection of private, personal and confidential data held by corporations. These regulations do not make distinctions on where the data is located. Confidential data can be stored in the relative safety of a mainframe computer or it can reside on desktop PCs or mobile devices such as laptop PCs. For example, California's Database Security Breach Notification Act (Effective July 1, 2003) SEC. 2. Section 1798.29 added to the Civil Code that:

“Any agency that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.”

On the federal level, proposed U.S. Senate Bill 1350 requires any U.S. company that collects personal data to make a public disclosure and notify private persons if there is a loss of control of that personal/private data.

The numerous legislative requirements of public disclosure of lost data can be extremely expensive, making it a top priority for the enterprise.

<sup>1</sup> Top Sources of Security Breaches, 2004, Jupiter Media Research Report

## **DOCUMENT INFORMATION**

A Guide to Reducing the Risk of Costly Data Breaches: The 3 Pillars of Data Protection

## **PRINTED**

June 2006

## **COPYRIGHT**

Copyright © 2006 Iron Mountain Incorporated. All Rights Reserved.

## **TRADEMARKS**

Iron Mountain and the design of the mountain are trademarks or registered trademarks and Connected is a registered trademark of Iron Mountain Incorporated. DataDefense and Iron Mountain Digital are trademarks of Iron Mountain Incorporated. All other trademarks and registered trademarks are the property of their respective owners.

## **CONFIDENTIALITY**

The information set forth herein represents the confidential and proprietary information of Iron Mountain. Such information shall only be used for the express purpose authorized by Iron Mountain and shall not be published, communicated, disclosed or divulged to any person, firm, corporation or legal entity, directly or indirectly, or to any third person without the prior written consent of Iron Mountain.

## **DISCLAIMER**

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of Iron Mountain Inc. The information in this document is subject to change without notice and should not be considered a commitment by Iron Mountain Inc. While Iron Mountain has made every effort to ensure the accuracy and completeness of this document, it assumes no responsibility for the consequences to users of any errors that may be contained herein.

## TABLE OF CONTENTS

	Page
<b>Why Protect Confidential Data?</b> .....	4
<b>White Paper Purpose</b> .....	5
<b>PC ENCRYPTION OVERVIEW: A NECESSARY BUT INCOMPLETE SECURITY SOLUTION</b> .....	6
<b>What is Encryption?</b> .....	6
<b>The Encryption Key</b> .....	6
<b>The Advanced Encryption Standard (AES)</b> .....	6
<b>Microsoft® Encrypting File System (EFS)</b> .....	7
<b>Whole Disk Encryption: Microsoft® Windows® Vista and Other 3rd Party Software Providers</b> .....	8
<b>Encryption — an Incomplete Data Protection Solution</b> .....	9
<b>INTRODUCING THE IRON MOUNTAIN THREE PILLARS OF DATA PROTECTION</b> .....	9
<b>THE FIRST PILLAR: POLICY MANAGEMENT AND CONTROL</b> .....	10
<b>Enterprise Ownership of the Data Protection Implementation</b> .....	10
<b>Iron Mountain’s DataDefense™ Product Overview</b> .....	10
<b>How the DataDefense Solution Works</b> .....	11
<b>Enterprise Management of Security Policies via DataDefense Server</b> .....	11
<b>Intelligent PC Encryption Through DataDefense</b> .....	11
<b>THE SECOND PILLAR: THREAT MONITORING AND RESPONSE</b> .....	12
<b>Enterprise Vigilance and Ability to Respond to Security Breaches</b> .....	12
<b>DataDefense Data Elimination Overview</b> .....	13
<b>DataDefense Threat Monitoring</b> .....	13
<b>DataDefense Data Destruction</b> .....	14
<b>THE THIRD PILLAR: DATA BACKUP AND RESTORATION</b> .....	15
<b>Ensuring Data Availability for the Enterprise</b> .....	15
<b>Connected® Backup/PC Overview</b> .....	15
<b>How the Connected Backup/PC Solution Works</b> .....	16
<b>Protecting Data in Transit: Connected Backup/PC Encryption</b> .....	17
<b>PUTTING IT ALL TOGETHER: IMPLEMENTING THE IRON MOUNTAIN THREE PILLARS</b> .....	17

## ABOUT IRON MOUNTAIN DIGITAL

Iron Mountain Digital is the world’s leading provider of data backup/recovery and archiving software as a service (SaaS). The technology arm of Iron Mountain Incorporated offers a comprehensive suite of data protection and e-records management software and services to thousands of companies around the world, directly and through a world-wide network of channel partners. Iron Mountain Digital is based in Framingham, MA with European headquarters in Frankfurt, Germany.

For more information, visit [www.ironmountain.com/digital](http://www.ironmountain.com/digital)

## Why Protect Confidential Data?

The enterprise faces potentially dire costs and consequences should unprotected consumer data be exposed. The Ponemon Institute<sup>2</sup> conducted a study examining the costs incurred by 14 companies that experienced a data breach. Breaches included in the survey ranged from 1,500 records to 900,000 records from 11 different industry sectors. A summary of these data breach costs is illustrated in the Table below:

Activity	Direct Costs (US \$)	Indirect Costs (US \$)	Lost Customer Costs (US \$)	Total Costs (US \$)
<b>Detection &amp; Escalation</b>				
Internal investigation	\$19,000	\$488,000	N/A	\$507,000
Legal, audit, consulting	\$463,000	\$51,000	N/A	\$514,000
<b>Notification</b>				
Letters	\$547,000	193,000	N/A	\$740,000
Emails	\$5,000	N/A	N/A	\$5,000
Telephone	\$913,000	\$105,000	N/A	\$1,018,000
Published media	\$48,000	N/A	N/A	\$48,000
Website	\$3,000	N/A	N/A	\$3,000
<b>Ex-Post Response</b>				
Mail	\$4,000	\$3,000	N/A	\$7,000
Emails	\$1,000	\$1,000	N/A	\$2,000
Internal call center	\$287,000	\$479,000	N/A	\$766,000
Outsourced call center	\$27,000	N/A	N/A	\$27,000
Public or investor relations	\$289,000	\$14,000	N/A	\$303,000
Legal defense services	\$1,288,000	N/A	N/A	\$1,288,000
Free or discounted services	\$810,000	N/A	N/A	\$810,000
Criminal investigations	\$286,000	\$13,000	N/A	\$299,000
<b>Lost Business</b>				
Lost existing customers	N/A	N/A	\$6,728,000	\$6,728,000
Lost new customers	N/A	N/A	\$730,000	\$730,000
<b>Average Cost Per Company</b>	<b>\$4,990,000</b>	<b>\$1,347,000</b>	<b>\$7,458,000</b>	<b>\$13,795,000</b>

## Ponemon Institute Data Breach Cost Analysis

Note that if these corporations had valid data security policies covering the lost data, they may have been able to avoid the costly public disclosure of data loss.

In fact, during the creation of this technical document alone, there have been three major news stories about lost or stolen data from corporate laptops:

- On January 26, 2006, the Associated Press reported that a stolen laptop from Ameriprise Financial put financial accounts at risk. Specifically, Ameriprise Financial had to notify about 226,000 people that their names and other personal data were stored on a laptop computer that was stolen from an employee's vehicle.
- On February 26, 2006, according to a report in the *Miami Herald*, Ernst & Young lost four laptops. According to security footage, two men entered the conference room a couple of minutes after the Ernst & Young staffers left and walked off with four Dell laptops.
- On March 24, 2006, the *Wall Street Journal* noted that laptops prove to be the weakest link in data protection. The journal noted that Boston-based mutual-fund giant Fidelity Investments disclosed that one of its laptop computers was stolen containing the personal information, including Social Security Numbers, of 196,000 current and former Hewlett-Packard employees.

<sup>2</sup> Lost Customer Information: What Does a Data Breach Cost Companies?, Nov. 2005, Ponemon Institute, LLC

Since many of the new laws have already gone into effect, corporations need to get systems, policies and procedures in place quickly to protect client and customer information. It is interesting that most of the new laws and regulations require some form of encryption and user authentication be utilized on mobile devices in order to provide some measure of data protection and insurance against the exposure of private customer or consumer data. However, although encryption is deemed a necessary security tool, it is by no means a complete data protection solution. Encryption, in fact, is only the first line of defense.

### **White Paper Purpose**

The purpose of this White Paper is to assist Iron Mountain customers and technical support personnel with understanding personal computer (PC) encryption technology (specifically Microsoft® Windows® encryption technology) and where encryption fits in creating a total enterprise PC data protection solution, what Iron Mountain calls *The Three Pillars of Data Protection*:

- 1. Policy Management and Control**
- 2. Threat Monitoring and Response**
- 3. Data Backup and Restoration**

These Three Pillars serve as a guide for customers establishing a PC security program.

Finally, as an example of a full security solution, this White Paper describes how Iron Mountain's DataDefense™ and Connected® Backup/PC data protection solutions can be utilized to create that total security solution in accordance with the Iron Mountain Three Pillars. The White Paper summarizes the following:

#### **PC Encryption Overview:**

- How Windows 2000 and XP Professional operating systems use Microsoft Encrypting File System (EFS) to encrypt files and folders
- Why encryption is important, but also why encryption is not a total data protection solution

#### **The Iron Mountain Three Pillars of Data Protection**

- The elements beyond encryption that are necessary for a complete data protection solution

#### **Using Iron Mountain's DataDefense and Connected Backup/PC Solutions to Provide All Three Pillars of Data Protection:**

- The methods used by Iron Mountain's DataDefense solution to encrypt files and ensure enterprise control over data access and compliance
- How the Connected Backup/PC solution backs up files and uses encryption to transmit data over the internet and ensures data availability to the enterprise
- How the DataDefense and Connected Backup/PC solutions work together to provide a total data protection solution for PCs in accordance with Iron Mountain's Three Pillars of Data Protection

Finally a series of recommendations are provided for customers to consider given the advent of the security laws and regulations, the extreme public disclosure costs that could be felt from lost, stolen, or missing PCs/laptops, and the need for a complete data protection solution.

**PC ENCRYPTION OVERVIEW: A NECESSARY BUT INCOMPLETE SECURITY SOLUTION**

**What is Encryption?**

Encrypted data is data that many people may have the ability to see (in encoded form), but only selected people can understand or use (decode). Once a tool restricted only to the military and political diplomats, data encryption is now important to anyone dealing with private information on a computer.

Encryption is a process that changes the letters and numbers of plain text into other letters and numbers in such a way that the message becomes unreadable. For example, you could apply a simple encryption by shifting letters of the alphabet five places forward:

A	B	C	D	E	F	G	H	I	J	K	etc.
F	G	H	I	J	K	L	M	N	O	P	

The message “I am here” becomes “N fr mjwj.” The encryption process would entail shifting the letters five places backward. This is a simple encryption algorithm that could easily be deciphered. Obviously, real-world encryption algorithms are much more complex and not easily compromised.

**The Encryption Key**

An encryption key is a string of characters (numbers, letters and symbols) used as the reference to scramble the data contained in a text file, or any other file whether audio, video, image or executable program. It is easiest to think of an encryption key as a key that is used to unlock a door. When data is encrypted using a key, the same key must be used to decrypt that data.

There are two general types of encryption methods: conventional and public-key. The encryption described above is an example of conventional or single-key encryption: there is one key, an encryption algorithm and a closely related decryption algorithm. Conventional encryption is effective in cases where data or text is being stored on a file server, and you do not want others to be able to view it. The encrypted text is stored on disk and then encrypted after being read back to the originating computer. With public-key encryption, there are two keys: one used to encode the message, and a different one used to decode the message. Before the message is sent, the receiver gives the sender a public key to use for encoding the message. The receiver also has a private key, which remains on the receiver’s own computer that works in conjunction with the public key to decode the message after it arrives. The sender encodes the data and transmits it, along with the public key. Since the public key is useless by itself, the data will not be compromised if intercepted. After the data is received, the receiver applies the private key and decodes the message.

**The Advanced Encryption Standard (AES)**

The encryption algorithm described previously is simple and obviously easy to crack. The United States government has adopted an encryption standard known as The Advanced Encryption Standard (AES) which evolved from its predecessor, the Data Encryption Standard (DES). Note that DES (developed in 1976) is now considered to be insecure for many applications, primarily due to the 56-bit key size being too small given the advances in computing power and speed. AES was adopted by the National Institute of Standards and Technology (NIST) as US FIPS PUB 197 in November 2001. The AES encryption key size can be 128, 192 or 256 bits. In June 2003, the U.S. Government announced that AES may be used for classified information:

“The design and strength of all key lengths of the AES algorithm (i.e., 128, 192 and 256) are sufficient to protect classified information up to the SECRET level. TOP SECRET information will require use

of either the 192 or 256 key lengths. The implementation of AES in products intended to protect national security systems and/or information must be reviewed and certified by NSA prior to their acquisition and use.”<sup>3</sup>

With regard to PCs and other related technologies, AES is widely used by many applications and protocols. In fact, Microsoft Windows operating system and numerous Windows utilities use AES 256-bit encryption.<sup>4</sup>

### Microsoft Encrypting File System (EFS)

Microsoft Encrypting File System (EFS) provides the core file and folder encryption technology used to store encrypted files on Microsoft Windows NTFS file system volumes within Windows 2000 and Windows XP Professional. Once a file or folder is encrypted, the user works with them as they would any file or folder. The user can email them and/or save them to disk. In each of these cases, the files are sent in an unencrypted state — EFS protects data on the device, but does not protect data in transit since attempting that would create complexity for users that would make the solution untenable. In short, encryption is transparent to the user that encrypted the file. The user does not have to manually decrypt the encrypted files before he can utilize them.

Microsoft Windows EFS allows users to encrypt or decrypt a folder or file by setting the encryption property for folders and files using file or folder properties. If a folder is encrypted, all files and subfolders created in the encrypted folder are automatically encrypted. Of course, the enterprise must rely on the user to follow corporate encryption protection regulations that require confidential data to reside in an encrypted state, and therefore must be stored in specific locations (folders) that are encrypted. The enterprise has no knowledge of whether a user is actually compliant — another possible security flaw with user-controlled encryption.

With regard to Microsoft Windows EFS, it is important to also note that:

- EFS is only included in Windows 2000 and Windows XP Professional editions.
- Only files and folders on NTFS volumes can be encrypted. Most external drives/media are NOT formatted as NTFS. As noted above, encrypted files can become decrypted if they are copied or moved to a volume that is not an NTFS volume (like a CD, DVD, or other media).
- Moving unencrypted files into an encrypted folder will automatically encrypt those files in the new folder. However, the reverse operation will not automatically decrypt files. Files must be explicitly decrypted.
- Files that are compressed cannot be encrypted using EFS.
- Encrypting a folder or file does not protect against deletion or listing of files or directories. Anyone with the appropriate permissions can delete, view or list encrypted folders or files — another reason why encryption is a necessary but not a complete security solution.
- The EFS encryption keys are located in the folder C:\Documents and Settings\“USER” \Application Data\Microsoft\Crypto\. If this file or folder is corrupted or deleted, then the files encrypted on the PC are no longer readable by the user (or anyone). Therefore, it is wise to ensure that a proper backup of this folder exists, as well as having a strong key management infrastructure.

<sup>3</sup> CNSS Policy #1, Fact Sheet No. 1, National Policy on the Use of the Advanced Encryption Standard (AES) to Protect National Security Systems & National Security Information, June 2003

<sup>4</sup> Retrieved from [http://en.wikipedia.org/wiki/List\\_of\\_applications\\_that\\_use\\_AES](http://en.wikipedia.org/wiki/List_of_applications_that_use_AES)



## *Backing up encryption keys is a vital part to any PC Encryption program*

### **Whole Disk Encryption: Microsoft Windows Vista<sup>5</sup> and Other 3rd Party Software Providers**

Whole disk encryption provides a higher level of security over file/folder encryption, but is still subject to some of the inherent security flaws of file/folder encryption. That is, once an authorized user gets past the initial authentication/logon step, the data is now exposed and cannot be secured by the user or enterprise. Therefore, an unauthorized user or intruder that cracks the login password will also have access to unencrypted data. As noted in the introduction, a recent Jupiter Research study concluded that loss of mobile devices and password compromise are the 3rd and 4th greatest causes of data protection breaches.<sup>6</sup> However, with full disk (or volume) encryption, the entire hard disk is rendered unreadable by anyone without the proper access credentials. Whole disk encryption provides encryption protection for the entire drive, including the operating system, applications and all data files. However, that is also the flaw with whole disk encryption — once the initial login has been achieved, the user has full access to all files on the hard drive.

The next release of the Windows operating system (Windows Vista) is expected to incorporate a full disk encryption option in addition to the file/folder level encryption provided by EFS. There are numerous third party software vendors currently providing full disk encryption products. Because whole disk encryption does not require users to have data in particular locations, it can be viewed as a better security solution than file/folder encryption. However, there are many drawbacks to a whole disk encryption system, including:

- It provides encryption capability only — The data is not secure once a user logs into the PC with proper credentials. There is no protection if password integrity is lost and no ability to control the threat reactively after a device is lost.
- There is an administrative burden to full disk encryption systems requiring the memorization of different passwords and more active IT/Help Desk management. Help Desk involvement is often extensive for disk failure and recovery. In addition, users may need to carry special rescue and emergency disks, creating another user compliance fault point.
- End-user training is usually required.
- Whole disk encryption software can add enough CPU cycle overhead to create noticeable performance degradation for users. In particular, the start up and shut down of the operating system can be elongated, causing users to circumvent the delays by using the “standby” feature — thereby eliminating the security benefit of encryption. In addition, it may interfere with operating system security and disk utilities, such as partitioning, image backup and data recovery programs.

*Like file/folder level encryption,  
whole disk encryption only provides security  
for data at rest, until the login password  
has been provided*

<sup>5</sup> Microsoft Windows Vista operating system is scheduled for release in early 2007

<sup>6</sup> Jupiter Research Citation

## Encryption — an Incomplete Data Protection Solution

When all the benefits and weaknesses of encryption technology are taken into account, it is clear that encryption is a necessary, *but incomplete*, PC security solution. Once a user logs into Windows, file and folder encryption no longer provides data protection. This is the weak link in file and folder encryption and the reason that this level of encryption is not a complete data protection solution. There need to be additional protections in place, as described later in this paper, to ensure data protection. However, encryption does provide protection from an intruder who tries to gain unauthorized physical access to encrypted files/folders by booting up the hard drive to another operating system such as Linux®. Hence, using EFS is similar to using permissions on files and folders.

*If the authorized user is logged in  
(or an intruder has cracked the authorized user's  
login credentials), encryption no longer  
provides data protection*

## INTRODUCING THE IRON MOUNTAIN THREE PILLARS OF DATA PROTECTION

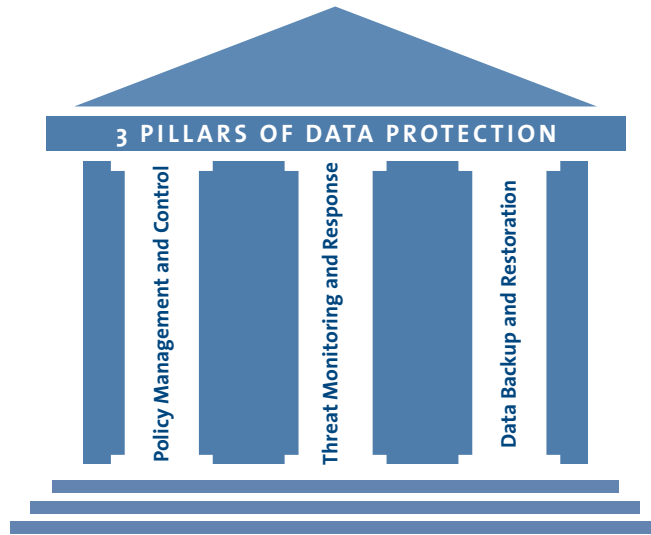
Whether it be Microsoft EFS or a third party whole disk encryption software technology, an enterprise needs to consider the following questions when deploying only a PC encryption technology:

- How will the enterprise ensure that the individual end user is compliant with corporate data protection policies?
- How will the enterprise maintain control over its data if the user's password is hacked or the users themselves become unauthorized?
- How will the enterprise address potential security threats such as PCs or laptops being stolen or lost?
- How will the enterprise ensure adequate secure data backup and availability if critical data is lost or corrupted on a PC?

Iron Mountain strongly recommends that any corporation, big or small, that carries confidential and private data on distributed devices such as laptops ensure that they have measures in place to address the Iron Mountain Three Pillars of Data Protection:

- 1. Policy Management and Control**
- 2. Threat Monitoring and Response**
- 3. Data Backup and Restoration**

In the following sections, a complete implementation of The Three Pillars will be described using Iron Mountain's DataDefense and Connected Backup/PC solutions.



*Iron Mountain Three Pillars of Data Protection*

## **THE FIRST PILLAR: POLICY MANAGEMENT AND CONTROL**

### **Enterprise Ownership of the Data Protection Implementation**

The weakest link in any security program is participant compliance with the security rules and structure. For data protection on distributed devices, particularly PCs and laptops, this is especially true. Therefore, it is clearly important to the enterprise that the implemented security solution be managed and controlled by the enterprise — the data owners — as much as is possible.

Encryption provides a good first level of defense against unwanted access to private data. However, we have also identified numerous weaknesses that are not protected against with an encryption-only solution. For an enterprise to truly have a well-structured data protection implementation, the enterprise must ensure that:

- Reliance on user compliance with policies and procedures is minimized
- Installation and uptime are managed and ensured

While there are numerous encryption products in the marketplace, few provide the enterprise with the level of management and control necessary to meet the standard of the Iron Mountain First Pillar. One product that does supply centralized ownership of encryption security policy is Iron Mountain's DataDefense solution.

### **Iron Mountain's DataDefense Product Overview**

Iron Mountain's DataDefense solution intelligently encrypts and automatically eliminates data on a lost or stolen computer to prevent its compromise or misuse. A comprehensive and multi-layered approach to PC data protection, the DataDefense solution effectively secures data even when the PC is off-line.

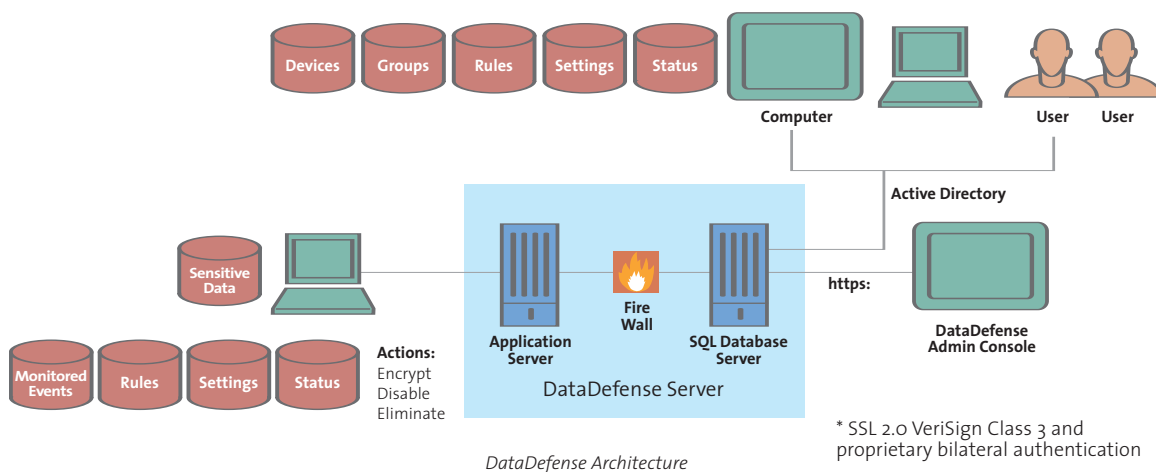
DataDefense, an enterprise management solution, enables the encryption process to occur, giving the

organization full control over the encryption implementation:

- Installation can be automated and applied remotely without impact to the user
- Determination of which files, file types and folders are to be encrypted can be defined
- Assurance that encryption is running can be monitored

### How the DataDefense Solution Works

The solution is comprised of server administration software combined with a client application that may be downloaded to enterprise PCs and remains transparent to the end user. The Figure below illustrates the DataDefense Client-Server relationship.



### Enterprise Management of Security Policies via DataDefense Server

Through the use of a password protected web portal into the DataDefense server, the enterprise security administrator sets the following DataDefense security policies:

- What data to encrypt
- What threats to safeguard against
- How to respond to different threats to data

In addition, the server application provides an enterprise dashboard view of the status of remote devices, as well as reports and detail views on those devices, providing the enterprise another layer of control.

### Intelligent PC Encryption Through DataDefense

The DataDefense client software implements the policies defined by the DataDefense server management console. It routinely checks in with the server, in the background, whenever an internet connection is present, requiring no end user intervention. If rules or device status is changed by the enterprise, these are communicated directly to the client agent transparently.

The DataDefense solution uses Microsoft's EFS to begin encrypting after the setting is downloaded by the DataDefense client during installation or check-in with the DataDefense server. This takes the encryption process compliance away from the user — the user has no choice or control over what gets encrypted on his PC.

The DataDefense solution encrypts all data files that are location based (My Documents, Desktop, specified

folders, or Local C drive, etc.) or file type based (\*.doc, \*.txt, \*.xls, \*.ppt, etc.), by using “Data Sets” to define what and where files are encrypted. DataDefense comes installed with predefined default data sets, as well as giving the enterprise the control to define new data sets to address the organization’s particular needs. In addition, DataDefense includes a blacklist of key operating system files that should not be encrypted to ensure smooth operation. The enterprise specifies the encryption location or file types. By encrypting the specified folders that contain these files, all newly created files in these folders are created in an encrypted state. In fact, with folder encryption, even the temporary files that are created in the encryption conversion process (during a first-time file encryption) are encrypted, ensuring complete data protection on those files. It does not, by default, encrypt the operating system or applications, thereby avoiding performance degradation and ensuring no interference with disk utilities such as partitioning, image backup and data recovery programs. In addition, the DataDefense solution automatically sweeps the device’s hard drive every six hours to ensure that any targeted files that may have been added or changed in different folders/locations will be encrypted.

A key strength of the DataDefense solution is how it manages the EFS encryption process. When the DataDefense solution is installed on the client, it turns on EFS for the locations and file types specified by the administration server. It sets the EFS encryption process as a background process in the user space to ensure that it has no measurable effect to the user on the application processing speed of the device. Given the intensive disk I/O necessary to encrypt files, this is a key capability to ensure that the additional security does not hamper the user’s ability to execute her work.

*DataDefense offers Intelligent Encryption that gives the enterprise control over the PC encryption process in accordance with Iron Mountain’s First Pillar of Data Protection: Policy Management and Control*

## **THE SECOND PILLAR: THREAT MONITORING AND RESPONSE**

### **Enterprise Vigilance and Ability to Respond to Security Breaches**

Even with the strongest of security implementations — with full enterprise control and management of the implementation — security will falter, as it is still subject to two major weaknesses:

- User compliance — the weakest link in any protection program
- Company loss of control over the data — an all too common occurrence as more distributed devices containing corporate data proliferate throughout the enterprise

Employees will lose their laptops, have them stolen or simply leave with them when they terminate employment with the company, and passwords will be hacked or compromised. Temporary employees present another set of security implications as well. The organization must have ways to monitor for these situations and an ability to react in a way that eliminates, or at least greatly minimizes, the potential losses from these events.

Obviously, encryption alone does not provide this level of data protection. In fact, in the situation where the device is no longer under the control of the enterprise, the data is always at risk, with no clear end date for the

organization to be certain the data no longer is a security risk. Clearly, the enterprise needs an additional solution that can:

- Monitor for abnormal behaviors signaling a compromised device
- Initiate defensive data elimination when that device has been identified as compromised

Again, the DataDefense solution can enable a security implementation that meets another Iron Mountain Data Protection Pillar.

### DataDefense Data Elimination Overview

The DataDefense solution ensures organizational control of that data even when the enterprise has lost control of the device. It monitors numerous scenarios to protect the distributed device and ensure data protection. This creates a vastly enhanced data protection solution when compared to existing encryption-only solutions. The table below shows how the DataDefense solution provides superior security over traditional encryption technologies.

Threat Condition	Example	Iron Mountain DataDefense	Full Disk Encryption	File/Folder Encryption
Password integrity is breached	Password is written down on a Post-it note on bottom of laptop	✓	–	–
Authorized user becomes unauthorized	Salesman quits abruptly with computer, data and password	✓	–	–
Stolen device is taken with power on/standby	Computer is stolen in office when worker steps away	✓	–	✓
Data is saved in non-compliant folder	User saves sensitive files to Desktop instead of My Documents	✓	✓	–
Former, temporary worker still possesses sensitive data	Marketing consultant analyzes consumer data on own computer for specific period	✓	–	–
Sensitive data left on removable drive	Laptop is lost with thumb drive containing data still in USB drive	✓	–	–
Compliance failure with FACTA Disposal rule	Consumer credit data on desktop not destroyed in timely way	✓	–	–
Hard drive pulled and used as slave	Thief attempts to read data off pulled drive without password	✓	✓	✓

*DataDefense Threat Condition Matrix*

In these situations, the enterprise needs a mechanism to ensure that their proprietary data is not compromised. The DataDefense solution provides that mechanism by having rules defined that will cause the data to be destroyed if the device has been identified as one that has been compromised, such as in the above scenarios.

### DataDefense Threat Monitoring

Iron Mountain's DataDefense solution monitors several threat conditions through a combination of client-based triggers and server-based statuses. When these triggers are activated, the client will then implement the data elimination protocol defined by the enterprise.

## CLIENT-BASED TRIGGERS

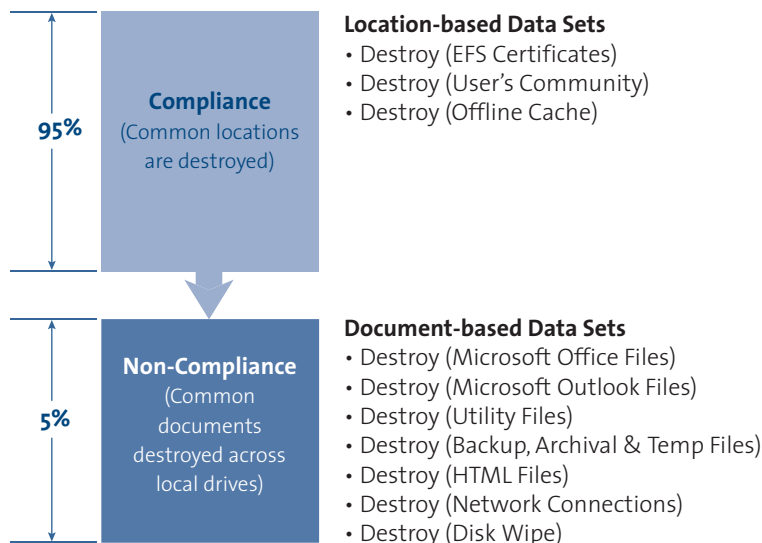
- Failed login attempts — The DataDefense client can be set to register each login attempt and execute data elimination after a defined number of failed attempts — typically a sign of an unauthorized person attempting to access the device.
- Lack of contact — The client can track time since the last successful connection to the DataDefense server. Once the enterprise-defined time period has expired since the last check-in, data elimination rules can be processed. This ensures that even if an unauthorized person were to gain access to the device, she would only have a limited amount of time before data on the device were eliminated.

## SERVER-BASED TRIGGERS

- Device Status — If a device is known to be missing, stolen or otherwise no longer under control of an authorized person, the server can identify that data as compromised. When that device is next connected to the Internet and completes a connection to the DataDefense server, the client can be triggered to execute the appropriate data elimination as defined by the enterprise.

## DataDefense Data Destruction



Much like how encryption rules are defined, the DataDefense solution defines data sets for destruction when certain conditions are met.



*Location-based and File Type-based Destruction Sets*

To ensure immediate data inaccessibility, the first files to be deleted are the files containing the encryption keys — guaranteeing that the encrypted data is no longer accessible to anyone. These files, located in the C:\Documents and Settings\\Application Data\Microsoft\Crypto\RSA folder, are necessary in order to decrypt any existing encrypted files owned by that user.

When data destruction is enacted, data is overwritten and then deleted in accordance with the DataDefense Secure Delete protocol or the DoD 5220.22-M standard of deleting data as specified in the National Industrial Security Program Operating Manual. This approach ensures that no data is left in an accessible format for unauthorized eyes.

	<b>Secure Delete</b>	<ul style="list-style-type: none"> <li>• Data is overwritten 1-8 times</li> <li>• Data is unrecoverable</li> </ul>
	<b>DoD Delete</b>	<ul style="list-style-type: none"> <li>• Complies with Department of Defense 5220.22-M</li> <li>• Data is unrecoverable</li> </ul>

*Iron Mountain's DataDefense provides sufficient Threat Monitoring and a complete Threat Reaction solution in accordance with Iron Mountain's Second Pillar of Data Protection: Threat Monitoring and Reaction*

## THE THIRD PILLAR: DATA BACKUP AND RESTORATION

### Ensuring Data Availability for the Enterprise

Now that the enterprise has taken the steps necessary to ensure that data on distributed devices is properly secured and safe from unauthorized access, the enterprise needs to ensure that it still has access to the data once it is no longer available on the distributed device. In particular, the company must be able to:

- Access the data if it is retrieved but the encryption keys on the device have already been destroyed
- Retain the corporate data that is lost or destroyed when the threat reaction has been activated
- Perform this data backup, and store the data in a manner consistent with the security approach supporting the First and Second Pillars

Clearly, the organization needs a backup and restore solution that will provide this access and retention, while ensuring that the backup process and storage mechanism maintain the necessary levels of security for the enterprise. Of course, this solution needs to be one that also adheres to the First Data Protection Pillar — that is, under the enterprise's management and control. One solution that meets these criteria, also offered by Iron Mountain, is the Connected Backup/PC solution.

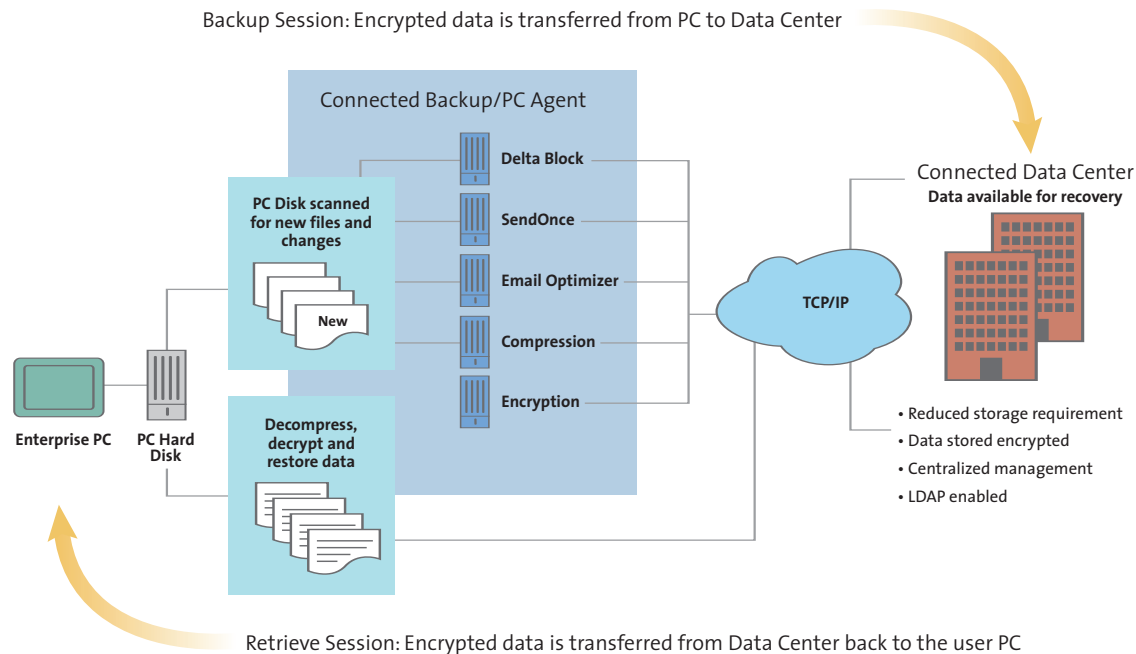
### Connected Backup/PC Overview

Iron Mountain's Connected Backup/PC solution provides data backup and restore security. This solution is a client-server system that allows file backup for personal computers over any TCP/IP network, such as the internet, to a central server cluster. That server cluster can be owned by the enterprise (using the product version) or managed by Iron Mountain (using the service version). The software is designed to provide effective backup or restore services even at connection bandwidths down to 28.8 kbps. It provides security at every level of the implementation, assuring full security both when sensitive corporate data is being transmitted for backup or restoration, as well as while the backup data is in storage.



## How the Connected Backup/PC Solution Works

Like DataDefense, Connected Backup/PC is a client-server system comprised of an agent that resides on the PC/laptop, and a server side that includes a web-based management console.



*Connected Backup/PC Architecture*

The agent can be configured to run on system startup and runs in the background requiring no user input. The application checks for an internet connection and activates itself to run the designated backups in the background. Each time the Agent is launched automatically, it performs the following sequence of operations:

- Scans the hard disk to identify all data
- Applies patented technology to reduce the amount of data that must be transferred to and stored at the secure Data Center
- Compresses the data to further reduce and optimize transmission time and storage at the secure Data Center
- Encrypts the data prior to transmission for security
- Connects and sends the data and all asset information to the mirrored secure Data Centers
- Disconnects and displays a session log for review by the PC user

The process is reversed when a user needs to recover data. The Agent receives archived files from the secure Data Center and then decrypts and decompresses the files. The user can manage the entire process, without IT help, by going to the main menu to:

1. Click "Retrieve"
2. Select the desired files
3. Click "Retrieve Now"

### Protecting Data in Transit: Connected Backup/PC Encryption

A key security component of the Connected Backup/PC solution is the use of encryption in the transmission and storage of the backup data. With Connected Backup/PC:

- *Data is protected in transit* — Each data set that is backed up is encrypted using 128-bit AES encryption before it is transmitted
- *Data is protected in storage* — All data stored in the servers is stored in its encrypted state, ensuring that unauthorized users cannot access it from the server
- *Data is protected when restored* — The data remains in the encrypted state when transmitted back to the PC/laptop

The Connected Backup/PC solution leverages strong encryption technology, ensuring the highest level of security is perpetuated through the backup, storage and restoration of the enterprise's data.

*Iron Mountain's Connected Backup/PC is a complete solution in accordance with Iron Mountain's Third Pillar of Data Protection: Data Backup and Restoration*

### PUTTING IT ALL TOGETHER: IMPLEMENTING THE IRON MOUNTAIN THREE PILLARS

We have detailed above that enterprises that incorporate only a PC encryption program to ensure the security of data on PCs and laptop are providing an insufficient PC security program.

Iron Mountain's Three Pillars of Data Protection provides a solid construct for an organization to plan and implement a data protection solution for its PCs, laptops and other data-carrying devices used throughout the enterprise. With the advent of numerous new legislative initiatives targeting consumer protection and placing more significant disclosure requirements on organizations, combined with increased activity by those determined to access private data or damage corporations, it is of utmost importance for enterprises to employ comprehensive security solutions adhering to the Three Pillars of Data Protection. For purposes of its PC and laptop community, the combination of Iron Mountain Digital's data protection solutions, DataDefense and Connected Backup/PC, provides a thorough solution that satisfies all Three Pillars:

- **Policy Management and Control** — Both the DataDefense and Connected Backup/PC solutions put control of the policies, implementation, and utilization fully with the enterprise. They minimize, or outright eliminate, the predominance of user compliance issues.
- **Threat Monitoring and Response** — The DataDefense solution provides the enterprise the mechanism to both monitor for abnormal or threatening behavior, and to act on those behaviors to destroy sensitive data before unauthorized parties have the opportunity to access the data.
- **Data Backup and Restoration** — The Connected Backup/PC solution gives the enterprise assurance that in the event that a PC or laptop is no longer under the control of the organization, the data that resides there can be retrieved. This solution does so while also ensuring, through its use of encryption throughout the backup and restore process, that it meets the security needs of the enterprise as well.

Of course no security solution is foolproof, but an organization that implements a solution set that adheres to the Three Pillars will be ensuring that it is doing the most it can to eliminate the enterprise's loss of reputation and the substantial financial costs associated with losing confidential data.